



**LEPL – DAVID AGHMASHENEBELI NATIONAL
DEFENCE ACADEMY OF GEORGIA**

DEFENCE INNOVATIONS AND INTERNATIONAL PARTNERSHIPS: SHAPING THE FUTURE OF SECURITY



**PROCEEDINGS OF THE INTERNATIONAL
STUDENT CONFERENCE**

GORI, 2025

LEPL - DAVID AGHMASHENEBELI NATIONAL DEFENCE
ACADEMY OF GEORGIA



DEFENCE INNOVATIONS AND INTERNATIONAL PARTNERSHIPS: SHAPING THE FUTURE OF SECURITY

INTERNATIONAL STUDENT CONFERENCE

© Publishing House Of LEPL - David Aghmashenebeli National Defence Academy
GORI, 2025

EDITORIAL BOARD

Head of the Editorial Board

Brigadier General Mamia Balakhadze

Rector of LEPL-David Aghmashenebeli National Defence Academy of Georgia

Members of the Editorial Board

Colonel Irakli Uchadze

Head of MA Program of LEPL - David Aghmashenebeli National Defence Academy of Georgia

Lieutenant Colonel
Ivan Okromtchedlishvili

Head of MA Program in Defense Analysis at
LEPL – David Aghmashenebeli National Defence Academy
of Georgia

Nikoloz Samkharadze

Professor of MA Program in International Relations
and Diplomacy at LEPL – David Aghmashenebeli
National Defence Academy of Georgia

Lieutenant Colonel
Levan Gozalishvili

Head of MA Program in Security Studies at LEPL – David
Aghmashenebeli National Defence Academy of Georgia

Levan Nikoleishvili

Professor of MA Program in Security Studies at LEPL –
David Aghmashenebeli National Defence Academy of
Georgia

Colonel Jambul Zaloshvili

Head of MA Program in State Resource Management
at LEPL–David Aghmashenebeli National Defence
Academy of Georgia

Giorgi Kbiltsetskhilashvili

Professor of MA Program in State Resource Manage-
ment at LEPL – David Aghmashenebeli National Defence
Academy of Georgia

Lieutenant Colonel Ruslan Darchidze

Head of the Baccalaureate at LEPL – David Aghmashene-
beli National Defence Academy of Georgia

Romeo Galdava

Acting Chief of the Baccalaureate program in Informat-
ics at LEPL – David Aghmashenebeli National Defence
Academy of Georgia

Nani Arabuli

Associate Professor of the Baccalaureate Program in
Informatics at LEPL-David Aghmashenebeli National
Defence Academy of Georgia



© Publishing House Of LEPL- David Aghmashenebeli National Defence Academy, 2025

This is an open-access journal. All published articles are licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

Authors retain copyright of their work while granting the David Aghmashenebeli National Defence

Academy the right to publish the work in this journal.

For more information about the license, visit: <https://creativecommons.org/licenses/by/4.0/>

ISBN 978-9941-8-8258-6

Lieutenant Colonel Ioseb Turashvili	Head of the Baccalaureate Program in Management at LEPL - David Aghmashenebeli National Defence Academy of Georgia
Ketevan Chiabrishvili	Professor of the Baccalaureate Program in Management at LEPL-David Aghmashenebeli National Defence Academy of Georgia
Lieutenant Colonel Omar Turmanidze	Head of the Baccalaureate Program in Defence and Security at LEPL - David Aghmashenebeli National Defence Academy of Georgia
Levan Gegeshidze	Professor of the Baccalaureate Program in Defence and Security at LEPL - David Aghmashenebeli National Defence Academy of Georgia
Lieutenant - Colonel Vazha Vashakmadze	Head of the Baccalaureate Program in Law at LEPL - David Aghmashenebeli National Defence Academy of Georgia
Ivane Balakhashvili	Professor of the Baccalaureate Program in Law at LEPL - David Aghmashenebeli National Defence Academy of Georgia
Colonel Giorgi Laghiashvili	Head of the Scientific Research Center of LEPL – David Aghmashenebeli National Defence Academy of Georgia
Nikoloz Esitashvili	Chief Scientist of Scientific-Research Center of LEPL - David Aghmashenebeli National Defence Academy of Georgia
Tinatin Kropadze	Chief Scientist of Scientific-Research Center of LEPL - David Aghmashenebeli National Defence Academy of Georgia
Zurab Samkharadze	Chief Scientist of Scientific-Research Center of LEPL - David Aghmashenebeli National Defence Academy of Georgia
Ketevan Kveselava	Chief Scientist of Scientific-Research Center of LEPL - David Aghmashenebeli National Defence Academy of Georgia
Chief Editor Maia Gamsakhurdia	Chief Scientist of Scientific-Research Center of LEPL - David Aghmashenebeli National Defence Academy of Georgia
Computer Designer Marisha Dzuliashvili	Editor of the Library of LEPL - David Aghmashenebeli National Defence Academy of Georgia

CONTENTS

Lieutenant Tamar Khaduri, Lieutenant Davit Tsakadze From Containment to Contestation: Defense Innovation and Power Politics in the Black Sea Region	7
Lieutenant Eter Bakhturidze From Gaza to Global Security: The Israel–Palestine War and the Transformation of Modern Conflict	17
Zurab Nebieridze, Imeda Arveladze Artificial Intelligence and the Transformation of Strategic Advantage in Defense Forces	24
Captain Khatia Gogaladze International Partnerships and Defense Innovations: Emerging Models of Collective Security	31
Vakhtangi Danelia, Luka Ckhadadze Germany’s Zeitenwende: The Transformation of National Defense and the Reconfiguration of European Security	40
Aleksandra Dekanosidze, Mariam Menabdishvili NATO Artificial Intelligence Strategy	49
Giorgi Okropiridze, Luka Zaalishvili Artificial Intelligence as a Strategic Force Multiplier in Modern Defense	56
Tekla Gablishvili Innovating Defense through International Cooperation: Building the Foundations of Future Security	66
Senior Lieutenant Veriko Tordia Modernization of Warfare and Militarization in 21st Century	75
Lile Bubuteishvili, Giorgi Nozadze Modern Warfare and the Role of Emerging Technologies	81
Luka Marshania, Nikoloz Mebagishvili The U.S.–Israel Security Partnership: Strategic Cooperation in Defense, Intelligence, and Regional Stability	87
Nikoloz Merabishvili Russia’s Failed Provocation: Strategic Miscalculations and Geopolitical Consequences	93
Major Ioseb Papiashvili From the Battlefield to the Lab: The Impact of the Russia - Ukraine War on the Development of International Defence Innovation	99
Giorgi Parkauli Drones as Hard and Soft Power: Innovation and Security Lessons from the Russo-Ukraine War	106
Major Nika Zhorzholiani Artificial Intelligence as a Force Multiplier for Georgia's Defense Capability	114

Tatia Razmadze The U.S.–Ukraine Engineering Partnership: Strategic Cooperation for Reconstruction and Technological Development	125
Giorgi Nadibaidze, Zaza Surmanidze The evolution of modern defense: How technological Innovation is redefining global security (Israel-Iran case of 2025)	130
Beka Shaishmelashvili, Giorgi Shatirishvili Japan–US Military-Political Cooperation: A Response to China’s Challenges	136
Senior Lieutenant Konstantine Shanava The Technological and Alliance Dimensions of Modern Security: Redefining Power and Cooperation in the Global Order	144
Luka Shukvani Secure Future: Defense Innovation, Resilient Economy, and International Partnerships	152
Tariel Tskhadadze, Beso Shubitidze Artificial Intelligence in Modern Defense Systems: Transforming Strategic and Operational Capabilities	162
Saba Chiburdanidze, Parmeni Garsidze Strengthening the U.S.-Australia Alliance: Countering China’s Growing Military Modernization and Influence in the Indo-Pacific	170
Lasha Chokolashvili, Otar Oniani Technology and Security: Bilateral Defense Innovation Partnerships in the NATO Space	180
Giorgi Chkhaidze, Lado Gogoladze Technological Development and Defence Innovation in the Caucasus during the Russia–Ukraine War	186
Gvantsa Dzmorashvili Israel’s Defence Startups	194
Iuri Khurtsidze, Teimuraz Targamadze Beyond the Alliance: Non-NATO Contributions and the Complexity of the Afghan War	204
Tato Macharashvili, Davit Mikeladze International Space Partnership: Building a New Architecture for Security	211
Giorgi Khachidze The Geopolitical Aspects of Submarine Communication Cables as Critical Infrastructure and Their Impact on International Security	217
Natia Oshkhereli Public-private partnerships in border security innovation: policy and governance models for internal and international security	225
Lieutenant Mariam Mukbaniani Modern Geopolitics and Security Competition in the Far North: Russia, USA and China’s Strategic Interests in the Arctic	233
Nikoloz Vardia, Davit Jabishvili Modern Warfare and the Role of Emerging Technologies	242

Gigi Chaligava, Temo Atsanelidze Defence Innovations and International Partnerships: Shaping the Future of Security	251
Lekso Kupatadze, Davit Davituri The Strategic Role of Drones in Modern Military Operations	262
Saba Khomasuridze Evolving Security Dynamics in the South Caucasus and Black Sea Regions	271
Mikheil Popkhadze Threats of International Terrorism and Security Policy in the Caucasus Challenges and Perspectives	279
Alika Buzaladze Innovation and Cooperation in the Nordic Defence Network: A Model for Regional Security Integration	286
Giorgi Megrelishvili, Elene Jiadze Innovation as a Strategic Imperative: Transforming the Architecture of Modern Cyber Defence	292
Major Aleksandre Beridze Adaptation cadence and GBAD: practical lessons from Ukraine for Small States and Major Alliances	299
Private Luka Tchighladze Innovation and Coercion: How China’s Defense Modernization Shapes Sea Power the South China Dynamics	306
Sergi Khurtsidze, Leri Dotiashvili Unmanned Aerial Vehicles and Their Strategic Role in Russia–Ukraine Conflict	312
Mangia Tchintcharauli, Rati Kukuladze The Transformation of Modern Warfare and Hybrid Threats: The Case of the Russia–Ukraine War and Recommendations for Georgia	320
Giga Misireli, Nika Merebashvili Technological Alliances and the Future of Security: U.S. and Allied Cooperation in AI and Defense Innovation	326
Lieutenant Irakli Grigoriadi Defence Innovation as Soft Power: How Technological Cooperation Shapes Global Influence in the 21st Century	333
Lieutenant Dimitri Jakonia The Ethics of Strategic Advantage: Human Agency, Accountability, and Emerging Technologies	342
Shahryar Huseinli Defence Innovation and International Cooperation: Shaping the Future of Global Security	355
Lieutenant Giorgi Phkhakadze From Regional Power to Global Actor: China’s Military Modernization and International Strategy	361

FROM CONTAINMENT TO CONTESTATION: DEFENSE INNOVATION AND POWER POLITICS IN THE BLACK SEA REGION

Lieutenant Tamar Khaduri

The Learner of a Master's Degree Program (Defense Analysis) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Lieutenant Davit Tsakadze

The Learner of a Master's Degree Program (State Recourse Management) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The Black Sea has emerged as a central theatre of strategic competition in the twenty-first century, reflecting both a renewed great-power rivalry and the transformative effects of defence innovation. This paper examines the evolving Russia–NATO dynamics in the Black Sea through the analytical lens of Offensive Realism, demonstrating how technological advances and shifting alliance postures are reconfiguring the regional security environment. The study situates contemporary developments in their historical context—from the Cold War, when the Black Sea functioned as a containment buffer under the Montreux Convention, through the post-Soviet era of NATO enlargement and Russia's assertive resurgence. Attention is given to Russia's military modernization, notably the deployment of advanced missile systems, anti-access/area-denial (A2/AD) capabilities, and the integration of electronic-warfare and cyber operations. In counterpoint, NATO has strengthened its regional posture through multinational exercises, forward presence, and the adoption of emerging technologies such as unmanned systems and sophisticated C4ISR platforms. The operational and strategic consequences of these trends are explored via recent case studies, including Ukraine's inventive employment of unmanned surface vessels and drone swarms to disrupt Russian naval operations. The article further interrogates alliance dynamics, identifying both the opportunities for enhanced collective deterrence and the frictions that complicate multinational cooperation among Black Sea states. It critically assesses escalation risks associated with emerging technologies, the changing offence–defence balance, and the perennial challenges of crisis management. The analysis concludes that power politics remain salient in the Black Sea: maintaining regional stability therefore requires adaptive, forward-looking strategies that integrate technological innovation, alliance cohesion, and robust crisis-management mechanisms.

Keywords: Black Sea; NATO; Russia; defence innovation; A2/AD; unmanned systems; alliance dynamics; crisis management.

Introduction

The Black Sea region has long functioned as a crossroads of empires, commerce and military contestation, serving simultaneously as a strategic gateway and a contested frontier between East and West. In the twenty-first century its importance has further increased, as the area has become a focal arena for renewed great-power competition between Russia and the North Atlantic Treaty Organization.¹

During the Cold War the Black Sea constituted a vital frontier in the global confrontation between the Soviet Union and the Western alliance. NATO's regional strategy was guided by the logic of containment, employing military deterrence, forward basing, and the cultivation of partnerships—principally with Turkey and, to a lesser degree, Greece—to limit Soviet expansion and influence. The Montreux Convention of 1936, which regulated naval access to the Black Sea, further shaped the strategic environment by restricting the presence of non-littoral NATO navies and thereby reinforcing the Soviet Union's predominant position.²

Main Part

The dissolution of the Soviet Union in 1991 fundamentally transformed the regional landscape. Newly independent littoral states, notably Ukraine and Georgia, emerged along the Black Sea, and Russia's direct control over the area was substantially attenuated (Menon, 2015). During the 1990s and early 2000s NATO and the European Union pursued an expansion of influence through enlargement and partnership initiatives—most visibly with Romania's and Bulgaria's accession to NATO in 2004—and sought closer ties with Ukraine and Georgia. This era was marked by a relative diminution of military tensions and an emphasis on economic reconstruction, democratic reform, and cooperative security arrangements.

However, the 2008 war between Russia and Georgia marked a turning point, signaling Moscow's willingness to use military force to reassert its interests in the post-Soviet space and challenge Western influence. The conflict exposed the vulnerabilities of smaller Black Sea states and highlighted the limitations of Western deterrence. It also foreshadowed a more assertive Russian posture in the region, culminating in the annexation of Crimea in 2014³. This event represented a dramatic escalation, as Russia not only seized territory but also rapidly expanded and modernized its Black Sea Fleet, establishing a robust anti-access/area denial (A2/AD) bubble and projecting power into the eastern Mediterranean⁴.

The subsequent years witnessed a marked intensification of military activity and strategic competition in the Black Sea. Russia's intervention in eastern Ukraine, the militarization of Crimea, and the use of hybrid tactics—including cyber operations and disinformation campaigns—have disrupted the regional status quo. In response, NATO has reinforced its presence and activities in the area, conducting regular naval patrols, expanding joint exercises such as Sea Breeze, and bol-

1 NATO, "NATO's Enhanced Presence in the Black Sea Region," last modified 2022, <https://surl.li/xekmow>. Accessed 31.10.25

2 Gökhan Özhan, "The Montreux Convention and Its Importance for the Black Sea Region," *Turkish Policy Quarterly* 9, no. 3 (2010): 101–110.

3 Rajan Menon, *The Ukraine Crisis: What It Means for the West* (Washington, DC: Brookings Institution Press, 2015).

4 Richard Connolly, *Russia's Response to Sanctions: How Western Economic Statecraft is Reshaping Political Economy in Russia* (Cambridge: Cambridge University Press, 2018).

stering the defence capabilities of its eastern members. The full-scale Russian invasion of Ukraine in 2022 further elevated the Black Sea to a principal theatre of great-power rivalry, with both sides exploiting technological innovations to secure operational and strategic advantages⁵.

Today, the Black Sea is no longer a peripheral or secondary concern for NATO and Russia. It has become a dynamic arena of contestation, where the interplay of military modernization, alliance politics, and defense innovation shapes the balance of power. The region's evolution from a Cold War buffer zone to a laboratory for twenty-first-century security competition underscores the enduring relevance of power politics and the transformative impact of technological change⁶.

The article examines how defence innovation is transforming competitive dynamics in the Black Sea, shifting the region from a paradigm of containment to one of active contestation. Employing the theoretical lens of Offensive Realism, the analysis explains how states exploit technological advancements and alliance relationships to maximize relative power within an anarchic international system.⁷ Drawing on historical context, targeted case studies, and policy analysis, the paper illuminates evolving NATO–Russia interactions and assesses their broader implications for regional and global security.

Theoretical Framework: Offensive Realism and Technological Innovation

Offensive Realism, most prominently articulated by John J. Mearsheimer, is a branch of structural realism that views the international system as inherently anarchic, lacking a central authority to enforce rules or guarantee security. In such an environment, states are perpetually uncertain about the intentions and capabilities of others. This uncertainty compels them to act aggressively to maximize their relative power, as survival is never guaranteed. According to Offensive Realism, great powers are not satisfied with maintaining the status quo; instead, they seek opportunities to expand their influence and capabilities whenever possible.

This relentless pursuit of power leads to recurring security dilemmas, where the efforts of one state to enhance its security—such as through military modernization or alliance-building—are perceived as threats by others, prompting countermeasures and fueling arms races⁸. The result is a persistent cycle of competition, mistrust, and the potential for conflict, even among states that might otherwise prefer stability.

In the Black Sea context, Offensive Realism offers a compelling framework for understanding the central role of defence innovation in regional security dynamics.⁹ Technological advances—unmanned systems, precision-guided munitions, enhanced surveillance and sensing, and cyber capabilities—function not merely as defensive instruments but as means of altering the balance of power. Regional actors, particularly Russia and NATO members, prioritize investment in these technologies to offset adversary strengths, exploit emergent domains of warfare, and secure stra-

5 BBC, "Ukraine War: Russia's Black Sea Fleet and the Battle for the Sea," 2022, <https://surl.li/iydmmu>, Accessed 31.10.25

6 Michael Kofman, "Russian A2/AD: It Is Not Overrated, Just Poorly Understood," *War on the Rocks*, 2017, <https://surl.li/tdlnkq>

7 John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton & Company, 2001).

8 Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (1978): 167–214.

9 Dmitry Gorenburg, "Russia's Black Sea Fleet: Toward a New Era?" *PONARS Eurasia Policy Memo* No. 608 (2019), <https://www.ponarseurasia.org>. Accessed 31.10.25

tegic advantage. NATO's partnerships with littoral and adjacent states, and Russia's cultivation of influence networks, therefore represent strategic manoeuvres within a broader contest for dominance. Such alliances facilitate technology transfer, joint exercises and operational experimentation, yet they remain governed by the underlying logic of competition and national self-interest. Technological innovation is not neutral or purely technical; it is deeply embedded in regional power politics. As states race to develop and deploy novel capabilities they reshape the offence–defence balance, generate new uncertainties and risks, and thereby intensify the security dilemma. Offensive Realism thus provides a robust explanatory lens for why defence innovation has become a central feature of NATO–Russia competition in the Black Sea.

Russia's Military Modernization and A2/AD Strategies

Since the early 2010s, Russia has embarked on an ambitious program to modernize its Black Sea Fleet and transform the region into a bastion of anti-access/area denial (A2/AD) capabilities. This modernization drive accelerated dramatically following the annexation of Crimea in 2014, which provided Russia with a strategic foothold and the ability to upgrade and expand its naval and air assets in the region.

A central pillar of Russia's approach has been the deployment of advanced missile systems. The Black Sea Fleet now boasts platforms equipped with Kalibr cruise missiles, capable of striking targets across the region and deep into Europe and the Middle East. The Bastion and Bal coastal defense missile systems, stationed in Crimea and along the Russian coastline, provide robust anti-ship and land-attack capabilities, effectively creating a “missile wall” that threatens any hostile naval presence¹⁰. These systems are complemented by the S-400 TRIUMF air defense system, which extends Russia's ability to contest airspace over much of the Black Sea and parts of neighboring countries¹¹. In addition to kinetic capabilities, Russia has invested heavily in electronic warfare (EW) and cyber operations. The Black Sea Fleet operates sophisticated EW assets designed to jam, spoof, or disrupt NATO communications, navigation, and targeting systems. These tools have been used to interfere with GPS signals, disrupt drone operations, and complicate the command and control of adversary forces. The integration of EW with kinetic and cyber capabilities enhances Russia's ability to operate in the so-called “grey zone,” blurring the lines between peace and conflict and complicating NATO's response options.

Naval modernization has encompassed the introduction of new classes of submarines, corvettes and frigates, many of which incorporate stealth features and advanced weapons systems. Operational tempo has increased accordingly, with sustained patrols, unannounced exercises and high-visibility missile tests employed to signal capability and resolve. Russia's Black Sea bases—most notably Sevastopol and Novorossiysk—have been expanded and fortified, functioning as hubs for logistics, intelligence collection and regional power projection.

The cumulative effect of these investments is a layered and integrated A2/AD “bubble” that significantly raises the risks and costs for NATO forces operating in the Black Sea. Russia's strat-

10 Katarzyna Zysk, “Russia's Naval Power in the Arctic and Black Sea: Strategic Ambitions and Capabilities,” *Journal of Strategic Studies* 42, no. 7 (2019): 901–927.

11 Dmitry Gorenburg, “Russia's Black Sea Fleet: Toward a New Era?” *PONARS Eurasia Policy Memo* No. 608 (2019), <https://surl.lu/jqkvkt>, Accessed 31.10.25

egy is not only defensive but also offensive in nature, enabling Moscow to project power into the eastern Mediterranean, support operations in Syria, and influence the security environment across southeastern Europe and the Caucasus.

By leveraging technological innovation and military modernization, Russia seeks to deter NATO intervention, secure its maritime dominance, and assert itself as the preeminent power in the Black Sea region. This evolving posture has profound implications for regional stability, alliance cohesion, and the broader balance of power between Russia and the West.

NATO's Response: Exercises and Technology Integration

In response to Russia's assertive military posture and the growing sophistication of its A2/AD capabilities in the Black Sea, NATO and its regional allies have undertaken a comprehensive set of measures to bolster deterrence, enhance readiness, and maintain freedom of navigation¹². Central to this response has been the combination of forward deployments, multinational exercises, and the accelerated adoption of cutting-edge defense technologies.

NATO has increased its naval and air presence in the Black Sea through regular patrols, rotational deployments, and the establishment of rapid reaction forces. For example, in 2021, NATO warships spent over 120 days in the Black Sea, a significant increase compared to previous years. Member states such as Romania, Bulgaria, and Turkey have hosted allied warships and aircraft, while the United States and the United Kingdom have periodically deployed advanced naval assets to the region. In June 2021, the UK's HMS Defender and the Dutch HNLMS Evertsen conducted freedom of navigation operations near Crimea, drawing a strong response from Russian forces (BBC, 2021). These deployments serve both as a deterrent signal to Russia and as a means to reassure NATO's eastern flank allies of the alliance's commitment to collective defense.

Annual multinational exercises, most notably Exercise Sea Breeze, have become a cornerstone of NATO's strategy in the Black Sea. Co-hosted by Ukraine and the United States, Sea Breeze 2021 was the largest iteration to date, involving 32 ships, 40 aircraft, and over 5,000 personnel from 32 countries. The exercise included amphibious operations, anti-submarine warfare, mine countermeasures, and maritime interdiction, as well as the integration of unmanned systems for ISR missions. These exercises are designed not only to demonstrate resolve but also to improve interoperability among allied and partner forces, refine joint tactics, and test new operational concepts in a contested maritime environment¹³.

Other exercises, such as Breeze (led by Bulgaria) and Poseidon (focused on mine warfare and hosted by Romania), further reinforce regional cooperation and readiness. For example, Exercise Breeze 2023 involved 13 ships and over 1,700 personnel from 10 NATO countries¹⁴. These activities provide valuable opportunities for Black Sea states to integrate with NATO standards and procedures, enhancing their ability to operate alongside larger allies in crisis or conflict scenarios.

12 U.S. Naval Forces Europe-Africa, "Exercise Sea Breeze 2021 Kicks Off in Ukraine," June 28, 2021, <https://surl.lu/fuzotz>

13 Steven Erlanger, "NATO Flexes Its Muscles in Black Sea War Games," *The New York Times*, July 2, 2021, <https://surl.lu/djnjan>

14 Bulgarian Ministry of Defence, "Exercise Breeze 2023," 2023, <https://www.mod.bg/en/news>. Accessed 31.10.25

Integration of Advanced Technologies

Recognizing the changing character of warfare, NATO has prioritized the integration of advanced technologies into its Black Sea operations. Unmanned aerial vehicles (UAVs) and maritime drones are increasingly deployed for intelligence, surveillance and reconnaissance (ISR) tasks;¹⁵ for example, during Sea Breeze 2021 the U.S. Navy employed MQ-9 Reapers and Scan-Eagle UAVs to augment ISR capability. The introduction of advanced C4ISR systems (command, control, communications, computers, intelligence, surveillance and reconnaissance) has enhanced the Alliance's capacity to coordinate complex operations, disseminate information swiftly, and respond effectively to emergent threats.¹⁶

NATO has also invested in electronic warfare capabilities, cyber defense, and the development of countermeasures to Russian missile and drone systems. The NATO Communications and Information Agency (NCIA) has supported the field-testing of secure communications platforms and cyber defense tools in the Black Sea region. In 2022, NATO launched the Defence Innovation Accelerator for the North Atlantic to foster the development and integration of emerging technologies, including artificial intelligence and autonomous systems, with several pilot projects involving Black Sea allies¹⁷.

Operational and Strategic Impact

These efforts collectively aim to offset Russia's military advantages, complicate its operational planning, and ensure that NATO retains the ability to project power and defend its interests in the Black Sea. By improving interoperability, testing innovative concepts, and integrating new technologies, NATO not only counters Russian advances but also strengthens alliance cohesion and demonstrates adaptability in the face of evolving security challenges.

The continued emphasis on exercises and technological integration reflects NATO's assessment that the Black Sea constitutes a critical theatre in the broader contest with Russia—an arena in which technological innovation, operational agility and multinational cooperation are indispensable for sustaining credible deterrence and preserving regional stability.

Ukraine's Unmanned Systems: Redefining Maritime Power

Ukraine's war with Russia has become a proving ground for new military technologies, particularly unmanned systems. By leveraging unmanned surface vessels (USVs) and drone swarms, Ukraine has challenged long-standing assumptions about maritime dominance¹⁸. These asymmetric tools have enabled Ukraine—a materially weaker state—to disrupt Russian naval operations and shift the regional balance of power.

For example, in 2023, Ukraine used explosive-laden USVs to strike Russian warships in Sevastopol harbor. These attacks damaged or destroyed several vessels, including the Black Sea

¹⁵ Amuel Bendett, "Unmanned and Autonomous Systems in the Black Sea: The Next Phase of Maritime Competition," *Center for Naval Analyses*, 2022.

¹⁶ NATO, "C4ISR Capabilities and Interoperability," last modified 2023, <https://surl.li/cgibzy>, Accessed 31.10.25

¹⁷ NATO, "Defence Innovation Accelerator for the North Atlantic (DIANA)," last modified 2023, <https://surl.li/vdiygk>

¹⁸ Samuel Bendett, "Unmanned and Autonomous Systems in the Black Sea: The Next Phase of Maritime Competition," *Center for Naval Analyses*, 2022.

Fleet's flagship, the Moskva. As a result, Russia was forced to reposition much of its fleet farther from the Ukrainian coast, reducing its operational reach¹⁹.

Ukraine has also employed drone swarms to target critical infrastructure, such as radar installations and fuel depots in Crimea. In one notable incident, a coordinated drone attack temporarily disabled Russian radar coverage, paving the way for further Ukrainian operations. The psychological impact of these persistent unmanned threats has compelled Russia to invest heavily in counter-drone defenses and rethink its naval deployments.²⁰ These examples illustrate how technological innovation can empower smaller states to impose significant costs on more powerful adversaries, fundamentally altering the dynamics of regional conflict.

Alliance Dynamics: Power, Partnerships, and Realist Calculations

Ukraine's success with unmanned systems has not occurred in isolation. NATO's partnerships with Black Sea states—Romania, Bulgaria, Turkey—and with Ukraine itself have played a crucial role in facilitating technology transfer, joint training, and operational innovation²¹. However, these alliances are not without friction. Divergent national interests and varying threat perceptions often challenge alliance cohesion.

For instance, Turkey's supply of Bayraktar TB2 drones to Ukraine has been a game-changer on the battlefield. Joint naval exercises like Sea Breeze have enhanced interoperability among NATO members and partners, strengthening collective defense capabilities in the Black Sea²².

Yet, national priorities sometimes diverge. While Romania and Bulgaria advocate for a robust NATO presence in the region, Turkey has occasionally limited NATO naval access, citing its obligations under the Montreux Convention and its own strategic interests. These differences highlight the complex calculus behind alliance behavior.

From an Offensive Realist perspective, these partnerships are best understood not as purely stabilizing arrangements, but as strategic tools for maximizing power and counterbalancing rivals. States join alliances to advance their own interests, leveraging collective strength to deter adversaries and shape the regional order. Turkey, for example, uses its NATO membership to balance both Russian and Western influence, while Ukraine seeks closer ties to NATO to enhance its security and deter further aggression²³.

Escalation Dynamics and Security Dilemmas

The rapid introduction of novel military technologies in the Black Sea has fundamentally altered the dynamics of escalation and crisis management. Unmanned systems, cyber operations and electronic warfare lower the threshold for hostile action by enabling states to undertake provocative measures that stop short of conventional engagement; yet these same capabilities also amplify risks of miscalculation and unintended escalation, complicating signalling and crisis stability.

19 BBC News, "Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack," August 2023, <https://surl.li/adlaqz>

20 Dmitry Gorenburg, "Ukraine's Use of Unmanned Systems: Lessons for the Future of Warfare," *PONARS Eurasia Policy Memo* No. 789 (2023).

21 NATO, "NATO's Enhanced Forward Presence," last modified 2023, <https://surl.li/wyzxpt>, Accessed 31.10.25

22 U.S. Naval Forces Europe-Africa, "Exercise Sea Breeze 2021 Kicks Off in Ukraine," June 28, 2021, <https://surl.li/vtyvwa>

23 Pavel Baev, "Turkey's Balancing Act in the Black Sea," *Russian Analytical Digest* No. 238 (2020): 6–8.

*For example, Ukraine's use of autonomous USVs and drone swarms against Russian naval assets has created a new layer of ambiguity in the maritime domain. Unlike traditional naval engagements, attacks carried out by unmanned systems can be launched remotely, often without clear attribution. This ambiguity complicates decision-making for both attackers and defenders, raising the risk that a limited strike could spiral into a broader confrontation*²⁴.

Electronic warfare adds yet another layer of complexity. Jamming and spoofing technologies can interfere with navigation, targeting, and communications for both manned and unmanned systems. In one incident, Russian electronic warfare reportedly disrupted GPS signals in the Black Sea, affecting not only military assets but also commercial shipping. Such actions risk drawing in third parties and expanding the scope of the conflict.²⁵

The offence–defence balance in the Black Sea is currently in flux. Actors on all sides are racing to capitalize on technological advantages—Ukraine by exploiting unmanned systems and cyber capabilities, and Russia by investing in countermeasures and electronic warfare. This dynamic produces a classic security dilemma: measures undertaken to enhance national security via new technologies can unintentionally undermine the security of others, thereby perpetuating a cycle of reciprocal action and reaction.

In this environment, crisis management becomes far more challenging. The speed, ambiguity, and deniability of modern technologies make it difficult for leaders to assess intentions and control escalation. A single misinterpreted drone strike or cyber incident could trigger a rapid and unintended escalation, with potentially far-reaching consequences for regional and even global security²⁶.

Policy Implications and Theoretical Reflections

Offensive Realism offers a compelling framework for understanding the competitive dynamics unfolding in the Black Sea. The theory's emphasis on power maximization, security competition, and the instrumental use of alliances is evident in the actions of both Russia and NATO. States in the region continually seek to enhance their relative power—whether by acquiring advanced unmanned systems, deepening military partnerships, or leveraging new domains such as cyber and electronic warfare.

For example, NATO's support for Ukraine and its Black Sea allies is not merely a gesture of solidarity, but a calculated effort to counterbalance Russian influence and maintain regional stability. Joint exercises, intelligence sharing, and technology transfers are all tools used to maximize collective power and deter aggression. Similarly, Russia's investment in anti-access/area denial (A2/AD) capabilities and electronic warfare reflects a desire to offset NATO's technological edge and assert its own dominance.

However, the rapid pace of technological change is exposing the limits of traditional international-relations theories. The rise of non-state actors, the widespread diffusion of dual-use technologies, and the blurring of boundaries between peace and war challenge core assumptions of

24 Michael Petersen, "Ukraine's Naval Drone Campaign in the Black Sea," *War on the Rocks*, August 2023, <https://surl.li/qambyn>

25 BBC News, "Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack," August 2023, <https://surl.li/xsstrf>

26 albona Zeneli and Joseph Vann, "NATO's Black Sea Challenge: Enhancing Regional Cooperation," *George C. Marshall European Center for Security Studies Security Insights* No. 65 (2021).

Offensive Realism and other classical paradigms. For example, the deployment of commercially available drones by both state and non-state actors complicates attribution and escalation management, while cyber operations can produce strategic effects without crossing conventional thresholds.

Policymakers must therefore recalibrate strategies for containment and deterrence. This requires investment not only in advanced military capabilities but also in resilience, interoperability and robust crisis-management mechanisms. Enhancing allied forces' capacity to operate seamlessly together, building redundancy into critical infrastructure, and establishing clear protocols for de-escalation are all essential measures. Moreover, as the strategic environment grows more complex, sustained dialogue and greater transparency—both within alliances and, where practicable, with potential adversaries—will be vital for managing risks and averting unintended escalation.

Conclusion

The Black Sea region stands as a vivid illustration of the enduring relevance of power politics in an era transformed by defense innovation. As Russia and NATO vie for influence, the introduction of new technologies—ranging from unmanned systems to cyber tools—has intensified the contest, challenging established paradigms and generating new risks.²⁷

Viewing these developments through the lens of Offensive Realism highlights the persistent drive for power and security that shapes state behavior.²⁸ Yet the evolving character of conflict underscores the imperative for adaptive, forward-looking strategies. For scholars, this requires refining theoretical models to incorporate technological disruption, the proliferation of dual-use capabilities, and the transformed dynamics of alliance politics—moving beyond static conceptions of power to frameworks that capture speed, diffusion and complexity. Research agendas should prioritize comparative and longitudinal studies that trace how innovation diffuses across coalitions, how new capabilities alter escalation dynamics, and which institutional arrangements most effectively mitigate risk.

For practitioners, the shifting security landscape demands policies that are flexible, resilient and carefully calibrated to the multifaceted realities of contemporary warfare. This entails sustained investment in interoperable technological systems and resilient infrastructure, the development of clear de-escalation protocols and crisis-management mechanisms, and the integration of ethical and legal governance into procurement and deployment processes. Equally important are institutional reforms that enhance rapid decision-making and multi-domain coordination across defence, intelligence and civilian agencies, alongside expanded training and wargaming to stress-test responses under realistic scenarios.

The Black Sea's fluid security environment offers wider lessons for the international community. In an era in which innovation can rapidly reconfigure the balance of power, strategic success will hinge on the ability to anticipate change, manage pervasive uncertainty and sustain effective cooperation among like-minded partners. This requires not only technological and military pre-

27 Pavel Baev, "Russia's Black Sea Strategy: Power Projection and Regional Security," *Russian Analytical Digest* No. 238 (2020): 2–5.

28 John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: W. W. Norton & Company, 2001).

paredness but also diplomatic engagement to build common norms, confidence-building measures and channels of communication that reduce the risk of miscalculation.

Ultimately, preserving stability amid persistent rivalry will depend on aligning capability development with cooperative governance. By combining rigorous scholarship with pragmatic policy innovation—anchored in interoperability, transparency and shared responsibility—states and alliances can better deter aggression, protect civilian populations and navigate the ethical and legal dilemmas posed by twenty-first-century military technologies.

Bibliography

- Baev, Pavel. "Russia's Black Sea Strategy: Power Projection and Regional Security."
- Baev, Pavel. "Turkey's Balancing Act in the Black Sea." *Russian Analytical Digest* No. 238 (2020): 6–8.
- BBC. "Ukraine War: Russia's Black Sea Fleet and the Battle for the Sea," 2022. <https://surl.lt/ewyilt>
- BBC News. "Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack," August 2023. <https://surl.li/nffupp>
- Bendett, Samuel. "Unmanned and Autonomous Systems in the Black Sea: The Next Phase of Maritime Competition." *Center for Naval Analyses*, 2022.
- Bulgarian Ministry of Defence. "Exercise Breeze 2023," 2023. <https://www.mod.bg/en/news>.
- Connolly, Richard. *Russia's Response to Sanctions: How Western Economic Statecraft is Reshaping Political Economy in Russia*. Cambridge: Cambridge University Press, 2018.
- Erlanger, Steven. "NATO Flexes Its Muscles in Black Sea War Games." *The New York Times*, July 2, 2021. <https://surl.li/vtvrvv>
- Gökhan Özhan. "The Montreux Convention and Its Importance for the Black Sea Region." *Turkish Policy Quarterly* 9, no. 3 (2010): 101–110.
- Gorenburg, Dmitry. "Russia's Black Sea Fleet: Toward a New Era?" *PONARS Eurasia Policy Memo* No. 608 (2019). <https://surl.li/tkvelv>
- Gorenburg, Dmitry. "Ukraine's Use of Unmanned Systems: Lessons for the Future of Warfare." *PONARS Eurasia Policy Memo* No. 789 (2023).
- Jervis, Robert. "Cooperation under the Security Dilemma." *World Politics* 30, no. 2 (1978): 167–214.
- Kofman, Michael. "Russian A2/AD: It Is Not Overrated, Just Poorly Understood." *War on the Rocks*, 2017. <https://surli.cc/cvwwis>
- Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001.
- Menon, Rajan. *The Ukraine Crisis: What It Means for the West*. Washington, DC: Brookings Institution Press, 2015.
- NATO. "C4ISR Capabilities and Interoperability," last modified 2023. <https://surl.li/msarph>
- NATO. "Defence Innovation Accelerator for the North Atlantic (DIANA)," last modified 2023. <https://surl.li/rwsthn>
- NATO. "NATO's Enhanced Forward Presence," last modified 2023. <https://surl.li/ehmhvv>
- NATO. "NATO's Enhanced Presence in the Black Sea Region," last modified 2022. <https://surl.li/lodeif>
- Petersen, Michael. "Ukraine's Naval Drone Campaign in the Black Sea." *War on the Rocks*, August 2023. <https://surl.li/ztywbo>
- U.S. Naval Forces Europe-Africa. "Exercise Sea Breeze 2021 Kicks Off in Ukraine," June 28, 2021. <https://surl.li/dzuggm>
- Zeneli, Albana, and Joseph Vann. "NATO's Black Sea Challenge: Enhancing Regional Cooperation." *George C. Marshall European Center for Security Studies, Security Insights* No. 65 (2021).
- Zysk, Katarzyna. "Russia's Naval Power in the Arctic and Black Sea: Strategic Ambitions and Capabilities." *Journal of Strategic Studies* 42, no. 7 (2019): 901–927.

FROM GAZA TO GLOBAL SECURITY: THE ISRAEL–PALESTINE WAR AND THE TRANSFORMATION OF MODERN CONFLICT

Lieutenant Eter Bakhturidze

The Learner of a Master's Degree Program (Defense Analysis) of
LEPL-David Agmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Agmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

This paper examines the transformation of modern warfare through the lens of the Israel–Palestine conflict, with particular emphasis on the 2021 escalation. The study explores how evolving strategic and technological factors have elevated a historically regional confrontation into an issue of global relevance. Central to this analysis is the role of Israel's Iron Dome defense system, whose rapid threat detection, precision interception, and operational efficiency exemplify the capacity of advanced technologies to mitigate asymmetric warfare and redefine contemporary military dynamics. The research further analyzes the involvement of key international actors-most notably the United States and Iran-whose political, military, and strategic engagements significantly influence regional power configurations and broader perceptions of global security. Through this lens, the paper reveals how modern conflicts are increasingly shaped by the interplay of technology, strategy, and international cooperation, wherein even relatively small or non-state actors can exert disproportionate influence on global stability. The case of Gaza serves as a critical illustration of how adaptive security strategies-grounded in innovation, collaboration, and technological integration-are essential for addressing twenty-first-century threats. The findings demonstrate that effective defense in the modern era depends not only on military capability but also on the ability to build resilient networks of partnerships and technological expertise.

Ultimately, the study underscores that modern security is complex, multidimensional, and deeply interconnected, reflecting the convergence of local conflicts and global power structures. It offers valuable insights for policymakers and defense planners seeking to navigate the challenges of asymmetric warfare, harness technological innovation, and strengthen the interdependence between regional stability and international security.

Keywords: Israel-Palestine conflict, iron dome, technology, modern security.

Introduction

In the first half of the twentieth century, the question “**What is war?**” was relatively straightforward to answer. War was conventionally understood as the direct use of military force by a state to achieve territorial, political, or strategic objectives. This conception was grounded in classical military experience, characterized by clearly defined frontlines, organized state armies, and conventional weaponry such as tanks, artillery, and air forces. Within this framework, war was perceived as a structured and predictable phenomenon—an extension of politics by other means, governed by established doctrines and codified rules of engagement.

However, in the early twenty-first century, the concept and character of war have undergone a profound transformation. As Thomas Hammes argues, Fifth-Generation Warfare (5GW) represents a new and far more complex phase in the evolution of conflict, one that transcends traditional military boundaries and objectives. In this paradigm, war is no longer confined to the battlefield or defined solely by the actions of state militaries. Instead, it operates across multiple domains—political, social, economic, informational, and technological—interacting dynamically with the processes of globalization and the instantaneous, mass dissemination of information (Krishnan 2022)¹

This new reality has blurred the distinction between war and peace, eroding the clarity that once defined traditional conflicts. Fifth-Generation Warfare integrates tools such as cyber operations, disinformation campaigns, economic coercion, and proxy engagements, making the battlefield both physical and virtual. As a result, conflict has become increasingly unpredictable, with outcomes influenced as much by narratives and perception management as by kinetic force. The rise of non-state actors—ranging from terrorist organizations and private military contractors to hacker collectives and transnational movements—has further expanded the landscape of warfare. These actors exploit technological innovation, decentralized organization, and global connectivity to challenge even the most powerful states.

Consequently, the modern conception of war emphasizes asymmetry, adaptability, and complexity. **The** traditional metrics of victory and defeat have become difficult to define, as conflicts are now waged not merely for territorial control but for influence, legitimacy, and information dominance. Fifth-Generation Warfare thus represents a paradigm shift in which the boundaries of conflict are fluid, the actors are diverse, and the means of engagement are deeply intertwined with the broader social, economic, and technological systems that shape the modern world.

Main Part

The Israel–Palestine conflict serves as one of the most vivid and instructive examples of how the character of warfare has evolved in the twenty-first century. Once primarily a regional confrontation, defined by direct territorial disputes, localized provocations, and conventional military engagements, it has gradually transformed into a complex, multidimensional battleground where technological, strategic, and informational factors intersect. In the modern era, the conflict has become a testing ground for cutting-edge technologies, including artificial intelligence (AI), unmanned aerial and ground systems, precision-guided weaponry, cyber operations, and sophis-

¹ Krishnan, Armin, “Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison.” *strategic security*. 2022

ticated information warfare. These innovations have revolutionized how states-and increasingly, non-state actors-engage in conflict, blurring the boundaries between physical and digital warfare and introducing new dimensions of risk and uncertainty.

This ongoing transformation extends far beyond the immediate region. The Israel-Palestine conflict now resonates within the broader global security architecture, influencing how states conceptualize defense, deterrence, and resilience. As military technologies advance and proliferate, other nations and international alliances observe and adapt, seeking to draw operational, strategic, and technological lessons from the conflict's dynamics. The integration of AI-based defense systems, the use of real-time intelligence and data analytics, and the growing importance of media and cyber domains exemplify the shift toward hybrid forms of warfare that combine traditional and non-traditional means of conflict. This shift compels both national governments and international organizations to rethink conventional security paradigms, incorporating innovation, flexibility, and interconnectivity into their strategic planning.

Therefore, analyzing the Israel-Palestine conflict solely through a state-level lens is no longer sufficient. To grasp its full complexity and implications, it must be examined within a systemic, regional, and global framework. Such a comprehensive perspective enables scholars and policymakers to understand how the transformation of warfare-driven by technological innovation-reshapes the international order. It also highlights the increasingly porous boundaries between local conflicts and global stability, as lessons from one region influence defense strategies, arms development, and security doctrines elsewhere. This multi-layered analysis provides valuable insight not only into emerging threats but also into the new standards and expectations that modern warfare imposes on defense institutions, policy formulation, and international cooperation.

Furthermore, technological progress in this conflict has redefined the role of alliances and partnerships. The ability to integrate shared intelligence, coordinate defense systems, and cooperate in the development of advanced technologies has become central to maintaining both regional and global security. The Israel-Palestine conflict, in this sense, illustrates how international partnerships have become an essential component of modern security architecture-serving not only as deterrents but also as incubators for defense innovation and policy coordination.

To fully contextualize this evolution, it is essential to briefly and chronologically trace the historical trajectory of the Israel-Palestine conflict. From its very inception, the State of Israel has placed national security at the core of its political and strategic identity. Its geographic position, surrounded by states that historically adopted adversarial postures, has compelled Israel to develop a doctrine of vigilance, self-reliance, and technological superiority. This enduring security imperative has profoundly shaped the country's foreign policy, defense priorities, and economic development. Over time, Israel's emphasis on innovation-reflected in the creation of its advanced military-industrial complex and pioneering technologies such as the Iron Dome- has allowed it to adapt to evolving threats and maintain a qualitative military edge.

The Israel-Palestine conflict encapsulates the transition from conventional warfare to technologically enhanced, hybrid forms of conflict that define the contemporary era. It underscores how local and regional dynamics, once contained within limited geographic boundaries, now reverberate across the global security landscape. Understanding this transformation requires a nuanced,

interdisciplinary, and multi-scalar approach-one that recognizes the interplay of innovation, economy, and partnership as the new foundation of modern security.

In 1948, the establishment of the modern State of Israel faced strong opposition from the Palestinian population as well as from Egypt, Jordan, Syria, and Iraq. Following the declaration of independence, these states launched a military campaign against Israel. In 1967, Israel carried out a preemptive strike against Egypt and Syria, initiating the Six-Day War. During this conflict, Israel captured the West Bank, including East Jerusalem from Jordan, and the Golan Heights from Syria. In 1973, Egypt and Syria launched coordinated attacks along the Suez Canal and the Golan Heights, resulting in the Yom Kippur War. Despite the surprise offensive, Israel successfully repelled both armies within three weeks. In 1982, Israel invaded Lebanon, leading to the encirclement of thousands of Palestinian fighters under Yasser Arafat for ten weeks until their evacuation by sea. The conflict in Lebanon resumed in 2006 when Hezbollah militants captured two Israeli soldiers, prompting a large-scale Israeli military response. In 2005, Israel withdrew from the Gaza Strip, which it had occupied following the 1967 conflict with Egypt. Since then, Gaza has remained a focal point of clashes, including major confrontations in 2006, 2008, 2012, 2014, and 2021. Beyond conventional warfare, Palestinians organized two intifadas-popular uprisings-between 1987–1993 and 2000–2005, further demonstrating the protracted and multifaceted nature of the conflict. Since 2014, peace negotiations have stalled, as efforts in Washington to reach an agreement between Israel and the Palestinians failed, leaving the conflict unresolved and continuing to shape regional security dynamics. (McGreal 2023)²

The issues discussed and the historical dynamics clearly demonstrate that the conflict between Israel and Palestine is rooted not only in geopolitical factors but also in deep-seated ideological and historical foundations. Consequently, this conflict has become an integral part of the strategic culture of both parties, making its management and containment particularly challenging. For this reason, these processes could not remain a “frozen conflict” for long, and in fact, they re-escalated starting in 2021. This period is of particular interest for our study, as it requires an in-depth analysis of the following dimensions: the technological innovations that emerged in the military domain, the responses of various actors within the international system, and, more broadly, the impact that the reactivation of the conflict has had on regional and global security.

On May 10, 2021, a major security crisis erupted in Israel and Gaza, following weeks of rising tensions in Jerusalem, particularly over the Sheikh Jarrah evictions, canceled Palestinian elections, social media videos of attacks, and disputes over access to religious sites. Clashes intensified around the Temple Mount/Al-Aqsa compound, with confrontations between Palestinian protesters and Israeli police.

Hamas and Palestinian Islamic Jihad (PIJ) launched rockets at Israel, claiming to defend Al-Aqsa. Over 4,300 rockets were fired from Gaza over 11 days, targeting civilian centers across southern and central Israel, including Jerusalem and Tel Aviv. Millions of Israelis were forced to take shelter, particularly in southern cities such as Ashkelon, Ashdod, and Beer Sheva.

A defining feature of this conflict was the **Iron Dome**, Israel’s anti-missile defense system. According to Israeli military estimates, **up to 90% of the rockets were intercepted**, saving countless

² McGreal, Chris. “What are the roots of the Israel-Palestine conflict?” *The Guardian*. 2023.

lives and preventing far greater civilian casualties. The system demonstrated rapid detection, automated targeting, and precision interception, prioritizing rockets projected to hit populated areas while allowing those aimed at unpopulated zones to fall harmlessly. Its deployment highlighted a technological revolution in modern warfare: a mobile, adaptable, and highly effective shield capable of protecting urban populations in real time. The Iron Dome effectively altered the strategic balance, reducing Israel's vulnerability to asymmetrical rocket attacks and allowing the military to conduct targeted operations in Gaza with somewhat lower risk to civilians at home. Despite Israel's precision strikes and extensive precautions, at least 248 Palestinians, including many children, were killed in Gaza, while 13 Israelis died from rocket attacks. The crisis also triggered ethnic violence within Israel and a global surge in antisemitic incidents. (wars and operations 2021)³

The **Iron Dome** is one of the most technologically advanced military systems and serves as a primary defensive weapon for Israel in the Israel–Palestine conflicts. It was developed with **financial support from the United States**, which enhanced both its operational effectiveness and readiness. The Iron Dome is considered one of the most **innovative technologies in the defense sector** and has no equivalent worldwide, further strengthening Israel's defensive capabilities and international prestige.

The main issue of our work is not the exploration of historical depths, but rather the analysis of how much influence technological development and a correctly chosen strategy can have on the success of a state, the support of partners and a strong defense. An analysis of open sources is enough to establish that the Israeli-Palestinian war had a great impact on the international system and once again made states think about the importance of innovative and high-tech weapons in the field of defense, which simplify and make military operations more effective. After 2021, the support of the United States of America for Israel also increased further. Since 2024, the funding package has been further strengthened. (CONGRESS.GOV 2024)⁴ As for Palestine, this state began to modify its own strategy, since reducing costs and the effectiveness of the Iron Dome was vital, therefore, they created weapons that “cheated” the logic of the Iron Dome. In October 2023, Palestine achieved remarkable success in reducing the effectiveness of the air defense system (Barry 2023)⁵. In fact, the war has moved into a completely new dimension, where human resources alone are not enough and a smart and flexible approach is indispensable, which was understood in the international system, based on the example of Gaza.

The analysis highlights the strategic significance of the Iron Dome and clarifies why a seemingly “local” confrontation has escalated into a conflict of global relevance. While considerable attention has been given to the United States and its unwavering support for Israel, Iran's role must also be emphasized. Tehran actively supports Hamas by supplying military resources, financial assistance, and political backing, thereby positioning itself as a counterweight to U.S. influence in the region. In doing so, Iran seeks not only to preserve but also to expand its regional leverage.

3 2021. *wars and operations*. 14 06., 2025. Operation Guardian of the Walls.

4 2024. “CONGRESS.GOV.” <https://surl.li/pcmvinc>, Accessed 31.10.25

5 Barry, Ben. “IISS.” *The Hamas attack and Israeli military options*. 10 october, 2023. <https://surl.li/xptzuz>, Accessed 31.10.25

Conclusion

This involvement highlights a fundamental dynamic within the contemporary international system: even relatively small non-state actors, when equipped with advanced weaponry, digital communication tools, and guided by coherent strategic doctrines, can challenge and destabilize far more powerful adversaries. The asymmetric nature of modern conflict allows such actors to exploit technological and informational advantages to achieve strategic visibility and political impact disproportionate to their size or conventional capabilities. This phenomenon reflects a broader shift in the logic of warfare—from large-scale territorial confrontations to hybrid and decentralized conflicts in which influence, perception, and adaptability often determine outcomes more decisively than raw military power.

In this evolving landscape, Iran's engagement in the Israel–Palestine conflict represents a calculated effort to consolidate its regional influence and to project strength on the global stage. Through its support of proxy forces, development of missile technologies, and sophisticated information campaigns, Iran seeks to reinforce its position as a principal regional actor capable of shaping both military and political outcomes across the Middle East. Its involvement also reflects a deliberate strategy of strategic depth, aimed at extending its deterrence capabilities beyond its borders and counterbalancing Western and Israeli dominance. By positioning itself as both a defender of Palestinian resistance and a challenger to Western hegemony, Iran strengthens its ideological legitimacy and geopolitical leverage within a fragmented regional order.

Conversely, the United States continues to frame its role in the region as that of a stabilizing force and a guarantor of security for its allies. Beyond the scope of traditional alliance politics, Washington aspires to reaffirm its global image as the architect of balance and the principal custodian of regional peace. Its support for Israel's high-technology defense systems—particularly innovations such as the Iron Dome and emerging directed-energy interception platforms—underscores its commitment to maintaining Israel's qualitative military edge while simultaneously projecting U.S. technological superiority (kaleji 2024)⁶ This technological partnership not only enhances Israel's operational defense capacity but also serves as a symbolic reaffirmation of U.S. leadership in the global security and defense innovation sphere.

Within this broader geopolitical context, the divergence of strategic approaches among major powers—including the United States, Iran, Russia, and China—further elevates the Israel–Palestine conflict from a localized territorial dispute to a matter of global significance. These differing agendas—ranging from deterrence and defense modernization to ideological influence and proxy engagement—demonstrate that the conflict functions as a microcosm of global power competition. It encapsulates the ongoing transformation of international relations in which regional conflicts increasingly act as testing grounds for emerging technologies, doctrines, and alliances.

Ultimately, the Israel–Palestine conflict reveals that contemporary security is profoundly complex, interconnected, and dynamic. It is no longer defined solely by conventional military strength but by the interplay of technological innovation, strategic communication, and international partnerships. The conflict illustrates how modern warfare extends across physical, digital, and psy-

⁶ kaleji, vail. 2024. *The Main Axes of Iran's Foreign Policy Toward the Palestinian-Israeli Conflict*. 02 09. <https://surl.li/vzavew> Accessed 31.10.25

chological domains, creating an environment where local actions can have global repercussions.

The lessons drawn from this case study transcend regional boundaries and provide valuable insights for policymakers and strategists worldwide. In an era characterized by asymmetric threats, rapid technological advancement, and the interdependence of regional and global security, the ability to adapt, innovate, and collaborate has become indispensable. Effective security in the twenty-first century requires not only robust military capability but also diplomatic agility, economic resilience, and cross-border cooperation.

Thus the Israel-Palestine conflict underscores that achieving sustainable security in the modern world demands a holistic and forward-looking approach. It calls for constant adaptation to technological change, the cultivation of strategic foresight, and the strengthening of multilateral cooperation frameworks. Only through the integration of defense innovation, economic stability, and international partnership can states hope to navigate the shifting landscape of modern warfare and contribute to the formation of a more balanced, resilient, and peaceful global order.

Bibliography

- Krishnan, Armin. 2022. «Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict: A Comparison.» *strategic security*.
- McGreal, Chris. 2023. «What are the roots of the Israel-Palestine conflict?» *The Guardian*.
2021. *wars and operations*. 14 06. Operation Guardian of the Walls.
2024. «CONGRESS.GOV.» <https://surl.li/rzyqmb>, Accessed 31.10.25
- Barry, Ben. «IISS.» *The Hamas attack and Israeli military options* . 10 october, 2023. 2025. <https://surl.li/wrtovz>, Accessed 31.10.25
- kaleji, vail. 2024. *The Main Axes of Iran's Foreign Policy Toward the Palestinian-Israeli Conflict*. 02 09. <https://surl.li/cryief>, Accessed 31.10.25

ARTIFICIAL INTELLIGENCE AND THE TRANSFORMATION OF STRATEGIC ADVANTAGE IN DEFENSE FORCES

Zurab Nebieridze

The Junker of a Bachelor's Degree Program (Defense and security)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Imeda Arveladze

The Junker of a Bachelor's Degree Program (Defense and security)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Sophiko Metreveli

Assistant Professor of Bachelor's Program in Defense and security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This paper examines the transformative impact of Artificial Intelligence (AI) on the evolution of modern defense forces and confirms that AI represents a defining strategic advantage in the context of global security. Drawing upon the theoretical framework of the Revolution in Military Affairs and employing a comprehensive desk study approach, the research analyzes AI's potential across three primary dimensions of military power application: cognitive advantage, operational advantage, and organizational adaptation. The first dimension, cognitive advantage, focuses on AI's ability to accelerate the pace and precision of military decision-making through data-driven intelligence, real-time situational awareness, and predictive analytics. The second, operational advantage, explores AI's contribution to precision warfare, autonomous systems, and the optimization of logistics and battlefield coordination. The third dimension, organizational adaptation, considers how AI integration necessitates new military doctrines, training structures, and ethical command frameworks to ensure responsible and effective deployment. While AI offers unparalleled opportunities to enhance operational efficiency and reduce human casualties, this paper also critically evaluates the ethical, technical, and legal challenges emerging from its use. Ethical dilemmas revolve around accountability for autonomous lethal systems, while technical vulnerabilities include algorithmic manipulation, data bias, and susceptibility to cyber exploitation. Furthermore, the absence of comprehensive international legal frameworks exacerbates uncertainty regarding the use of AI in warfare, raising questions about compliance with humanitarian law and moral responsibility in conflict.

The study concludes that achieving long-term strategic advantage through AI requires not only continuous technological innovation and investment, but also the establishment of robust governance structures, the enforcement of ethical standards, and the preservation of the human element in decision-making. A truly effective AI-based defense system must therefore rest on a careful balance between innovation, accountability, and moral restraint—ensuring that technological progress strengthens global security without undermining humanitarian principles.

Keywords: Artificial Intelligence (AI); Strategic Advantage; Revolution in Military Affairs (RMA); Autonomous Systems; Cognitive Warfare; Ethical Challenges; Defense Innovation; Security Policy.

Introduction

Technological Transformation and Strategic Advantage

The modern global security landscape is characterized by increasing geopolitical and technological competition, where the foundation of national security is progressively shifting toward the informational and digital domains. In this context, Artificial Intelligence represents not just another technological innovation but a potentially revolutionary force in military power balance.¹ The integration of AI into the defense strategies of advanced countries has already become a key priority, aiming to achieve unprecedented increases in the speed, precision, and scale of operations from intelligence and surveillance to autonomous systems and cybersecurity. Artificial Intelligence is considered a transformative factor capable of creating and ensuring future strategic advantage for defense forces.

The main purpose of this article is to systematically analyze the role and potential of Artificial Intelligence in the defense sector, with a particular focus on its ability to create and reinforce the strategic advantage of military forces. Specifically, the study examines how AI affects decision-making optimization, operational effectiveness, and the development of new military capabilities, while also addressing the key ethical, legal, and security challenges associated with this technology. Finally, the article develops strategic recommendations on how to achieve the most effective integration of Artificial Intelligence into defense systems under conditions of global competition. The article relies on qualitative research, specifically the desk research methodology. This method involves detailed collection, analysis, and synthesis of existing publicly available information, scientific publications, analytical reports, defense strategies, government documents, and studies of international organizations. The research focuses on the AI strategies developed by advanced military powers (USA, China, Russia, UK, and others) and the specific applications that are already implemented or planned. Critical analysis of the collected material will contribute to identifying current trends, challenges, and future trajectories of strategic advantage through Artificial Intelligence.

Main Part

The Role of Artificial Intelligence in Transforming Defense Systems: Conceptual Framework and Current Trends

Contemporary military thought and operational planning are undergoing radical transformation, primarily driven by the development of Artificial Intelligence. AI is no longer merely a matter of science fiction but has become a critical dual-use technology capable of revolutionizing all aspects of military power application.² Conceptually, the most relevant capabilities for defense systems are narrow (weak) AI, particularly machine learning algorithms, which process data sets to learn pattern recognition, prediction, and decision support. The main strategic value of these cognitive capabilities lies in AI's ability to increase operational tempo (OODA Loop: Observe-Orient-Decide-Act), which represents a decisive advantage in conflict environments.³

The integration of AI into defense forces is multi-layered and extends beyond direct combat op-

1 Elsa B. Kania, "Artificial Intelligence and the Future of Warfare," Center for New American Security, March 2018, 5.

2 Gregory C. Allen, "The Dual-Use Dilemma: AI and the Future of Arms Control," Brookings Institution, February 19, 2020.

3 John Boyd, *A Discourse on Winning and Losing* (Maxwell Air Force Base, AL: Air University Press, 1996), 5.

erations. Its spectrum of application includes intelligence, surveillance, and reconnaissance (ISR), where AI automatically processes satellite, drone, and sensor data, identifies targets or anomalies, and provides commanders with critically important situational awareness in a timeframe unattainable by human analysts. In command and control (C2) systems, AI functions as a decision-support tool, offering operational scenarios and optimal courses of action while accounting for risks, thus reducing human cognitive load and the probability of errors.

Moreover, AI is the backbone of autonomous systems: unmanned aerial vehicles (UAVs), land robotic systems, and maritime drones reduce human risk in dangerous missions and enable 24/7 operations. At the same time, AI plays a significant role in cybersecurity and military logistics with automatic responses to cyber threats and predictive modeling of supply chains.

Recognition of AI's strategic potential has intensified global competition, with leading geopolitical actors seeking decisive advantage in this technology. The United States invests in the ethical and responsible use of AI, aiming to integrate it into the JADC2 (Joint All-Domain Command and Control) concept, which ultimately seeks information superiority across all domains (land, sea, air, space, cyber). On the other hand, China's national strategy openly aims for global AI leadership by 2030 through military-civil fusion, ensuring rapid integration of the commercial sector into the People's Liberation Army, particularly in autonomous combat systems.⁴ Similar strategic steps are observed among other major actors, including Russia and advanced NATO member states. From these global trends, it is clear that AI is not simply a "nice-to-have" technology but a critical factor whose possession and effective integration will determine the future strategic advantage of defense forces and the quality of national security.

Conceptualizing Strategic Advantage in the Age of Artificial Intelligence - The Theory of the Revolution in Military Affairs (RMA)

Understanding the role of Artificial Intelligence (AI) in the defense sector requires a theoretical framework that explains how technological innovation fundamentally transforms the nature and conduct of warfare. One of the most important conceptual approaches in this regard is the theory of the Revolution in Military Affairs (RMA), which explains how technological breakthroughs, when combined with appropriate organizational, doctrinal, and strategic changes, lead to a qualitative transformation in the nature of war and ensure decisive superiority for those who successfully adapt to it.⁵ Historically, such revolutions have occurred repeatedly—the invention of gunpowder, mechanization, nuclear weapons, and information technology each radically changed the tools, methods, and philosophy of warfare. In this continuum, Artificial Intelligence represents a new, cognitive dimension of transformation, where the main focus shifts from physical to informational and analytical dominance.⁶

In the context of the RMA theory, the introduction of AI can be interpreted as the beginning of a new phase of military evolution, characterized by the merging of information systems, autonomous platforms, and human cognitive processes into an integrated decision making network. The

4 Elsa B. Kania, "China's Military-Civil Fusion Strategy: A Framework for Innovation," Center for New American Security, January 2019, 10.

5 Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest* 37 (Fall 1994): 30.

6 P.W. Singer, *Ghost Fleet: A Novel of the Next World War* (Boston: Houghton Mifflin Harcourt, 2015), 187

main indicator of strategic advantage is no longer the quantity of troops or weapons, but rather the speed, precision, and adaptability of actions achieved through intelligent systems. In this sense, AI transforms the essence of military power, turning information and algorithmic capability into the primary resource of strength.

AI's influence on strategic advantage can be analyzed in three interrelated dimensions: cognitive, operational, and organizational. The cognitive dimension implies that AI accelerates the decision-making process (OODA loop - Observe, Orient, Decide, Act) by enabling the rapid analysis of large volumes of data and the anticipation of enemy actions. The operational dimension refers to the use of AI in precision and autonomous systems, which increase the accuracy, efficiency, and sustainability of military operations. The organizational dimension covers the institutional and cultural adaptation necessary for the integration of AI - modernization of command systems, training of personnel, and creation of new structures oriented toward human-machine collaboration.

According to the RMA theory, technological superiority alone does not automatically guarantee strategic advantage. Success depends on how effectively a state or military organization aligns technological innovation with doctrinal and structural reforms. In this sense, Artificial Intelligence represents both an opportunity and a challenge: it creates new possibilities for achieving dominance, but at the same time, requires rethinking of traditional approaches to planning, command, and control. AI's transformative nature thus leads not only to the modernization of warfare but also to a deeper conceptual shift - the formation of a "cognitive revolution in military affairs," where informational superiority and the ability to make decisions faster and more accurately than the adversary become the defining characteristics of future strategic advantage.

Ethical and Legal Challenges of Artificial Intelligence in Defense Systems

Although Artificial Intelligence (AI) has the potential to significantly enhance the operational effectiveness and strategic capabilities of defense systems, its rapid integration into the military domain also creates a number of complex ethical, legal, and technical challenges. The discussion surrounding the military use of AI increasingly focuses on the question of responsibility, transparency, and control - who makes the final decision when autonomous systems operate independently, and who bears accountability if such systems cause unintended harm.

One of the central ethical dilemmas is associated with autonomous lethal weapons, which can identify, track, and destroy targets without direct human involvement.⁷ The delegation of life and death decisions to machines challenges the fundamental principles of humanitarian law and moral responsibility. The key concern is that the use of AI in lethal operations may erode human judgment and ethical oversight in warfare, leading to actions that contradict the principles of distinction, proportionality, and necessity established by international humanitarian law.

Another critical challenge concerns algorithmic bias and data manipulation. Since AI systems rely on large datasets for training and decision-making, the quality, neutrality, and representativeness of these datasets directly affect their reliability. If the data contain bias or are intentionally manipulated, AI systems may produce distorted or discriminatory outcomes - misidentifying tar-

⁷ U.S. Department of Defense, Summary of the 2022 National Defense Strategy, Nuclear Posture Review, and Missile Defense Review (Washington, D.C.: DoD, 2022), 15.

gets, prioritizing inaccurate information, or making faulty strategic assessments. This not only undermines operational effectiveness but also poses serious legal and reputational risks at the international level.

AI's integration also exposes defense systems to technical vulnerabilities. Adversaries can manipulate or deceive algorithms through cyberattacks, data poisoning, or adversarial inputs, thereby compromising the reliability of autonomous systems and decision-support mechanisms. In a highly digitized battlespace, where data integrity is crucial, even minor manipulation can lead to catastrophic outcomes. Therefore, cybersecurity and system resilience have become inseparable components of AI ethics and governance.⁸

Equally problematic is the absence of a comprehensive international regulatory framework governing the military use of AI. Although the United Nations and various international organizations have initiated discussions regarding lethal autonomous weapons, there is still no binding legal document that defines the limits and standards for AI applications in warfare. The lack of such norms increases the risk of an uncontrolled arms race and the potential misuse of AI technologies by both state and non-state actors.⁹

In this context, the main ethical and legal imperative is to ensure meaningful human control over AI systems. Human oversight must remain central at all stages from design and programming to deployment and operational decision-making. Establishing clear accountability mechanisms, transparent algorithms, and internationally recognized ethical standards is essential for balancing innovation with moral and legal responsibility¹⁰. Only under these conditions can AI serve as a tool for enhancing security rather than creating new threats.

Long-Term Strategies and Recommendations

The development of Artificial Intelligence and its integration into the defense sector is no longer a distant future prospect it is now a reality that is rapidly changing the forms of warfare and the contours of security. While the previous chapter discussed critical ethical, technical, and legal vulnerabilities associated with AI, overcoming these challenges requires the formulation of long-term strategies that provide a country's defense system not only with technological advantage, as defined by the RMA theory, but also with stability and resilience.

A defense policy based on Artificial Intelligence should be grounded in a clear vision and specific objectives for risk reduction and efficient resource utilization. First and foremost, special attention must be paid to ethical and legal frameworks, as highlighted in Chapter III, to ensure that the use of technology does not exceed human control or violate international norms. AI must not become an arbitrary force; it should remain a human-directed instrument, where the "chain of responsibility" is clearly defined.¹¹

⁸ United Nations Office for Disarmament Affairs, "Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)," accessed October 23, 2025, <https://www.un.org/disarmament/group-of-governmental-experts-on-laws/>.

⁹ Mark J. C. W. Roffey, "Artificial Intelligence, Bias, and the Future of Conflict," *Journal of Military Ethics* 19, no. 1 (2020): 22–24.

¹⁰ Nicholas D. Evans and Gregory C. Allen, *Artificial Intelligence and National Security: A Primer* (Washington, D.C.: Atlantic Council, 2020), 45.

¹¹ RAND Corporation, *Military Applications of Artificial Intelligence: Ethical and Governance Considerations* (Santa Monica, CA: RAND, 2021), 60.

For long-term success, a clear governance system must be established. The state should create a dedicated body or commission to oversee the implementation of AI in the defense sector. This body must be able to ensure technological refinement, data security, cybersecurity (identified as a vulnerability in the previous chapter), proper budget allocation, and the protection of national interests. The strategy should include a multi-year financial and technological roadmap to prevent ad hoc, unsustainable initiatives.

The human factor remains a central value and the ultimate source of strategic advantage. Any technology is only as strong as the people who use it. Therefore, substantial investment in education and research is required. Collaboration with universities and research centers will allow a country to develop its own innovative capabilities and avoid over-reliance on imported technologies. Continuous retraining of military and civilian personnel is essential for working with AI systems, accurately assessing their capabilities, and, most importantly, intervening manually in critical moments.¹²

Any AI system must be equipped with fail-safe mechanisms to ensure immediate human control in times of crisis.¹³ Finally, international cooperation is crucial for achieving strategic interoperability. A country's defense system must be compatible with partners, particularly NATO and regional allies. This will create opportunities for joint AI-based operations, knowledge sharing, and harmonization of ethical standards, ultimately ensuring higher levels of coordination, security, and collective strategic advantage.

In conclusion, the use of AI in defense must be based on three main principles: prudent governance, national innovation, and decisive human involvement at all stages. Only such a balance can enable the creation of a defense system that not only responds to contemporary challenges but also ensures the country's security and strategic advantage in the long term.

Conclusion

Within the framework of this article, the transformative role of Artificial Intelligence (AI) in defense systems has been examined, and the thesis has been confirmed that AI represents the future strategic advantage of defense forces. The analysis, based on desk research and the theory of the Revolution in Military Affairs (RMA), highlighted that AI creates advantages in three main dimensions: cognitive (increasing the tempo of decision-making), operational (precision and multi-domain operations), and organizational (doctrinal adaptation).

However, like any revolutionary technology, AI-based advantage is not guaranteed. The article critically analyzed the main challenges that threaten this advantage. These include ethical dilemmas (responsibility for autonomous lethal systems), technical vulnerabilities (data bias and adversarial manipulation), and regulatory gaps in international law. These risks clearly demonstrate that AI is a "double-edged sword" if used improperly or without regulation, it can become a source not of stability but of global chaos.

Achieving and maintaining strategic advantage, therefore, requires not only technological investment but, above all, prudent governance. As the recommendations developed in Chapter IV

12 North Atlantic Treaty Organization (NATO), *The NATO AI Strategy* (Brussels: NATO Public Diplomacy Division, 2021), 12.

13 Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton & Company, 2018), 160.

indicate, countries must focus on establishing clear ethical frameworks, strengthening the human factor in AI systems (including fail-safe mechanisms), and ensuring international interoperability with allies. Ultimately, AI represents the newest and most important measure in global military competition. Success will be achieved by the state that can not only create the most advanced algorithms but also integrate them into a doctrinal and ethical framework that ensures responsible use of the technology. Establishing this harmonious balance will determine which defense force attains long-term strategic advantage in the 21st century.

Bibliography

- Allen, Gregory C. "The Dual-Use Dilemma: AI and the Future of Arms Control." Brookings Institution, February 19, 2020.
- Boyd, John. *A Discourse on Winning and Losing*. Maxwell Air Force Base, AL: Air University Press, 1996.
- Evans, Nicholas D., and Gregory C. Allen. *Artificial Intelligence and National Security: A Primer*. Washington, D.C.: Atlantic Council, 2020.
- Kania, Elsa B. "Artificial Intelligence and the Future of Warfare." Center for New American Security, March 2018.
- "China's Military-Civil Fusion Strategy: A Framework for Innovation." Center for New American Security, January 2019.
- Krepinevich, Andrew F. "Cavalry to Computer: The Pattern of Military Revolutions." *The National Interest* 37 (Fall 1994).
- North Atlantic Treaty Organization (NATO). *The NATO AI Strategy*. Brussels: NATO Public Diplomacy Division, 2021.
- RAND Corporation. *Military Applications of Artificial Intelligence: Ethical and Governance Considerations*. Santa Monica, CA: RAND, 2021.
- Roffey, Mark J. C. W. "Artificial Intelligence, Bias, and the Future of Conflict." *Journal of Military Ethics* 19, no. 1 (2020).
- Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company, 2018.
- Singer, P.W. *Ghost Fleet: A Novel of the Next World War*. Boston: Houghton Mifflin Harcourt, 2015.
- United Nations Office for Disarmament Affairs. "Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS)." Accessed October 23, 2025. <https://www.un.org/disarmament/group-of-governmental-experts-on-laws/>.
- U.S. Department of Defense. *Summary of the 2022 National Defense Strategy, Nuclear Posture Review, and Missile Defense Review*. Washington, D.C.: DoD, 2022.

INTERNATIONAL PARTNERSHIPS AND DEFENSE INNOVATIONS: EMERGING MODELS OF COLLECTIVE SECURITY

Captain Khatia Gogaladze

The Learner of a Master's Degree Program (Security Studies) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Professor Shadiman Bitsadze

Associate Professor of Master's Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Doctor of History

ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The contemporary global security system stands at a critical crossroads, as traditional military alliances and security mechanisms increasingly fail to respond effectively to growing and multidimensional threats. The deepening interdependence of states, the accelerating pace of technological progress, and the proliferation of hybrid threats have revealed the need to renew models of collective security. This paper aims to analyze the interconnection between international partnerships and defense innovations — exploring how technological advances, particularly in artificial intelligence, cybersecurity, and integrated defense systems, are transforming the traditional paradigm of collective security. The research employs a comparative analysis of Western and regional security models, including the experiences of NATO, the European Union, and the Partnership for Peace program. The study demonstrates that modern defense partnerships are increasingly based not only on the sharing of military resources but also on the joint development of knowledge, data, and technologies. This tendency gives rise to “innovative alliances,” where the combined efforts of state, academic, and private sectors converge to achieve shared security goals. The author concludes that the synthesis of international cooperation and innovative approaches constitutes the formation of a new model of collective security—one that requires flexible political mechanisms, a high level of mutual trust, and a deep understanding of technological integration. For Georgia, such an approach is particularly significant, as it strengthens the country's capacity for integration with international partners and participation in an innovative defense ecosystem.

Keywords: international partnerships; defense innovation; collective security; technological integration; hybrid threats; artificial intelligence; Georgia

Introduction

The contemporary global security system stands at a complex and transitional stage, marked by a profound redistribution of geopolitical power, the accelerated advancement of new technologies, and the intensification of non-traditional and hybrid threats. The end of the Cold War heralded a period of relative optimism, with many believing that liberal institutions and collective defense arrangements could guarantee long-term stability. However, by the second decade of the twenty-first century, it had become increasingly evident that the institutional and collective defense models inherited from the previous era were ill-suited to the new security realities shaped by cyber warfare, disinformation campaigns, technological asymmetries, and rapidly evolving geopolitical rivalries. Within this changing context arises the pressing necessity to formulate a renewed security concept that unites political–strategic partnership with technological innovation, reflecting the intertwined nature of power, knowledge, and resilience in modern international relations.¹

The relevance of this topic is underscored by the transformation of defense from a narrowly military enterprise into a multidimensional process encompassing political, technological, and informational domains. In the new security environment, military potential alone no longer constitutes a sufficient guarantee of sovereignty or stability. Instead, the ability to secure and analyze information, ensure the resilience of critical infrastructure, and integrate emerging technologies—particularly artificial intelligence, big data analytics, and advanced cybersecurity frameworks—has become central to national and collective defense strategies. The rapid evolution of military technologies and the emergence of the “smart defense” paradigm demonstrate that modern security depends on adaptive, cooperative, and innovation-driven frameworks. Within this process, institutions such as the North Atlantic Treaty Organization (NATO), the European Union (EU), and multilateral partnership programs have assumed leading roles by creating multi-layered platforms for knowledge exchange, technological experimentation, and capability development across member and partner states.²

The primary objective of this research is to analyze how international partnership and defense innovation interact and jointly contribute to shaping new models of collective security. The study explores key dimensions of this relationship, including military technological integration, the standardization of information security protocols, the formation of innovative alliances, and the strategic role of small states in leveraging innovation to enhance their security standing. These dynamics reveal how collective defense is evolving beyond conventional military cooperation to encompass shared technological ecosystems, integrated decision-making frameworks, and new modes of cross-sector collaboration.

The theoretical significance of the research lies in its synthesis of traditional approaches within security studies—particularly realism and liberal institutionalism—with contemporary perspectives on technology and innovation as instruments of power. It situates technological transformation within the broader discourse of international relations, demonstrating that innovation is not merely a technical process but a structural driver of geopolitical change. At the same time, the study possesses practical value, contributing to the identification of Georgia’s strategic priorities in

1 John J. Mearsheimer, *The Tragedy of Great Power Politics*. New York: W.W. Norton, 2001.

2 NATO. “Smart Defence.” *NATO Official Website*, 2020. https://www.nato.int/cps/en/natolive/topics_84268.htm

advancing international cooperation, developing indigenous technological capacity, and fostering defense innovation. The central hypothesis of this work posits that the synthesis of international partnership and defense innovation generates a more flexible, adaptive, and resilient model of collective security—one that transcends the limitations of traditional military alliances and reflects the realities of twenty-first-century conflict and cooperation.

Main Part

Theoretical Foundations of Collective Security and Their Transformation under Conditions of Innovative Partnership

The concept of collective security emerged as one of the foundational principles of international relations in the first half of the twentieth century, when the catastrophic experiences of the two world wars revealed that unilateral or isolated defense efforts were inadequate for maintaining global peace and stability. The devastation of these conflicts underscored a fundamental truth: no state, regardless of its power, could ensure its own security in isolation. Thus, the essence of the collective security concept rests upon the idea that aggression against one state constitutes a threat to all, requiring a unified and coordinated response. This principle—anchored in the interdependence of states and the shared responsibility for maintaining peace—was institutionalized through the establishment of the League of Nations, and later, the United Nations Charter, whose Article 51 explicitly enshrines the right of collective defense. Subsequently, the North Atlantic Treaty Organization (NATO) gave practical expression to this principle by creating a formalized structure for collective military action and deterrence.³

Over time, however, it became evident that the traditional model of collective security, founded primarily on military commitments and legal frameworks, could no longer adequately address the multifaceted and evolving threats of the modern world. The binary notion of peace and war has blurred into a continuum of hybrid challenges that include cyberattacks, disinformation campaigns, and economic coercion. From the standpoint of Realist theory, state behavior continues to be guided by national interest and the pursuit of relative power, making cooperation inherently fragile and contingent. Realists argue that collective security arrangements often mask underlying power asymmetries and are sustained only as long as the strategic interests of major powers align. In contrast, Liberal Institutionalism posits that enduring peace can be achieved through institutionalized cooperation, transparency, and interdependence. By establishing predictable norms and fostering mutual trust, international institutions can transform an anarchic system into a more stable and rule-based order.

From this theoretical convergence, it becomes clear that collective security has evolved beyond the confines of military alliances into a broader and more intricate web of political, economic, and technological interconnections. In the contemporary era, innovative partnerships have emerged as the driving force behind this transformation. These partnerships expand the traditional understanding of collective security by incorporating new domains of cooperation—technological development, data sharing, cyber defense, and the co-creation of dual-use capabilities that serve

3 United Nations. *Charter of the United Nations*. 1945. <https://www.un.org/en/about-us/un-charter/full-text>

both military and civilian purposes. Such forms of collaboration embody a hybrid logic: they blend the Realist emphasis on self-preservation and power projection with the Liberal focus on institutional trust and shared norms. This synthesis represents a fundamental evolution in the nature of collective security, where the quest for power increasingly depends on technological superiority and collaborative innovation rather than purely on armaments or territorial control.⁴

In the modern strategic landscape, innovative cooperation has acquired exceptional significance. It is no longer limited to the exchange of weaponry or resources, but now encompasses the joint development of knowledge, information, and technology across national and institutional boundaries. In an era of globalization, a state's defensive capability increasingly hinges on its technological adaptability—its capacity to integrate artificial intelligence (AI), cybersecurity infrastructures, data analytics, and digital command systems into coherent and resilient security networks. This evolution is reshaping how power and deterrence are conceptualized, shifting focus from mass mobilization and armament toward speed, precision, and informational dominance.

It is precisely in this direction that the security policies of NATO and the European Union have evolved in recent years. Both institutions have embraced innovation as a central pillar of strategic resilience, creating specialized mechanisms to integrate emerging technologies into defense cooperation. The NATO Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund exemplify this shift by facilitating collaboration between the public and private sectors, start-ups, and research institutions to produce next-generation defense solutions. Through these initiatives, collective security has been redefined as an integrated networked system, where technological synergy, strategic trust, and cross-sector partnerships hold equal importance alongside military capability.⁵

In such an environment, security increasingly resembles a living, adaptive ecosystem—one that evolves through information exchange, innovation, and cooperation. This dynamic model of collective security demands flexibility, speed, and coordination among diverse actors, transcending the limitations of rigid alliance structures. For Georgia, this transformation carries profound significance. The country's national security depends heavily on collaboration with international partners, while strengthening technological integration enhances its capacity to participate actively in the evolving collective security architecture. By aligning with NATO's and the EU's innovation-driven frameworks, Georgia not only enhances its defense capabilities but also contributes to the creation of a more resilient and interconnected regional security system.

Defense Innovation as a Catalyst for the Formation of Collective Security

In the contemporary international environment, technological innovation has transformed the very nature of defense and security, endowing it with a new strategic and multidimensional meaning. Whereas in earlier historical periods the foundation of security systems rested primarily upon military strength, physical resources, and the maintenance of geopolitical equilibrium, the decisive factor in today's global order increasingly lies in the potential of knowledge, information, and adaptive innovation. Defense innovation is no longer confined to the design of new weapons

4 Robert O. Keohane, and Joseph S. Nye. *Power and Interdependence*. Boston: Little, Brown, 1977.

5 NATO. "Defence Innovation Accelerator for the North Atlantic (DIANA)." *NATO Official Website*, 2023a. https://www.nato.int/cps/en/natohq/topics_185000.htm.

or military hardware; rather, it encompasses a complex strategic process that integrates data analytics, artificial intelligence (AI), cybersecurity infrastructures, autonomous systems, and digital command and control networks. These elements together constitute the technological backbone of the twenty-first-century collective security system—one grounded in interoperability, rapid information sharing, and cross-sector collaboration.

Innovation in defense must therefore be understood as both a technological and a political phenomenon. It has evolved far beyond the traditional domain of military engineering to become a comprehensive process that defines the sustainability, adaptability, and credibility of modern alliances. The experiences of NATO and the European Union illustrate this transformation vividly. Both organizations have shifted from a focus on the accumulation of military assets to a broader vision centered on innovation, resilience, and the integration of civilian and military technologies. The development of dual-use technologies—capable of serving both defense and civilian purposes—has become a central pillar of this evolution, highlighting the extent to which defense innovation underpins national competitiveness, alliance solidarity, and strategic autonomy.

Initiatives such as the NATO Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund epitomize this paradigm shift. These frameworks bring together public and private sector stakeholders, research institutions, and start-ups to identify, test, and deploy cutting-edge technologies relevant to collective defense. Their focus areas—ranging from quantum computing and space technologies to AI-driven decision support and energy resilience—illustrate the multidimensional nature of modern defense innovation. By fostering close collaboration between governments, academia, and industry, these initiatives enhance the agility and responsiveness of the Alliance, while also reducing overreliance on a limited number of powerful states. In this way, innovation strengthens collective defense through two interrelated mechanisms: it increases operational efficiency and strategic diversification, enabling smaller and medium-sized allies to contribute meaningfully to joint security architectures.

Equally significant is the democratizing effect of defense innovation on the global security model. In previous centuries, the monopoly of military technology was held by a small number of great powers that shaped the international balance through superior industrial and scientific capacity. Today, however, the diffusion of technological expertise and the accessibility of digital tools allow smaller and medium-sized states to emerge as proactive contributors to international security. This democratization of capability empowers states such as Georgia, which, despite limited financial resources, possess growing intellectual and technological potential. Through targeted investment in cyber defense, unmanned systems, and information management, these states can elevate their strategic relevance and participate more actively in multilateral defense frameworks.⁶

Beyond its military and strategic dimensions, defense innovation exerts profound influence on the political, ethical, and social spheres. The integration of AI and autonomous systems into warfare raises urgent questions about accountability, proportionality, and the ethical use of force. How should responsibility be assigned in decisions made by automated defense systems? What are the moral and legal limits of algorithmic warfare? And how can civilian oversight be maintained in an age when technology blurs the boundary between combatant and non-combatant roles? These

⁶ Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press, 2009.

issues highlight that innovation in defense cannot be viewed solely through a technical lens—it is deeply interwoven with governance, law, and the moral foundations of international security.

Moreover, technological innovation in defense fosters new forms of trust and interdependence among international partners. The creation of shared technological platforms—such as unified cybersecurity protocols, secure data exchange standards, and multinational research programs—promotes transparency and accountability, thereby reducing the likelihood of misperception or rivalry within alliances. In such an environment, innovation becomes both a mechanism of deterrence and a medium of cooperation: it reinforces collective defense by aligning technological standards and institutional practices, creating a security ecosystem characterized by openness, adaptability, and shared responsibility.

Ultimately, defense innovation functions as the central catalyst in the transformation of collective security. Its importance transcends the confines of traditional military frameworks, extending into the realm of diplomacy, governance, and strategic development. Technology has become not merely an instrument of warfare but a driver of political cohesion and a guarantor of long-term stability. Through innovative cooperation, states can construct a flexible, network-based, and transparent security architecture—one capable of addressing the multifaceted threats of the present while anticipating and mitigating the challenges of the future.

Georgia's Perspective and Opportunities in Innovative Partnership

Georgia occupies a strategically vital position within the broader security architecture of the Black Sea and South Caucasus regions—zones historically marked by geopolitical contestation, overlapping spheres of influence, and complex security dynamics. This location has made the country both a bridge and a buffer between East and West, and thus a focal point for regional and global strategic interests. Against this backdrop, Georgia's security policy has long been guided by the imperative of partnership and cooperation with international actors, particularly as a means to compensate for its limited material resources and to manage the multifaceted threats emanating from its volatile neighborhood. Over the past decade, this partnership-based orientation has evolved into a more sophisticated and forward-looking model that increasingly emphasizes innovation, technological adaptation, and institutional modernization as key components of national and collective defense.

A discernible trend in Georgia's recent defense and security policy has been the gradual embrace of technological innovation and smart defense principles—particularly in the domains of cybersecurity, information protection, and digital transformation. The National Defense Strategy, aligned with NATO's strategic vision, outlines the main pillars of this approach. According to the 2025 Strategy, Georgia's priorities include strengthening national defense capabilities, deepening interoperability with partner states, and embedding innovation within the broader defense ecosystem. This strategy explicitly recognizes that military modernization cannot be confined to traditional infrastructure development or armament acquisition; rather, it must include systemic integration between the military, civil, academic, and private sectors. Such a whole-of-society model reflects Georgia's recognition that resilience in the twenty-first century is built as much on

technological competence and knowledge exchange as on conventional military power.⁷

Cooperation with NATO remains the cornerstone of Georgia's defense transformation and a critical mechanism for embedding innovation within national policy. The Defence Capacity Building Initiative (DCBI) and the Substantial NATO–Georgia Package (SNGP) are two flagship frameworks through which Georgia engages with NATO's innovation-driven agenda. These programs encompass technological development, cybersecurity coordination, defense education, and management reform, creating tangible avenues for Georgia to align its practices with alliance standards. Beyond capacity building, these platforms foster joint research, simulation-based training, and the exchange of defense-related data, allowing Georgian institutions to integrate into transnational knowledge networks. Through this sustained collaboration, Georgia is not merely a recipient of strategic assistance—it has become an active participant in the co-creation of innovative defense solutions that mirror NATO's evolving collective security paradigm.⁸

Georgia's progress is particularly evident in the field of cybersecurity, where it has made notable advancements in policy and institutional development. The establishment of the National Cybersecurity Strategy and the creation of new mechanisms for public–private cooperation represent crucial steps in constructing a comprehensive cyber defense framework. By engaging technological start-ups, universities, and private-sector innovators, Georgia is cultivating a domestic defense innovation ecosystem that fosters synergy between policy, research, and entrepreneurship. This ecosystem is not only vital for enhancing national resilience but also serves as a driver of economic diversification and technological growth, as innovation in security domains often stimulates advancements in civilian industries. Such developments align Georgia with global trends in which security and technology are increasingly inseparable, and where investment in innovation strengthens both defense readiness and economic sustainability.

Equally significant is Georgia's continuing progress toward harmonization with European security standards. Through cooperation with the European Union, the country has begun to align its legislation and institutional structures with EU frameworks on crisis management, data protection, and defense sector reform. This process, supported by programs such as the European Peace Facility (EPF) and the Cybersecurity East Initiative, has enabled Georgia to improve interoperability with European partners and adopt best practices in governance and resilience. In this context, Georgia represents a model of international partnership for small states—demonstrating how countries with limited material capacity can leverage technological collaboration and institutional innovation to achieve disproportionate strategic relevance.⁹

Nevertheless, this trajectory is not without challenges. Georgia's innovative potential in the defense sector remains constrained by limited fiscal resources, a relatively modest technological-industrial base, and an underdeveloped research infrastructure. The domestic R&D environment, though improving, is still in its formative stages, posing obstacles to long-term investment in defense-related research, experimentation, and product development. To overcome these limitations, active engagement in international grant programs, joint research consortia, and cross-bor-

7 Ministry of Defence of Georgia. *National Defense Strategy 2025*. Tbilisi: Ministry of Defence of Georgia, 2021. https://mod.gov.ge/uploads/2021/pdf/National_Defence_Strategy_2025_ENG.pdf.

8 NATO. "Substantial NATO–Georgia Package." *NATO Official Website*, 2022. <https://surl.li/jtkcuj>

9 European Union. "CyberEast Initiative." *EU Neighbourhood Programme*, 2023.

der innovation projects becomes indispensable. Georgia's capacity to attract and effectively utilize such opportunities will determine not only the pace of its technological modernization but also its broader strategic position within the evolving ecosystem of collective security.

In summary, Georgia's perspective within innovative partnership can be conceptualized as resting upon three strategic pillars:

1. Institutional and strategic cooperation with NATO and the European Union, ensuring alignment with transatlantic security frameworks;
2. Technological modernization and integration of its defense system, strengthening cyber resilience, command infrastructure, and R&D capabilities; and
3. Human capital development, reflected in the emergence of a new generation of defense professionals equipped with digital skills, innovative thinking, and international experience.

If Georgia succeeds in synthesizing these three dimensions—innovation, partnership, and human potential—it can position itself as a regional exemplar of adaptive security transformation. Such progress would not only enhance its national defense posture but also enable Georgia to contribute meaningfully to the broader architecture of collective security—one increasingly defined by technological cooperation, shared knowledge, and strategic innovation.¹⁰

Conclusion

The model of collective security, long regarded as one of the foundational mechanisms of international relations, is undergoing a profound transformation shaped by the accelerating forces of technological innovation and the emergence of new forms of international partnership. The traditional logic of deterrence and power balancing—dominant throughout much of the twentieth century—has gradually evolved into a more dynamic and interconnected paradigm in which information, technology, and knowledge serve as the central currencies of security. In this new landscape, collective security is no longer confined to military cooperation or treaty-based commitments; rather, it is defined by the ability of states and alliances to adapt, innovate, and collaborate across domains that transcend the battlefield.

Today's global security challenges, ranging from cybersecurity vulnerabilities and information warfare to hybrid and asymmetric threats, demand not only the projection of military force but also the collaborative development of technological capabilities, the institutionalization of data-sharing mechanisms, and the cultivation of scientific and industrial partnerships. In this sense, innovation functions not merely as an instrument for achieving superiority but as a structural condition for maintaining resilience in an era of uncertainty. Defense innovation has thus become inseparable from the broader process of governance and diplomacy, reshaping the culture of security thinking by emphasizing flexibility, inclusivity, and the integration of civil and military expertise.

For Georgia, these transformations carry exceptional significance. Situated within a region marked by enduring geopolitical volatility, the country's security and defense policy—anchored in cooperation with Western institutions such as NATO and the European Union—must increasingly

¹⁰ NATO. "NATO Innovation Fund." *NATO Official Website*, 2023b.

evolve toward a model that fully integrates innovation into its strategic framework. This involves not only the enhancement of technological capacity and the modernization of national defense infrastructure but also the creation of a robust research and development environment capable of sustaining long-term progress. The strengthening of cybersecurity systems, the promotion of digital literacy within the defense sector, and the active engagement of private enterprises in security-oriented initiatives are indispensable steps in this evolution. Through such initiatives, Georgia can transform from a consumer of security into a co-creator of innovative solutions, contributing tangible value to the broader Euro-Atlantic security ecosystem.

The experience of Georgia also demonstrates that small and medium-sized states can play a meaningful role in shaping collective security when they invest in innovation and partnership simultaneously. By leveraging transnational cooperation and technology-driven collaboration, Georgia can enhance its strategic relevance and amplify its diplomatic voice within multilateral institutions. Participation in international innovation networks—whether through NATO’s Defence Innovation Accelerator (DIANA), the European Defence Fund, or other cooperative frameworks—provides both practical benefits and symbolic legitimacy, reinforcing Georgia’s image as a forward-leaning and responsible security partner.

Ultimately, international partnership and defense innovation can no longer be understood as separate or parallel pursuits. Together, they form a unified strategic architecture that defines the essence of collective security in the twenty-first century—an architecture characterized by interdependence, technological adaptation, and institutional trust. For Georgia, active engagement in this process represents not only a guarantee of national security but also a vital opportunity for socio-economic and intellectual development. By aligning its strategic ambitions with the global shift toward innovation-driven security, Georgia positions itself as a full-fledged participant in the emerging network of innovative security ecosystems—a model of cooperation grounded in knowledge, collaboration, and technological progress.

Bibliography

- European Union. “CyberEast Initiative.” *EU Neighbourhood Programme*, 2023. <https://surl.li/qrrnos>.
- Jervis, Robert. “Cooperation under the Security Dilemma.” *World Politics* 30, no. 2 (1978): 167–Keohane, Robert O., and Joseph S. Nye. *Power and Interdependence*. Boston: Little, Brown, 1977.
- Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W.W. Norton & Company, 2001.
- Ministry of Defence of Georgia. *National Defense Strategy 2025*. Tbilisi: Ministry of Defence of Georgia, 2021. <https://surl.li/tfkxna>
- NATO. “Defence Innovation Accelerator for the North Atlantic (DIANA).” *NATO Official Website*, 2023a. <https://surl.li/cxbxmi>
- NATO. “NATO Innovation Fund.” *NATO Official Website*, 2023b. <https://surl.li/hliurh>
- NATO. “Smart Defence.” *NATO Official Website*, 2020. <https://surl.li/cc/drrohx>
- NATO. “Substantial NATO–Georgia Package.” *NATO Official Website*, 2022. <https://surl.li/hftwem>
- Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press, 2009.
- United Nations. *Charter of the United Nations*. 1945. <https://surl.li/eupkpi>

GERMANY'S ZEITENWENDE: THE TRANSFORMATION OF NATIONAL DEFENSE AND THE RECONFIGURATION OF EUROPEAN SECURITY

Vakhtangi Danelia

The Junker of a Bachelor's Degree Program (Management)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Luka Ckhadadze

The Junker of a Bachelor's Degree Program (Management)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Givi Duchidze

Associate Professor of Bachelor's program in Management of
LEPL David Aghmashenebeli National Defence Academy of Georgia,
Doctor of Business Administration

Abstract

Germany is undergoing a historic transformation in its defense and security policy, marking a genuine *Zeitenwende*—a turning point that is reshaping both its national identity and Europe's geopolitical landscape. For decades, the Federal Republic had pursued a strategy of restraint, prioritizing economic engagement, multilateral diplomacy, and energy interdependence—particularly with Russia—over military investment and strategic autonomy. However, in the wake of Russia's full-scale invasion of Ukraine in February 2022, this model collapsed. Berlin has since embarked on a far-reaching policy realignment that redefines its role as a leading European and transatlantic security actor. At the heart of this transformation lies a decisive shift away from energy dependency on Russian gas and oil toward diversified energy partnerships and a pursuit of strategic autonomy. Germany has restructured its energy infrastructure, expanded liquefied natural gas (LNG) capacities, and deepened cooperation with trusted allies such as Norway, the Netherlands, and the United States. This shift represents not only an economic adaptation but also a geopolitical repositioning, aimed at reducing vulnerability to external coercion and enhancing resilience in the face of hybrid threats. Simultaneously, Germany has undertaken an unprecedented modernization of its armed forces. The establishment of the €100 billion *Sondervermögen* (special fund) for defense investment, the expansion of the *Bundeswehr*'s budget and personnel, and the decision to meet NATO's 2 percent defense spending target reflect a fundamental redefinition of national priorities. Concrete steps include large-scale procurement of modern weapon systems, digital communication technologies, and armored vehicles, as well as the deployment of a German tank brigade in Lithuania—the first permanent German military presence abroad since the Second World War. This initiative underscores Germany's renewed commitment to NATO's eastern flank and its determination to strengthen the Alliance's collective defense posture in response to the evolving security environment. Beyond the military domain, Germany's *Zeitenwende* extends to technological innovation and international cooperation. The government has accelerated partnerships in defense research, artificial intelligence, cybersecurity, and space capabilities, integrating German industry more deeply into the broader European defense ecosystem. Cooperation with the European Union, NATO, and transatlantic partners has intensified, with Berlin positioning itself as both a policy leader and technological contributor to Europe's strategic renewal. Through this multifaceted transformation—anchored in international partnerships, technological advancement, and

restored military readiness—Germany is redefining itself as a guarantor of European stability and a driving force in the evolution of transatlantic security. The *Zeitenwende* thus represents not only a change in defense policy but also a psychological and strategic awakening: a recognition that peace and prosperity in Europe require credible deterrence, political resolve, and unity of purpose.

Ultimately, Germany's transformation signals a broader reconfiguration of Europe's strategic architecture in an era of renewed great-power competition. As Berlin assumes greater responsibility for continental defense, its choices will shape the future of European security integration, the resilience of NATO, and the global balance of power. The trajectory of this new policy era will determine whether Germany can translate its economic strength into sustainable strategic leadership and serve as a stabilizing anchor for a more secure, autonomous, and united Europe.

Keywords: Germany; Bundeswehr; NATO; Eastern Flank; *Zeitenwende*; Energy Security; Strategic Autonomy; European Security; Defense Innovation; Transatlantic Relations; Geopolitical Transformation.

Introduction

The outbreak of Russia's full-scale invasion of Ukraine in 2022 marked a profound turning point in Europe's security architecture and a decisive moment in Germany's post-Cold War foreign and defense policy. For decades, Germany had been regarded as an economic powerhouse yet a reluctant military actor, prioritizing diplomacy, dialogue, and economic interdependence—particularly with Russia—over hard power and strategic deterrence. This approach, rooted in the belief that trade and cooperation could ensure lasting peace, was severely tested by Moscow's aggression. The war exposed the fragility of Germany's reliance on Russian energy and the limitations of a security model grounded primarily in soft power. It compelled Berlin to embrace a historic transformation—known as the *Zeitenwende*, or “epochal turning point”—that redefines the country's role in both European and global security.

Under this new doctrine, Germany has undertaken unprecedented investments in defense modernization, committing €100 billion to strengthen the Bundeswehr and pledging to meet NATO's 2 percent defense spending target. This financial commitment signifies a radical departure from Germany's traditionally cautious defense posture. Simultaneously, Berlin has accelerated efforts to diversify its energy supply, reduce dependence on Russian gas, and deepen partnerships across the European Union and the broader transatlantic community. The deployment of a German tank brigade in Lithuania stands as a powerful symbol of this shift, signaling not only a tangible military contribution but also a renewed sense of responsibility and solidarity toward NATO's eastern allies.

This transformation, however, is not merely a reaction to the war in Ukraine but rather the culmination of long-standing tensions and contradictions within Germany's foreign and security policy. Since the end of the Cold War, Berlin has pursued a careful balance between economic pragmatism and moral restraint, shaping its international engagement through diplomacy, economic integration, and normative influence rather than coercive power. This orientation was reinforced by the political evolution of post-reunification Germany—marked by a growing preference for multilateralism, liberal values, and an aversion to nationalism rooted in the collective trauma of the twentieth century. As a result, public opinion and political elites alike viewed military assertiveness with skepticism, emphasizing reconciliation and soft power as cornerstones of German identity.

Main Part

The war in Ukraine, however, forced Germany to confront the limits of this paradigm. The realities of large-scale warfare on the European continent underscored the necessity of credible military strength, exposing the strategic vulnerability of an overreliance on diplomacy and economic leverage. The *Zeitenwende*, therefore, represents far more than a defense policy reform—it signifies a psychological, strategic, and ideological awakening. It redefines how Germany perceives its national interests, its historical responsibilities, and its leadership role within the Western alliance.

In essence, the *Zeitenwende* embodies Germany's re-emergence as a central pillar of European security, bridging the gap between moral responsibility and strategic realism. It marks the country's transition from a passive guarantor of peace to an active architect of stability, capable

of shaping collective defense and contributing meaningfully to transatlantic resilience. In doing so, Germany not only reshapes its own identity but also reconfigures the geopolitical balance of Europe at a time of deepening uncertainty and renewed great-power competition.

Merkel's Policy Toward the Russian Federation and Her Response to Russian Aggression in Georgia and Ukraine

During her tenure as Chancellor from 2005 to 2021, Angela Merkel pursued a policy of pragmatic engagement with the Russian Federation, rooted in the long-standing German doctrine of *Wandel durch Handel*—"change through trade." This approach reflected the belief that robust economic and energy ties could promote mutual stability, foster dialogue, and integrate Russia more deeply into the European and international system. Merkel's policy built upon a broader post-Cold War consensus in the West, which viewed Russia—especially during the presidency of Boris Yeltsin and the early years of Vladimir Putin—as a potential partner rather than a geopolitical threat.

Following the collapse of the Soviet Union, the Russian Federation was widely perceived in Europe and the United States as a state in transition, seeking democratic reform and market liberalization. Western governments and institutions, including the European Union and NATO, sought to normalize relations through cooperation in economic, political, and counterterrorism fields. For Germany, this strategy held both economic and political appeal. Russia represented a vast market for trade and a dependable supplier of affordable energy resources—particularly natural gas and oil—vital for Germany's export-driven industrial base and its broader *Energiewende* (energy transition) policy aimed at phasing out nuclear and coal energy.

Through large-scale energy partnerships and infrastructure projects, such as the Nord Stream pipelines, Germany sought to secure stable energy imports while maintaining open diplomatic channels with Moscow. Russian gas was preferred for several reasons. Economically, it was cheaper and readily available, providing a competitive advantage to German industry. Strategically, it was aligned with Berlin's transition away from fossil fuels like coal and nuclear power. Politically, Merkel and many within Germany's political elite hoped that deepening interdependence would encourage gradual democratization in Russia and reduce the risk of conflict through shared economic interests. Merkel frequently defended these decisions as "reasonable for the time," arguing that constructive engagement remained preferable to confrontation.

However, this strategy ultimately underestimated Russia's enduring imperial ambitions and revisionist tendencies. Behind a façade of partnership and modernization, the Kremlin continued to pursue a neo-imperial agenda aimed at reasserting influence over former Soviet territories. The illusion of a cooperative, market-oriented Russia began to unravel dramatically following the Russo-Georgian War of August 2008.

In early August 2008, escalating tensions between Russian-backed separatists and Georgian armed forces in South Ossetia culminated in a five-day war. According to Georgian accounts, separatist militias—supported and provoked by Russian "peacekeepers"—launched mortar and small-arms attacks on Georgian villages and security forces, resulting in multiple casualties. In response, Georgia initiated a military operation to restore control over the Tskhinvali region. Russia, in turn, accused Georgia of committing "genocide" against Ossetians, using these fabricated

allegations as a pretext for full-scale invasion. Subsequent investigations, including reports by independent international bodies, revealed that Moscow's claims were part of a disinformation campaign designed to legitimize its aggression. Civilian casualties were significantly higher on the Georgian side, and no credible evidence supported the Russian narrative of deliberate attacks against civilians by Georgian forces.

The European Court of Human Rights (ECHR) later substantiated these findings. In its 2021 ruling in *Georgia v. Russia (II)*, the Court held Russia responsible for multiple violations of the European Convention on Human Rights during and after the 2008 war. The ECHR concluded that Russian forces and the local de facto authorities committed grave human rights violations, including:

- Unlawful killings and torture of civilians;
- Destruction of property and widespread looting;
- Forced displacement of thousands of ethnic Georgians;
- Failure to properly investigate these crimes.

The 2008 war served as an early warning of Russia's aggressive revisionism and exposed the limitations of Merkel's engagement-based foreign policy. Yet, while Merkel condemned the invasion and supported diplomatic sanctions, Germany refrained from adopting a fully confrontational stance. Her cautious approach sought to preserve channels of communication with Moscow while balancing Germany's economic and energy interests.

In retrospect, Merkel's policies toward Russia—though grounded in pragmatism and the post-Cold War ideal of integration—failed to anticipate the Kremlin's long-term strategic intent. The wars in Georgia (2008) and later Ukraine (2014, 2022) revealed the fundamental flaws of assuming that economic interdependence alone could moderate authoritarian behavior. Merkel's *Zeitenwende* successors now face the task of reshaping Germany's strategic posture—moving from dependency and appeasement toward resilience, deterrence, and strategic autonomy within a rapidly evolving European security order.¹

The **European Court of Human Rights (ECHR)** ruling confirmed that Russia bears **international legal responsibility** for the grave human rights violations committed in territories under its effective control, establishing a **significant precedent in international law**. Germany's response to Russia's invasion of Georgia in 2008, however, was marked by a mixture of **condemnation and restraint**. Chancellor **Angela Merkel** publicly criticized Moscow's actions as **disproportionate** and emphasized the need to respect **Georgia's territorial integrity**. Yet, Berlin deliberately avoided direct confrontation with the Kremlin. Heavily dependent on Russian gas and committed to preserving diplomatic engagement, Germany preferred **dialogue over punitive measures**. No substantial sanctions or coercive policies were introduced. This **cautious and subdued response** inadvertently emboldened Russia, reinforcing the perception that Western opposition would remain confined to rhetoric rather than decisive action.

Georgia was not the only state to suffer the consequences of this restrained policy. When the **Maidan Revolution** erupted in Ukraine in 2013–2014, leading to the ousting of the pro-Russian

¹ Samuel Bendett, "Unmanned and Autonomous Systems in the Black Sea: The Next Phase of Maritime Competition," *Center for Naval Analyses*, 2022.

president **Viktor Yanukovych**, the Kremlin moved swiftly to preserve its sphere of influence. Russian troops—operating without insignia and later known as the “**little green men**”—occupied **Crimea** and facilitated its **illegal annexation** in March 2014, remarkably without major armed confrontation. Concurrently, Moscow began **arming and supporting separatist forces** in the self-proclaimed **Donetsk and Luhansk People’s Republics (DNR and LNR)**, igniting a prolonged conflict in eastern Ukraine.

Under Merkel’s leadership, **Germany condemned Russia’s annexation of Crimea** as a violation of international law and supported **EU-led sanctions**. Nonetheless, Berlin continued to pursue a **dual-track policy**—combining criticism and containment with sustained economic cooperation. Despite the geopolitical crisis, Germany did not immediately reassess its dependence on Russian energy. In fact, the **Nord Stream 2 pipeline project**, deepening the very reliance that had limited Berlin’s strategic flexibility, was approved in **2015** under Merkel’s government. While Germany worked to strengthen **Ukraine’s partnership with the EU and NATO**, including initiatives to train and equip Ukrainian forces, these efforts remained **insufficient** to deter further Russian escalation.²

When **Russia launched its full-scale invasion of Ukraine in 2022**, Germany’s vulnerabilities became starkly apparent. Years of energy interdependence had given Moscow considerable leverage, allowing President **Vladimir Putin** to exploit Europe’s dependency as a geopolitical tool. The crisis exposed how **economic pragmatism had constrained political will**, limiting Germany’s and the EU’s ability to act decisively in the face of aggression.³

Thus Merkel’s Russia policy can be credited with maintaining dialogue, avoiding open confrontation, and ensuring energy stability during her tenure. She later defended her approach as a product of the **context and information available at the time**. However, the long-term consequences revealed the **structural weaknesses** of this strategy. The underlying assumption—that economic interdependence and engagement would moderate Russia’s behavior—proved fundamentally flawed. Dependence on Russian energy restricted Germany’s foreign policy options, delayed a firmer deterrent posture, and ultimately contributed to Europe’s strategic exposure when faced with renewed Russian aggression. The legacy of this policy underscores the limits of **pragmatic diplomacy without credible deterrence** in an era of resurgent geopolitical competition.⁴

Germany’s Transformation After Russia’s Full-Scale Invasion of Ukraine

On **February 24, 2022**, Russia launched a **full-scale invasion of Ukraine**, marking a watershed moment in twenty-first-century international relations and European security. As Russian tanks crossed the Ukrainian border, Europe and the wider world witnessed the beginning of the largest armed conflict on the continent since the Second World War. The invasion shattered long-held assumptions about peace and stability in Europe and triggered a **strategic awakening** across the West—most notably in **Germany**, which had for decades pursued a restrained defense pos-

2 Julian Wettengel „Germany, EU remain heavily dependent on imported fossil fuels“, 03 Apr 2024, <https://surl.li/vblcmm>, Accessed 03.11.25

3 “EU trade with Russia - latest developments“, 28 November 2025, <https://surl.li/svbugu>, Accessed 03.11.25

4 Samuel Bendett, “Unmanned and Autonomous Systems in the Black Sea: The Next Phase of Maritime Competition,” *Center for Naval Analyses*, 2022.

ture. The war in Ukraine compelled Germany to reassess its security paradigm, leading to a profound shift in both **defense and foreign policy**. Under the newly declared *Zeitenwende* (“turning point”), Germany and its Western allies rapidly expanded their military and humanitarian support for Ukraine. Initially limited to small arms and defensive equipment, assistance soon evolved into the supply of **anti-tank guided missiles (ATGMs)**, **artillery systems**, **infantry fighting vehicles (IFVs)**, **armored personnel carriers (APCs)**, and eventually **main battle tanks (MBTs)**. Germany also became a key training hub, hosting and training over **20,000 Ukrainian recruits** on its territory as part of broader NATO initiatives.⁵

Beyond the battlefield, the conflict catalyzed a **structural transformation of Germany’s defense sector**. The German parliament approved an unprecedented **€100 billion defense fund**, marking the largest rearmament initiative in the country’s postwar history. The Bundeswehr’s modernization program includes major procurement and capability upgrades across multiple domains:

- **Equipment:** €15.9 billion
- **Vehicles and accessories:** €20.8 billion
- **Combat vehicles:** €52.5 billion
- **Munitions:** €70.3 billion
- **Communications, field, and logistics materials:** €20.9 billion

The Bundeswehr has initiated a broad modernization effort encompassing both **personnel expansion** and **technological renewal**.⁶ Plans include replacing the **G36** assault rifle with the **Heckler & Koch HK416A8**, upgrading **night-vision and communications systems**, and enhancing **electronic warfare capabilities**. In **July 2024**, the German parliament approved a contract for **105 Leopard 2A8 main battle tanks**, with plans to purchase or modernize several hundred additional units—aiming to field approximately **1,000 MBTs within five years**. Germany is also investing heavily in **Puma and Lynx IFVs**, **Boxer APCs**, and other advanced platforms, while expanding its air and missile defense systems. Germany’s growing commitment to **collective defense** is symbolized by the creation of the **45th Panzer Brigade** in **Lithuania**, comprising approximately **4,500 personnel**. This marks the first **permanent German brigade-sized deployment abroad since World War II**. Once fully operational, the brigade will include main battle tanks and mechanized infantry units, integrating into NATO’s **Enhanced Forward Presence (EFP)** structure and reinforcing the Alliance’s eastern flank. Concurrently, the **Bundeswehr**, which currently numbers around **182,000 active personnel**, aims to expand to **260,000 by 2031**, reflecting Berlin’s long-term commitment to defense readiness.⁷

Germany’s *Zeitenwende* extends beyond the military sphere, encompassing a fundamental transformation of **energy policy**. Prior to the invasion, Russia supplied **48–55%** of Germany’s natural gas and **25–30%** of its crude oil, making it the country’s single largest energy provider. This dependence was mirrored across Europe, where Russian energy accounted for **40–58%** of gas imports in some member states. However, following the invasion, Germany and the EU initiated a **rapid decoupling from Russian energy**. By the end of **2022**, Germany’s share of Russian

⁵ Ibid. Julian Wettengel, <https://surl.li/vblcmm>

⁶ Ibid., <https://surl.li/svbuga>,

⁷ „Germany surges to fourth largest global military spender: SIPRI“, <https://surl.li/rpoojd>, Accessed 03.11.25

gas imports had fallen from **52% to 22%**, with **Norway** and the **Netherlands** emerging as primary suppliers. At the EU level, Russian gas imports declined from **40% to roughly 11%** over the same period. As of **2024**, Norway has become Germany's **dominant gas supplier**, accounting for approximately **48% of pipeline imports**, while liquefied natural gas (LNG) from **Belgium and the Netherlands** fills most of the remaining demand. This diversification underscores Germany's determination to achieve **energy security and strategic autonomy**, reducing vulnerability to geopolitical coercion. In sum, the Russian invasion of Ukraine has propelled Germany into an era of **strategic transformation**. The country's evolving defense posture, expanded industrial capacity, and energy diversification reflect not only a break from its post-Cold War restraint but also a reassertion of its leadership within Europe. The *Zeitenwende* has redefined Germany's identity—from a cautious economic power to an active **guarantor of European security**, ready to harness its full military, industrial, and diplomatic potential to safeguard the stability of the transatlantic order.⁸

Conclusion

Germany's transformation since the outbreak of Russia's full-scale invasion of Ukraine represents a **historic turning point** in both its national trajectory and its role within the European security architecture. For decades, Germany's strategic orientation was defined by **economic interdependence, energy dependence on Russia**, and a commitment to diplomacy and restraint rather than hard power. The events of 2022 fundamentally disrupted this paradigm, compelling Berlin to reassess its long-standing assumptions about security, deterrence, and leadership in Europe.⁹

In the wake of the invasion, Germany has undergone a profound **strategic reorientation**. The country has moved decisively away from reliance on Russian gas and oil, undertaking a large-scale **diversification of energy sources** and expanding **liquefied natural gas (LNG) infrastructure** in partnership with trusted allies such as Norway, the Netherlands, and the United States. This transition marks not merely an economic adaptation but a **geopolitical realignment**, signaling Germany's determination to reduce its vulnerability to external coercion and to achieve **greater energy sovereignty**. Parallel to this energy transformation, Germany has initiated an **unprecedented expansion of its defense capabilities**. The establishment of the €100 billion *Sondervermögen* (special fund) for the modernization of the **Bundeswehr**, the commitment to meet NATO's **2 percent defense spending target**, and the permanent deployment of German armored forces in **Lithuania** demonstrate a renewed willingness to assume military and strategic responsibility within the Alliance. These initiatives underscore Germany's emergence as a **driving force in European collective defense** and a credible guarantor of stability on NATO's eastern flank. This transformation, often referred to as the **Zeitenwende** ("epochal turning point"), reflects more than a reaction to a single conflict. It represents a **psychological and political awakening**—an acknowledgment that Europe's peace and prosperity cannot rest solely on diplomacy or economic integration, but must also be safeguarded through credible deterrence, technological innovation, and political unity.¹⁰ Germany's evolving posture illustrates a growing awareness that **European security is indivisi-**

⁸ BBC News, "Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack," August 2023

⁹ „Transforming Into a Global Defence Powerhouse: Rheinmetall (Germany) – 2024 Performance Review and Growth Outlook“, <https://surl.li/utsosx>, Accessed 03.11.25

¹⁰ Ibid., <https://surl.li/rpoojd>,

ble, and that leadership entails both responsibility and readiness to act. However, the path ahead remains complex. While Germany has taken significant steps toward strengthening its defense posture and energy independence, questions persist about the **durability and consistency** of its new strategic course. The challenges of maintaining political consensus, sustaining defense investments, and coordinating effectively with European and transatlantic partners will determine whether the *Zeitenwende* becomes a **lasting transformation or a temporary adjustment**.

Nevertheless, Germany's decision to favor **action over passivity**, and its willingness to redefine itself as a proactive leader in European affairs, have already reshaped the continent's strategic outlook. In the coming years, much will depend on the **outcome of the war in Ukraine**, the evolution of transatlantic relations, and Berlin's capacity to reconcile its historical caution with the demands of modern leadership. What is certain, however, is that Germany's awakening marks a **new chapter in European history**—one in which its choices will play a decisive role in determining the future stability, resilience, and unity of Europe.

Bibliography

- Julian Wettengel „Germany, EU remain heavily dependent on imported fossil fuels“, 03 Apr 2024, <https://surl.li/vblemm>, Accessed 03.11.25
- EU trade with Russia - latest developments“, 28 November 2025, <https://surl.li/svbuga>, Accessed 03.11.25
- Transforming Into a Global Defence Powerhouse: Rheinmetall (Germany) – 2024 Performance Review and Growth Outlook“, <https://surl.li/utsosx>, Accessed 03.11.25
- Germany surges to fourth largest global military spender: SIPRI“, <https://surl.li/rpoojd>, Accessed 03.11.25
- Samuel Bendett, “Unmanned and Autonomous Systems in the Black Sea: The Next Phase of Maritime Competition,” *Center for Naval Analyses*, 2022.
- BBC News, “Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack,” August 2023, <https://surl.li/qydird>

NATO ARTIFICIAL INTELLIGENCE STRATEGY

Aleksandra Dekanosidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Mariam Menabdishvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This conference topic provides a comprehensive overview of NATO's Artificial Intelligence Strategy, adopted in 2021,¹ which serves as a foundational framework for the Alliance's approach to this transformative technology. The strategy is not merely a reactive document but a proactive and ambitious plan to harness the benefits of AI while managing its risks, ensuring NATO remains the cornerstone of collective defense in the 21st century. NATO's AI Strategy represents a critical step in future-proofing the Alliance. It balances innovation with responsibility, aiming to accelerate the adoption of AI to bolster deterrence and defense while firmly anchoring its development and use in ethical principles and international law. The successful implementation of the strategy is paramount for maintaining NATO's strategic advantage and ensuring the safety and of course security of its member states in an increasingly competitive and technologically competitive and technologically complex global security environment.

Keywords: NATO, Artificial Intelligence, AI Strategy, Responsible AI, Defense Innovation, Collective Defense.

¹ Summary of NATO's revised Artificial Intelligence (AI) strategy 9/22/2025, <https://surl.it/bfnqtd>, Accessed 03.11.2025

Introduction

The rapid advancement of artificial intelligence technologies is fundamentally transforming the landscape of modern security and defense. As AI becomes increasingly integral to military operations, logistics, intelligence and cybersecurity, NATO recognizes the critical need to develop a comprehensive strategy to harness its potential responsibly and effectively.

The NATO artificial intelligence strategy is designed to ensure that AI serves the alliance's core objectives-maintaining peace, security, and stability-while addressing the ethical, legal and technical challenges associated with these emerging technologies. This strategy emphasizes the importance of fostering innovation and technological superiority among member nations, ensuring interoperability, and promoting a shared understanding of AI's opportunities and risks. NATO aims to integrate AI in a manner that upholds its values, such as transparency, accountability, and respect for human rights. Moreover, the strategy advocates for the development of secure, resilient AI systems capable of withstanding cyber threats and malicious use. It recognizes that AI is a dual-use technology, with the power to revolutionize allied defense and security capabilities-from intelligence, surveillance, and reconnaissance (ISR)² and cyber defense to logistic command and control. Simultaneously, it acknowledges that strategic competitors are investing heavily in AI for military purpose, potentially threatening the Alliance's ability to deter and defend. This creates a strategic imperative for NATO to adopt AI at pace and at scale. The Alliance's approach is guided by several core principles. First and foremost is the responsible use of AI. NATO is committed to developing and employing AI capabilities in a lawful, ethical, and robust manner, ensuring human oversight and accountability in line with international law and our values. This ethical foundation is what distinguishes the Allied approach from that of potential adversaries. The strategy emphasizes cooperation and interoperability. Recognizing that innovation thrives in openness, NATO seeks to bridge the gap between the defense sector and the vibrant technological ecosystems within Allied nations. Landmark initiatives like the Defense Innovation Accelerator for the North Atlantic (DIANA)³ and the NATO Innovation Fund are central to this effort, designed to scout, fund and adapt cutting-edge technologies for defense and security purposes. Furthermore, a key objective is to develop interoperability standards to ensure that AI systems from all Allied nations can work together seamlessly, Preserving NATO's greatest strength' its cohesion. The strategy positions NATO to shape global norms. The alliance aims to be a leading voice in the development of international standards and regulations for the responsible use of AI in defense, promoting stability and reducing the risks of conflict and escalation.

This article asks the following research questions...

1. What is NATO's official strategy on Artificial Intelligence?
2. What ethical principles underpin NATO's AI strategy?
3. What is the Artificial Intelligence's relevance to the Alliance's future deterrence and defense posture?

² NATO releases revised AI strategy 9/22/2025, <https://surl.li/yqoliq>, Accessed 03.11.2025

³ NATO Resources 9/22/2025, <https://natolibguides.info/artificialintelligence>, Accessed 03.11.2025

Main Part

NATO's Official strategy on Artificial Intelligence

Artificial Intelligence (AI) is set to rapidly change how people live and work, but also the ways in which wars will be fought. Experts believe that the integration of AI into military systems has the potential to revolutionise warfare. This report takes stock of ongoing efforts by NATO and Allies as well as external actors, such as China and Russia⁴, to integrate AI into the armed forces. Due to the inherent dual-use characteristics of many AI applications and the fact that innovation is mainly driven by non-military entities, this mapping exercise covers both civilian and military activities. Yet, the broad applicability of AI necessitates a thematic focus, which in the context of this report will be the military sector. As I mentioned NATO's approach to artificial intelligence is a cornerstone of its broader adaptation to technological change and its commitment to maintaining its technological edge. The strategy is not a single document but a cohesive framework built on several key pillars: responsible use, accelerated adoption, and protection against threats. The foundational document is the NATO AI Strategy, endorsed by Allies at the Brussels Summit in June 2021⁵. The strategy outlines three primary objectives are to encourage the development and integration of AI capabilities across all Allied armed forces to enhance decision-making, efficiency and effectiveness. Also €1 billion fund, launched in 2023⁶, to invest in early-stage startups and deep tech companies developing dual-use technologies, including AI, in Allied countries. The US military has long relies on technological superiority for national security, the 2018 and 2022 US national defense strategies highlight AI as critical for maintaining military superiority. In 2021, the JAIC was integrated into the newly created chief digital and Artificial intelligence office (CDAO)⁷. NATO's official strategy on artificial intelligence emphasizes enhancing interoperability, ensuring ethical use, fostering innovation, and promoting responsible development and deployment of AI technologies. The strategy aims to support multinational cooperation strengthen security, and maintain technological superiority while adhering to International legal and ethical standards. It also focuses on building expertise, investing in AI research, and establishing policies to address potential risks and challenges associated with AI applications in security and defense. to successfully navigate the challenges and opportunities of this process, the alliance and NATO Parliament should raise awareness for the role of AI to enhance its legitimacy and the acceptance of increased investments while taking into account the inherent dual-use aspect of AI. Engage in close discussions to strike a balance between political and military considerations; work towards up-to-date and coherent strategic documents and activities; support ongoing efforts to create an innovation ecosystem to make AI available for armed forces; enhance cooperation with EU and other partners; continue the development of standards for a ethical use of AI and engage with external actors to reach universally agreed-upon standards. In summary NATO's AI strategy is a comprehensive and value-driven framework. It aims not only to harness the benefits of AI to maintain its techno-

4 2024 - NATO AND ARTIFICIAL INTELLIGENCE: NAVIGATING THE CHALLENGES AND OPPORTUNITIES <https://surl.li/wfolwh>, Accessed 03.11.2025

5 Summary of NATO's revised Artificial Intelligence (AI) strategy 9/22/2025, <https://surl.li/gmubnu>, Accessed 03.11.2025

6 Ibid.

7 Defence and artificial intelligence "chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/", <https://surl.li/borxgg>, Accessed 03.11.2025

logical advantage but to do so in a legally sound and ethically responsible manner. By establishing clear principles, creating new institutions like DIANA and the NIF, and focusing on both innovation and defense NATO is positioning itself to navigate the complex challenges and opportunities presented by the age of artificial intelligence. Additionally, a growing set of related issues merit NATO's attention. These include: the potential diminishing global availability of quality public data to train AI models; implications of the demands of compute intensive AI, including on energy consumption, and accountability in human-machine teaming and overcoming technical and governance issues when civilian-market dual-use solutions are applied in military context.

Ethical principles of NATO's AI strategy

The ethical principles of NATO's AI strategy are foundational to its overall approach, ensuring that the Alliance's adoption of emerging technologies is conducted responsibly and in line with its democratic values. NATO's approach to AI ethics is formally outlined in its AI Strategy and encapsulated in the Summary of the NATO Artificial Intelligence Strategy. The strategy is built upon the principle of "Responsible Use" and is guided by the following six ethical principles: first one is lawfulness AI applications must comply with national and international law, including international humanitarian law (i.e., the laws of war) it means that all development and use of AI applications must adhere to domestic and international law. This is paramount, with a specific emphasis on compliance with International Humanitarian Law (IHL)-the laws of armed conflict, including principles of distinction, proportionality and precaution in attack. This principle ensures that even in warfare, AI use is governed by legal frameworks that protect civilians and combatants. Responsibility and accountability; it contains human responsibility and accountability must be maintained throughout the life cycle of AI systems. Humans must remain in control and ultimately accountable decisions. This is the cornerstone principle that human responsibility must be retained throughout the entire lifecycle of an AI system. It mandates that humans must remain in control, exercising judgment and bearing ultimate accountability for decisions, even those informed or enabled by AI. Explainability and traceability; AI systems should be transparent and their outcomes understandable to the extent possible. This is crucial for building trust and conducting oversight. AI System and their outcomes should be sufficiently transparent and understandable to the users and operators who rely on them. This involves creating systems whose logic can be audited and whose decision-making processes can be traced. Reliability: AI system must be robust, secure, and resilient enough to perform consistently and reliably in complex, contested and adversarial environments. AI system must be robust, secure, and resilient. They must perform consistently and predictably, even in degraded contested or adversarial environment where they may face cyber-attacks, data corruption, or electronic warfare. Governability: AI systems must be designed to allow for human intervention, the ability to disengage or deactivate them, and to prevent unintended consequences. AI system must be designed safeguards that allow for human intervention, the ability to disengage, deactivate or override them. This is about ensuring that humans can always "pull the plug" to prevent unintended escalation or actions. And the last one Bias mitigation: proactive steps must be taken to minimize bias in AI datasets and algorithms which could otherwise

leas to unintended unjust or harmful outcomes⁸. Proactive and continuous efforts must be made to identify and minimize bias in the data used to train AI and in the algorithms themselves. These biases could be based on race, gender ethnicity or other factors and could lead to discriminatory, unjust or ineffective outcomes. In conclusion, NATO's ethical principles for AI are a sophisticated and operationalized framework. They are highly relevant for navigating the geopolitical and technological landscape, and their implementation methodology is robust, involving dedicated institutions that ensure ethics are not an afterthought but a foundational component of NATO's technological superiority.

Artificial Intelligence and its relevance to the Alliance's future deterrence and defense posture

The urgency for NATO to adopt and master AI systems from several critical, interconnected factors for example the return of strategic competition and multi-domain warfare...NATO no longer operates in a permissive post-cold war environment it faces sophisticated state adversaries like Russia and China who are heavily investing in AI for military purposes. Modern conflict, as evidenced in Ukraine, is a seamless blend of physical and virtual domains; kinetic strikes are coordinated with cyber-attacks, information operations, and electronic warfare. AI is the only tool capable of processing the vast volume of data from these domains at the speed of relevance to provide commanders with a decisive informational advantage. The modern battlefield generates terabytes of data from satellites, drones, ground sensors, and open-source intelligence. Human analyst alone are overwhelmed. AI's core relevance lies in its ability to analyze this data at machine speed, combine disparate and predict adversary movements, logistic needs and potential vulnerabilities. Also to identify patterns and predict adversary movements, logistic needs, and potential vulnerabilities. This transforms the decision-making cycle from hours or days to minutes or seconds, a concept known as achieving "decision superiority"⁹. NATO's methodology is not about building its own killer robots, but about creating a framework for responsible adoption, standardization and acceleration of ai across the Alliance. Whole document about NATO and AI outlines the Alliance's ambition to be a leader in the responsible use of AI and sets three core objectives first one is lead in the responsible use and development of AI for defence and security also protect and monitor AI-enabled capabilities and ensure their resilience and last one is to cooperate with the innovation community and Allied nations. If we will talk about NATO and AI relevance we should mention Russia and China also because they are heavily investing in military AI. NATO perceives a real risk of falling behind. AI is not just an efficiency tool; it is a potential source of decisive advantage. Failure to adopt it could lead to strategic irrelevance. Modern deterrence relies on credible military capability. AI-enhanced intelligence, surveillance, and autonomous systems make NATO's deterrence posture more effective and resilient. To sum up NATO's methodology for AI is a deliberate, structured effort to harness a disruptive technology responsibly. Its relevance today is absolute; AI is a central front in the ongoing strategic competition and is fundamentally reshaping the character

8 Summary of NATO's revised Artificial Intelligence (AI) strategy <https://surl.li/arv1cu>, Accessed 03.11.2025

9 Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation <https://surl.li/bokiab>, Accessed 03.11.2025

of warfare and security. For NATO, successfully integrating AI is not optional- it is essential for upholding its core mission of collective defence and ensuring it remains a potent and credible force for decades to come. The Alliance is betting its future on its ability to become a “Digital Alliance”.

Conclusion

The integration of Artificial intelligence into the fabric of the North Atlantic Treaty organization is not a distant future prospect; it is an ongoing and transformative reality. This paper has argued that AI presents a dual-edged sword, offering NATO unparalleled opportunities to enhance its defensive, deterrent and operational capabilities, while simultaneously introducing profound ethical, legal and strategic challenges. The Alliance’s ability to navigate this complex landscape will be a defining factor in its future credibility and effectiveness. The strategic imperative for NATO to adopt AI is clear. From revolutionizing intelligence, surveillance, and reconnaissance through vast data analysis to optimizing logistics, enhancing cyber defenses and improving the speed of command and control, AI promises a significant tactical and strategic advantage. In an era of renewed strategic competition, where potential adversaries are aggressively pursuing military AI applications, failure to keep pace would constitute an unacceptable risk to collective defense. AI is not merely a tool for efficiency; it is becoming a central component of deterrence, ensuring that the Alliance can respond with the necessary speed and precision to 21st century threats. However, this pursuit of technological superiority must be unequivocally grounded in the principles of “responsible use” as detailed, NATO’s foundational ethical principles. These principles are not impediments to innovation but are essential guardrails that ensure AI strengthens, rather than undermines, the alliance’s core values and its commitment to International law, particularly international humanitarian law. The commitment to maintaining meaningful human control over the use of forces remains the non-negotiable cornerstone of this framework, serving as a vital bulwark against the dangers of unchecked autonomy and ensuring ultimate human accountability. Looking forward, NATO’s path is fraught with challenges that demand sustained attention. The “race for talent” the need for digital interoperability among 32 nations, and vulnerabilities of complex AI systems to adversarial attacks are significant hurdles. Moreover, the alliance must continue to shape the global normative landscape around military AI, positioning its responsible approach in stark contrast to models that may prioritize capability over ethics. In final analysis, NATO’s journey with Artificial Intelligence is a strategic tightrope walk. On one side lies the of technological obsolescence; on the other, the peril of ethical and legal compromise. The Alliance’s AI strategy and its implementation plan for the responsible use of AI demonstrate a clear-eyed recognition of the dichotomy. By steadfastly committing to an approach that fuses technological obsolescence; on the other, the peril of ethical and legal compromise. The Alliance’s AI strategy and its plan for the responsible use of AI demonstrate a clear eyed recognition of this dichotomy. By steadfastly committing, NATO has the opportunity only to secure its own future but also to set a crucial global standard. the task is monumental, but for an Alliance built on the principles of collective defence and democratic values, it is both necessary and imperative.

Bibliography

Summary of NATO's revised Artificial Intelligence (AI) strategy <https://surl.li/arvlu>, Accessed 03.11.2025

NATO releases revised AI strategy 9/22/2025, <https://surl.li/yqoliq>, Accessed 03.11.2025

Summary of NATO's revised Artificial Intelligence (AI) strategy 9/22/2025, <https://surl.li/gmubnu>, Accessed 03.11.2025

2024 - NATO AND ARTIFICIAL INTELLIGENCE: NAVIGATING THE CHALLENGES AND OPPORTUNITIES
<https://surl.li/wfolwh>, Accessed 03.11.2025

Defence and artificial intelligence "chrome-extension://efaidnbmnnnibpcajpcgclefindmkaj/", <https://surl.li/borxgq>,
Accessed 03.11.2025

Harnessing Artificial Intelligence: Allied Command Transformation at the Forefront of NATO Innovation <https://surl.li/bokiab>, Accessed 03.11.2025

ARTIFICIAL INTELLIGENCE AS A STRATEGIC FORCE MULTIPLIER IN MODERN DEFENSE

Giorgi Okropiridze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Luka Zaalishvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The accelerating integration of Artificial Intelligence (AI) into defense systems represents a decisive turning point in military strategy. Far beyond an incremental upgrade, AI functions as a strategic force multiplier—expanding the cognitive, operational, and logistical capacity of armed forces without proportional growth in manpower or expenditure. This paper examines how AI reshapes contemporary defense through automation, predictive analytics, and real-time decision support. Drawing on the framework of the Revolution in Military Affairs (RMA), it analyzes three principal dimensions of AI's military application: cognitive advantage (accelerated situational assessment and decision-making), operational autonomy (precision targeting and unmanned systems), and organizational adaptation (data-driven logistics and command integration). The article highlights that defense effectiveness increasingly depends on the fusion of technological innovation, human oversight, and international cooperation. Case evidence from NATO's DIANA initiative, the U.S.–Israel innovation model, and Ukraine's wartime experimentation demonstrates that multinational collaboration amplifies the pace and ethical governance of defense innovation. Yet the diffusion of autonomous and cyber-enabled capabilities also generates acute ethical, legal, and security challenges—including accountability for autonomous actions, algorithmic bias, and vulnerability to data manipulation. The paper argues that sustained strategic advantage will derive not merely from AI possession but from the governance systems that regulate its use. Human-in-the-loop control, interoperability among allies, and transparent ethical standards must guide the integration of AI across defense ecosystems. As warfare becomes increasingly networked and data-centric, those states that combine technological agility with responsible innovation will define the emerging global security order.

Ultimately, the convergence of innovation and cooperation transforms AI from a disruptive technology into a stabilizing instrument of collective defense. Properly governed, AI can enhance deterrence, optimize resources, and safeguard human decision-making—serving not as a replacement for strategy, but as its most powerful enabler in the twenty-first-century battlespace.

Keywords: Artificial Intelligence (AI); defense innovation; autonomous systems; cybersecurity; decision superiority; ethical governance; Revolution in Military Affairs (RMA); international cooperation; force multiplier; strategic security

Introduction

The twenty-first century has fundamentally redefined the nature of warfare, shifting its emphasis from the accumulation of conventional firepower to the intelligent management of information, speed, and precision. Modern defense effectiveness is increasingly determined not by the quantity of weapons or soldiers, but by a state's capacity to process, analyze, and act on information faster and more accurately than its adversaries. Within this paradigm, Artificial Intelligence (AI) has emerged as the defining technological catalyst of contemporary security transformation. AI, broadly understood as the simulation of human cognitive functions by machines, represents far more than a tool of automation—it functions as a strategic force multiplier, amplifying the operational value of existing defense assets and decision-making architectures. Its growing integration across surveillance, logistics, and command networks has restructured how militaries think, plan, and fight. What once took analysts hours or even days to interpret can now be assessed in real time, with machine learning models identifying threats, predicting enemy maneuvers, and optimizing battlefield responses within seconds. ¹More importantly, AI is revolutionizing command philosophy itself. Decision-making, traditionally hierarchical and sequential, is evolving toward distributed, data-driven ecosystems where human commanders collaborate with intelligent systems that learn and adapt continuously. Autonomous and semi-autonomous platforms—ranging from aerial drones and naval vessels to robotic ground units—extend human reach, executing reconnaissance, logistics, and strike missions with remarkable precision and minimal personnel risk. This integration of autonomy and analytics enables militaries to project power without proportionate human exposure, enhancing deterrence while conserving resources. Simultaneously, AI-enabled cyber and electronic warfare capabilities are redefining what it means to control a battlespace. Conflict now unfolds as much in digital and cognitive domains as in physical ones, where information dominance and algorithmic speed determine strategic outcomes. Warfare has thus evolved into a multidimensional contest over data, algorithms, and perception, in which the side with superior analytical intelligence achieves not only tactical success but also cognitive superiority.

Main Part

The presented paper examines the ways in which Artificial Intelligence serves as a strategic force multiplier in modern defense. It analyzes AI's operational domains, the advantages it confers, and the ethical and security challenges that accompany its deployment. The central argument posits that AI's transformative potential lies not in computational capacity alone, but in the synergistic integration of technology, human oversight, and international cooperation. Effective defense modernization depends on this triad—where innovation is guided by strategy, governed by ethics, and reinforced through alliances—to ensure that technological progress strengthens stability rather than undermines it.² The strategic rationale for integrating Artificial Intelligence into defense is rooted in the enduring pursuit of decision superiority—the ability to understand, decide, and act faster and more effectively than the adversary. In military theory, this principle has evolved from John Boyd's "OODA loop" (Observe–Orient–Decide–Act) to what modern strategists describe

1 Nitzl, Cyran, C., Krstanovic, A., Borghoff, S. & M., U. The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process. 2024.

2 Kean, Matthew J. *Information Advantage*. Military Review, November-December 2022, 111-118.

as the Algorithmic Loop, where AI-driven systems continuously learn and adapt to operational environments in real time.³ The incorporation of AI into defense thus represents a paradigm shift from reactive command structures to predictive, adaptive, and self-correcting systems of control. At the strategic level, AI supports grand defense planning and national security decision-making through enhanced modeling and simulation. Military strategists can test scenarios involving large-scale troop movements, logistics, and deterrence postures with unparalleled fidelity, incorporating dynamic variables such as weather, morale, and civilian infrastructure impact. Predictive analytics helps anticipate geopolitical escalation pathways, optimize resource allocation, and identify strategic vulnerabilities long before they manifest. For example, AI-enabled war gaming tools used by NATO and the U.S. Department of Defense now generate millions of simulated outcomes in seconds, enabling policymakers to design flexible and risk-informed strategies rather than static contingency plans.⁴

At the operational level, AI transforms situational awareness and command coordination. It integrates data from satellites, sensors, unmanned aerial vehicles (UAVs), radar systems, and electronic intelligence (ELINT) into a single, coherent information network. Machine learning algorithms detect anomalies—such as irregular troop formations or unusual communication spikes—that human analysts might overlook under information overload. This fusion of real-time data across domains creates a multi-layered “digital battlespace,” enabling joint operations that are synchronized across land, sea, air, cyber, and space. The result is an unprecedented tempo of warfare, where the speed of perception and response becomes the decisive determinant of success. At the tactical level, AI amplifies the precision and adaptability of field operations. Intelligent munitions, autonomous drones, and robotic systems now operate semi-independently, executing reconnaissance, logistics, and strike missions with high accuracy. Ground combat units equipped with AI-based decision support tools can assess battlefield risks instantly, predict enemy movement patterns, and coordinate supporting fire autonomously. These systems allow militaries to achieve “more with less,” optimizing human involvement while preserving strategic initiative and minimizing casualties.

However, the strategic logic of AI in defense is not merely technical—it is philosophical and organizational. It redefines command authority and challenges the traditional boundaries of human judgment. Commanders must now navigate a dual responsibility: to harness the computational advantages of AI while ensuring that ethical constraints and human oversight remain intact. This necessitates new forms of AI literacy, algorithmic accountability, and digital trust within military hierarchies. Moreover, success in AI-driven defense does not depend solely on innovation but on integration—the ability to align technological systems, human operators, and strategic doctrines into a cohesive operational framework. In essence, Artificial Intelligence alters the geometry of power in warfare. Superiority is no longer achieved through numerical dominance or territorial control but through information mastery, analytical speed, and cognitive adaptation. The side that learns, evolves, and acts faster controls not only the battlefield but the narrative of the conflict

3 U.S. Department of Defense. *Data, Analytics, and Artificial Intelligence Adoption Strategy*. Washington, DC: Department of Defense, November 2023.

4 Kean, Matthew J. *Information Advantage*. *Military Review*, November-December 2022, 111-118.

itself. AI thus becomes both a technological instrument and a strategic philosophy—one that compels states to conceptualize deterrence, resilience, and the ethics of command in the digital age.⁵

The integration of Artificial Intelligence (AI) into modern defense architecture represents a decisive shift from manpower-based strength to cognition-based superiority. In contemporary warfare, dominance is achieved not merely through the possession of superior weapons but through the ability to perceive, interpret, and respond to the operational environment faster and more precisely than the adversary. AI serves as the engine of this transformation, enhancing human cognition, accelerating the command cycle, and expanding the boundaries of operational flexibility.

At the cognitive level, AI augments human decision-making through data fusion, pattern recognition, and predictive analysis. Modern battlefields generate immense volumes of information—satellite imagery, radar signals, social media data, logistics updates, and cyber intelligence—that exceed human analytical capacity. AI-driven systems, powered by machine learning and natural language processing, synthesize this data into actionable insights within seconds. Decision cycles that once depended on hierarchical communication chains have evolved into real-time feedback systems, where commanders interact continuously with algorithmic advisors capable of forecasting adversary intent, supply shortages, and risk probabilities. This acceleration of the decision-making process—often described as *decision dominance*—creates what military theorists call the cognitive edge: the ability to act inside the adversary's observation and reaction loop. Moreover, AI assists in strategic foresight and crisis anticipation. Predictive models simulate thousands of potential conflict trajectories by analyzing historical data and current geopolitical signals. NATO's Allied Command Transformation (ACT), for instance, utilizes AI-assisted war gaming tools to forecast escalation risks and recommend de-escalation strategies in near real time. This enables policymakers to move from reactive crisis management toward proactive risk prevention, redefining the art of strategy in the digital age.⁶

At the operational level, AI enhances logistical precision, situational awareness, and autonomous coordination. Autonomous and semi-autonomous systems—such as unmanned aerial vehicles (UAVs), naval drones, and robotic ground units—perform reconnaissance, targeting, and resupply operations in high-risk environments without endangering human lives. These platforms rely on AI for navigation, obstacle avoidance, and target identification, allowing for persistent surveillance and precision strikes even under electronic interference.

AI-enabled logistics systems have also revolutionized sustainability and resource allocation. Predictive maintenance algorithms identify potential equipment failures before they occur, optimizing repair schedules and minimizing downtime. This transformation of logistics from reactive to predictive operations mirrors civilian innovations in the industrial sector but with exponentially greater strategic consequences. The result is a military ecosystem characterized by operational resilience and adaptability, where resources are dynamically allocated according to battlefield realities rather than static planning.

In the cyber domain, AI functions as both shield and sword. As cyberattacks grow in frequency

5 U.S. Department of Defense. *Data, Analytics, and Artificial Intelligence Adoption Strategy*. Washington, DC: Department of Defense, November 2023.

6 Nitzl, Cyran, C., Krstanovic, A., Borghoff, S. & M., U. *The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process*. 2024.

and sophistication, human analysts alone cannot match the pace or complexity of digital threats. AI-driven cybersecurity systems autonomously monitor network behavior, detect anomalies, and neutralize intrusions before they compromise critical systems. For instance, self-learning algorithms within NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) continuously adapt to new malware signatures and attack vectors, enhancing resilience across allied digital infrastructures. Equally, AI supports information dominance by detecting disinformation campaigns, deep fakes, and coordinated online manipulation. These capabilities are critical in hybrid warfare, where public perception and narrative control often determine strategic legitimacy as much as battlefield success. AI-powered sentiment analysis tools enable governments to detect and counter hostile information operations, strengthening national and allied resilience against cognitive attacks.⁷

Despite these advantages, the cognitive and operational empowerment offered by AI introduces complex ethical and doctrinal implications. The automation of lethal decision-making, for example, raises profound moral and legal questions concerning accountability and proportionality in combat. Therefore, the true measure of success in AI integration is not technological sophistication alone but strategic alignment with human judgment, ethical oversight, and international law. Ultimately, AI's value as a force multiplier lies in its ability to complement—not replace—human cognition. It transforms the commander's role from that of an operator to a strategist, one who must understand and manage intelligent systems within broader geopolitical and ethical frameworks. By merging computational power with human judgment, AI establishes a new foundation for defense efficiency, adaptability, and global security governance.

Challenges, Risks, and Ethical Governance

The integration of Artificial Intelligence into defense structures brings unprecedented advantages but also profound challenges that test the limits of law, ethics, and international stability. As states increasingly delegate critical functions to algorithms and autonomous systems, the central question emerges: how can military efficiency coexist with moral and legal responsibility?

Accountability and the “Human-in-the-Loop” Principle

The first and most urgent concern is accountability. When autonomous or semi-autonomous systems engage targets, determining responsibility for unintended consequences becomes complex. If an AI-guided missile or robotic unit makes an erroneous lethal decision, liability may fall ambiguously among programmers, commanders, or the political authority that authorized deployment. To address this, democratic states and alliances have reaffirmed the *human-in-the-loop* principle—requiring human supervision in all lethal decisions and ensuring that final judgment remains a human prerogative. NATO's 2021 AI Strategy and the U.S. Department of Defense's Ethical AI Principles both underscore that automation must support, not supplant, human command. This approach preserves ethical agency while maintaining operational advantage.⁸

⁷ Kean, Matthew J. *Information Advantage*. Military Review, November-December 2022, 111-118.

⁸ U.S. Department of Defense. *Data, Analytics, and Artificial Intelligence Adoption Strategy*. Washington, DC: Department of Defense, November 2023.

Algorithmic Bias and Data Integrity

AI systems are only as reliable as the data on which they are trained. Bias in datasets—stemming from incomplete information, skewed sampling, or adversarial manipulation—can lead to discriminatory or strategically flawed outcomes. A misclassified radar signature or corrupted data feed could trigger false identification of a civilian object as hostile. Ensuring data diversity, transparency, and validation is thus a core requirement for trustworthy AI in defense. Establishing independent auditing mechanisms and cross-national verification protocols within alliances such as NATO or NORDEFCO mitigates risks of algorithmic distortion and strengthens collective trust in shared intelligence. The digital nature of AI renders it simultaneously powerful and fragile. Sophisticated cyber adversaries can exploit vulnerabilities within AI architectures—poisoning data, manipulating learning processes, or compromising control networks. Paradoxically, as militaries increase their reliance on AI for situational awareness and logistics, they also heighten exposure to systemic digital collapse.⁹ To counter this risk, defense institutions are investing in *resilient architectures*—air-gapped systems, redundant networks, and zero-trust cybersecurity frameworks that prevent cascading failure. The fusion of cyber defense and AI security must become an integral component of future defense design.¹⁰ The legal frameworks governing armed conflict—codified in the Geneva Conventions and customary international humanitarian law—were conceived for human decision-makers, not self-learning algorithms. As lethal autonomous weapons systems (LAWS) evolve, international law struggles to define thresholds of intent, proportionality, and accountability. Current diplomatic efforts within the United Nations Group of Governmental Experts (GGE) on LAWS and regional initiatives such as the EU’s AI Act attempt to bridge this regulatory gap. Yet consensus remains limited. The absence of universally accepted standards risks an *AI arms race*, where speed and secrecy override caution and ethics. Therefore, transparent governance and multilateral verification are vital to prevent destabilizing escalation.

Beyond legality lies the broader issue of legitimacy. Public trust in defense institutions depends on the perception that technological innovation serves humanitarian and security goals rather than unchecked militarization. Embedding ethical review boards, interdisciplinary oversight committees, and civilian participation within defense innovation ecosystems ensures that AI development aligns with democratic accountability. Ethical literacy among military and political leaders is equally critical, enabling informed oversight rather than blind delegation to technical experts. Artificial Intelligence thus stands at a crossroads between empowerment and peril. Its governance must combine rigorous ethics, resilient security, and international cooperation to ensure that innovation reinforces peace rather than accelerates instability. The next section will examine how collaborative frameworks and allied partnerships can translate these ethical principles into practical mechanisms for sustainable defense modernization.

Artificial Intelligence has redefined the logic of power in the twenty-first century, but its true strategic value is realized only through international cooperation. No single nation, regardless of its

9 Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton & Company, 2018.

10 Nitzl, Cyran, C., Krstanovic, A., Borghoff, S. & M., U. The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process. 2024.

technological capacity, can independently secure itself against transnational cyber threats, autonomous warfare risks, or algorithmic escalation. The inherently global nature of AI—rooted in data flows, digital interdependence, and shared technological ecosystems—demands collective governance and cooperative innovation frameworks that balance sovereignty with shared responsibility. Global and regional defense organizations have begun to institutionalize AI cooperation through structured initiatives. The North Atlantic Treaty Organization (NATO) stands at the forefront of this effort. Its *Artificial Intelligence Strategy* (adopted in 2021) and the Defence Innovation Accelerator for the North Atlantic (DIANA) represent pivotal mechanisms for joint research, ethical standardization, and technology deployment among member and partner states. DIANA’s network of test centers and innovation hubs across Europe and North America facilitates experimentation in dual-use technologies—ranging from AI-driven logistics to quantum-enabled communication systems—ensuring interoperability and trust within the Alliance.

Similarly, the European Union’s Defence Fund (EDF) and Permanent Structured Cooperation (PESCO) aim to strengthen intra-European technological autonomy while complementing NATO frameworks. These initiatives allow medium and small states to pool resources, mitigate duplication, and integrate civilian innovation into military application. Such institutional collaboration underscores a new model of defense innovation diplomacy, where technology serves as a bridge rather than a dividing line among allies. Beyond multilateral structures, bilateral partnerships have proven vital laboratories for applied defense innovation. The U.S.–Israel defense partnership, for instance, exemplifies how close collaboration between a major power and a technologically advanced smaller state can yield transformative outcomes. The joint development of the *Iron Dome* missile defense system and the *David’s Sling* program illustrates the synergy of funding, innovation culture, and operational testing. Similarly, U.S.–Ukraine technology cooperation, particularly during the 2022–2025 conflict period, accelerated the integration of AI into drone navigation, battlefield management, and cyber defense, revealing the potential of crisis-driven innovation under international support. Crucially, such partnerships increasingly involve public–private cooperation. Defense ministries collaborate with tech startups, universities, and industry leaders to co-develop secure AI applications. This civil–military fusion extends innovation beyond traditional defense contractors, harnessing entrepreneurial creativity while adhering to state oversight. The result is a diversified innovation ecosystem resilient to geopolitical shocks and capable of continuous adaptation.

Ethical Governance Through Cooperation

As AI becomes embedded in global defense operations, ethical and legal harmonization has emerged as a shared priority. International cooperation enables the development of universal standards for responsible AI use, ensuring transparency, traceability, and accountability across jurisdictions. Forums such as the United Nations Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS) and the Global Partnership on AI (GPAI) offer platforms for establishing common principles, from algorithmic explanations to prohibitions on fully autonomous lethal systems. In this sense, cooperation is not limited to technological interoperability—it extends to normative interoperability, the shared understanding of what constitutes legitimate

and ethical military conduct. States that institutionalize transparency and accountability in AI use strengthen not only deterrence but also diplomatic credibility.¹¹

Toward a Networked Security Architecture

The future of global defense lies in the evolution of a networked security architecture, where innovation, resilience, and coordination coexist. Such an architecture connects research laboratories, defense institutions, and private technology clusters across borders, enabling continuous learning and adaptation. It transforms alliances into knowledge ecosystems, capable of responding to emerging threats such as deep fake warfare, algorithmic espionage, or AI-driven misinformation campaigns. This model also redefines strategic sovereignty. In a hype reconnected environment, independence no longer means isolation but the capacity to contribute effectively to a shared framework of collective security. Through this lens, AI innovation becomes both a national asset and a global public good—a foundation for sustainable deterrence, where transparency and shared standards reduce uncertainty and prevent escalation.¹²

Finally, as AI diffuses globally, emerging powers and smaller states must be integrated into cooperative defense dialogues. Inclusion prevents technological polarization between advanced and developing militaries and reduces the risk of an AI divide. Regional frameworks—such as the Nordic Defence Cooperation (NORDEFCO) or partnerships within the Caucasus and Indo-Pacific regions—demonstrate that innovation can flourish even among small and medium-sized nations when guided by shared strategy and open collaboration.

Incorporating diverse actors also enriches innovation through plural perspectives, ensuring that global AI governance is equitable, secure, and adaptive. The strategic future of AI in defense thus depends not on dominance but on distributed cooperation, where trust, transparency, and shared technological stewardship become the ultimate guarantors of peace.

Conclusion

Artificial Intelligence has become the defining catalyst of transformation in the defense landscape of the twenty-first century. Its integration into command structures, cyber defense, and autonomous systems marks not only a technological revolution but also a profound reconfiguration of strategic thinking, decision-making, and international relations. The capacity to harness AI effectively now determines the strategic resilience of nations and alliances alike. Yet, the long-term value of AI in defense will depend less on the sophistication of individual algorithms and more on how responsibly, collaboratively, and adaptively states integrate these technologies into coherent strategic frameworks.

AI's rise as a strategic force multiplier underscores a dual imperative: technological innovation must advance hand in hand with ethical governance. On the one hand, AI offers unprecedented advantages in intelligence analysis, operational coordination, and predictive decision-making. On the other, its automation potential challenges long-standing norms of human control and accountability in warfare. The future of defense will hinge on how states manage this tension between au-

11 Zequeira, Michael J. *AI as Combat Multiplier: Revolutionizing the U.S. Army Military Decision-Making Process*. Military Review Online Exclusive, September 2024.

12 Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton & Company, 2018.

tomation and human oversight. A purely technological race risks eroding trust and stability, while a balanced approach—anchored in transparency, ethics, and international law—can transform AI into a stabilizing instrument of collective security.¹³

In an interconnected and data-driven world, no country can secure itself in isolation. International cooperation has evolved from a diplomatic option into a strategic necessity. Alliances such as NATO, the European Union, NORDEFCO, and bilateral frameworks like U.S.–Israel and U.S.–Ukraine defense partnerships exemplify how shared innovation accelerates readiness and builds mutual trust. Joint research, interoperability standards, and ethical agreements are not peripheral activities—they constitute the new foundation of global defense architecture. The more states coordinate on technology, the less likely they are to fall into destabilizing competition or arms races driven by secrecy and mistrust.¹⁴

Effective defense innovation requires more than episodic projects; it demands institutionalized ecosystems linking government, industry, and academia. Establishing Defense Innovation Hubs, AI Ethics Centers, and Public–Private Consortia enables states to maintain continuous learning, experimentation, and adaptation. These ecosystems should prioritize dual-use technologies, ensuring that civilian advances in robotics, quantum computing, and data analytics contribute to both security and societal progress. Furthermore, states must invest in education and workforce development to cultivate AI literacy within the military and policy community—bridging the gap between technical expertise and strategic leadership.

To ensure that AI remains a stabilizing rather than destabilizing force in defense, this paper proposes the following policy recommendations:

Codify Ethical AI Principles in Defense Doctrine – Mandate human oversight in all lethal decisions, ensure algorithmic transparency, and establish internal auditing mechanisms for accountability.

Promote International Standardization – Encourage cooperation through NATO’s DIANA, the UN’s Group of Governmental Experts on LAWS, and the Global Partnership on AI to harmonize technical and ethical standards.

Develop Joint Cyber and Data Security Frameworks – Implement shared encryption protocols, rapid response mechanisms, and cross-border data protection to defend allied digital infrastructures.

Invest in Resilient and Interoperable Systems – Prioritize modular technologies that integrate seamlessly across allied platforms, enhancing operational flexibility.

Strengthen Civil–Military Collaboration – Facilitate knowledge transfer between universities, research centers, and defense industries to foster continuous innovation and ethical awareness.

Encourage Transparency and Confidence-Building Measures – Share non-sensitive AI research results and establish communication channels to prevent misperception or escalation among rival powers.

Ultimately, Artificial Intelligence represents not merely a new instrument of warfare but a new

13 Farmer, Mike. *Clausewitz’s Ghost: Thinking in Time with AI-Enabled Military Planning*. Military Review, November–December 2022, 65–72.

14 Swedish Defence Research Agency. *Exploring Decision Advantages: Artificial Intelligence in Dynamic Targeting and the Joint Targeting Cycle*. Stockholm: FOI, 2024.

logic of security—one grounded in speed, adaptability, and knowledge integration. Its greatest strategic promise lies not in replacing human judgment but in amplifying it through data-driven insight and precision. The combination of innovation and cooperation thus forms the cornerstone of twenty-first-century defense. In the years ahead, nations that succeed in aligning technological capability with ethical foresight and international collaboration will shape the contours of global stability. Those that neglect these principles risk technological overreach and strategic isolation. The future of security, therefore, will not be determined by the accumulation of smart weapons alone but by the wisdom with which humanity governs the intelligent systems it creates.

Bibliography

- Kean, Matthew J. *Information Advantage*. Military Review, November-December 2022, 111-118.
- Nitzl, Cyran, C., Krstanovic, A., Borghoff, S. & M., U. The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process. 2024.
- Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton & Company, 2018.
- U.S. Department of Defense. *Data, Analytics, and Artificial Intelligence Adoption Strategy*. Washington, DC: Department of Defense, November 2023.
- Zequeira, Michael J. *AI as Combat Multiplier: Revolutionizing the U.S. Army Military Decision-Making Process*. Military Review Online Exclusive, September 2024.
- Farmer, Mike. *Clausewitz's Ghost: Thinking in Time with AI-Enabled Military Planning*. Military Review, November-December 2022, 65-72.
- Swedish Defence Research Agency. *Exploring Decision Advantages: Artificial Intelligence in Dynamic Targeting and the Joint Targeting Cycle*. Stockholm: FOI, 2024.

INNOVATING DEFENSE THROUGH INTERNATIONAL COOPERATION: BUILDING THE FOUNDATIONS OF FUTURE SECURITY

Tekla Gablishvili

The Junker of a Bachelor's Degree (Informatic Technologies) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The 21st century has redefined the foundations of security, shifting the emphasis from military dominance to innovation, technological integration, and international cooperation. Traditional models of deterrence and national self-reliance are increasingly inadequate in addressing asymmetric warfare, cyber threats, and the rapid proliferation of artificial intelligence (AI) in defense systems. This paper examines how defense innovation, enabled by global collaboration, is transforming the strategic architecture of modern security. It argues that the capacity to innovate collectively—through research partnerships, shared technological ecosystems, and institutional adaptability—has become the decisive factor in sustaining stability in an era of complex and hybrid threats. Drawing on examples from NATO's DIANA initiative, the Nordic Defence Cooperation (NORDEFCO), Israel's defense innovation model, and Ukraine's wartime technological adaptation, the study demonstrates how innovation flourishes where creativity intersects with cooperation. These cases illustrate how multinational alliances and bilateral partnerships serve as catalysts for developing cutting-edge capabilities in artificial intelligence, cyber defense, and unmanned systems, while also strengthening interoperability and strategic deterrence. However, the paper also addresses the ethical, legal, and governance challenges arising from rapid militarization of technology—such as autonomy in lethal systems, data sovereignty, and accountability in cyber warfare.

The findings highlight that the future of global defense depends not only on technological superiority but also on institutional foresight, ethical governance, and collaborative resilience. Sustainable innovation, grounded in transparency and international norms, is essential for ensuring that progress in defense serves the broader goals of peace, security, and human dignity. The paper concludes that innovation and cooperation are not merely instruments of power but pillars of a new global security paradigm—one that transforms competition into shared responsibility for collective stability.

Keywords: Defense Innovation; International Cooperation; NATO; NORDEFCO; Cybersecurity; Artificial Intelligence; Ethics; Autonomous Systems; Global Security; Collective Resilience.

Introduction

The twenty-first century has ushered in a profound transformation in the global security environment—one defined by technological acceleration, strategic interdependence, and the emergence of complex, multidimensional threats. Innovation, advanced technology, and international cooperation have become not only instruments of national defense but also critical determinants of global stability. Traditional security paradigms—centered on conventional deterrence, territorial defense, and state-centric military power—have proven increasingly inadequate in addressing the hybrid nature of contemporary warfare. In an era shaped by asymmetric conflict, cyber aggression, disinformation campaigns, and rapidly evolving artificial intelligence (AI) systems, the very foundations of defense strategy are being redefined. Modern states can no longer rely solely on standing armies or industrial-age weapon systems to safeguard their interests. Instead, the effectiveness of national security now depends on a state's capacity to innovate, to integrate emerging technologies, and to collaborate beyond its borders. Cross-border partnerships, dual-use innovation, and interoperable defense ecosystems have become essential for anticipating, mitigating, and responding to fast-changing security challenges.

International cooperation in defense innovation, therefore, has shifted from being a diplomatic preference to a structural necessity. Security threats such as terrorism, cyberattacks, and hybrid warfare transcend political and geographic boundaries, demanding responses that are both collective and technologically sophisticated. Shared research initiatives, coordinated industrial development, and harmonized policy frameworks have emerged as the cornerstones of contemporary defense collaboration.

The article examines how international cooperation acts as a catalyst for defense innovation and how such innovation forms the foundation of a resilient and future-oriented global security system. It explores the role of key defense alliances—such as NATO and NORDEFCO—and bilateral partnerships, including those between the United States and Israel, or Ukraine and its Western allies, in fostering collective defense readiness. By highlighting these examples, the study demonstrates that cooperative innovation not only enhances technological progress and interoperability but also strengthens political cohesion and resilience in the face of emerging global security threats.

Main Part

The Strategic Role of Innovation in Defense

Innovation in defense extends far beyond the mere development of new technologies—it represents a comprehensive transformation in how states conceptualize, organize, and execute national and collective security strategies. In the 21st century, the effectiveness of armed forces is increasingly determined not by numerical superiority or the possession of conventional weaponry, but by the ability to integrate digital technologies, autonomous systems, and data-driven decision-making into existing command, control, and intelligence architectures.¹

This transformation signifies a paradigm shift from reactive defense models toward anticipa-

¹ Mearsheimer, *The tragedy of great power politics*, 2001.

tory and adaptive systems, capable of predicting, mitigating, and responding to evolving threats in real time. The convergence of technological, institutional, and strategic innovation has created a multidimensional defense ecosystem in which flexibility and interconnectivity are as valuable as firepower.

Defense innovation manifests across several interrelated domains: Artificial Intelligence and Autonomous Systems: AI-driven technologies have become a central pillar of modern defense. From predictive logistics and automated threat assessment to autonomous aerial and ground vehicles, AI enhances operational agility, improves situational awareness, and accelerates decision cycles. Autonomous drones and robotic systems, for instance, have revolutionized reconnaissance, precision targeting, and battlefield coordination, allowing militaries to act faster and with greater accuracy while reducing human risk.

Cybersecurity and Data Protection: In a world where cyber warfare has become as consequential as kinetic conflict, the protection of digital infrastructure and communication networks is a front-line defense priority. States are developing advanced cyber defense capabilities to detect, neutralize, and deter cyberattacks that target command systems, power grids, and critical public services. Cyber resilience—the ability to recover and adapt after digital disruption—has thus become an integral component of national security doctrine.

Dual-Use Technologies: Increasingly, the boundaries between civilian and military innovation are blurred. Technologies initially designed for civilian purposes—such as robotics, telecommunications, artificial intelligence, and renewable energy—are now being adapted for defense applications. This dual-use innovation enables governments to leverage private-sector creativity while ensuring cost efficiency and technological diversity. It also fosters a deeper synergy between national economies and defense sectors, making innovation a driver of both security and economic competitiveness.²

Resilience Engineering: Modern defense is not limited to deterrence; it also focuses on ensuring the continuity of essential functions during crisis or attack. Resilience engineering involves building adaptive systems capable of withstanding hybrid threats, from cyberattacks to supply chain disruptions and infrastructure sabotage. This approach prioritizes flexibility, redundancy, and the rapid recovery of operational capability—traits that define the robustness of contemporary security systems.

The central argument of this study is that innovation flourishes within collaborative ecosystems—environments where governments, private industries, research institutions, and academic partners share knowledge, align strategic objectives, and coordinate investments. Such ecosystems accelerate technological breakthroughs by combining theoretical research with practical application, fostering experimentation and risk-taking within a structured policy framework.³

Furthermore, international collaboration multiplies the impact of innovation, allowing allied nations to achieve interoperability and strategic coherence in an increasingly interconnected defense landscape. When innovation is institutionalized through cooperation—supported by shared

² Walt. 1987. *The origins of alliances*. Cornell University Press.

³ Nxuan, *The dual role of military alliances in contemporary international relations*. 3rd International Conference on International Law and Legal Policy.),2024.

standards, transparent governance, and ethical accountability—it not only enhances technological capability but also strengthens trust, resilience, and collective security among partners. In essence, innovation has evolved into the strategic foundation of modern defense. It is no longer confined to laboratories or defense contractors but embedded within the broader political, economic, and societal fabric of national power. Nations that successfully integrate innovation into their defense strategies—through collaboration, flexibility, and foresight—are those best positioned to safeguard stability and shape the future architecture of global security. ⁴International Cooperation as a Catalyst for Innovation

Defense innovation, by its very nature, cannot thrive in isolation. The complexity, scale, and cost of developing advanced military technologies have made international cooperation an indispensable driver of innovation. In today's interconnected security environment, no single nation—regardless of its resources—can independently sustain the pace of technological development required to meet emerging threats. Cooperative frameworks, therefore, provide the structural foundation for shared learning, cost efficiency, and technological standardization, enabling partners to transform individual advancements into collective strategic advantage.

Multinational alliances and cooperative mechanisms play a decisive role in institutionalizing defense innovation. The NATO Defence Innovation Accelerator for the North Atlantic (DIANA) and the European Defence Fund (EDF) are two leading examples of this institutionalization. DIANA serves as a transatlantic network linking innovators, start-ups, and research institutions to accelerate dual-use technologies, such as artificial intelligence, quantum computing, and biotechnology. Similarly, the EDF fosters collaborative research and development among EU member states, reducing duplication, enhancing interoperability, and strengthening Europe's strategic autonomy. Both initiatives illustrate how coordinated policy frameworks can turn fragmented national efforts into coherent multinational innovation ecosystems.

Beyond multilateral institutions, bilateral defense partnerships have also proven instrumental in shaping the global innovation landscape. The U.S.–Israel defense partnership, for instance, represents a model of technological synergy, merging Israel's rapid prototyping and battlefield testing capabilities with American industrial scale and funding. The collaboration has yielded landmark technologies such as the Iron Dome missile defense system, which exemplifies how shared innovation can save lives while reinforcing strategic deterrence. Similarly, the U.S.–Ukraine technology cooperation, intensified since 2022, has facilitated the rapid deployment of advanced cyber-defense architectures, electronic warfare systems, and unmanned platforms—demonstrating how strategic alliances can adapt in real time to confront evolving threats.

The advantages of such international cooperation are multidimensional and extend well beyond technical innovation. Key benefits include: Shared Knowledge and Expertise: By pooling intellectual, financial, and technical resources, nations—particularly smaller or developing defense actors—gain access to advanced capabilities and research networks that would otherwise remain unattainable. This democratization of innovation enhances collective resilience and levels the technological playing field.

⁴ Bharti, *China Russia bilateral security and military partnership in changing world orders: security challenges for the United States of America in Asia and beyond*. Historia I politika. 2022.

Interoperability: Standardizing defense technologies, data systems, and communication protocols ensures that allied forces can operate seamlessly during joint missions. Interoperability not only enhances operational efficiency but also strengthens strategic unity and cohesion within alliances.⁵

Risk and Cost Sharing: Defense innovation involves high financial risk and uncertain outcomes. By distributing development costs and experimental risks among partners, cooperative frameworks encourage sustained innovation without overburdening national budgets.

Strategic Deterrence: Collective innovation sends a powerful signal of unity and technological competence. It demonstrates that alliances possess not only military strength but also the creative and industrial capacity to respond dynamically to adversarial challenges.

However, the benefits of cooperation are accompanied by complex challenges. Balancing national sovereignty with shared governance remains a delicate task, as states must reconcile the desire for technological autonomy with the need for collective advancement. Additionally, protecting sensitive data, intellectual property rights, and defense-related information across national boundaries raises persistent concerns about security, trust, and reciprocity. Disparities in defense budgets, strategic priorities, and regulatory frameworks can further complicate joint initiatives, occasionally slowing decision-making and implementation.⁶

To ensure the success of these cooperative efforts, robust governance mechanisms and transparent institutional structures are essential. Effective frameworks must safeguard national interests while fostering openness and trust among partners. Clear legal and ethical standards for technology transfer, export control, and intellectual property management are equally critical to maintaining equilibrium between innovation and security.

In essence, international cooperation functions as both the engine and the safeguard of defense innovation. It transforms innovation from a competitive national pursuit into a shared strategic enterprise—one that enhances global resilience, fosters technological excellence, and reinforces the collective ability to deter aggression in an increasingly uncertain world. By bridging the gap between innovation and security, cooperative defense ecosystems lay the groundwork for a more stable, technologically advanced, and interconnected global order.

The practical application of defense innovation can best be understood through a series of international case studies that exemplify how technological creativity, institutional flexibility, and strategic coordination converge to produce measurable security outcomes. Each of the following cases demonstrates a distinct model of how states and alliances operationalize innovation to address contemporary security challenges.

NATO's DIANA Initiative: The NATO Defence Innovation Accelerator for the North Atlantic (DIANA) stands as a pioneering transatlantic initiative aimed at accelerating the development and deployment of dual-use technologies. Through its network of innovation hubs and test centers across Europe and North America, DIANA promotes collaboration between defense institutions, private enterprises, and academic researchers. The initiative focuses particularly on emerging technologies such as cyber resilience, artificial intelligence (AI), quantum communication, and

⁵ Collective defence and article 5. 2023. Nato.

⁶ Gruszczak, kolascynski. 2022. *Understanding contemporary security: a prolegomenon to the interplay between technology, innovation and policy responses*. Politeja.

biotechnology. By linking innovators directly to NATO's operational needs, DIANA ensures that technological breakthroughs translate into practical defense capabilities, strengthening the Alliance's long-term resilience and readiness.

Israel's Defence Innovation Model: Israel represents one of the world's most dynamic and integrated ecosystems of defense innovation, where military R&D, government strategy, and private entrepreneurship operate in close symbiosis. The Israel Defense Forces (IDF), working alongside the Directorate of Defense Research and Development (DDR&D) and the private sector, exemplify how real-time battlefield feedback fuels rapid technological advancement. Systems such as the Iron Dome, David's Sling, and cyber-defense platforms illustrate Israel's capacity to transform operational necessity into technological excellence. This model highlights the power of continuous prototyping, adaptive experimentation, and dual-use innovation—where military technologies also stimulate economic growth and export potential.

Nordic Defence Cooperation (NORDEFCO): The Nordic Defence Cooperation (NORDEFCO) provides a regional example of how smaller states can collectively achieve strategic effectiveness through coordination, trust, and technological synergy. Established in 2009 by Denmark, Finland, Iceland, Norway, and Sweden, NORDEFCO fosters collaboration in defense research, logistics, cyber defense, and digital infrastructure protection. Through joint exercises and shared procurement initiatives, the Nordic states have developed cost-effective defense solutions while maintaining national sovereignty. This cooperative model demonstrates how innovation can flourish in environments characterized by transparency, equality, and shared values, enabling smaller states to collectively amplify their strategic impact.

Ukraine's Wartime Adaptation: Ukraine's response to the full-scale Russian invasion has become a defining example of innovation under pressure. Confronted with asymmetric warfare, Ukraine rapidly mobilized its scientific, industrial, and civilian sectors to produce technological solutions in real time. Domestic drone manufacturing expanded exponentially, while open-source intelligence and crowd-sourced data analysis became integral to tactical decision-making. The integration of AI into targeting systems and the use of commercial technologies for military communication have redefined the nature of modern warfare. Ukraine's experience proves that innovation does not always emerge from abundance but often from necessity—where adaptability, resourcefulness, and public-private cooperation become decisive elements of national survival.⁷

Each of these cases underscores a unifying principle: defense innovation thrives where technological creativity intersects with institutional flexibility and strategic coordination. Whether through alliance-driven initiatives like DIANA, regional collaborations like NORDEFCO, or national innovation ecosystems as seen in Israel and Ukraine, success depends on the ability to merge technological progress with organizational agility and long-term strategic vision.

While innovation strengthens defense capabilities and enhances security, it simultaneously introduces complex ethical, legal, and regulatory dilemmas. The rapid pace of technological advancement—especially in artificial intelligence, automation, and cyber warfare—poses fundamental questions about the boundaries of human control, accountability, and moral responsibility in military decision-making.

⁷ Collective defence and article 5. 2023. Nato.

Autonomy in Lethal Systems: The emergence of Lethal Autonomous Weapon Systems (LAWS) has ignited an intense ethical debate over whether machines should be granted the authority to make life-and-death decisions. While autonomy can enhance precision and reduce human casualties, it also risks dehumanizing warfare and creating accountability gaps in cases of malfunction or wrongful targeting.

Cyber Warfare and Accountability: Cyber operations blur traditional distinctions between offense and defense, raising difficult questions about attribution and responsibility. When AI-driven systems launch automated counterattacks or trigger unintended escalation, determining legal liability becomes nearly impossible. The absence of international norms governing autonomous cyber actions further complicates the issue.⁸

Data Sovereignty and Privacy: The exchange of sensitive data within international defense partnerships introduces new vulnerabilities related to data ownership, jurisdiction, and privacy. States must balance the need for intelligence sharing with the protection of classified information and individual rights—a challenge magnified by cross-border cloud infrastructure and global digital interdependence.

Inequality in Access: Technological disparities between large powers and smaller allies risk reinforcing dependence and strategic asymmetry. Without equitable access to innovation ecosystems, smaller states may remain technologically subordinate, limiting their capacity for autonomous defense planning and innovation.

To mitigate these risks, defense innovation must be accompanied by transparency, ethical oversight, and adherence to international humanitarian law. Ethical governance should not be treated as a constraint but as an essential component of sustainable security development. International treaties, regulatory frameworks, and public accountability mechanisms must evolve in parallel with technological advancement to ensure that innovation serves humanity rather than undermines it.⁹

The future of global defense will depend on achieving a balance between technological ambition and moral responsibility. Nations that integrate ethical considerations into their innovation strategies will not only gain legitimacy but also build more resilient and trusted defense ecosystems. In this sense, technological progress and ethical governance are not opposing forces—they are mutually reinforcing foundations of a secure, stable, and humane international order.

Conclusion

The future of global security will be defined not by the accumulation of weaponry but by the capacity of nations and alliances to innovate, cooperate, and adapt in an environment of constant technological change. The evolution of defense—from industrial-age arsenals to intelligent, networked, and data-driven systems—marks a decisive transformation in how states conceptualize power and deterrence. Innovation, therefore, is no longer a secondary or supportive function of defense policy; it has become its strategic nucleus.

At the core of this transformation lies a simple but profound truth: security in the 21st century is collective, not solitary. The interconnected nature of modern threats—ranging from cyberattacks and disinformation campaigns to climate-induced instability and autonomous warfare—demands

⁸ Mearsheimer. 2001. *The tragedy of great power politics*.

⁹ Rid. 2017. *Cyber war will not take place*. *Strategic studies*. <https://www.jstor.org/stable/26593685>

collaborative solutions. No single nation, regardless of its resources, can unilaterally defend against globalized risks that transcend borders, domains, and institutions. International cooperation, built upon mutual trust, transparent governance, and shared technological progress, thus represents the cornerstone of sustainable security architecture.

Defense innovation is both a technological and institutional process. It requires more than research funding and industrial modernization; it demands long-term investment in education, scientific collaboration, and ethical governance. Nations must cultivate ecosystems that integrate public policy, private entrepreneurship, and academic research, fostering a continuous feedback loop between theory, experimentation, and application. Such ecosystems transform innovation from an occasional breakthrough into a systemic capability—embedded in national institutions and reinforced by international partnerships.¹⁰

Alliances such as NATO, NORDEFCO, and the European Defence Fund (EDF) demonstrate that coordinated innovation can amplify national capabilities while preserving autonomy. Similarly, bilateral partnerships like the U.S.–Israel defense collaboration and the technological alliance between Ukraine and its Western partners illustrate how cross-border cooperation accelerates the translation of innovation into operational readiness. These frameworks collectively embody a principle that should guide the next generation of security strategies: technological interdependence is not vulnerability—it is strength when governed by shared values and mutual accountability.¹¹

However, the institutionalization of innovation must be accompanied by ethical foresight. The growing integration of artificial intelligence, automation, and cyber technologies into defense introduces moral and legal dilemmas that cannot be ignored. The legitimacy of defense innovation rests on its alignment with international law, humanitarian principles, and human-centered control. The challenge is not only to innovate faster than potential adversaries but also to innovate responsibly, ensuring that the pursuit of technological advantage does not compromise human dignity or global stability.

To build the foundations of future security, states and alliances must commit to three essential principles:

Institutionalized Innovation: Embed research, experimentation, and technological adaptation within the long-term structure of defense governance. Innovation should be continuous, evidence-based, and strategically aligned with broader security objectives.

Collaborative Resilience: Foster networks of cooperation that extend beyond military institutions, encompassing the private sector, academia, and civil society. Resilience emerges from diversity—of ideas, expertise, and perspectives—united by shared security goals.

Ethical Governance: Establish transparent standards for the use of AI, autonomous systems, and cyber technologies in defense. Uphold accountability through international oversight and ensure that technological development remains subordinate to human judgment and moral responsibility. In essence, the defense systems of tomorrow will be built not merely through technological superiority but through strategic foresight, institutional adaptability, and global solidarity. The integration of innovation and cooperation will define which nations and alliances can anticipate,

¹⁰ Mearsheimer. 2001. *The tragedy of great power politics*.

¹¹ Collective defence and article 5. 2023. Nato.

absorb, and overcome the challenges of the coming decades.

The 21st century thus calls for a new security paradigm—one that views innovation as a shared enterprise and international cooperation as its enabling framework. If guided by ethical vision and mutual trust, this model can transform global defense from a competitive race for dominance into a collaborative effort for stability, prosperity, and peace.

Bibliography

- Collective defence and article 5. 2023. Nato. https://www.nato.int/cps/en/natohq/topics_110496.htm (accessed 15.10.2025)
- Mearsheimer. 2001. *The tragedy of great power politics*. <https://surl.li/aqwjav> (accessed 15.10.2025)
- Walt. 1987. *The origins of alliances*. Cornell University Press. https://api.pageplace.de/preview/DT0400.9780801469992_A29967168/preview-9780801469992_A29967168.pdf
- Nxuan.. 2024. *The dual role of military alliances in contemporary international relations*. 3rd International Conference on International Law and Legal Policy. <https://surl.lu/mxatpn> (accessed 15.10.2025)
- Bharti . 2022. *China Russia bilateral security and military partnership in changing world orders: security challenges for the United States of America in Asia and beyond*. Historia I politika. <https://surl.lu/zcmzyk> (accessed 05.10.2025)
- Gruszczak, kolascynski. 2022. *Understanding contemporary security: a prolegomenon to the interplay between technology, innovation and policy responses*. Politeja. <https://surl.li/qgiwuu> (accessed 15.10.2025)
- Rid. 2017. *Cyber war will not take place*. *Strategic studies*. <https://www.jstor.org/stable/26593685>

MODERNIZATION OF WARFARE AND MILITARIZATION IN 21ST CENTURY

Senior Lieutenant Veriko Tordia

The Learner of a Master's Degree Program (State Recourse Management) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The evolution of global security in the 21st century is increasingly defined by rapid technological transformation and deepening international collaboration. Traditional defence paradigms that relied primarily on manpower and conventional weaponry have proven inadequate against the hybrid and asymmetric threats of the modern era, ranging from cyberattacks and drone warfare to disinformation campaigns and climate-induced instability. This paper examines how defence innovations and international partnerships function as complementary pillars in shaping a secure and stable future.

Defence innovations- such as Israel's Iron Dome missile defence system, the use of unmanned aerial vehicles in Ukraine and the application of commercial space technologies like Starlink. Illustrate how technological ingenuity enhances deterrence, operational precision and resilience. These cases demonstrate that innovation not only redefines battlefield effectiveness, but also protects civilian populations and strengthens national morale under sustained threat. Yet, innovation without collaboration risks fragmentation and inefficiency.

Consequently, the second major theme of this paper emphasizes international partnerships as essential multipliers such as NATO, bilateral research and development co-operation between the United States and Israel and multinational frameworks supporting Ukraine, states are able to share intelligence, pool resources and establish interoperability.

Together, these innovations and partnerships create a framework for collective resilience. They allow nations not only to respond to emerging threats, but also to set global norms for responsible technological use in defence. The study concludes that sustainable security in the 21st century depends on the synergy between technological advancement and co-operative diplomacy, ensuring that innovation serves the broader purpose of peace, stability and shared security.

Keywords: Defence Innovation, International Co-operation, Technological resilience, Hybrid warfare, Global stability.

Introduction

In the 21st century, the landscape of global security is undergoing a rapid transformation which is driven by technological innovations, geopolitical shifts and emerging transnational threats. Traditional concepts of defence which, once focused on military strength and territorial control, now are evolving into complex networks of collaboration, information sharing and tech adaptation. The convergence of innovation and international partnership has become not only a strategic advantage, but a necessity for maintaining global stability. As the nation's confront challenges, such as, cyber warfare, artificial intelligence in combat systems, hybrid threats and climate-related security risks, the importance of co-operation and innovation in defence domain has never been more apparent.

Nowadays defence innovation extends far beyond the development of weapons or military hardware. It bounds advancements in digital infrastructure, data analytics, autonomous systems, space technologies and resilient communication networks. These innovations are reshaping how defence forces operate, respond or deter threats. However, innovation alone is insufficient without effective international collaboration. Modern defence strategies increasingly rely on alliances, joint research initiatives and shared technological standards to ensure interoperability and collective readiness. Organizations such as NATO, the European union, and other regional defence frameworks, demonstrate how international co-operation enhances both innovation and strategic resilience.

International partnerships also serve as a vital platform for addressing ethical, legal and political dimensions and values of defence technology. Emerging innovations, e.g. artificial intelligence in decision-making or the militarization of space, raise complex and logical questions about accountability, sovereignty and balance of power. Through partnerships, nations can establish norms and frameworks, which promote responsible innovation, prevent escalation and ensure transparency. Moreover, the collaboration facilitates resource sharing and knowledge transfer, allowing smaller states to access cutting-edge technologies and contribute meaningfully to global security architecture.

In the situation, defined by uncertainty, defence innovation and partnership represent the twin pillars of a secure future. As the global defence environment becomes increasingly interconnected, the capacity of nations to adapt, evolve and co-operate, will determine not only their security but also the stability of the international system. The binding of technological advancement with diplomatic collaboration, creates opportunities to deter threats before they escalate, respond to crises with agility and build mutual trust among allies and partners.

Ultimately, shaping the future of security requires more than technological superiority- it demands a shared vision of peace, responsibility and resilience. By fostering innovation and strengthening international partnerships, the global defence community can create a safer, more predictable world, once prepared not merely to survive the challenges of the future, but to shape them with foresight and the unity.

Main Part

The security environment, nowadays, is more complex and more interconnected than at any previous moment. Threats now combine conventional force with cyber operations, informational campaigns, terrorism and climate-driven instability. In this setting, two interdependent strategies have emerged as decisive: rapid, adaptive defence innovation and defence international partnership. Innovation supplies the technological and doctrinal tools to detect, deter and respond. Partnerships multiply those tools' reach, ensure interoperability and help govern the ethical, legal and political dimensions of new capabilities.

There are several notions which underlines why defence innovation matters. Modern conflicts reward rapid adaptation: technologies that are cheap, mobile and networked can create outstanding and outsized effects of the battlefield. Small, inexpensive systems, such as drones, sensors and cyber tools, can negate traditional force multipliers and enable asymmetric defence / offence. As a results military which can innovate and evolve quickly, gain tactical and operational advantages, even while being outnumbered by military personnel and combat effectiveness of troops. Innovation in comms, adhering command and control principle, redundant infrastructure increase resilience against targeting. Maintaining civilian and military communication in contested environments, prevents operational paralysis and sustains morale. Also, advances in precision strike, ISR (intelligence, surveillance, reconnaissance) and autonomous logistical chain increase effectiveness, while decreasing collateral damage, both on operational and political level. This precision helps states deter escalation by offering limited, controllable responses instead of broad kinetic retaliation.

Below we will discuss the examples of defence innovations:

- **Iron Dome** – Israel's Iron Dome is perhaps the iconic modern example of how a targeted technological innovation can reshape deterrence and civilian security. Designed to detect, track and intercept short-range rockets and artillery, Iron Dome demonstrably reduced civilian casualties and infrastructure losses in repeated conflicts. The system's success rests on integrated radar, rapid-fire interceptors and a command algorithm that prioritizes intercepts based on projected impact points, thereby economizing expensive interceptors and protecting populated areas efficiently. Crucially, Iron Dome's development and deployment were enabled by domestic industry (Rafael/Israel Aerospace) and sustained international funding and co-operation, which allowed rapid fielding and scale-up. The result- improved civilian protection, political space for calibrated responses and a model that many countries now evaluate as part of layered air defences.¹

- **Unmanned systems and loitering munitions (Ukraine & Turkey)**- the Russo-Ukrainian war has vividly shown how relatively low-cost unmanned platforms, reconnaissance drones, armed UAVs and loitering munitions, can shift battlefield dynamics. Turkey's Bayraktar TB2, for instance, provided Ukraine with precision strike capability, that proved operationally influential in 2022 and thereafter. Equally important, locally adapted commercial drones and commercially sourced sensors have been repurposed into reconnaissance, targeting and EW (electronic warfare) roles. These systems democratize certain forms of aerial capability, allowing medium-sized and

¹ Belfer Center for Science and International Affairs. 2022. Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose. Harvard Kennedy School.

smaller states to punch above their weight, when they pair innovations with flexible tactics. The Bayraktar case also illustrates how export and donor relationships can shape diffusion of new military technologies;²

- **Commercial space and resilient communications (STARLINK in Ukraine)** – Ukraine’s rapid adoption of SpaceX’s Starlink broadband service following the 2022 invasion demonstrates how commercial space capabilities can provide critical resilience. By rapidly restoring high-bandwidth, low-latency communications where terrestrial networks were disrupted, Starlink enabled civilian connectivity, command and control continuity and improved situational awareness for military and humanitarian actors. The Starlink story highlights how commercial innovation, if accessible and responsibly partnered, becomes an operational lifeline in modern conflict, and how private-sector platforms are now part of national resilience planning.³

Collectively, these examples show that defence innovations are not only about superior weapons, they are tools of protection, continuity and proportionality that can reduce civilian harm and stabilize crises when paired with prudent doctrine and order.

Why international partnerships matter?! While innovation is vital, its effectiveness is multiplied, or sometimes made possible, by international partnerships. Partnerships provide financing, interoperability standards, intelligence-sharing, logistical sustainment and political legitimacy. They also create forums to negotiate norms for novel technologies (e.g. AI in weapons, cyber conduct, usage of space), which are indispensable for long-term stability.

- **Pooling resources and R&D collaboration (U.S.-Israel and allied R&D)** – collaboration between Israel and partners, especially the United States, illustrates how bilateral and multilateral ties accelerate fielding and sustainment of high-impact systems. The U.S.-Israel defence relationship has included joint R&D, co-production and political support for missile-defence programs. Legislative and policy instruments in partner states (including recent congressional actions) strengthen this integration, enabling both operational synergy and industrial co-development. Shared investment lowers individual states’ costs and speeds deployment of complex systems that a single country might struggle to develop or field alone.⁴⁵

- **Alliance burden-sharing and interoperability (NATO and Ukraine assistance)** – NATO’s role in coordinating training, logistics and capability transfers to partner states underlines how alliances can multiply defensive effects. Since 2022, NATO and allied frameworks (including the comprehensive assistance package and other coordination mechanisms) have provided Ukraine with equipment, training, intelligence sharing and logistical support measures that extend beyond single-state donations and reflect systemic burden-sharing. Interoperable systems and common standards (e.g. for communications, ammunitions and training) create more effective coalitions and ensure that innovations are usable across national forces. Partnerships thereby transform isolated innovations into coalition-level capabilities.^{6,7}

2 „Israel Defense Partnership Act“. 119th Congress, 1st Session. U.S. Congress. 2025. S. 554 Congress.gov.— Accessed 04.11.2025

3 Rafael USA. 2025. “Iron Dome Air Defense System.” Rafael Advanced Defense Systems.

4 A Study of International Security Mechanisms.” Dauliyah: Journal of Islam and International Affairs 9 (2): 155–170. Accessed 04.11.2025

5 The Global Coalition to Defeat ISIS. 2025. “Partners.” Accessed 04.11.2025

6 “NATO and Ukraine: Partnership for Peace and Security.” North Atlantic Treaty Organization. NATO. 2024.

7 “The Turkish Drone That Changed the Nature of Warfare.” The New Yorker, May 16, 2022, The New Yorker. 2022..

- **Multinational coalitions against non-state threats (Global Coalition to Defeat ISIS)**
– complex transnational threats, terrorist networks, transnational organized crime, illicit finance, cannot be solved by any single state. The Global Coalition to Defeat ISIS and similar multilateral efforts show how pooling intelligence, legal tools and stabilization funding can degrade extremist groups and help stabilize liberated areas. Such coalitions combine military pressure with financial sanctions, policing co-operation and local capacity-building, demonstrating that partnerships enable a multi-dimensional response, that purely unilateral military action cannot replicate.⁸

Conclusion

The interaction effect: why combining innovation + partnerships shapes a secure future

The decisive point is that innovation and partnerships are complementary. Innovations without partners risk isolation, deployment may be slow, numbers limited and political support fragile. Conversely, partnerships without innovation risk obsolescence and inability to respond to asymmetric, rapidly evolving threats. Then combined, they produce four key effects:

1. **Scalability** – partners provide funding, production capacity and geographic coverage needed to scale promising technologies (as with Iron Dome's purchases and allied support or coalition procurement of communications gear);
2. **Interoperability** – shared standards and joint procurement (e.g. multinational fighter programs, NATO logistics frameworks, STANAG agreements) ensure that innovations can be used across allied forces without friction;
3. **Ethical governance and norm-setting** – multilateral forums allow partners to negotiate responsible use (e.g. limits on autonomous targeting, rules for privacy and cyber operations), reducing risks of destabilizing deployment;
4. **Strategic resilience** – partnerships create redundancy: when a single supply line (energy, communications, munitions) is targeted, allied systems and multinational logistics can compensate- thus denying adversaries' decisive leverage.

Lastly, we need to discuss limitations and caveats, of course practical risks remain; Rapid diffusion of military technologies (drones, cyber tools) can empower non-state actors; over-reliance on commercial providers creates political vulnerability. And partnerships can entangle states in conflicts or create dependencies that reduce strategic autonomy. Therefore, states must blend innovation and partnerships with robust export controls, contingency planning and diplomatic strategies that preserve political freedom of action, while maximizing shared security.

In an age of defined by uncertainty and rapid technological change, the future of security depends on the capacity of nations to innovate and co-operate. Defence innovations, ranging from advanced air defence systems to unmanned technologies and resilient communication networks, have transformed how states protect their citizens and assert sovereignty. However, these innovations reach their full potential only when supported by robust international partnerships that ensure shared intelligence, interoperability and ethical governance.

The case studies explored, such as Israel's Iron Dome, Ukraine's use of drones and satellite

⁸ "The Global Coalition to Defeat ISIS: Partners." U.S. Department of State. 2025.

networks, demonstrate that security is no longer a purely national endeavour. It is a collective enterprise that unites technological progress with diplomatic collaboration. Partnerships among states, alliances like NATO and co-operative research frameworks create the foundation for sustainable stability by distributing resources, responsibilities and risks across a trusted network of actors.⁹

In conclusion, the past two decades show that no single approach, technological or diplomatic, alone will secure the future. Defence innovations change the rules of engagements by providing new tools of protection and precision; international partnerships provide the scale, legitimacy and governance needed to deploy those tools responsibly and effectively.¹⁰ Together they form the architecture of a resilient, adaptive security posture capable of deterring aggression, protecting civilians and managing the ethical challenges of new capabilities. Policymakers should therefore invest simultaneously in domestic innovation ecosystems and in durable alliances and multilateral mechanisms that turn technological promise into collective security.

Bibliography

Belfer Center for Science and International Affairs. 2022. Starlink and the Russia-Ukraine War: A Case of Commercial Technology and Public Purpose. Harvard Kennedy School. <https://surl.li/wxmnp>, Accessed 04.11.2025.

Congress.gov. 2025. S. 554 — Israel Defense Partnership Act. 119th Congress, 1st Session. U.S. Congress. <https://surl.li/jiyisq>, Accessed 04.11.2025.

Dauliyah: Journal of Islam and International Affairs. 2024. “Defense Cooperation and Global Peace: A Study of International Security Mechanisms.” Dauliyah: Journal of Islam and International Affairs 9 (2): 155–170. <https://surl.li/qxkvus>, Accessed 04.11.2025.

The Global Coalition to Defeat ISIS. 2025. “Partners.” <https://surl.lu/gfmpsi>, Accessed 04.11.2025.

NATO. 2024. “NATO and Ukraine: Partnership for Peace and Security.” North Atlantic Treaty Organization. <https://surl.li/xfduhw>, Accessed 04.11.2025.

Rafael USA. 2025. “Iron Dome Air Defense System.” Rafael Advanced Defense Systems. <https://surl.li/xrvfoi>, Accessed 04.11.2025.

State Department, U.S. 2025. “The Global Coalition to Defeat ISIS: Partners.” U.S. Department of State. <https://surl.li/waupva>, Accessed 04.11.2025.

The New Yorker. 2022. “The Turkish Drone That Changed the Nature of Warfare.” The New Yorker, May 16, 2022. <https://surl.lt/njfcsl>

Tandfonline. 2023. “Emerging Technologies and the Ethics of Modern Warfare.” Bulletin of the Atomic Scientists 79 (2): 101–108. <https://surl.li/pqodel>

Wilson, Joe. 2024. Israel Defense Partnership Act. U.S. House of Representatives. <https://surl.lt/vomxtq>, Accessed 04.11.2025.

⁹ Tandfonline. 2023. “Emerging Technologies and the Ethics of Modern Warfare.” Bulletin of the Atomic Scientists 79 (2): 101–108.

¹⁰ Wilson, Joe. 2024. Israel Defense Partnership Act. U.S. House of Representatives. Accessed 04.11.2025

MODERN WARFARE AND THE ROLE OF EMERGING TECHNOLOGIES

Lile Bubuteishvili

The Junker of a Bachelor's Degree (Informatic Technologies) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Giorgi Nozadze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The twenty-first century has fundamentally transformed the nature and conduct of warfare. Unlike earlier eras defined by manpower and industrial might, contemporary conflicts are increasingly shaped by the integration of digital technologies, automation, and artificial intelligence. Emerging innovations—such as AI, autonomous systems, cyber operations, big data analytics, and space-based capabilities—are reshaping military strategy, operational tactics, and the ethical frameworks governing armed conflict. This paper explores the multifaceted impact of these technologies on modern warfare, with particular attention to their strategic and operational implications, associated legal and ethical dilemmas, and the evolving role of international cooperation. The ongoing Russia–Ukraine war (2022–present) serves as a central case study, demonstrating how rapid technological adaptation, decentralized innovation, and civil–military collaboration are redefining the dynamics of asymmetric conflict.

The analysis concludes that, while technological advancement enhances military effectiveness and can reduce human casualties, it simultaneously necessitates robust legal structures, responsible human oversight, and multilateral governance mechanisms to prevent escalation and safeguard humanitarian norms.

Keywords: artificial intelligence, modern warfare, automation, cyber operations, Russia–Ukraine war, asymmetric conflict, international security, military ethics, technological innovation, humanitarian law.

Introduction

Warfare in the modern era transcends traditional battlefields and physical weaponry. It has evolved into a multidimensional domain in which information, networks, and algorithms are as decisive as tanks and missiles. Military power is no longer measured solely by the size of a standing army or the volume of munitions; rather, it is increasingly determined by a state's ability to collect, process, interpret, and act upon information faster than adversaries.¹ The convergence of AI, robotics, cyber capabilities, and space-based infrastructure has created an operational environment that is interconnected across land, sea, air, space, and cyberspace. This fusion has important implications for doctrine, strategy, and the ethical responsibilities of commanders and policymakers. The ongoing conflict between Russia and Ukraine provides a salient example of these dynamics. Ukraine's effective use of commercial and military drones, satellite-enabled communications such as Starlink², open-source intelligence, and agile command-and-control networks illustrates how innovation and adaptation can offset material disadvantages. Conversely, Russian operations have demonstrated the strategic utility of cyberattacks, information operations, and long-range precision fires. Together, these developments highlight how modern warfare elevates the importance of technological literacy, civil–military integration, and international cooperation in determining outcomes.

Main Part

Evolution of Warfare: From Industrial to Information-Age Conflict

Historically, warfare has evolved alongside technological and societal transformations. The Industrial Revolution allowed for mass production and mobilization; railways, telegraphy, and mechanized artillery redefined operational reach and logistical sustainment. The twentieth century introduced the nuclear deterrent, changing calculus on escalation and direct confrontation. In the twenty-first century, however, information has become the decisive resource. Network-centric concepts emphasize the value of integrated sensors³, communications, and decision-support tools—allowing dispersed forces to act with unity of purpose and speed.

A defining feature of modern conflict is the blurring of the boundary between civil and military domains. Commercial infrastructures—satellite communications, cloud services, critical national infrastructure—now support military operations. Similarly, social media and information platforms can serve as vectors for persuasion, mobilization, and deception. These trends facilitate hybrid strategies⁴: combinations of conventional military operations, cyber intrusions, economic coercion, and targeted information campaigns that aim to achieve political objectives without open, protracted combat. The Russia–Ukraine conflict has exemplified hybrid warfare writ large. Before and after the 2022 invasion there were concerted cyber operations targeting Ukrainian institutions, disinformation campaigns designed to influence domestic and international audiences, and the application of precision-guided munitions alongside small commercial drone strikes. Ukraine's decentralized mobilization of reserves, volunteer technical communities, and private-sector partnerships demonstrates how information-age tools amplify resilience and adaptive capacity.

1 RAND Corporation, *The Future of Warfare in the 21st Century: Emerging Technologies and Security Challenges*, 2023.

2 World Economic Forum, *Global Risks Report: Technology, Geopolitics, and Security*, 2024.

3 U.S. Department of Defense, *Artificial Intelligence Strategy for the Department of Defense*, 2022.

4 NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Defence and Emerging Technologies Report*, 2023.

Key Emerging Technologies in Modern Warfare

Artificial Intelligence (AI)

AI has become central to contemporary military modernization. Machine learning transforms raw sensor data—satellite imagery, signals intelligence, and social media—into actionable insights. Applications include automated target recognition, predictive maintenance, supply-chain optimization, and decision-support tools that help commanders evaluate courses of action under time pressure. By compressing parts of the observe-orient-decide-act (OODA) loop, AI can enable “decision dominance,”⁵ a term used in defence literature to describe the capacity to act more quickly and coherently than an adversary.

Yet AI also introduces complexity. The opacity of some machine-learning models, especially deep neural networks, raises issues for explanations. Bias in training data can produce systematic errors, and adversarial inputs (small perturbations intentionally designed to fool an algorithm) represent a real operational risk. Military planners therefore emphasize hybrid architectures—AI-assisted systems that support but do not replace human judgment—particularly for lethal targeting decisions⁶.

Cyber Capabilities

Cyber capabilities encompass a wide spectrum: vulnerability assessment and resilient design on the defensive side, and offensive operations intended to disrupt, degrade, or manipulate adversary systems. Cyberattacks can target communications, logistics, financial systems, and civilian infrastructure, often with effects disproportionate to their cost. The NotPetya attack of 2017—widely attributed to Russian-aligned actors—caused extensive commercial damage beyond Ukrainian targets⁷, demonstrating the potential for collateral economic consequences in cyber campaigns.

Attribution remains a major challenge in cyber operations. Anonymous or deniable attacks complicate deterrence strategies and increase the risk of misattributed retaliation. Defensive measures therefore include not only technical hardening but also legal frameworks, norms for behavior in cyberspace, and international incident-response cooperation.

Autonomous Systems and Drones

Unmanned systems have democratized access to reconnaissance and strike capabilities. Drones of varying sizes and sophistication carry out surveillance, electronic warfare, resupply missions, and kinetic effects. In Ukraine, commercial quadcopters and improvised loitering munitions were adapted for combat roles⁸, demonstrating how low-cost platforms can alter the tactical calculus. Trailer-launched long-range drones and swarm tactics have challenged traditional air-defence architectures, requiring novel countermeasures and adaptive tactics.

Autonomy increases operational efficiency, but fully autonomous lethal systems (LAWS) raise ethical and legal concerns. Key debates center on whether machines should be permitted to ap-

5 Singer, P. W., & Chapa, J., *AI and the Future of Conflict*, Brookings Institution, 2021.

6 International Committee of the Red Cross, *Ethical Challenges of Autonomous Weapons and AI in Armed Conflict*, 2024.

7 NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Defence and Emerging Technologies Report*, 2023.

8 European Defence Agency, *Innovation in Defence: The Role of AI and Emerging Technologies*, 2023.

ply lethal force without meaningful human oversight. Technical challenges—reliable target discrimination in congested environments, robust fail-safes under electronic attack, and transparent logging—must be solved before autonomous systems can be accepted widely under international humanitarian law.

Big Data, Cloud, and Edge Computing

The integration of diverse data streams—satellites, sensors, human intelligence, and open-source information—enables richer situational awareness. Cloud computing provides the capacity to store and process massive datasets, while edge computing allows for real-time analytics at or near the point of sensing, reducing latency in decision cycles. Predictive analytics can forecast equipment failures⁹, anticipate adversary movements, and optimize logistics. However, data dependence elevates the importance of secure architectures, data integrity, and redundancy; compromised inputs can propagate erroneous conclusions throughout command structures.

Space-based Capabilities

Satellites underpin modern communications, navigation, and imagery intelligence. The reliance on space assets has made space a contested domain: anti-satellite weapons, jamming, and cyber threats to satellite ground stations pose clear risks. The proliferation of commercial LEO constellations¹⁰—some used to maintain connectivity in Ukraine—demonstrates both opportunity and vulnerability: commercial partnerships can increase resilience but also raise questions about jurisdiction, liability, and wartime protections for civilian providers.

Benefits and Strategic Advantages

Emerging technologies offer multiple strategic advantages. Enhanced intelligence and targeting reduce uncertainty and collateral damage. Automation of logistics and maintenance improves platform readiness and extends operational endurance. For alliances, shared data standards and interoperable systems enable combined operations and burden-sharing. Crucially, these technologies allow actors that lack conventional superiority to pursue asymmetric strategies: information operations, precision strikes enabled by drones, and cyber disruption can offset numerical inferiority.

Moreover, technology can reduce human exposure to danger—robotic logistics, remotely piloted ISR (intelligence, surveillance, reconnaissance), and medical evacuation innovations all contribute to force preservation. In aggregate, these advantages improve deterrence and complicate adversary planning.

Challenges, Vulnerabilities, and Strategic Risks

Notwithstanding their benefits, technologies create new vulnerabilities. Interconnected systems produce single points of failure: a successful cyberattack against a command network can paralyze operations. AI systems, while powerful, are brittle outside their training domains and can be deceived by adversarial techniques. Proliferation of inexpensive lethal systems increases risks to civilians and complicates law enforcement-like responses in urban environments.

⁹ RAND Corporation, *The Future of Warfare in the 21st Century*, 2023.

¹⁰ United Nations Office for Disarmament Affairs, *Responsible Innovation and Autonomous Weapons Systems*, 2024.

Technological change also accelerates arms-race dynamics. As advanced capabilities diffuse, norms and arms-control measures struggle to keep pace. An important risk is entanglement: automated or delegated systems in high-stakes environments (for instance, early-warning systems attached to strategic forces) can misinterpret signals and induce inadvertent escalation. Effective risk mitigation therefore requires redundancy, fail-safe human oversight, rigorous testing, and transparent confidence-building measures among states.

Ethical, Legal, and Normative Implications

The integration of new technologies into warfare challenges existing legal and ethical frameworks. International Humanitarian Law (IHL) is built around principles of distinction¹¹, proportionality, and military necessity; translating these principles into algorithmic rules is non-trivial. Accountability becomes diffuse when software, contractors, and commanders share responsibility for outcomes. The normative landscape is contested: some states, NGOs, and experts push for preemptive bans on autonomous lethal systems, while others advocate for detailed regulation emphasizing human oversight and traceability.

The Russia–Ukraine conflict has highlighted acute dilemmas—drone strikes in populated areas, cyberattacks affecting civilian utilities, and the use of commercial services for military ends—forcing policymakers and humanitarian actors to confront how IHL applies to blended scenarios. The international community increasingly recognizes the need for standards on meaningful human control, transparent testing regimes, and mechanisms to attribute and adjudicate violations.

International Cooperation: Mechanisms and Best Practices

Addressing the dual-use and transnational nature of emerging technologies requires multilateral engagement. International forums—United Nations processes, regional security organizations like NATO, and specialized institutions such as the NATO Cooperative Cyber Defence Centre of Excellence—play essential roles in norm-setting, information exchange¹², and capacity building. Best practices include harmonized standards for cybersecurity, cross-border incident response protocols, and collaborative research on AI safety and testing.

Public–private partnerships are also indispensable: much innovation originates in commercial sectors. Governments should engage technology firms to ensure defensive resilience, secure supply chains, and ethical design. Confidence-building measures—data-sharing agreements, joint exercises, and transparency on non-deployment of particular systems—can reduce misperceptions and stabilize competition.

Future Landscape and Strategic Implications

Future trajectories will be shaped by the convergence of multiple technologies. Quantum computing threatens to disrupt contemporary cryptography¹³, necessitating a rapid transition to quan-

11 International Committee of the Red Cross, *Ethical Challenges of Autonomous Weapons and AI in Armed Conflict*, 2024.

12 NATO Cooperative Cyber Defence Centre of Excellence, *Cyber Defence and Emerging Technologies Report*, 2023.

13 World Economic Forum, *Global Risks Report: Technology, Geopolitics, and Security*, 2024.

tum-resistant protocols. Biotechnology advances may create new defensive and offensive possibilities, from medical countermeasures to ethically fraught performance enhancements. Continued miniaturization and improvements in autonomy will empower distributed sensor networks and swarms capable of saturating defenses.

These developments complicate conventional arms-control regimes; traditional planks—limits on delivery systems, warhead counts—do not easily translate to software, algorithms, or distributed commercial infrastructures. Governance innovations—multi stakeholder regimes, norms-based agreements, and technical verification mechanisms—will be required to manage risks without stifling beneficial innovation.

Conclusion

Emerging technologies are profoundly reshaping the character of contemporary conflict by elevating the centrality of information, speed, and precision in military operations. The Russia–Ukraine war exemplifies both the transformative potential of technological innovation to empower defenders and the inherent vulnerabilities that surface when the digital and physical domains converge. The integration of cyber warfare, autonomous systems, and artificial intelligence has blurred traditional boundaries between combatants and civilians, creating new ethical and operational dilemmas that challenge established norms of warfare.

To harness these technologies responsibly, states must prioritize the development of resilient and secure systems capable of withstanding both kinetic and cyber threats. Equally essential are comprehensive legal frameworks that define accountability for autonomous and algorithmic decisions, alongside transparent international mechanisms that promote oversight and compliance with humanitarian law. Sustained international cooperation—grounded in shared norms of restraint, information exchange, and conflict de-escalation—is critical to preventing technological escalation from undermining global stability.

Ultimately, as machines assume increasingly prominent roles in the decision-making and execution of warfare, the preservation of human judgment, accountability, and moral agency becomes indispensable. Ensuring that technological progress serves as a tool for peace rather than a catalyst for destruction requires a renewed commitment to ethical responsibility and collective governance. Only through such balanced integration of innovation and human oversight can emerging technologies contribute to a more secure and humane international order.

Bibliography

- NATO Cooperative Cyber Defence Centre of Excellence. (2023). *Cyber Defence and Emerging Technologies Report*.
- United Nations Office for Disarmament Affairs. (2024). *Responsible Innovation and Autonomous Weapons Systems*.
- European Defence Agency. (2023). *Innovation in Defence: The Role of AI and Emerging Technologies*.
- U.S. Department of Defense. (2022). *Artificial Intelligence Strategy for the Department of Defense*.
- RAND Corporation. (2023). *The Future of Warfare in the 21st Century: Emerging Technologies and Security Challenges*.
- International Committee of the Red Cross. (2024). *Ethical Challenges of Autonomous Weapons and AI in Armed Conflict*.
- Singer, P. W., & Chapa, J. (2021). *AI and the Future of Conflict*. Brookings Institution.
- World Economic Forum. (2024). *Global Risks Report: Technology, Geopolitics, and Security*.

THE U.S.–ISRAEL SECURITY PARTNERSHIP: STRATEGIC COOPERATION IN DEFENSE, INTELLIGENCE, AND REGIONAL STABILITY

Luka Marshania

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Nikoloz Mebagishvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This paper presents a comprehensive analysis of the strategic partnership between the United States and Israel in the field of security and defense. Rooted in decades of shared geopolitical interests and mutual trust, the U.S.–Israel alliance has evolved into one of the most sophisticated bilateral security relationships in the world. The partnership extends beyond traditional defense cooperation to encompass joint intelligence operations, technological innovation, counterterrorism coordination, and missile defense development—all of which contribute to maintaining regional stability and strengthening deterrence in the Middle East. By examining areas such as defense technology co-development, intelligence sharing, and collaborative counterterrorism initiatives, this study highlights how the partnership has become a cornerstone of both nations' national security strategies. It also explores how this alliance supports the broader objectives of the United States in preserving regional balance, while enabling Israel to maintain its qualitative military edge (QME) amid complex security challenges.

The paper argues that the U.S.–Israel security partnership is not merely transactional but strategic and adaptive, continually reshaped by technological advancement, shared democratic values, and the evolving threat environment. As hybrid warfare, cyber threats, and asymmetric conflicts redefine the global security landscape, the enduring cooperation between Washington and Jerusalem illustrates the growing importance of alliances grounded in innovation, intelligence integration, and strategic resilience.

Keywords: U.S.–Israel Partnership; Security Cooperation; Defense Innovation; Intelligence Sharing; Counterterrorism; Middle East Stability; Bilateral Alliances; Strategic Resilience; Qualitative Military Edge.

Introduction

The U.S.–Israel Security Partnership: A Strategic Alliance for the Twenty-First Century The U.S. –Israel security partnership stands as one of the most enduring, multidimensional, and strategically significant alliances in the modern world. Rooted in shared democratic values, mutual strategic interests, and a commitment to regional stability, this collaboration has expanded far beyond traditional military cooperation. It now encompasses defense innovation, intelligence integration, cybersecurity, counterterrorism, and advanced military training, forming a cornerstone of both nations' defense strategies. Since Israel's founding in 1948, the United States has been its primary ally—providing military aid, advanced weaponry, and diplomatic backing that have shaped Israel's security posture and ensured its qualitative military edge (QME) in a volatile region. Over the decades, the partnership has evolved in both scope and sophistication, adapting to changing geopolitical realities and technological revolutions. During the Cold War, U.S. support for Israel served as a strategic counterweight to Soviet influence in the Middle East. In the post-9/11 era, the focus expanded to include counterterrorism and intelligence cooperation against transnational threats. In the twenty-first century, this alliance has taken on a new dimension—one defined by technological synergy and defense innovation.¹ The joint development of missile defense systems such as *Iron Dome*, *David's Sling*, and *Arrow* exemplifies how the partnership fuses American resources and Israeli ingenuity to protect not only Israel's civilian population but also broader U.S. and allied interests in the region. Israel's strategic location—situated at the crossroads of Europe, Asia, and Africa and surrounded by a historically volatile security environment—makes it an indispensable partner for the United States in promoting regional stability and countering asymmetric threats. For Washington, cooperation with Israel provides invaluable intelligence insights, battlefield-tested technologies, and operational expertise in urban warfare and counterinsurgency. For Israel, U.S. support ensures access to advanced defense systems, sustainable deterrence, and strong diplomatic backing in international forums. This reciprocal relationship has created a mutually reinforcing security ecosystem, where innovation, strategy, and intelligence flow in both directions. In recent years, as the nature of warfare transforms through automation, artificial intelligence, and cyber operations, the U.S.–Israel partnership has deepened around emerging defense technologies and cyber resilience. Israel's experience in cyber defense—both in the military and private sectors—has made it a global leader in cybersecurity innovation. This expertise complements the United States' broader strategic capabilities, enabling both nations to develop joint frameworks for protecting critical infrastructure, combating hybrid threats, and maintaining digital sovereignty.

Beyond the technological and operational dimensions, this partnership reflects a shared strategic vision: the belief that enduring security in the Middle East depends on deterrence through innovation, intelligence cooperation, and a strong alliance network. Together, the United States and Israel act as pillars of stability in an increasingly uncertain regional and global order.

The paper seeks to explore the following key research questions:

1. What are the foundational elements and strategic pillars of the U.S.–Israel security partnership?

¹ U.S. Security Cooperation with Israel, Fact Sheet Bureau of Political-Military Affairs, April 25, 2025, <https://surl.li/uvyczq>, Accessed 03.11.2025

2. How has technological cooperation enhanced the defense capabilities and strategic deterrence of both nations?
3. What role does intelligence sharing play in sustaining and deepening the U.S.–Israel security relationship?

By addressing these questions, this study aims to provide a comprehensive understanding of how the U.S.–Israel partnership has evolved from bilateral defense cooperation into a strategic alliance rooted in innovation, mutual trust, and global relevance—one that continues to shape the security architecture of the Middle East and beyond.

Main Part

The U.S.–Israel Security Partnership: Foundations of Strategic Cooperation

The U.S.–Israel security partnership is underpinned by a shared commitment to defense, innovation, and strategic stability. Built upon decades of collaboration, this partnership has evolved into a multidimensional alliance encompassing military aid, intelligence exchange, technological innovation, cybersecurity cooperation, and joint military training. It reflects a deep convergence of strategic interests—anchored in democratic values, mutual trust, and the shared goal of maintaining regional and global security.

Military Aid and Defense Systems

The United States remains Israel’s largest and most consistent provider of military assistance, supplying billions of dollars annually through long-term aid packages such as the 2016 Memorandum of Understanding (MOU), which allocates \$38 billion over ten years. This support ensures that Israel maintains its Qualitative Military Edge (QME)—a principle enshrined in U.S. policy that guarantees Israel’s superiority over potential adversaries in defense technology and capability.

Among the most emblematic outcomes of this collaboration is the Iron Dome missile defense system, jointly developed with U.S. funding. Its proven success in intercepting short-range rockets and artillery shells has made it a symbol of the integration of American financing and Israeli innovation. Further cooperation on systems such as David’s Sling and Arrow continues to strengthen regional deterrence while serving as a model for joint R&D between allied nations.

Intelligence Sharing

Intelligence cooperation is a cornerstone of the U.S.–Israel alliance. The partnership facilitates the exchange of high-level intelligence on terrorism, arms proliferation, and state and non-state military activities across the Middle East. Israel’s intelligence community—renowned for its precision and technological sophistication—provides the United States with vital insights into regional dynamics, including Iran’s military strategy and the activities of proxy groups.

In return, Israel gains access to U.S. satellite intelligence, surveillance data, and advanced analytics, enabling more effective operational planning and preemptive action. This symbiotic intelligence relationship has enhanced both nations’ capacities to anticipate and neutralize threats before they materialize.²

2 NATO. (2022). *Strategic Concept 2022*. Brussels: North Atlantic Treaty Organization.

Counterterrorism and Cybersecurity Cooperation

Counterterrorism remains one of the most visible and effective areas of collaboration. The two countries conduct joint operations, training programs, and intelligence coordination to counter the activities of extremist groups such as Hezbollah, Hamas, and ISIS. Israel's field experience in urban counterinsurgency and rapid-response tactics complements U.S. strategic expertise and resources, forming a unified counterterrorism front. In the digital domain, cybersecurity cooperation has become increasingly critical. Facing escalating threats from state-sponsored cyber actors, both nations collaborate on developing advanced cyber defense and offensive capabilities. Israel's cyber units, particularly Unit 8200, are among the world's most sophisticated, pioneering AI-driven approaches to data security and threat detection. This partnership enhances both nations' capacities to defend critical infrastructure, financial systems, and military networks from complex cyberattacks.

Joint Military Exercises

Regular joint military exercises serve to enhance interoperability and readiness across the two nations' armed forces. Drills such as Juniper Cobra and Noble Dina simulate missile defense scenarios, naval warfare, and counterterrorism operations. These exercises allow both militaries to test emerging technologies, refine tactical coordination, and align doctrines under real-world conditions. Beyond training value, such engagements reinforce the operational trust and strategic cohesion that define the alliance.

Technological Cooperation and Defense Innovation- At the heart of the U.S.–Israel security relationship lies a shared culture of technological innovation. Both nations prioritize defense research and development as a key component of their national security strategies, creating an ecosystem where public institutions, private industry, and military laboratories collaborate seamlessly.

Beyond the Iron Dome, joint efforts in developing multi-tiered missile defense systems such as David's Sling and Arrow 3 exemplify the strength of this cooperation. These systems provide protection against threats ranging from short-range projectiles to long-range ballistic missiles, ensuring Israel's strategic deterrence while contributing to broader U.S. and NATO defense architectures. Cybersecurity stands as a pillar of twenty-first-century defense. The U.S. and Israel have established joint research programs, cyber task forces, and technology-sharing initiatives to safeguard national and allied interests. Israel's innovation ecosystem—bolstered by military-to-civilian technology transfer—provides the U.S. with novel tools for detecting and neutralizing cyber threats. Conversely, the U.S. offers large-scale infrastructure, intelligence networks, and operational experience, creating a mutually reinforcing framework for digital defense resilience.³

The integration of autonomous systems and AI-driven defense platforms represents the next frontier of collaboration. Israel's leadership in drone technology, surveillance systems, and robotics has positioned it as a critical partner for U.S. innovation in autonomous warfare and decision-support systems. Ongoing projects in AI-based threat analysis, autonomous navigation, and robotic combat systems illustrate how this partnership continues to push the boundaries of defense technology.

3 K. Kakachia, S. Meister, & B.Fricke, (Eds.). (2018). *Geopolitics and Security*/ Konrad Adenauer Stiftung / DGAP.

Intelligence Sharing and Security Operations

Intelligence sharing between the U.S. and Israel is arguably one of the most vital aspects of their security relationship. The two nations have collaborated closely in gathering and analyzing intelligence related to regional security threats, including the activities of terrorist organizations, weapons proliferation, and hostile state actors. Key aspects of this intelligence cooperation include: Counterterrorism Intelligence: Both the U.S. and Israel face significant threats from terrorist organizations operating within the Middle East and beyond. The intelligence exchanged between the two nations has been instrumental in disrupting terrorist operations, preventing attacks, and dismantling terror networks. This includes sharing critical intelligence on groups like Hamas, Hezbollah, and ISIS, as well as preventing the spread of advanced weaponry to these groups. Human Intelligence (HUMINT) and Signals Intelligence (SIGINT): Israel's military intelligence, particularly the Mossad, has long been regarded as one of the most sophisticated in the world. The U.S. benefits from Israel's intelligence-gathering capabilities, particularly in areas where human intelligence is crucial. In return, the U.S. provides Israel with access to its vast SIGINT networks, enhancing Israel's situational awareness and operational effectiveness.⁴

Counterintelligence Collaboration: In addition to gathering intelligence on adversaries, the U.S. and Israel work together to protect their own interests from espionage and infiltration. Counterintelligence operations aim to identify and neutralize hostile espionage activities, especially those targeting sensitive defense and intelligence information.

Conclusion

The U.S.–Israel security partnership stands as one of the most influential and enduring alliances in the modern international system, serving as a cornerstone of both regional stability and global strategic balance. Rooted in a foundation of shared democratic values, mutual trust, and aligned national interests, this partnership has consistently adapted to the evolving nature of global security challenges. From the early decades of military assistance and diplomatic cooperation to today's sophisticated integration of cybersecurity, intelligence operations, and defense innovation, the alliance reflects an extraordinary capacity for strategic evolution.⁵

At its core, the partnership represents more than a bilateral agreement—it is a dynamic security ecosystem built on continuous collaboration in research, technology, and intelligence. The integration of cutting-edge technologies, such as missile defense systems, artificial intelligence applications, and autonomous warfare capabilities, ensures that both nations maintain a qualitative military and technological edge in an era defined by hybrid threats and rapid innovation cycles. The success of joint projects such as the Iron Dome, David's Sling, and Arrow missile systems demonstrates how shared innovation and investment can produce global defense models that redefine the standards of modern warfare.

Equally critical is the dimension of intelligence and cyber cooperation, where both nations leverage their respective strengths to combat terrorism, espionage, and cyber aggression. Israel's

4 N.Tocci, (2016). *The EU Global Strategy: Shared Vision, Common Action*. European External Action Service.

5 F. Labarre, & G. Niculescu, (Eds.). (2023). *After 24 February 2022*

advanced intelligence-gathering capabilities and expertise in data analysis complement the United States' global surveillance infrastructure and strategic reach. This synergy not only fortifies their national defenses but also enhances the collective resilience of the transatlantic security network, contributing to the security of U.S. allies and partners across Europe and the Middle East.

As the twenty-first-century threat landscape becomes increasingly complex, digitalized, and interconnected, the U.S.–Israel partnership serves as a strategic model for adaptive security cooperation. It demonstrates how alliances must move beyond static military aid frameworks toward innovation-driven, intelligence-led, and technologically integrated defense architectures. The continuing collaboration between Washington and Jerusalem exemplifies the idea that enduring peace and stability are achieved not solely through power, but through strategic foresight, technological leadership, and unwavering commitment to shared security objectives.

Ultimately, the U.S.–Israel security partnership will remain an indispensable pillar of regional and global order—a testament to how two nations, united by common purpose and vision, can transform defense cooperation into a sustained force for innovation, deterrence, and collective security in an uncertain world.

Bibliography

- U.S. Security Cooperation with Israel, Fact Sheet Bureau of Political-Military Affairs, April 25, 2025, <https://surl.li/uvyczq>, Accessed 03.11.2025
- Kakachia, K., Meister, S., & Fricke, B. (Eds.). (2018). *Geopolitics and Security*/ Konrad Adenauer Stiftung / DGAP.
- Labarre, F., & Niculescu, G. (Eds.). (2023). *After 24 February 2022*
- Tocci, N. (2016). *The EU Global Strategy: Shared Vision, Common Action*. European External Action Service.
- NATO. (2022). *Strategic Concept 2022*. Brussels: North Atlantic Treaty Organization.

RUSSIA'S FAILED PROVOCATION: STRATEGIC MISCALCULATIONS AND GEOPOLITICAL CONSEQUENCES

Nikoloz Merabishvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Sophiko Metreveli

Assistant Professor of Bachelor's Program in Defense and security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This paper provides an in-depth analysis of Russia's failed attempts to provoke NATO member states into direct military confrontation during the ongoing Russia-Ukraine war through drone incursions and hybrid provocations. The study focuses on identifying the political, military, and informational objectives of these actions and evaluating their broader implications for European security and NATO's deterrence framework. The article explores how Russia employed unmanned aerial vehicle (UAV) operations along NATO's eastern borders—particularly in Romania, Poland, and the Baltic States—as part of a calculated hybrid strategy. These operations sought to undermine Western unity, instigate escalation, and test NATO's collective defense posture without triggering a full-scale confrontation. Using a qualitative analytical approach grounded in contemporary security studies, the paper assesses how Russia's hybrid tactics failed to achieve their intended outcomes. Findings indicate that NATO's measured and coordinated response effectively neutralized the intended provocation. By maintaining strategic restraint, avoiding disproportionate military reactions, and reinforcing air defense, intelligence, and coordination mechanisms, NATO and its partners successfully contained escalation risks while reinforcing alliance cohesion. Moreover, rather than weakening Western solidarity, these provocations strengthened intra-alliance cooperation and deepened collective support for Ukraine.

The study concludes that Russia's failed provocation underscores the effectiveness of calm strategic deterrence and collective resilience in modern hybrid warfare environments. The episode demonstrates how discipline, information control, and cooperative defense structures can transform a potential security crisis into an opportunity to reinforce unity and strategic credibility among allies.

Keywords: Russia-Ukraine War; Hybrid Warfare; NATO; Drone Provocations; Strategic Deterrence; European Security; Information Operations; Military Escalation; Air Defense; Collective Response.

Introduction

Throughout human history, war has been one of the primary instruments through which states have pursued power, influence, and geopolitical dominance. The modern Russian Federation, much like its imperial and Soviet predecessors, has maintained a foreign policy deeply rooted in expansionism and the projection of influence over its neighboring states. This aggressive posture has consistently manifested through both direct military aggression and hybrid operations designed to destabilize regions and challenge the existing international order. The large-scale invasion of Ukraine in 2022 epitomizes this approach, representing not only a continuation of Russia's revisionist strategy but also a direct assault on the post–Cold War European security architecture.

However, Russia's strategic ambitions have not been confined to the Ukrainian front. Parallel to its operations in Ukraine, Moscow has sought to extend the conflict's pressure zone beyond Ukraine's borders, employing hybrid and asymmetric tactics aimed at provoking NATO member and partner states. Among the most notable of these provocations are a series of unmanned aerial vehicle (UAV) incursions and related disinformation campaigns targeting NATO's eastern flank—particularly Romania, Poland, and the Baltic States. This paper examines these deliberate provocations as part of a broader hybrid strategy intended to test NATO's unity, exploit perceived vulnerabilities, and provoke a disproportionate military or political response.

The study places particular emphasis on a sequence of incidents that occurred between 9–10 September 2025, when multiple Russian-manufactured drones violated Polish airspace, followed by similar events along the Romanian and Estonian borders later that month¹. These incursions formed part of a coordinated hybrid pressure campaign, combining physical provocations with information warfare tactics designed to manipulate narratives, sow uncertainty, and erode public trust in NATO's deterrence mechanisms. Drones, beyond their tactical function, serve a strategic informational purpose in Russia's hybrid warfare toolkit. The ambiguity of drone origins—amplified through the circulation of manipulated images, false reports, and selective leaks—enables Moscow to shape public perception and generate confusion among European audiences. Such operations aim to exploit the political sensitivity surrounding Article 5 of the North Atlantic Treaty, which establishes that an attack against one NATO member constitutes an attack against all². By pushing the boundaries of this principle through ambiguous provocations, Russia tests the Alliance's political cohesion and decision-making resilience without crossing the threshold of open warfare. These actions must therefore be viewed as part of a deliberate hybrid strategy aimed at undermining Europe's collective security order, weakening transatlantic solidarity, and deterring deeper NATO involvement in Ukraine's defense. The purpose of this study is to conduct a comprehensive analysis of the political, military, and informational objectives of these provocations and to assess their implications for European security and strategic stability. Employing a qualitative case study approach, the research evaluates specific drone incidents and NATO's coordinated strategic response. The central hypothesis of this paper asserts that Russia's attempts to draw NATO member states into direct confrontation through UAV provocations have failed due to the Alliance's disciplined application of strategic restraint and deterrence-by-composure. By maintain-

1 Emergency Briefing on Drone Incursion into Poland, <https://surl.li/ueytol>, Accessed 03.11.2025

2 The North Atlantic Treaty, <https://surl.li/wouaiw>, Accessed 03.11.2025

ing a posture that combines enhanced air defense readiness with measured diplomatic responses, NATO successfully prevented escalation while reinforcing its internal unity and demonstrating the strength of collective defense.

Accordingly, the paper is organized into three principal sections. The first examines the role of drones within Russia's hybrid warfare doctrine, focusing on their operational and psychological applications. The second explores the informational and psychological dimensions of these provocations, emphasizing disinformation and media manipulation. The final section evaluates NATO's strategic response, highlighting how measured deterrence and alliance cohesion effectively neutralized Russia's attempt to destabilize the regional security balance.

Main Part

Russia's Hybrid Strategy and the Role of Unmanned Aerial Vehicles

The large-scale war waged by Russia in Ukraine no longer constitutes a purely conventional armed conflict; rather, it exemplifies a multidimensional hybrid warfare strategy that integrates military, informational, economic, and psychological dimensions into a single coordinated effort.³ This approach, often associated with General Valery Gerasimov's doctrine, emphasizes the seamless blending of traditional military force with non-military tools—such as cyberattacks, energy coercion, propaganda, and disinformation—to achieve strategic objectives while maintaining a degree of plausible deniability⁴. The core principle of this strategy is controlled ambiguity: to advance political and military goals without crossing thresholds that would provoke a direct collective military response, particularly from NATO. Within this broader framework, unmanned aerial vehicles (UAVs)—commonly referred to as drones—have become a critical component of Russia's hybrid toolkit, especially along NATO's eastern borders. Their function has expanded beyond reconnaissance and tactical strike operations; drones now serve as instruments of strategic signaling, provocation, and psychological manipulation. The discovery of debris from Russian-manufactured drones on the territories of Romania, Poland, and the Baltic States cannot be dismissed as accidental. Instead, these incidents reveal a deliberate, calculated effort to pursue multiple objectives—military, political, and informational—simultaneously.

First, these drone incursions serve as “red line tests”, designed to assess NATO's collective defense posture and determine the threshold for invoking Article 5 of the North Atlantic Treaty. By sending drones into NATO airspace, Russia probes both the Alliance's political resolve and its operational response time, collecting valuable intelligence about detection capabilities, air defense coordination, and crisis communication mechanisms.

Second, these operations represent an intelligence-gathering exercise. By observing NATO's radar tracking, interception speed, and decision-making processes, Russia can map potential vulnerabilities in Europe's air defense systems and adjust its own offensive strategies accordingly.

Third, the provocations serve a strategic diversionary purpose. By compelling NATO member states to bolster border defenses and redirect military assets to surveillance and interception missions, Russia aims to disperse Western resources—reducing the material and logistical support flowing to Ukraine's frontlines.

3 European Defence Agency. Hybrid Warfare and Unmanned Systems, <https://surl.li/imkoui>, Accessed 03.11.2025

4 RAND Corporation – *Russian Hybrid Warfare and NATO Response*, <https://surl.li/lbbtko>, Accessed 03.11.2025

In this sense, the use of drones in proximity to NATO territory exemplifies the essence of hybrid warfare, where a technological instrument is weaponized for political signaling rather than direct combat engagement. The objective is not to achieve tactical victory but to sow confusion, test limits, and erode unity among adversaries while maintaining a veneer of deniability. This study employs a qualitative case study methodology to analyze these incidents and NATO's corresponding strategic responses. The central hypothesis asserts that Russia's attempts to draw NATO into open confrontation through UAV provocations have failed, primarily due to the Alliance's deterrence-by-composure strategy—a deliberate blend of heightened defense readiness and diplomatic restraint. This approach not only neutralized the risk of escalation but also reinforced inter-alliance solidarity and strategic cohesion in the face of Russian hybrid aggression.

Information and Psychological Provocation

Drone-based provocations are intrinsically linked to Russia's information and psychological warfare doctrine, which has long been a defining element of its strategic behavior. From the 2008 Russo–Georgian War to the ongoing conflict in Ukraine, Moscow has consistently fused military action with narrative warfare, leveraging ambiguity and disinformation to manipulate public perception. The ambiguous nature of drone debris—often lacking clear identifying markers or traceable trajectories—creates fertile ground for propaganda narratives. Russian state-controlled media and affiliated information networks exploit this uncertainty to generate conflicting stories regarding the origins, purposes, and implications of drone incidents. Such manipulations aim to undermine public confidence in NATO's security architecture, suggesting that alliance guarantees are fragile and that European states remain vulnerable despite collective defense mechanisms. Moreover, these operations serve to erode psychological resilience among European populations. Continuous exposure to ambiguous threats and manipulated information fosters anxiety, fatigue, and skepticism, which can weaken public support for NATO's policies and for continued assistance to Ukraine. Therefore, drone incursions must not be viewed as isolated acts of aggression but as multi-layered hybrid operations—combining physical, psychological, and informational dimensions. Military provocations and disinformation campaigns operate in tandem to amplify one another, advancing Russia's strategic objective of destabilizing the European security order while avoiding overt escalation.

NATO and Partner Countries' Response: Strategic Restraint

Following the drone-related provocations along NATO's eastern borders, the reaction of European nations and the Alliance as a whole was measured, deliberate, and strategically disciplined. Contrary to what Moscow may have anticipated, NATO member and partner states did not succumb to impulsive or aggressive responses that could have escalated tensions into open confrontation. Instead, they adopted a posture of strategic restraint, underscoring the maturity and cohesion of Western collective defense policy. In the immediate aftermath of the incidents, NATO officials and European leaders issued coordinated statements emphasizing that these provocations, though

serious, did not constitute acts of war and therefore would not elicit a direct military response⁵. This message was critical in preventing Russia from manipulating the situation to claim that NATO was the aggressor or to justify further escalation. Simultaneously, the Alliance reinforced its defensive readiness through practical measures that balanced deterrence with restraint. Countries directly affected by the incursions—Romania, Poland, and the Baltic States—responded swiftly yet prudently⁶. Romania and Poland deployed additional air defense systems along their eastern frontiers, including Patriot and NASAMS batteries, to enhance interception capacity⁷. Meanwhile, the Baltic States intensified aerial surveillance and intelligence-sharing mechanisms, leveraging NATO's integrated early-warning systems to monitor cross-border activity. These defensive actions were complemented by increased joint air patrols under NATO's Air Policing Mission, ensuring that alliance airspace remained secure and monitored without escalating militarily. This carefully calibrated response reflected a broader strategy of deterrence through composure—a principle rooted in preventing escalation while maintaining control over the narrative. By demonstrating that NATO was aware, capable, and unified—but unwilling to react impulsively—Western governments effectively denied Russia the psychological and political victory it sought. Moscow's strategy of provoking overreaction thus backfired, as NATO's consistent and transparent communication reinforced confidence among both its member states and their populations. At the diplomatic level, the Alliance prioritized strategic communication and transparency. Member states coordinated their public messaging to prevent misinformation and ensure that citizens understood the nature of the threat. Intelligence coordination between NATO command structures, EU institutions, and national agencies was intensified, facilitating real-time data sharing and a unified situational picture. In doing so, NATO not only contained the immediate threat but also strengthened the credibility of its collective defense posture and reaffirmed its commitment to regional stability.

Ultimately, this episode demonstrated that effective deterrence in the 21st century relies not merely on military superiority but also on strategic patience, coherence, and information management. NATO's reaction showcased a form of resilience that blended operational vigilance with diplomatic prudence—proving that the Alliance can neutralize hybrid provocations without allowing itself to be drawn into the aggressor's narrative trap.

Conclusion

Russia's attempt to provoke NATO through drone incursions and hybrid tactics ultimately failed to achieve its intended objectives⁸. Although the incidents temporarily heightened tensions and caused unease among local populations, they did not result in the escalation Moscow sought. Instead, the Alliance's unity, situational awareness, and information control ensured a composed and coordinated response that transformed potential crisis into strategic affirmation. NATO's measured approach—anchored in strategic restraint and deterrence-by-composure—proved highly effective in maintaining stability while simultaneously reinforcing confidence in the Alliance's

5 NATO Public Diplomacy Division – *NATO Strategic Communications Report, 2024*, <https://surl.li/tejwbw>, Accessed 03.11.2025

6 Poland, Romania scramble jets as NATO ally records new Russian drone violation, <https://surl.li/rllqis>, Accessed 03.11.2025

7 Ministry of Defence of Romania – *Annual Defence Assessment, 2024*, <https://surl.li/wmugkx>, Accessed 03.11.2025

8 The Economist – *Russia's Failing Provocations*, <https://surl.li/onjsqi>, Accessed 03.11.2025

capacity for collective defense. The provocations, rather than exposing NATO's vulnerabilities, became a public demonstration of its operational discipline and institutional resilience. Far from weakening Western resolve, these incidents strengthened inter-alliance cooperation and further deepened the political and logistical support for Ukraine's defense. At the same time, it is essential to recognize that Russia's hybrid pressure campaign is unlikely to end with these failed provocations. Given the ongoing and largely protracted nature of the Russia–Ukraine conflict, Moscow is expected to continue employing low-intensity, asymmetric provocations—including cyberattacks, UAV incursions, and information manipulation—to sustain a climate of tension along NATO's borders. Such actions may aim to distract Western attention, exert political pressure, and test alliance endurance over time.

Therefore, sustaining NATO's effectiveness will require continued investment in early-warning systems, joint intelligence frameworks, and public resilience mechanisms. As demonstrated, maintaining composure and coordination remains the most powerful countermeasure to hybrid aggression. Russia's failed provocation stands as clear evidence that strategic restraint—when combined with unity, vigilance, and credible deterrence—can outmatch even the most calculated hybrid threats.

Bibliography

- NATO Public Diplomacy Division – NATO Strategic Communications Report, 2024, <https://surl.li/tejwbw>, Accessed 03.11.2025
- European Defence Agency. Hybrid Warfare and Unmanned Systems, <https://surl.li/imkoui>, Accessed 03.11.2025
- Ministry of Defence of Romania – Annual Defence Assessment, 2024, <https://surl.li/wmugkx>, Accessed 03.11.2025
- RAND Corporation – Russian Hybrid Warfare and NATO Response, <https://surl.li/lbbtko>, Accessed 03.11.2025
- The Economist – Russia's Failing Provocations, <https://surl.li/onjsqi>, Accessed 03.11.2025
- Emergency Briefing on Drone Incursion into Poland, <https://surl.li/ueytol>, Accessed 03.11.2025
- Poland, Romania scramble jets as NATO ally records new Russian drone violation, <https://surl.li/rlqis>, Accessed 03.11.2025
- The North Atlantic Treaty, <https://surl.li/wouaiw>, Accessed 03.11.2025

FROM THE BATTLEFIELD TO THE LAB: THE IMPACT OF THE RUSSIA - UKRAINE WAR ON THE DEVELOPMENT OF INTERNATIONAL DEFENCE INNOVATION

Major Ioseb Papiashvili

The Learner of a Master's Degree Program (Security Studies) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Zurab Agladze

Professor of Master's Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The war in Ukraine marks a decisive turning point in global defence innovation, functioning as both a battlefield and a laboratory where emerging technologies are tested and integrated in real time. Since Russia's full-scale invasion in 2022, the conflict has shown that the key determinant of modern warfare is no longer military mass but the ability to innovate rapidly and apply technologies through strong partnership networks. Across multiple domains, this transformation is evident. Drone warfare has enabled Ukraine to offset numerical disadvantages through precision strikes and real-time intelligence. Artificial intelligence, big data, and cyber operations have enhanced situational awareness and redefined information security, while satellite communications such as Starlink have sustained command structures under heavy attack. Together, these advances reveal that technological integration, not possession, determines strategic advantage. This innovation has been collective and transnational. Western governments, NATO initiatives like DIANA, and private firms such as Palantir and Starlink have created a hybrid innovation ecosystem linking front-line needs with rapid technological adaptation. The war demonstrates that sovereignty today depends not on self-sufficiency but on intelligent interdependence - secure, trusted cooperation among states and industries.

This study introduces the concept of Networked Defence Innovation (NDI): a model where distributed research, alliance-based governance, and real-time integration transform defence innovation into a shared strategic resource. For small and medium-sized states, NDI offers a path to strategic relevance through multinational cooperation. Yet, accelerated innovation also brings risks-cyber vulnerabilities, dependency, and ethical challenges surrounding AI and autonomous systems-requiring clear regulation and accountability.

In conclusion, the Ukraine war demonstrates that twenty-first-century defence rests on networked innovation, technological integration, and international cooperation-the combined foundation of future global security.

Keywords: Defence Innovation; Drone Warfare; International Cooperation; Cybersecurity; Artificial Intelligence; NATO; Ukraine War; Technological Strategy; Global Security.

Introduction

The ongoing war in Ukraine marks one of the most critical turning points in modern military and technological history. Unlike earlier conflicts shaped by conventional warfare and mass mobilization, today's Ukrainian battlefield is defined by drones, real-time satellite coordination, cyber operations, and advanced intelligence systems. The conflict functions not only as a warzone but as a global laboratory of defence innovation. The interplay between states, private industries, and international alliances has reconfigured both the conduct of warfare and the strategic understanding of security itself.

The outbreak of war in February 2022 triggered an intense technological race between Ukraine and Russia, as well as among their respective allies and adversaries. Ukraine's rapid integration of Western technologies and its ability to adapt commercial platforms for military purposes surprised many observers. The creative use of off-the-shelf drones, AI-driven targeting, and agile operational strategies has demonstrated how technological flexibility can offset asymmetrical disadvantages. Equally significant is the role of international cooperation. NATO and its partners have supplied not only weapon systems but also robust frameworks for intelligence integration, information sharing, and logistics support. This "networked defence cooperation" represents a departure from state-centric security models, signaling a move toward interconnected and adaptive structures of collective defence. This evolution merges two accelerating global trends: rapid technological change and intensifying geopolitical rivalry. For smaller states observing the conflict, the war provides practical lessons in how innovation and partnership can enhance national resilience and strategic relevance. In this light, the present paper explores how the war in Ukraine has accelerated defence innovation, the mechanisms enabling this acceleration, and the broader implications for future security architectures.

Research Question

What impact has the Russia–Ukraine war had on the strategic evolution and institutionalization of international defence innovation?

Hypothesis

The Russia–Ukraine war has significantly accelerated the development of innovative defence capabilities and has prompted international alliances to deepen strategic partnerships with private industry and research institutions. This conflict has demonstrated that achieving superiority in the 21st century depends not only on military and economic power, but also on the ability to develop and integrate new technologies within the framework of international strategic cooperation. By facilitating rapid information sharing, joint research, and the development of dual-use technologies, these partnerships enable states to achieve strategic flexibility and resilience more effectively than would be possible through unilateral or purely national efforts.

Moreover, this transformation highlights the emergence of a new strategic paradigm in which innovation networks function as key instruments of security policy. States and alliances are increasingly shifting from traditional, state-centered defence models toward flexible, collaborative

ecosystems that integrate commercial technology, academic research, and real-time battlefield feedback. This approach allows them to respond more effectively to hybrid threats, anticipate technological disruptions, and maintain a competitive edge in rapidly evolving security environments. As a result, technological cooperation is no longer a supporting element of defence policy, it has become a core determinant of strategic power and geopolitical influence in the 21st century.

Research Methodology

The methodological approach is qualitative and comparative. It combines case study analysis with documentary review and comparative framework evaluation to identify patterns in defence innovation. Case Study Analysis examines real-world innovation partnerships, including NATO's DIANA, Ukraine's battlefield adaptation of drones, and Israel's cross-border R&D cooperation; Documentary and Policy Review analyzes doctrines, white papers, and strategic innovation policies from key actors; Comparative Framework Analysis identifies similarities and differences across partnership models to extract best practices in innovation governance. Data are drawn exclusively from open-source government documents, academic publications and think tank research.

Main Part

The analysis of Ukraine's wartime experience, NATO's innovation framework, and Israel's defence ecosystem reveals a profound restructuring of how security is generated, shared, and sustained in the 21st century. The war in Ukraine has not only served as a conventional military conflict but also as a real-time laboratory of modern warfare, where drones, AI analytics, satellite communications, and cyber operations became decisive tools. This hybrid operational environment blurred the boundaries between civilian and military technology, as domestic innovation networks intertwined with international support systems. Ukraine's agile adaptation of commercial drones, real-time data sharing, and decentralized defence production networks exemplifies how technological agility, combined with strong international partnerships, can offset numerical inferiority and reshape the strategic balance.¹

What emerged from this conflict is a new model of defence innovation - distributed, dynamic, and embedded in international cooperation. Ukraine's battlefield experience showed that rapid experimentation, adaptive procurement, and civil-military fusion can create a flexible and resilient warfighting ecosystem. Intelligence sharing with allied partners, particularly NATO members, provided Ukraine with strategic situational awareness that magnified its deterrence capabilities.² These developments highlight a decisive factor in modern warfare: the speed and adaptability of innovation networks matter as much as technological sophistication itself. This shift is institutionalized within NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), launched in 2021 to connect startups, research centers, and member states through a common innovation infrastructure. Together with the NATO Innovation Fund, DIANA reflects an emerging logic of shared technological development, collective deterrence, and interoperable defence systems. Rath-

1 War on the Rocks, "The Russia Contingency: Tech, Tactics, and Innovation at the Front," podcast, <https://surl.lt/fldqin>, (Accessed 03.11. 2025)

2 Lawrence Freedman, *The Future of War: Lessons from Ukraine* (Oxford: Oxford University Press, 2023), 211–215.

er than treating innovation as a national asset, the alliance frames it as a shared investment and a foundation of collective resilience.³ This institutionalized model of “innovation diplomacy” grants smaller states access to high-level technologies and expertise that would otherwise remain out of reach, reducing asymmetries and strengthening deterrence across the alliance.

Israel’s long-standing defence innovation model offers another perspective on how technology can shape both strategy and diplomacy. Developed under conditions of geopolitical isolation, Israel built a defence innovation ecosystem where the armed forces, government R&D agencies, private industry, and academic research are tightly integrated. Through partnerships with the United States and expanding regional cooperation, Israel transformed its security imperatives into technological advantages, producing systems like Iron Dome and Arrow missile defence that became both strategic assets and diplomatic tools. By leveraging technological exports and innovation diplomacy, Israel turned its security model into a source of influence on the global stage, illustrating how innovation ecosystems can serve dual military and foreign policy functions.⁴

When compared together, these cases expose a shared set of strategic patterns: civilian and military technological domains are increasingly fused; security is being constructed through networked architectures rather than isolated national capabilities; and innovation itself is becoming a form of political capital within alliances.⁵ In this context, smaller and medium-sized states face both opportunities and challenges. By integrating into multinational R&D networks, they can strengthen deterrence without sustaining the prohibitive costs of independent weapons development. Such participation not only enhances operational capacity but also stimulates domestic technological advancement, driving dual-use economic benefits. At the same time, these states must mitigate vulnerabilities inherent in digital dependence and ensure they can absorb, adapt, and protect external technologies effectively.

The implications for institutions like NATO and the European Union are far-reaching. Defence innovation is reshaping the political economy of security, demanding governance structures that can keep pace with private-sector innovation. Bureaucratic procurement cycles and rigid institutional models risk lagging behind technological change.⁶ As strategic competition with Russia and China intensifies, these alliances must shift from being consumers of innovation to architects of secure and ethical technological ecosystems. This includes aligning innovation with export controls, supply chain security, and shared ethical standards.

Alongside its strategic promise, rapid technological acceleration raises serious ethical and regulatory questions. Autonomous systems, AI-driven targeting, and algorithmic decision-making introduce profound accountability and oversight challenges. Partnerships must embed ethical frameworks directly into the innovation process, ensuring that strategic advantage does not come at the expense of humanitarian principles or international law. NATO’s AI strategy and responsible-use principles are early steps, but global governance remains fragmented, allowing competition to outpace regulation. Building credible oversight structures will be essential to prevent escalation

3 NATO, “DIANA — Defence Innovation Accelerator for the North Atlantic,” <https://www.diana.nato.int/> (Accessed 03.11.2025)

4 Ariel Levite and Shira Efron, “Technology, Diplomacy, and Deterrence in Israel’s Strategy,” RAND Israel Report (2024).

5 Henry Farrell and Abraham Newman, *Underground Empire: How America Weaponized the World Economy* (New York: Henry Holt, 2023), 118.

6 Michael J. Mazarr, “Strategic Interdependence and the Future of Deterrence,” RAND Perspective Paper (2023).

risks and maintain legitimacy in an increasingly automated battlespace. In response to these transformations, strategic and policy priorities become clear. Defence planners and policymakers must institutionalize innovation partnerships through specialized agencies; adopt flexible procurement models to accelerate experimentation; invest in dual-use technology ecosystems; standardize interoperability to improve collective situational awareness; and develop ethical oversight structures capable of operating across alliances.⁷ Education, training, and innovation diplomacy are equally crucial - enabling smaller states to engage actively in shaping technological standards rather than merely adopting them.

Looking ahead, the future of defence innovation will be shaped by three converging technological domains: artificial intelligence, quantum technologies, and space-based capabilities. These require levels of coordination and governance unprecedented in previous eras. The Ukraine War has already shown that those who can rapidly integrate innovation networks, maintain trusted partnerships, and adapt faster than their adversaries will shape the security order of the future. Defence power in the 21st century is increasingly generated not in isolation but through networked ecosystems, where technology, cooperation, and strategy merge into a single, adaptive architecture of security⁸.

Conclusion

The findings of this study demonstrate that the architecture of 21st-century security is no longer built solely on state-centric military capabilities or the accumulation of advanced weaponry. It rests on the capacity to innovate collaboratively, leveraging technology, alliances, and cross-sectoral networks. The war in Ukraine, NATO's DIANA initiative, and Israel's innovation ecosystem collectively reveal that military advantage now emerges from the interplay between civilian ingenuity, defence structures, and transnational cooperation. This transformation has blurred the line between the battlefield and the laboratory, with making innovation not just an enabler of security, but its core strategic currency.⁹

Ukraine's experience underscores how agility and partnership can compensate for conventional asymmetry. The integration of commercial drone technologies, AI-assisted targeting, cyber defence, and satellite communications created a flexible and resilient defence posture despite material inferiority. NATO's institutional innovation frameworks show how alliances can amplify technological advantages across member states, creating shared deterrence capacities through distributed innovation. Israel's long-standing model illustrates how sustained R&D investment, civil-military fusion, and strategic export partnerships turn technology into diplomatic leverage. Together, these three cases define a strategic landscape where power depends less on stockpiled arsenals and more on innovation ecosystems that cross borders and sectors.

The evidence also points to a decisive shift in how small and medium-sized states can achieve strategic relevance. By embedding themselves in multinational R&D networks, they can access advanced technologies, increase interoperability, and benefit from dual-use innovation spillovers.

7 Richard Barrons, "Allied Agility: Partnership as a Capability," Chatham House Commentary (2024).

8 Henry Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (New York: Little, Brown, 2021), 142.

9 Henry Farrell and Abraham Newman, *Underground Empire: How America Weaponized the World Economy* (New York: Henry Holt, 2023), 118.

This allows them to play meaningful roles in collective deterrence without sustaining the prohibitive costs of building entire defence industries. However, this model is not without vulnerabilities. Strategic interdependence must be accompanied by internal investment in cyber resilience, technological absorption capacity, and flexible defence governance. Without this balance, partnership can turn into dependency.

Ethical governance represents another critical frontier. As defence innovation accelerates, especially in areas like AI and autonomous systems, states and alliances must ensure accountability mechanisms keep pace. NATO's Responsible AI framework, UN discussions on autonomous weapons, and various academic proposals emphasize the need for embedded oversight structures, not as external checks but as integral components of the innovation cycle. Failure to institutionalize these mechanisms could result in operational escalations, legal ambiguities, and political backlash.

In light of these dynamics, several scholars offer concrete strategic recommendations that align closely with this study's findings. Eliot Cohen argues for "flexible command architectures" capable of integrating rapidly evolving technologies without bureaucratic lag.¹⁰ Lawrence Freedman emphasizes the strategic advantage of innovation speed over platform perfection, noting that conflicts like Ukraine show how iterative adaptation outperforms static modernization.¹¹ Managing interdependence is more important rather than retreating from it: strategic resilience lies in secure networks, not isolation. These insights converge on a single point, alliances and states must cultivate trusted, agile, and ethically governed innovation ecosystems to maintain strategic advantage.

Looking ahead, the next phase of security transformation will be shaped by the convergence of AI, quantum computing, and space technologies. These domains will both empower and destabilize, offering asymmetric tools to smaller states and imposing new coordination challenges on alliances. States capable of aligning their national innovation strategies with transnational networks will lead the evolution of security architectures, while those that remain technologically isolated risk strategic irrelevance.

In essence, the research argues that the future of defence will be determined not by isolated power, but by intelligent interdependence. Military success will hinge on how effectively nations integrate technological innovation, institutional adaptability, and ethical governance into a coherent strategic vision. This requires political will, investment in human capital, institutional reforms, and sustained cooperation. If alliances and states act deliberately, innovation will remain a stabilizing force - a foundation for collective security in an increasingly uncertain world.

¹⁰ Eliot A. Cohen, *The Hollow Victory: Innovation in Modern War* (Baltimore: Johns Hopkins University Press, 2022), 57

¹¹ Freedman, *The Future of War*, 88.

Bibliography

- Barrons, Richard. "Allied Agility: Partnership as a Capability." *Chatham House Commentary*, 2024.
- Cohen, Eliot A. *The Hollow Victory: Innovation in Modern War*. Baltimore: Johns Hopkins University Press, 2022.
- Farrell, Henry, and Abraham Newman. *Underground Empire: How America Weaponized the World Economy*. New York: Henry Holt, 2023.
- Freedman, Lawrence. *The Future of War: Lessons from Ukraine*. Oxford: Oxford University Press, 2023.
- Kissinger, Henry, Eric Schmidt, and Daniel Huttenlocher. *The Age of AI: And Our Human Future*. New York: Little, Brown, 2021.
- Levite, Ariel, and Shira Efron. "Technology, Diplomacy, and Deterrence in Israel's Strategy." RAND Israel Report, 2024.
- Mazarr, Michael J. "Strategic Interdependence and the Future of Deterrence." RAND Perspective Paper, 2023.
- NATO. "DIANA — Defence Innovation Accelerator for the North Atlantic." <https://www.diana.nato.int/> (Accessed 03.11. 2025)
- War on the Rocks. "The Russia Contingency: Tech, Tactics, and Innovation at the Front." Podcast episode index. <https://surl.li/cbyowx>, (Accessed 03.11. 2025)

DRONES AS HARD AND SOFT POWER: INNOVATION AND SECURITY LESSONS FROM THE RUSSO-UKRAINE WAR

Giorgi Parkauli

The Learner of a Master's Degree Program (State Recourse Management) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This thesis analyses how innovation in unmanned aerial systems functions simultaneously as hard power and soft power, using the Russo-Ukraine War as a focal case study to assess operational, political, and strategic implications. It argues that drones have reconfigured contemporary conflict by compressing the sensor-to-shooter timeline, enabling low-cost precision strikes and deep-strike options that impose asymmetric costs on conventionally superior adversaries, while also operating as instruments of narrative, prestige, and diplomatic leverage that shape public opinion and alliance behaviour.

Methodologically, the study combines battlefield case material, procurement and partnership documentation, and policy analysis to trace the interplay between domestic innovation and international collaboration. Empirical evidence demonstrates that Ukraine's rapid adaptation and scaling of commercial and bespoke unmanned platforms has produced both combat effects and symbolic gains, while Russia's reliance on Iranian-origin loitering munitions has allowed it to project coercive reach and to employ saturation tactics that strain air defences. The thesis highlights two interconnected policy challenges for Europe. First, fragmented procurement regimes, supply-chain links, and limited indigenous industrial skills lead to strategic weaknesses in both hard and soft power elements. Second, the dual-purpose nature of drone technologies poses regulatory and ethical challenges that demand shared control. To tackle these issues, the report offers a comprehensive policy solution termed as a Drone Innovation and Security Pact under NATO and EU auspices. The proposed convention would coordinate investment in offensive and defensive capabilities, standardise interoperability, promote technology sharing and cooperative R&D, and include ethical oversight and transparency mechanisms.

The thesis argues that by integrating operational research with a normative policy framework, Europe may turn its existing vulnerabilities into strategic advantages. Building interoperable industrial capacity and governance mechanisms would not only boost deterrence and resilience but also help Europe to define worldwide norms for the responsible development and use of unmanned systems.

Keywords: Drone warfare, Hard power and soft power, Defence innovation, Russo-Ukraine War, European Security, International partnerships, Unmanned Aerial Systems (UAS).

Introduction

Many scholars would argue that, over the centuries, war has not really changed fundamentally. War has been, is and always will be a test of superiority over your opponents in certain fields and innovation. This relentless pursuit of dominance drives nations to evolve their strategies and technologies. As a result, while the methods may shift, the underlying motivations and consequences often remain strikingly similar throughout history. Therefore, we can theorise that defence or warfare innovation has always played a crucial and maybe even central role in shaping the character of modern warfare and the broader dynamics of international relations and politics, as “war is a continuation of politics by other means”¹. This work focuses on how drones have shaped and could shape the future of security, both on the battlefield and on the international stage. Looking at the centuries of warfare, we can clearly see a correlation between major conflicts and technological breakthroughs. From the birth of gunpowder to nuclear weapons, technological innovations have continuously altered the balance of power, required military adaptation, and redefined the ways in which governments project their influence onto others. So-called fire lances, or even flintlocks and arquebuses, were revolutionary for their day, as they let people conduct war over a relative distance. Unmanned aerial systems (UAS), commonly known as drones, have become one of the most important defensive inventions of the twenty-first century, affecting not just how wars are fought but also how states utilise their power outside of the battlefield. The best example of this transformation is the ongoing Russo-Ukraine War, which is the first major conflict in which drones have been deployed significantly².

The development of drone warfare goes beyond its use in the military. Drones absolutely add to a country’s hard power by spying, delivering accurate strikes, and projecting economic might. At the same time, they can also be employed as tools of soft power. Drone warfare creates compelling narratives, from propaganda films that are displayed all over the world to weapon systems that stand for resistance or technological dominance. Drones have been both a tactical necessity and a political symbol of Ukraine’s inventiveness and defiance. Iranian-supplied Shahed drones have allowed Russia to stand up to Western sanctions while still carrying out military activities. In the same manner, drones have become tools of foreign policy for nations like Turkey and Israel, who have boosted their geopolitical standing through defence cooperation and exports. Drones are particularly essential in modern security conversations since they can be employed for both conflict and as symbols.

From the aforementioned, a research question arises – **how are drone innovations considered as both hard power and soft power in modern warfare?** To promptly address it, we must comprehend the distinctions between “soft” power and “hard” power. In international relations, soft power and hard power are the methods of influence employed by a country in its interactions with other states. Soft power is a nation’s ability to achieve its objectives by appealing to other countries through attractiveness and psychological influence. A nation enhances its allure through cultural resources, political principles, and diplomatic strategies. Hard power refers to a nation’s capacity to achieve desired goals by coercing other countries through economic and military strength. Its mechanisms consist of incentives, such as financial rewards, and coercive measures, including economic sanctions and military intervention, to guarantee adherence. The integration of a nation’s soft and hard power policies to mutually support one another is termed smart power. The most efficacious techniques in international relations encompass a combination of soft and hard power.³

Overall, a thesis forms - Drone warfare innovation demonstrates a blend of physical and soft power. In Ukraine, drones are crucial fighting equipment (hard power) and effective tools of persuasion and nar-

1 Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 87.

2 Joachim Klerx, “Outlook into the Future of Warfare with Innovation Race,” *Navigating Human Enhancement* (2025): 445–449

3 “Soft and Hard Power,” EBSCO Research Starters

rative-building (soft power). These two factors underscore the significance of foreign partnerships for Europe's future security.

Main Part

Hard Power

Drones have changed tactical sensing and strikes in ways that disproportionately favour forces who are able to grow and adapt them swiftly. On the surveillance side, affordable commercial quadcopters (and adapted civilian platforms) deliver persistent reconnaissance and precision targeting that previously needed dedicated aircraft or expensive sensor packages. These systems commonly send real-time video for artillery correction, route clearance, and electronic order-of-battle updates, greatly enhancing tempo and accuracy at little expense⁴. First-person-view (FPV) drones and loitering munitions have transformed that sensing advantage directly into lethal consequences. FPV platforms - small, highly manoeuvrable, pilot-flown systems - are employed to hit soft-skinned vehicles, fortifications, and even to breach armour at close range; their agility makes them hard to detect and engage with traditional air-defence systems. At the same time, Iranian-designed Shahed (Geran) loitering munitions operate as longer-endurance, low-cost strike weapons intended to overwhelm air defences through massed launches and saturation attacks. The combination of multiple small FPVs for tactical strikes and bigger loitering bombs for strategic pressure produces a tiered drone strike environment⁵.

The ability to strike deep has changed quickly. Ukrainian-made strike UAVs and modified long-range systems have shown that they can hit logistics hubs, airbases, and energy facilities far behind the front line. These targets used to require manned aircraft or ballistic/missile weapons. These attacks have big effects on the economy and the way things work. For instance, destroying or disabling repair depots, fuel storage, and rail nodes makes enemies spread out, change their routes, and use expensive air defences, which makes it harder for them to do what they usually do. Using cheap drones to threaten high-value rear targets, on the other hand, creates a chronic imbalance because low-cost UAS can force high-cost responses. This changes how planners think about defence and deterrence⁶.

The asymmetric edge that drone warfare affords is one of the most interesting aspects about it. Often dubbed as the "poor man's air force", drones allow governments and even non-state actors access to surveillance and striking capabilities at a fraction of the expense of traditional airpower. Unlike manned aircraft, drones may be built or modified cheaply (with 3D printing) and deployed in vast numbers. This accessibility allows actors with modest resources to challenge technologically superior militaries by exploiting flaws in their defences. Russia's frequent deployment of Iranian-supplied Shahed loitering munitions practically equalises this disparity. By unleashing waves of cheap drones against Ukrainian infrastructure, Moscow compels Kyiv and its allies to use expensive NATO-standard surface-to-air missiles to protect themselves. This produces an adverse economic ratio: a \$20,000–\$50,000 high-end drone can compel the firing of a \$1–2 million interceptor missile. The saturation technique not only exhausts air defence inventories but also impairs Ukraine's capacity to choose higher-value targets such as cruise or ballistic missiles. This dynamic is driving theological shift - Initially seen as auxiliary instruments for reconnaissance or one-off strikes, drones have already become fundamental to modern military planning. Swarm tactics, where dozens or even hundreds of drones work simultaneously, are being evaluated as possible game-changers for overpowering defences and modifying battlefield geometry. The cost disparity is clear: a \$20,000 FPV

4 Juan Chulilla, "Ukraine Is the First 'Hackers' War," IEEE Spectrum, March 3, 2025

5 Arvid Carlstedt and Mikael Lyth, Usage, Effectiveness and Recent Trends of FPV-Drones in the Russian Invasion of Ukraine Based (Stockholm: Swedish Defence Research Agency, 2025), accessed October 8, 2025

6 "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond," CSIS, May 29, 2025, accessed October 8, 2025

drone, controlled by an experienced operator, in most cases will destroy approximately a \$3–5 million tank. And in some cases, an FPV drone costing as little as \$300 may destroy some military equipment ten and a hundred times its price⁷.

In this way, drones redefine hard power itself, moving emphasis from pricey platforms to scalable, cost-effective systems that affect both tactical battles and strategic deterrence.

Soft Power

Soft Power Drones do not qualify as weapons of mass destruction; yet, they possess significant soft power. It is important to comprehend, primarily, the symbolism they embody, the diplomatic advantages they may confer to a nation, the prestige linked to the novel inventions, and, last, the internet information warfare related to drone utilisation. During the initial phases of the conflict, the Bayraktar TB2 drone has evolved from a simple armament into a powerful emblem of Ukrainian defiance and fortitude. Since its introduction in the Russo-Ukrainian war, the Bayraktar drone has been associated with songs, street graffiti, murals, and numerous social media campaigns. The most notable of these is a Ukrainian patriotic song titled “Bayraktar”, released in March 2022, which commemorates the drone’s role in impeding the Russian advance⁸. The narrative of employing unmanned precision strike systems and adapting them to meet specific requirements contributes to global public sentiment, bolstering views of Ukraine’s technological innovation and bravery against a significantly larger opponent. Civilians, troops, and international supporters collectively assert that the Bayraktar transcends the definition of a mere drone⁹. Furthermore, drones like Bayraktar have also become tools of diplomatic leverage and influence. For Turkey, the production and export of the TB2 platform have enhanced its standing in numerous regions, placing Ankara not only as a drone provider but also as a partner with leverage in foreign policy. In Ukraine’s situation, the necessity for these drones has galvanised global aid, procurement, and diplomatic alignment. Financial campaigns and global contributions have facilitated Ukraine’s procurement of TB2 drones, while ally states have used the provision of these drones as an indication of political endorsement and shared principles¹⁰.

In September 2025, President of Ukraine Volodymyr Zelenskyy declared that domestic manufacturing of drones was so high that they will start exporting them to allied countries in the following years. Thus, it could be said that states which supply or maintain drone systems gain bargaining power in multilateral settings, especially when drone capability is perceived as shifting the balance in conflict or deterrence. Drones are formidable in not simply causing physical damage but moulding perceptions, narratives, and morale. In the Russo-Ukraine War, video footage from drone strikes – notably those on symbolic targets like airbases or logistic hubs – circulates widely, used by both Ukrainian and Russian sides to reinforce the narrative of fragility, reach, and high-stakes fight. The Guardian recounts how the repeated drone strikes in Crimea are designed to prove that behind-the-lines are not safe, bringing psychological pressure to bear on Russian forces¹¹. Online social media increases this effect by a lot—each and practically every day video clips of FPV/kamikaze drone assaults and damaged Russian gear serve as propaganda tools, increasing internal morale of Ukrainians and earning international sympathy from like-minded people. The obvious presence of drones in news feeds both normalises their threat and highlights the changing character of conflict, where transparency and image are part of the battlefield. Lastly, while on the theme of soft power, we

7 Kay Wackwitz, “FPV Drones and Military Use,” Drone Industry Insights (blog), September 22, 2025

8 Taner Dogan, “What Ukraine’s Viral Drone Song Says About Modern Day Warfare and Resistance,” LSE Media Blog, July 22, 2022, accessed October 8, 2025

9 Kateryna Panasiuk and Mykyta Vorobiov, “The Drone That Won Ukrainian Hearts,” CEPA, April 15, 2023, accessed October 8, 2025

10 Tom Joyner, “Türkiye’s Killer Drones in Ukraine Are Making Vladimir Putin’s Life Miserable, but Recep Tayyip Erdoğan Is Keeping Him Onside,” ABC News, December 2, 2022, accessed October 8, 2025

11 Dan Sabbagh, “Ukraine Strikes Psychological Blows in Drone Warfare Over Crimea,” The Guardian, August 22, 2022

must emphasise the prestige and influence through drone innovation. The ability to produce, deploy, and export drones has become a key tool for states seeking international prestige. Ukraine, for example, has seen its domestic UAV industry expand dramatically since 2022, as more than 500 drone manufacturers have emerged in the country (by December 2024)¹². This expansion not only boosts military capabilities but also strengthens national pride and sustains myths of technological resilience. By mid-2025, Ukraine was reputedly the world's top producer of tactical and long-range UAVs, with most of its UAVs originating from Ukrainian producers¹³.

Prestige in this sense operates partly as soft power: governments that are viewed as technologically sophisticated acquire credibility, attract foreign investment, and command attention in diplomatic forums. Their voices carry more weight in international debates about norms, defence strategies, and the regulation of emerging military technologies. Drone reputation thus becomes a resource: one that both governments, like Ukraine and Turkey, are intentionally building, linking their defence-industrial achievements with narratives of sovereignty, modernity, and influence.

Case Study

The most obvious case study for drone warfare innovation is the ongoing Russo-Ukrainian war. This war between Russia and Ukraine, which began in February 2022, has fast grown into a proving ground for new types of warfare, especially for unmanned aerial systems. Russia's initial advantage of scale and conventional strength has been mitigated by Ukraine's imaginative use of drones—both for its own operations and in creating foreign collaborations that magnify its capabilities. The struggle highlights how modern warfare is no longer merely about tanks, artillery, and force numbers—but about adaptation, coalition building, and integrating innovation under pressure. Although Ukraine's domestic production of drones has been well established, in practice the country has also leveraged strategic partnerships and external support to scale aggressive drone use, deepen strike ranges, and improve supporting systems. Over these past years we have seen several big developments in this case, like the innovation hub establishment in the capital of Ukraine, Kyiv, and the birth of the Drone Coalition. In late 2024 the EU launched a defence innovation hub in Kyiv, which has encouraged many different European drone manufacturers and R&D centres to set up operations in Ukraine — businesses from Germany, Estonia and Latvia have already opened their tiny factories. And discussing Latvia - In 2024, the Drone Coalition led by Latvia and the UK contributed €1.8 billion towards strengthening Ukraine's UAV capabilities, which covered procurement and production scale-ups¹⁴.

Let us proceed onto Russia. Russia has emphasised growing its drone warfare capability as a form of hard power: increasing sortie numbers, extending range, and overwhelming Ukrainian defences. On a production level, President Vladimir Putin declared that Russia was boosting up drone production almost tenfold to fulfil combat demands, with estimates aiming for over 1.4 million drones annually to continue sustained pressure on Ukraine. Key among these are the Iranian-origin Shahed loitering munitions, which Moscow uses to strike Ukrainian infrastructure, missile depots, energy supply systems, and civilian targets¹⁵. Russia likewise exploits its drone policy for soft power, though with variable outcomes. Through repeated drone strikes on Ukrainian territory, Moscow aims to project narrative power by showing capability, reach, and resilience despite sanctions and logistical constraints. The regular barrage of drones over Ukraine, especially targeting important infrastructure, conveys to both domestic and foreign audiences that

12 Interfax-Ukraine, "Over 500 Drone Manufacturers Emerge in Ukraine Over Past Three Years," December 16, 2024

13 Vladyslav Nedashkivskyi, "How Ukraine Became Global Leader in UAV Production and Deployment," Censor.net, August 5, 2025, accessed October 8, 2025

14 "Drone Coalition," Ministry of Defence – Republic of Latvia, accessed October 8, 2025

15 Reuters, "Putin Says Russia Is Ramping Up Drone Production Tenfold," September 19, 2024, accessed October 8, 2025

Russia remains able to hit even distant, well-defended targets¹⁶. This terrorises civilian morale, influences public opinion, and sends warnings to adversaries and allies about Russian perseverance. Russian soft power seems to rely more on coercion and propaganda than true appeal, as narrative attempts like “Russkiy Mir” have practically no influence or attractiveness compared to European democratic norms for normal Ukrainians who are afflicted by war.

Moreover, a critical vector of Russia’s drone expansion is its cooperation with Iran. Since at least late 2022, Iran has provided Russia with hundreds to possibly thousands of Shahed-series loitering munitions and Mohajer-6 drones. One of the major manifestations is the Alabuga Special Economic Zone in Tatarstan, where Iran is alleged to have shared documentation, technical know-how, and components to help Russia locally produce Iranian drone designs under licence or via reverse engineering. The aim is not only to scale up production but also to localise much of the supply chain, minimising dependence on external entities¹⁷.

European Security Implications

The extensive use of drones in the Russo-Ukraine War has caused Europe to immediately reassess its security posture. Recent drone incursions in Denmark, Poland, Romania and Estonia threaten the integrity of EU and NATO airspace, essential infrastructure, and civilian movement as they generate airspace alerts, cause the shutdown of airports and put a burden on border defences. Procurement, industrial capacity, and logistical agility appear as important vulnerabilities. Many EU states still rely on imported components like sensors and communications gear, and they suffer from fragmented defence procurement procedures. On the innovation front, the war has fostered innovations in drone tech. Ukraine is at the centre of this development, acting as a source of lessons and industrial production for Europe. Close cooperation between Ukrainian drone manufacturers, European start-ups, and EU member states is generating more modular, durable systems capable of functioning in contested electronic warfare scenarios. EU-Ukraine joint ventures and innovation hubs have been developed to increase knowledge transfer and build capacity¹⁸. Even more recent developments suggest that Europe is pushing for strategic autonomy and dual-use (civilian-military) innovation. Europe’s drone startups are also focused on applications outside combat, like surveillance, infrastructure monitoring, delivery and emergency response. The confluence of military innovation with civilian tech means that policies on export control, regulation, and standards will become crucial¹⁹. And lastly, lowering the dependence on foreign/imported components, primarily from China and South-Eastern Asian countries, and building greater joint EU/NATO production and procurement capability is increasingly considered as critical to Europe’s defence resilience²⁰.

Conclusion

Drone warfare in the Russo-Ukraine War has revealed a dual transformation in how states wage conflict, as today drones serve as both hard power tools (by shifting battlefield economics, enabling precise strikes, and saturating air defences) and soft power instruments (by shaping narratives of resistance, prestige, and technological leadership). For Ukraine, this has meant not only domestic innovation and production but also successful foreign alliances that boost its capabilities and symbolic position. Russia, however,

16 Global Defence News, “Russia Ramps Up Shahed Drone Production with \$1.7 Billion Iran Deal Amid Ukraine Conflict,” August 27, 2025, accessed October 8, 2025

17 European Pravda, “Washington Post Received Evidence of Iran–Russia Collaboration in Manufacturing Shahed Drones,” August 17, 2023

18 “Minding the Drone Gap: Drone Warfare and the EU,” European Union Institute for Security Studies, February 7, 2025, accessed October 8, 2025

19 “When Stars Align: Leveraging European Defence Budgets to Drive a Dual-Use Tech Boom,” European Union Institute for Security Studies, July 10, 2025, accessed October 8, 2025

20 Hilde Vautmans, “European Drone Capabilities and Defence Autonomy: Steps to Reduce Dependency on China and Foster Innovation in Drone- and Counter-Drone Systems,” European Parliament, 2025, accessed October 8, 2025

utilises drones for projected reach and durability, and its partnership with Iran has increased its own drone deployment, even during sanctions.

For Europe, these developments present both strategic opportunity and pressing risk. The continent's fragmented procurement procedures, dependency on foreign components, and shorter innovation cycles render it vulnerable to asymmetric drone threats. Yet Europe can also utilise the moment to develop strategic autonomy through combined R&D with Ukraine, standardised technologies, shared counter-drone infrastructure, and legislative frameworks that enable innovation while maintaining accountability and ethical values.

As a recommendation, European security policy should embrace a "Drone Innovation and Security Pact" under NATO and EU auspices. This pact would commit to coordinated investment in drone and counter-drone technologies, reciprocal tech sharing, compatible standards, and balanced hard/soft power development. Building such a framework will let Europe respond effectively to shifting threats, alter its defensive posture, and recapture strategic initiative in the drone era.

Bibliography

- Carlstedt, Arvid, and Mikael Lyth. 2025. Usage, effectiveness and recent trends of FPV-drones in the Russian invasion of Ukraine based. Research, Stockholm: Swedish Defence Research Agency. <https://surl.lu/moyvik>, Accessed 03.11.2025.
- Chulilla, Juan. 2025. "Ukraine Is the First 'Hackers' War'." IEEE Spectrum, March 3, 2025. <https://surl.li/lwdbwf>. Accessed 03.11.2025.
- Clausewitz, Carl von. On War. Translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1976.
- Dogan, Taner. 2022. What Ukraine's viral drone song says about modern day warfare and resistance. 22 July. <https://surl.li/sfuznu>, Accessed 03.11.2025.
- "Drone Coalition." n.d. Ministry of Defence - Republic of Latvia. <https://surl.li/mzcrug>, Accessed 03.11.2025.
- European Pravda. 2023. "Washington Post Received Evidence of Iran-Russia Collaboration in Manufacturing Shahed Drones." European Pravda, August 17, 2023. <https://surl.li/hsxivu>, Accessed 03.11.2025.
- Global Defence News. 2025. Russia Ramps Up Shahed Drone Production with \$1.7 Billion Iran Deal Amid Ukraine Conflict. 27 August. <https://surl.lu/xjktov>, Accessed 03.11.2025.
- Interfax-Ukraine. 2024. "Over 500 Drone Manufacturers Emerge in Ukraine Over Past Three Years." Interfax-Ukraine, December 16, 2024. <https://surl.li/jdvunm>, Accessed 03.11.2025.
- Joyner, Tom. 2022. "Türkiye's Killer Drones in Ukraine Are Making Vladimir Putin's Life Miserable, but Recep Tayyip Erdoğan Is Keeping Him Onside." ABC News. December 2, 2022. <https://surl.li/qwliire>, Accessed 03.11.2025.
- Klerx, Joachim. 2025. "Outlook into the future of warfare with innovation race." Navigating Human Enhancement 445-449. <https://surl.li/htccqh>, Accessed 03.11.2025.
- "Minding the Drone Gap: Drone Warfare and the EU." 2025. European Union Institute for Security Studies. February 7, 2025. <https://surl.li/etvkxh>, Accessed 03.11.2025.
- Nedashkivskiy, Vladyslav. 2025. How Ukraine became global leader in UAV production and deployment. 5 August. <https://surl.lu/fveake>, Accessed 03.11.2025.
- Panasiuk, Kateryna, and Mykyta Vorobiov. 2023. "The Drone That Won Ukrainian Hearts." CEPA. April 15, 2023. <https://surl.li/jsjvwq>, Accessed 03.11.2025.
- Reuters. 2024. Putin says Russia is ramping up drone production tenfold. 19 September. <https://surl.li/pzcddu>, Accessed 03.11.2025.
- Sabbagh, Dan. 2022. "Ukraine Strikes Psychological Blows in Drone Warfare Over Crimea." The Guardian, August 22, 2022. <https://surl.li/uiubgw>, Accessed 03.11.2025.
- "Soft and Hard Power | Research Starters | EBSCO Research." n.d. EBSCO. <https://surl.li/vskaut>, Accessed 03.11.2025.
- "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond." 2025. May 29, 2025.. <https://surli.cc/itnriv>, Accessed 03.11.2025.

- Vautmans, Hilde. n.d. "Parliamentary Question | European Drone Capabilities and Defence Autonomy: Steps to Reduce Dependency on China and Foster Innovation in Drone- and Counter-drone Systems | E-000668/2025 | European Parliament." © European Union, 2025 - Source: European Parliament. <https://surl.li/boupmr>, Accessed 03.11.2025.
- Wackwitz, Kay. 2025. "FPV Drones and Military Use | Drone Industry Insights 2025." Drone Industry Insights (blog). September 22, 2025. <https://surl.li/xngubz>, Accessed 03.11.2025.
- "When Stars Align: Leveraging European Defence Budgets to Drive A." 2025. European Union Institute for Security Studies. July 10, 2025. <https://surl.li/xejxpt>, Accessed 03.11.2025.

ARTIFICIAL INTELLIGENCE AS A FORCE MULTIPLIER FOR GEORGIA'S DEFENSE CAPABILITY

Major Nika Zhorzholiani

The Learner of a Master's Degree Program (Security Studies) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Zurab Agladze

Professor of Master's Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This article investigates how the integration of Artificial Intelligence (AI) improves the efficiency of the Military Decision-Making Process (MDMP), focusing on smaller nations like Georgia. They face asymmetric threats and resource constraints. The hypothesis is that AI enhances MDMP effectiveness by speeding up data processing in Intelligence Preparation of the Battlefield (IPB) and shortening the decision cycle. Operational challenges during the 2008 Russia-Georgia War underscore the need for faster, more comprehensive decision support tools.

AI can serve as a force multiplier for the Georgian Defense Forces (GDF), increasing efficiency without proportional rises in personnel or traditional equipment. AI integration accelerates MDMP phases, rapidly processes data for Mission Analysis, and creates situational awareness. In Course of Action (COA) Development, it offers a broader array of planning options under time pressure. AI-enhanced IPB automates terrain analysis and improves prediction of enemy actions—critical in Georgia's complex topography. These capabilities help accelerate the OODA Loop (Observe, Orient, Decide, Act) and achieve a tempo advantage.

To ensure human command authority and ethical accountability, AI implementation requires a Human-in-the-Loop model. The GDF should establish a robust data infrastructure for training AI models. They also need comprehensive personnel training for the critical evaluation of AI outputs. AI offers an asymmetric advantage for the GDF. It accelerates analysis and improves decision quality. These benefits directly support the strategic technological goals outlined in the Ministry of Defense's Vision 2030.

Keywords: Artificial Intelligence, Georgian Defense Forces, Military Decision-Making Process, OODA Loop, Human-Machine Teaming, Force Multiplier

Introduction

Modern warfare depends on the speed and quality of decision-making at all command levels.¹ AI integration into military planning processes represents technological shifts in contemporary defense operations. For smaller nations, which face asymmetric threats and resource constraints, AI offers potential advantages. It could serve as a force multiplier. AI enhances capabilities without proportional increases in personnel or traditional equipment.

The 2008 Russia-Georgia War demonstrated challenges in military decision-making under time pressure. The Georgian Armed Forces (GDF) were ordered to prevent Russian military vehicles from passing through the Roki Tunnel; suppress positions attacking Georgian forces; and protect civilian populations.² The challenges faced by GDF include rapid intelligence processing, course of action development, and synchronized multi-domain operations against a numerically superior adversary. Georgia's Ministry of Defense Vision 2030 recognizes the changing character of conflict. According to the Strategic document, Russia will continue aggressive actions through hybrid pressure, and technological innovation is essential for Georgian defense. This creates policy space for AI integration initiatives.³ International interest in military AI applications is growing. The United States' near-peer adversaries (Russia and China) recognize AI's potential to transform military operations. They are pursuing it to enhance the speed, reach, precision, and lethality of their operations. Despite this, there is limited research on how smaller nations can effectively integrate these technologies.⁴

Research Question (RQ): Can artificial intelligence integration reduce the Military Decision-Making Process cycle time by at least 40% while maintaining or improving decision quality in resource-constrained military forces?

Hypothesis (H): Artificial intelligence reduces the Military Decision-Making Process cycle time from 24-48 hours to 12-18 hours (40-50% reduction) while increasing COA generation from 2-3 to 8-10 viable options and maintaining 85%+ decision quality metrics.

Variable Operationalization. Independent Variable - AI integration level measured through: Automation degree: 0-100% of analytical tasks automated; Processing speed: Documents analyzed per hour (baseline 50-100 vs AI-enabled 1000+); Human-machine configuration type (Human-in-Loop as primary model). Dependent Variable - MDMP effectiveness measured through: Decision cycle time: Reduction percentage from baseline 24-48 hours; Planning quality metrics: COA quantity: Number of viable options generated (baseline 2-3); Threat assessment accuracy: Percentage of correctly predicted enemy actions (baseline 70%); Wargaming iterations: Number of scenarios tested (baseline 1-2).

Methodology: The Study employs qualitative research methods. Utilizes content analysis and case study approaches. The research draws on secondary sources, including military doctrine publications, academic literature on AI military applications, and historical case analysis. The Georgia 2008 case provides evidence for examining decision-making challenges in conventional military

1 J. Kean, Matthew „Information Advantage“. Military Review, November-December 2022, p.111-118.

2 Cornell, Svante E., and S. Frederick Star. Guns of August 2008: Russia's War in Georgia. Oxford, UK: Routledge, 2009. p. 169

3 საქართველოს თავდაცვის სამინისტრო. სამინისტროს ხედვა 2030. თბილისი: საქართველოს თავდაცვის სამინისტრო, 2021. <https://surl.li/pnateq>, pdf.გვ. 14

4 Ryan Fedasiuk, Emily S. Weinstein, and Anna Puglisi. „Harnessing Lightning: How the Chinese Military is Adopting Artificial Intelligence“. Center for Security and Emerging Technology, Georgetown University, October 2021., p. 5

operations. This research has limitations: Analysis relies on publicly available information, and classified AI capabilities are unavailable. Findings represent the 2024-2025 timespan.

Main Part

Research examines three interconnected frameworks: MDMP, IPB, and the OODA Loop. Understanding these established military planning methodologies helps analyze how AI integration enhances them.

The Military Decision-Making Process (MDMP)

MDMP is a systematic approach to military planning. The US and most NATO member countries use it. The Georgian Defense Forces have adopted this planning methodology. The seven-step process provides structure to military planning under uncertain conditions. Steps are: receipt of mission, mission analysis, course of action development, course of action analysis, course of action comparison, course of action approval, and orders production.⁵

Recent research demonstrates how AI can augment specific MDMP steps. During mission analysis, AI algorithms rapidly process vast amounts of data from diverse sources. They include intelligence reports, sensor feeds, and open-source information. Then it provides commanders with a situational understanding. In the course of action development, AI generates multiple options. COAs are based on facts and assumptions about enemy capabilities, terrain effects, and logistics constraints. This expands the range of planning options beyond what staff could manually develop in the available time. AI addresses a central challenge: time pressure. Traditional MDMP requires 24-48 hours for brigade-level planning. When operating inside an enemy's decision cycle, this timeline becomes a critical vulnerability.⁶ AI-driven automation of routine analytical tasks can reduce this timeline while potentially improving analysis quality. AI handles larger data volumes and identifies patterns humans might miss.

Intelligence Preparation of the Battlefield (IPB)

IPB serves as an input to MDMP. The four-step IPB process influences all subsequent planning: define the operational environment, describe environmental effects, evaluate the threat, and determine threat courses of action.⁷ AI applications in IPB focus on data synthesis and pattern recognition. Modern conflicts generate enormous volumes of intelligence from multiple sources: satellite imagery, signal intelligence, human intelligence reports, cyber domain indicators, and open-source materials. Processing information manually creates bottlenecks that delay decision-making. Machine learning algorithms might automate terrain analysis, identifying key terrain features, mobility corridors, and defensible positions across large operational areas. AI might process historical data on threat organizations. It predicts likely courses of action with probabilistic assessments.

⁵ U.S. Army. Field Manual 5-0, Planning and Orders Production. Washington, DC: Headquarters, Department of the Army, November 2024.p. 5-1

⁶ Michael J. Zequeira, „Modernizing MDMP: Leveraging AI to Transform the Military Decision-Making Process“. Military Review Online Exclusive, August 2025.p. 2

⁷ U.S. Army. Army Techniques Publication 2-01.3, Intelligence Preparation of the Battlefield. Washington, DC: Headquarters, Department of the Army, March 2019.p. 1-2

The OODA Loop Framework

John Boyd, a former US pilot, has constructed the OODA Loop: Observe, Orient, Decide, and Act. It provides a conceptual model for decision-making cycles in competitive environments. The OODA Loop is foundational to Western military thought about decision superiority.

The Observe phase collects information from sensors and human observation about the environment. Staff face an overwhelming volume of observations from numerous sources. AI excels at filtering and prioritizing this information. AI allows human decision-makers to focus on relevant data rather than being flooded by raw feeds. The Orient phase involves making sense of observations through the lens of experience, cultural background, and analytical frameworks. Boyd considered this phase to be critical. AI might identify patterns and relationships in data, but it still requires human judgment to determine meaning and significance. An efficient approach combines AI's pattern recognition capabilities with human contextual understanding. In the Decide phase, commanders select courses of action from available options. AI supports it by rapidly war-gaming multiple options and identifying the strengths and weaknesses of each. Then AI provides probabilistic assessments of outcomes. The final decision remains with human commanders who bear responsibility for ethical and strategic considerations. The Act phase is the execution of decisions. While this paper does not address autonomous weapons, AI can coordinate complex actions across multiple domains, deconflict fires, and manage logistics in ways that exceed human processing capacity. Boyd argued that victory goes to the side that can cycle through this loop faster than their opponent, creating a tempo advantage that compounds over time.⁸

AI as a Force Multiplier: Conceptual Foundation

The concept of force multiplier refers to capabilities that increase the effectiveness of military forces without proportional increases in size. Examples include radio communication, precision-guided munitions, and night vision technology. These innovations allowed smaller forces to achieve effects previously requiring much larger formations. AI functions as a force multiplier through the following mechanisms. It enables faster decision-making by automating routine analytical tasks. It improves decision quality by processing more information than human staff can manually. It allows a small staff to manage a capability that previously required much larger organizations.⁹ For GDF, these multiplier effects are particularly relevant given constraints on defense personnel and budget.

Human-Machine Teaming Models

Understanding how humans and AI systems interact requires clear frameworks for their relationship. Three models have emerged from research. Human-on-the-Loop, where AI systems operate with autonomy, but humans maintain the ability to intervene and override decisions. The human monitors system behavior and adjusts parameters. It is suitable for time-sensitive tactical

⁸ Patrick Hofstetter, Marius Geller, and Florian Gerster. „The Impact of Artificial Intelligence on the Military Decision-Making Process and Mission Command“. The Defense Horizon Journal, September 2025.p. 7.

⁹ Zachary S. Davis, „Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise“. In Strategic Latency: Red, White, and Blue - Managing the National and International Security Consequences of Disruptive Technologies, edited by Zachary S. Davis and Michael Nacht. Lawrence Livermore National Laboratory, Center for Global Security Research, 2018.p. 4

applications where millisecond response times matter. Here, human judgment remains essential for ethical and legal compliance.

Human-in-the-Loop requires explicit human approval before AI recommendations become actions. AI provides analysis, develops options, and presents recommendations. Human makes final decisions. This approach maintains clear accountability and control, while staff benefit from AI's analytical capabilities. Most operational planning applications employ this model during the MDMP and IPB processes, where ethical considerations are paramount.

Human-outside-the-Loop: Fully autonomous systems operate without human involvement in real-time decisions. This offers maximum speed, but it also presents risks related to accountability, ethics, and strategic coherence.¹⁰ Current international humanitarian law and military ethics generally oppose making lethal decisions without human oversight. This model may be appropriate for certain support functions, such as logistics or the defensive cyber domain.¹¹

For the GDF, the human-in-the-loop model is an appropriate approach for MDMP and IPB applications. This preserves command authority and decision-making responsibility while gaining AI's speed and analytical advantages. MDMP provides structure but often requires substantial time—24 to 72 hours at battalion and brigade levels for complete planning cycles. Time pressure represents the most significant challenge when facing adversaries who can act faster. AI integration addresses this challenge in specific ways for each MDMP phase.

Mission Analysis (MDMP)

Mission analysis converts higher headquarters' orders into an understanding of specified tasks, implied tasks, and mission variables. Staff analyzes mission, terrain, weather, enemy, troops, time available, and civil considerations. This analysis generates products including restated mission, commander's critical information requirements, and initial planning guidance. AI might process reports, open-source information, and sensor data faster than human analysts working manually. A traditional intelligence section might review dozens of intelligence summaries and reports over several hours. AI algorithms might process hundreds/thousands of documents in minutes, identifying relevant information and flagging items that require human attention. Recent applications show AI analyzing satellite imagery to identify changes in enemy dispositions, processing signals intelligence to map communication networks, and fusing multiple intelligence sources. These capabilities enable the intelligence cell to provide commanders with a more complete situational understanding in less time. Quantitative improvements demonstrated in recent studies show: document processing increased from 50-100 reports per day to over 1000 reports per day (10-20x increase). Analysis time: From 6-8 hours to 45-90 minutes for brigade-level mission analysis (80% reduction). Critical information extraction: 95% accuracy in identifying the commander's critical information requirements compared to a 70% manual baseline.¹²

10 Swedish Defence Research Agency. „Exploring Decision Advantages: Artificial Intelligence in Dynamic Targeting and the Joint Targeting Cycle“. Stockholm: FOI, 2024.p. 243

11 Paul Scharre, „Army of None: Autonomous Weapons and the Future of War“. New York: W.W. Norton & Company, 2018.p. 29-30

12 Michael J. Zequeira, „Modernizing MDMP: Leveraging AI to Transform the Military Decision-Making Process“. Military Review Online Exclusive, August 2025.p. 3

Course of Action Development (MDMP)

Developing multiple courses of action requires staff sections to consider numerous factors: enemy capabilities, terrain effects, logistics constraints, timing requirements, and risk assessment. Traditional planning typically generates two to three detailed COAs due to time and human factors. More options provide commanders with flexibility, but manual development of additional COAs exceeds available staff capacity. Research indicates AI-enabled planning can generate 8-10 distinct, doctrinally sound COAs. At this time, traditional staff prepare two to three options. Each option includes complete task organization, scheme of maneuver, and synchronization matrix. It means a 300-400% increase in planning options. More COAs provide commanders with decision space rather than minor variations on a single concept. AI systems might generate broader ranges of potential courses of action by exploring combinations of schemes of maneuver, support plans, and timing. AI technology evaluates each option against planning factors. Technology identifies feasible approaches and eliminates options that violate physical or doctrinal constraints.¹³ Quality control remains essential. AI should generate realistic, executable options rather than theoretical possibilities that ignore practical constraints.

Course of Action Analysis – Wargaming (MDMP)

Wargaming tests COAs against enemy responses. It identifies strengths, weaknesses, and required resources. Traditional wargaming follows doctrinally prescribed methods. The manual process is time-consuming and produces somewhat subjective results, depending on staff experience and assumptions. AI might conduct rapid computerized wargaming. AI runs multiple iterations with varied assumptions about enemy actions and friendly capabilities. This approach provides probabilistic assessments of outcomes rather than single most likely scenarios. For example, AI wargaming might indicate that a COA succeeds in 70% of simulation runs, while an alternative succeeds in 85% of runs under the same conditions. Quantitative analysis from military simulations shows: Traditional wargaming: 1-2 iterations with single most-likely enemy COA; AI-enabled wargaming: 100+ iterations testing multiple enemy responses; Outcome prediction accuracy: Improved from 60% to 85% when validated against historical operations; Time requirement: Reduced from 4-6 hours to 30-45 minutes per COA. In 2008, GDF faced decisions about defensive positions near the Roki Tunnel: whether to defend forward, establish a defense in depth, or conduct mobile defense. AI wargaming could have rapidly evaluated each option against various Russian force dispositions and arrival times, helping commanders assess trade-offs between options.¹⁴

AI Enhancement of Intelligence Preparation of the Battlefield

IPB provides the intelligence foundation for operations, analyzing the operational environment to understand how terrain, weather, and enemy capabilities affect operations. The four-step process generates products, including modified combined obstacle overlays (MCOO), threat evaluation matrices, and situation templates (SITTEMP), which show likely enemy courses of action.

¹³ Mike Farmer, „Clausewitz’s Ghost: Thinking in Time with AI-Enabled Military Planning. Military Review“, November-December 2022, 65-72. p. 69

¹⁴ Ibid. Farmer, 2022, p. 72.

Terrain Analysis Automation

Identifying key terrain, avenues of approach, obstacles, cover, and observation traditionally requires intelligence analysts to study maps and conduct reconnaissance. The process takes days for large areas of operation and produces static products. They may not reflect the enemy's current conditions. Machine learning models can automate much of this analysis using digital elevation data, satellite imagery, and geospatial databases. Neural networks trained on military terrain analysis can identify mobility corridors, feasible defensive positions, and likely engagement areas across the entire AO. This automation reduces the time required for initial terrain analysis and enables rapid updates when conditions change. For Georgia's terrain, characterized by mountains, river valleys, and limited road networks, automated terrain analysis offers advantages. The complex topography creates potential avenues of approach and defensive positions that manual analysis might overlook. AI can systematically evaluate these options, ensuring planning staff consider the full range of terrain-based opportunities. Performance metrics for AI-enabled terrain analysis include: Area coverage: 100 km² analyzed in 15 minutes vs 4-6 hours manually; Mobility corridor identification: 95% accuracy compared to ground reconnaissance; Defensive position evaluation: 200+ potential sites assessed vs 10-20 manually; Update frequency: Real-time vs daily/weekly updates.¹⁵

Threat Evaluation and COA Prediction

Understanding enemy capabilities and predicting likely courses of action represents one of IPB's most challenging aspects. Intelligence staff must analyze enemy doctrine, recent operations, command philosophy, and capabilities to develop enemy COA templates. This analysis often relies heavily on analyst experience and may miss novel approaches adversaries might employ. AI systems can process historical data on enemy operations, identifying patterns in how specific units or commanders behave. Machine learning algorithms might recognize operational signatures—patterns of preparation and execution that indicate particular approaches. This pattern recognition supplements human analysis, potentially identifying enemy COAs that analysts might not consider. This application requires caution. Adversaries may deliberately deviate from historical patterns to achieve surprise. AI trained on past behavior might fail to predict innovative approaches.

OODA Loop Acceleration Through AI

Observation Enhancement: Modern military forces collect enormous volumes of observations. The challenge is not a lack of data but information overload—human operators cannot process everything available. Important indicators may be missed because analysts cannot review all incoming information in real time. AI excels at prioritizing information streams. Algorithms might monitor multiple intelligence feeds simultaneously and flag items that match priority intelligence requirements.¹⁶ This automated filtering allows intelligence staff to focus attention on relevant observations. For smaller defense forces, observation enhancement is particularly valuable. The limited number of intelligence analysts cannot match the collection processing capacity of larger militaries.

¹⁵ Cyran, C.Nitzl, A. Krstanovic, S. Borghoff, & M., U. The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process. 2024.p 10-17.

¹⁶ Ibid. Hofstetter et al., 2025, p. 8

Orientation Support: This is where experience, cultural understanding, and judgment matter most. AI integration becomes most complex, as orientation involves subjective interpretation that machines cannot fully replicate. AI might support orientation by identifying patterns and relationships in data that human analysts might miss. Correlation analysis might reveal connections between seemingly unrelated events. Trend analysis might identify gradual changes that become significant only when viewed over time. Network analysis might map relationships between threat actors, identifying key nodes and influence patterns. The key is treating AI as an assistant rather than a replacement for human judgment. AI provides data-driven insights that inform orientation. Final interpretation requires human contextual understanding and ethical judgment.

Decision Support: The decision phase involves selecting a course of action from available options. AI cannot make decisions for commanders—accountability and ethical responsibility require human decision-making. However, AI can structure decision-making by presenting options with associated assessments of risks, resource requirements, and probable outcomes. Decision support systems can rapidly evaluate multiple options against the commander's criteria, ranking alternatives and highlighting trade-offs. For example, if a commander prioritizes minimizing friendly casualties while maintaining offensive momentum, AI can assess which COAs best balance these competing objectives based on wargaming results. This support is particularly valuable under time pressure when commanders must decide quickly. Rather than relying entirely on intuition or experience, commanders can rapidly review AI analysis of options. The final decision remains human, but the supporting analysis provides a systematic evaluation that time pressure might otherwise prevent.

Case Application: 2008 Russia-Georgia War

The August 2008 conflict between Russia and Georgia provides a context for understanding how AI-enhanced decision-making might function in realistic operational conditions. While this analysis cannot definitively prove AI would have changed outcomes, it illustrates where technology might have addressed specific decision-making bottlenecks. **Decision-Making Challenges in 2008:** Georgian forces faced several critical decision-making challenges during the conflict. **Time pressure:** Russian troops moved through the Roki Tunnel faster than Georgian planners had anticipated. Georgian commanders had to make rapid decisions about defensive positions, counterattack timing, and force allocation without time for comprehensive planning processes. Georgian forces dealt with incomplete intelligence about Russian force composition and arrival timing. **Uncertainty** about enemy strength and capabilities complicated planning, as did limited intelligence about Russian intentions beyond South Ossetia.¹⁷ **Coordination** across multiple units and domains proved difficult. Air defense, maneuver, and logistics operated somewhat independently rather than as integrated operations.

Potential AI Applications: AI-enhanced MDMP could have addressed some of these challenges. Rapid IPB analysis of terrain, identifying defensive positions, engagement areas, and Russian avenues of approach, might have enabled faster development of defensive plans. Automated terrain analysis could have evaluated multiple defensive options simultaneously, presenting commanders with assessed alternatives rather than requiring staff to develop each option manually.

¹⁷ Ibid. Farmer, 2022, p. 68

Hypothetical AI-Enhanced Analysis. Based on Farmer's research using Theater Analysis Model calculations, AI wargaming of the 2008 scenario would have provided Georgian commanders with quantitative assessments: Forward defense at Tskhinvali: 30% probability of success against Russian main effort; Defense at Roki Tunnel: 70% probability if Georgian 4th Brigade deployed within 6 hours; Defense in depth near Gori: 85% probability but conceding South Ossetia's Russian force combat power: 59 (TAM value) requiring 2:1 Georgian force ratio for successful defense; Critical timing: 6-8 hour window to position forces before Russian breakthrough. These probabilistic assessments, generated in 1-2 hours rather than 24-48 hours of traditional planning, would have enabled faster, more informed decision-making under extreme time pressure. AI wargaming of different defensive approaches could have provided probabilistic assessments of outcomes.¹⁸ For instance, if AI analysis indicated that defending forward near Tskhinvali had a low probability of success against Russian forces moving through the Roki Tunnel, it would suggest a strategic reevaluation. At the same time, defense in depth near Gori offered better prospects; commanders could have weighed this analysis in their decision-making.

However, technology alone would not have resolved all challenges. Even with faster planning tools, Georgian forces faced fundamental limitations in combat power relative to Russian forces. AI might have enabled better use of available capabilities, but could not overcome material disadvantages. This illustrates an important principle: AI serves as a force multiplier for existing capabilities rather than a substitute for military power.

Data Infrastructure Requirements: AI systems require substantial data for training and operation. Machine learning algorithms learn from historical examples, meaning Georgia would need archives of past operations, intelligence assessments, and planning products to train AI effectively.¹⁹ Additionally, real-time data feeds from sensors and intelligence sources are necessary for AI to provide current analysis. Building this data infrastructure represents a significant investment. Defense forces should establish data collection protocols, storage systems, and data management practices. This infrastructure development should begin before procuring the central AI system, as algorithms cannot function without adequate data foundations.

Military personnel should understand AI capabilities and limitations to use these tools efficiently. This requires education and training at multiple levels: commanders need conceptual understanding to supervise AI-assisted planning; staff officers need practical training on specific AI tools; and technical specialists need deep expertise in AI system operation and maintenance. Georgia's military education system should incorporate AI-related content into professional military education. This education should emphasize critical evaluation of AI outputs rather than uncritical acceptance. As Georgia pursues NATO integration, defense systems should maintain compatibility with Alliance standards and procedures. This means adopting AI approaches that align with NATO doctrine, using data formats compatible with Alliance systems, and supporting the ability to operate with partner forces. NATO itself is developing AI policies and standards that Georgia should track closely. Early adoption of emerging NATO AI frameworks would position Georgia favorably for eventual membership while ensuring AI investments align with Alliance requirements.

¹⁸ Ibid., p. 70

¹⁹ U.S. Department of Defense. Data, Analytics, and Artificial Intelligence Adoption Strategy. Washington, DC: Department of Defense, November 2023, p. 5

Conclusion

Key Findings validate the hypothesis: AI integration reduces MDMP cycle time by 40-50%, from 24-48 hours to 12-18 hours at the brigade level, while maintaining decision quality. This time reduction comes primarily from 80% faster IPB processing and a 10x increase in document analysis capacity. Planning quality improves through the generation of 8-10 viable COAs compared to the traditional 2-3, providing commanders with genuine options. Threat assessment accuracy increases from 70% to 85% through pattern recognition and probabilistic analysis of enemy courses of action.

AI excels at information filtering and pattern recognition. The machine helps intelligence staff manage information overload and identify relevant indicators in large data volumes. Decision-making ultimately requires human judgment. The human-in-the-loop model is appropriate for operational planning applications. AI implementation requires careful attention to data quality, personnel training, and doctrinal integration. Technology alone provides no benefits. Organizations should develop data infrastructure, train personnel, and adapt procedures to employ AI capabilities effectively. For Georgia, these implementation challenges are manageable but require sustained institutional commitment. AI offers particular advantages related to resource constraints. The GDF cannot match larger neighbors in personnel or equipment quantities. AI-enhanced decision-making offers a potential asymmetric advantage. This force multiplication effect directly addresses Georgia's strategic challenges.

The 2008 Russia-Georgia War case illustrates specific decision-making challenges: Time pressure, incomplete intelligence, and coordination difficulties. While AI would not have eliminated these challenges, it could have provided tools for faster intelligence processing, more systematic evaluation of actions, and better coordination across domains. Looking forward, Georgia's Ministry of Defense Vision 2030 correctly identifies technological innovation as essential for defense capabilities. The technology enables rather than replaces traditional military capabilities.

This research identified areas requiring additional study. A detailed cost-benefit analysis of specific AI systems would inform procurement decisions. Controlled experiments comparing traditional and AI-assisted MDMP. This would generate data on actual time savings and decision quality improvements.

Bibliography

- საქართველოს თავდაცვის სამინისტრო. *სამინისტროს ხედვა 2030*. თბილისი: საქართველოს თავდაცვის სამინისტრო, 2021. <https://surl.li/mpcrs>
- Cornell, Svante E., and S. Frederick Star. *Guns of August 2008: Russia's War in Georgia*. Oxford, UK: Routledge, 2009.
- Davis, Zachary S. *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise*. In *Strategic Latency: Red, White, and Blue - Managing the National and International Security Consequences of Disruptive Technologies*, edited by Zachary S. Davis and Michael Nacht. Lawrence Livermore National Laboratory, Center for Global Security Research, 2018.
- Farmer, Mike. *Clausewitz's Ghost: Thinking in Time with AI-Enabled Military Planning*. *Military Review*, November-December 2022, 65-72.
- Fedasiuk, Ryan, Emily S. Weinstein, and Anna Puglisi. *Harnessed Lightning: How the Chinese Military is Adopting*

- Artificial Intelligence*. Center for Security and Emerging Technology, Georgetown University, October 2021.
- Hofstetter, Patrick, Marius Geller, and Florian Gerster. *The Impact of Artificial Intelligence on the Military Decision-Making Process and Mission Command*. The Defense Horizon Journal, September 2025.
- International Committee of the Red Cross. *Artificial Intelligence and Related Technologies in Military Decision-Making on the Use of Force in Armed Conflicts: Current Developments and Potential Implications*. Geneva: ICRC and Geneva Academy, March 2024.
- Kean, Matthew J. *Information Advantage*. Military Review, November-December 2022, 111-118.
- Nitzl, Cyran, C., Krstanovic, A., Borghoff, S. & M., U. The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process. 2024.
- Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton & Company, 2018.
- Swedish Defence Research Agency. *Exploring Decision Advantages: Artificial Intelligence in Dynamic Targeting and the Joint Targeting Cycle*. Stockholm: FOI, 2024.
- U.S. Army. *Army Techniques Publication 2-01.3, Intelligence Preparation of the Battlefield*. Washington, DC: Headquarters, Department of the Army, March 2019.
- U.S. Army. *Field Manual 5-0, Planning and Orders Production*. Washington, DC: Headquarters, Department of the Army, November 2024.
- U.S. Department of Defense. *Data, Analytics, and Artificial Intelligence Adoption Strategy*. Washington, DC: Department of Defense, November 2023.
- Zequeira, Michael J. *AI as Combat Multiplier: Revolutionizing the U.S. Army Military Decision-Making Process*. Military Review Online Exclusive, September 2024.
- Zequeira, Michael J. *Modernizing MDMP: Leveraging AI to Transform the Military Decision-Making Process*. Military Review Online Exclusive, August 2025.

THE U.S.–UKRAINE ENGINEERING PARTNERSHIP: STRATEGIC COOPERATION FOR RECONSTRUCTION AND TECHNOLOGICAL DEVELOPMENT

Tatia Razmadze

The Junker of a Bachelor's Degree (Mechanical Engineering) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The presented paper offers a comprehensive analysis of the strategic cooperation between the United States and Ukraine in the domain of engineering equipment, infrastructure materials, and technological exchange. In the context of ongoing conflict and large-scale destruction of Ukraine's critical infrastructure, the study underscores that the rapid and efficient restoration of transportation, energy, and industrial systems constitutes not only an element of postwar recovery but also a vital component of Ukraine's broader national security and economic stability strategy. The research focuses on two principal dimensions of this cooperation. The first examines the supply of American heavy engineering machinery and advanced construction materials, which play a decisive role in rebuilding damaged roads, bridges, and energy infrastructure. The second explores the transfer of technological knowledge and engineering expertise, which contributes to the gradual adoption of modern Western standards of construction, logistics management, and industrial safety within Ukraine's reconstruction efforts. Furthermore, the paper analyzes the U.S. involvement in engineering modernization projects, particularly through funding mechanisms, private-sector partnerships, and the integration of digital monitoring systems for infrastructure resilience. Special attention is given to the reconstruction of Ukraine's road networks and power systems, areas identified as critical for ensuring operational continuity, economic mobility, and regional connectivity.

In addition to identifying achievements, the paper discusses the primary challenges facing this partnership, including persistent security risks, logistical constraints, and coordination gaps among local and international actors. The study concludes by evaluating the long-term prospects of U.S.–Ukraine engineering cooperation in the context of sustainable reconstruction, technological sovereignty, and Euro-Atlantic integration, arguing that this collaboration serves as a model for resilience-oriented infrastructure policy in post-conflict settings.

Keywords: Strategic Cooperation; Engineering Reconstruction; Technological Transfer; Infrastructure Resilience; U.S.–Ukraine Partnership; Sustainable Development; Euro-Atlantic Integration.

Introduction

Since February 2022, Ukraine has faced the most large-scale infrastructural damage in Europe, including the massive destruction of critical facilities—such as power plants, road networks, and residential buildings. The urgent and effective need for reconstruction is not only an economic challenge; it is directly linked to the safety of Ukraine’s population, the humanitarian crisis, and the nation’s overall stability. Addressing this challenge requires not only financial resources but also advanced engineering technologies, equipment, and expertise. The speed and efficiency of Ukraine’s recovery depend largely on the quality of international cooperation. The United States is one of the most important strategic partners in this process.

Despite the broad humanitarian and military assistance, U.S.-Ukraine partnership in the engineering sector still requires in-depth analysis. The central issue lies in understanding how cooperation in the supply of engineering equipment and materials ensures the efficiency of critical infrastructure reconstruction, and how this partnership contributes to the implementation of sustainable and modern engineering standards in Ukraine.¹

This paper aims to assess the current impact and long-term prospects of the U.S.-Ukraine engineering partnership. How will the heavy engineering equipment, critical materials, and technological expertise provided by the United States impact the operational effectiveness of Ukraine’s reconstruction process? What long-term impact does this partnership have on the introduction of modern, Western engineering standards in Ukraine, and how does this process contribute to the sustainability of the country’s infrastructure and Euro-Atlantic integration?

What are the key security, logistical and governance challenges facing this collaboration and how are these risks being mitigated?

Supply of Heavy Engineering Equipment and Its Role - One of the most important components of U.S. assistance is the supply of heavy construction and engineering machinery. This equipment is crucial for the timely clearance of debris, demolition, and acceleration of new construction processes. The supplied machinery includes high-performance excavators, bulldozers, graders, mobile cranes, and specialized bridge-building equipment. These technologies help optimize resources and minimize human error. For example, advanced American machinery significantly reduces the time required to restore critical road infrastructure—an essential factor in maintaining logistical supply chains.

The long-term impact of this cooperation lies in knowledge transfer. American engineers and consultants are actively involved in project management and technical training. Ukrainian engineers and builders receive training on operating new U.S.-made machinery and processing innovative materials. Moreover, with American support, the use of digital systems such as DREAM has expanded, enhancing project management transparency, improving budget accuracy, and reducing corruption risks.²

The importance of equipment supply is not only quantitative but also qualitative, as American machinery is known for its high operational standards and reliability. This minimizes the risk of accidents and increases work efficiency under critical conditions. Partnerships between the U.S.

¹ “Sustainable and Resilient Infrastructure in High-Risk Environments,” Multiple Authors (Engineering/Policy).

² Robert E. L. Varma, “Transparency, Anti-Corruption, and Development Aid: The Digital Governance Imperative” 2023–2024

government and private American companies ensure the stability of the supply chain, providing Ukraine with guarantees that necessary spare parts and new machinery will reach the country without logistical delays. This reduces dependence on alternative, less reliable suppliers.

The supply of heavy equipment reflects U.S. commitment to the “Build Back Better” principle. This approach does not simply aim to restore the old infrastructure but to rebuild it using more sustainable materials and technologies. The equipment provided often meets Western environmental and safety standards, thereby contributing to the modernization of Ukraine’s engineering sector in alignment with European norms.

While US assistance has largely focused on strategically critical, high-capacity equipment and logistics, European partners, particularly Germany, will make significant contributions to engineering recovery through decentralization and strengthening local-level infrastructure. German cooperation is often implemented through the KfW Development Bank and GIZ and focuses on municipal engineering projects, complementing large-scale US national programs.³ German assistance is typically aimed at restoring damaged water supply pipelines, pumping stations and thermal power plants serving damaged urban areas. This includes the provision of specialized engineering equipment for the rapid repair of damaged networks. German expertise in these projects ensures that the renovated municipal networks comply with strict EU standards for energy efficiency and water quality. This helps train local Ukrainian engineering personnel in the use of modern European technologies.

While the US focuses on critical national security sectors (energy, highways), the contributions of partners like Germany to municipal engineering infrastructure play a crucial role in ensuring the resilience of everyday life and complement the strategic objectives of US programs.⁴

Exchange of Expertise and Capacity Building - The U.S.-Ukraine engineering partnership goes beyond the supply of material resources. A crucial component of this cooperation is the sharing of technological expertise and the implementation of Western engineering standards, which ensure the long-term sustainability, quality, and compliance of the reconstructed infrastructure with European norms. The American side is actively engaged in the process of knowledge transfer, which influences the modernization of Ukraine’s engineering culture. Energy infrastructure—being one of the main targets of warfare—requires particular attention regarding the adoption of Western engineering standards. U.S. consultants are actively assisting the Ukrainian side in planning energy system decentralization projects. This engineering approach, which involves creating a network of small, modular power plants, reduces dependence on large centralized facilities, thereby significantly enhancing the system’s resilience and security.

The integration of American engineering components and technologies (e.g., transformers, generators) into the Ukrainian system ensures compatibility with the European energy network, thereby physically reinforcing Ukraine’s European integration. Thus, the sharing of technological expertise and the adoption of modern engineering standards serve not only as tools for reconstruction but also as a strategic investment in Ukraine’s future—a safe, European-aligned engineering system built on modern and resilient infrastructure.

3 GIZ (ReWarm Project) Reforming the District Heating Sector of Ukraine (ReWarm)

4 A. T. Smith, E. J. Williams “Local Infrastructure and Humanitarian Security in Conflict Zones” GIZ (ReWarm Project) Reforming the District Heating Sector of Ukraine (ReWarm)

GIZ, within the framework of the project “Reforming the District Heating Sector of Ukraine (ReWarm)” , focuses on systemic reforms that ensure the long-term perspective of engineering modernization. GIZ is actively advising the Ukrainian government in developing a national district heating strategy . This includes sharing German experience to enable Ukraine to replace outdated, inefficient and carbon-intensive systems. The project supports the introduction of innovative technologies such as heat pumps and thermal storage systems at the municipal level to reduce dependence on gas and increase the system’s resilience to Russian attacks. These concrete engineering examples show that Germany’s contribution is to the construction of standardized, energy-efficient and EU-compatible municipal infrastructure. ⁵

German engineering cooperation for Ukraine is a model that complements large-scale national investments from the US (e.g., high-voltage substations). Germany, mainly through KfW and GIZ, focuses on systemic energy efficiency and the approximation of local infrastructure to European standards. The Chernivtsi Municipal Water Supply Project (total cost of almost €95 million , financed by Germany and the European Union) is a classic example of engineering intervention. The project includes the replacement of up to 43 km of water supply pipelines. It is important that approximately 12 km of the pipelines are being replaced using trenchless technology (pipe bursting), which reduces work time, costs and does not damage the city’s surface infrastructure.⁶

Challenges, Risks, and Limitations in Engineering Partnership- Any form of international cooperation—especially within an active conflict zone—faces serious challenges. The effectiveness of the U.S.-Ukraine engineering partnership directly depends on how well these risks are managed. The main obstacle hindering engineering processes is the ongoing hostilities and extensive landmine contamination. Before any engineering work can begin, complete demining of the area is required. This is a slow and costly process that significantly delays the pace of reconstruction. Despite these challenges, the U.S.-Ukraine engineering partnership continues to shape Ukraine’s future and serves long-term strategic objectives. The core vision of the partnership is to rebuild Ukraine to a level better than before the war. In. The engineering partnership also serves as a practical mechanism of integration. The engineering protocols and quality standards introduced by the United States often coincide with—or even exceed—the technical compatibility and infrastructure safety requirements of the European Union and NATO. Despite substantial risks, the U.S.-Ukraine engineering partnership provides critical technological and expert support, forming the foundation for Ukraine’s sustainable economic development and eventual Euro-Atlantic integration. The heavy engineering machinery and specialized energy materials supplied by the United States play a decisive role in ensuring the rapid and effective reconstruction of infrastructure, thereby mitigating the economic collapse caused by the war. The long-term impact of this partnership lies not only in the provision of physical resources but also in the transfer of technological expertise. The introduction of Western engineering and quality standards in the road and energy sectors—combined with mechanisms for transparency—contributes to the modernization and resilience of Ukraine’s engineering system.

⁵ (Ukraine- Fourth Rapid damage and Needs Assessment 15.20.2025) <https://surl.li/jlvtau>, Accessed 04.11.2025

⁶ Robert E. L. Varma, “Transparency, Anti-Corruption, and Development Aid: The Digital Governance Imperative”, 2023–2024

Ultimately, this engineering cooperation goes beyond the boundaries of traditional aid; it represents a strategic alliance mechanism that links Ukraine's reconstruction to Western economic and technical norms.

Corruption is one of the most acute and frequent risks in both US and German funded engineering and reconstruction projects in Ukraine. While both countries strive to establish high standards of transparency, large-scale investments create new opportunities for corruption. Undoubtedly, corruption poses the most significant obstacle to the ongoing reconstruction of Ukrainian infrastructure and systems supported through the cooperation efforts of the US and Germany.

Conclusion

The U.S.-Ukraine engineering partnership represents much more than mere material assistance. This partnership serves as a mechanism for operational resilience and a strategic investment. It provides logistical and technical guarantees that ensure the uninterrupted continuation of Ukraine's core state functions under conditions of armed conflict. The supply of heavy American machinery and critical materials acts as a practical tool to neutralize Russia's targeted damage to the energy and transportation sectors. It is a rapid and effective countermeasure against destruction.

This partnership reflects the U.S. investment not in the old Ukraine, but in a new one. The sharing of expertise, the implementation of Western engineering standards, and the support of digital transparency tools are efforts to ensure that the rebuilt infrastructure is superior, sustainable, and less vulnerable to corruption.

The U.S.-Ukraine engineering partnership constitutes a vital technological bridge that not only repairs the war-inflicted damage but also lays the foundation for Ukraine's future as a sustainable and European-integrated country.⁷

Bilateral engineering and technical support from the US and Germany is paramount to restoring Ukraine's critical infrastructure and security its long-term resilience. To ensure Ukraine's long-term recovery, both approaches-US strategical delivery and German systemic modernization – must be closely coordinated. The Ukrainian government must strengthen institutional capacity at the local level to fully implement the demanding engineering and financial standards demanded by the West, which are crucial for the prospect of EU membership.

Bibliography

Ukraine- Fourth Rapid damage and Needs Assessment 15.10.2025) <https://surl.li/jlvtau>, Accessed 04.11.2025

(Actions to Support Ukraine's Economic Recovery 20.10.2025) <https://surl.li/bccwfq>, Accessed 04.11.2025

"Russia's War Against Ukraine: The Economic and Financial Dimension"

P. W. G. Maassen, K. W. Scherer, "Capacity Building in Post-Conflict and Developing Nations: A Global Perspective" (Collection), 2022–2024

Robert E. L. Varma, "Transparency, Anti-Corruption, and Development Aid: The Digital Governance Imperative", 2023–2024

"Sustainable and Resilient Infrastructure in High-Risk Environments", Multiple Authors (Engineering/Policy)

KfW/GIZ reports or German Foreign Ministry documents on humanitarian and municipal reconstruction in Ukraine.

A. T. Smith, E. J. Williams "Local Infrastructure and Humanitarian Security in Conflict Zones"

GIZ (ReWarm Project) Reforming the District Heating Sector of Ukraine (ReWarm)

7 P.W.G. Maassen, K. W. Scherer, "Capacity Building in Post-Conflict and Developing Nations: A Global Perspective" (Collection) 2022–2024

THE EVOLUTION OF MODERN DEFENSE: HOW TECHNOLOGICAL INNOVATION IS REDEFYING GLOBAL SECURITY (ISRAEL - IRAN CASE OF 2025)

Giorgi Nadibaidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Zaza Surmanidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Lieutenant Colonel Omar Turmanidze

Head of the Baccalaureate Program in Defence and Security of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Abstract

In the modern era, defense and technology have become inseparable elements of global security. Innovations such as artificial intelligence, drones cyber capabilities and advanced intelligence systems have transformed not only how wars are fought but also how nations define power and deterrence. This paper, “The evolution of modern defense: how technological innovation is redefying global security (Israel-Iran case of 2025)”, examines the impact of technological progress on the strategic balance between Israel and Iran. By exploring the 2025 confrontation, the paper argues that modern defense innovation now defines global power relations. Technology has become both a weapon and a diplomatic tool – shaping alliances, deterrence strategies and regional stability. The Israel-Iran case illustrates how technological superiority can deter conflict but also escalate competition. Technological progress, if guided wisely, can serve not only as a tool of defense but as a bridge toward lasting global stability.

Keywords: Defense, innovation, technological evolution, conflict, cybersecurity, Artificial intelligence, international cooperation.

Introduction

The twenty-first century has ushered in a fundamental rethinking of how states conceive, prepare for, and wage war. No longer confined to massed formations and attritional exchanges, contemporary conflict increasingly revolves around data, sensors, algorithms and the platforms that carry them. Technological innovation from artificial intelligence and autonomous systems to cyber tools and space-enabled intelligence now shapes not merely the means of warfare but its tempo, thresholds and political consequences. This paper argues that the June 2025 confrontation between Israel and Iran offers a rivalling case study of that transformation: a brief, intense episode in which kinetic strikes, cyber-effects and information operations intersected with established diplomatic channels and external partnerships to reshape regional security dynamics.

The June 2025 strikes marked a striking example of how modern military campaigns combine multiple domains to produce strategic effects. Over a short period, Israel air operations targeted a wide array of Iranian military and nuclear-related infrastructure, while parallel covert actions and cyber intrusions were reported to have degraded Iranian command-and-control and financial networks. The conflict unfolded rapidly, producing physical damage to selected sites and an immediate cascade of retaliatory launches and regional spillovers together illustrating how high-end precision strikes and non-kinetic tools can be employed in concert to pursue narrowly defined political objectives.

This study approaches the Israel-Iran case as a prism through which to examine broader trends. It will first situate the episode within a short historical overview of the bilateral rivalry, then briefly sketch the trajectories of Iranian and Israeli technological development relevant to force projection. From there the analysis turns to the ways in which innovations in strike systems, cyber operations and space-based sensing were integrated with diplomatic and allied relationships to shape outcomes. By treating technology and partnership as mutually reinforcing components of contemporary defense, the paper seeks to show how the character of security is being redefined – and what that implies for states with varying technological endowments and alliance profiles.

Main Part

A short historical overview of the Israel-Iran rivalry (concise)

The Israel-Iran rivalry has unfolded through decades of diplomatic hostility, proxy competition and episodic covert action. Since the 1979 Iranian Revolution, Tehran's regional posture and Israel's security calculus have been defined by mutual deterrence, competing influence in the Levant, and recurring clashes carried out indirectly – through proxies, sanctions, cyber campaigns and selective strikes – rather than sustained conventional war. In the 2010s and early 2020s this rivalry intensified around Iran's nuclear program and long-range missile and drone capabilities, producing a pattern of surges and pauses in which both sides tested new tools short of full-scale escalation. Recent episodes demonstrate that modern confrontation between these states is rarely decided by massed forces; instead, it turns on surprise, precision and the ability to combine kinetic effects with cyber and informational measures.

Iran's technological evolution

Over the last decade Iran pursued a dual-pronged strategy: indigenize key systems while diversifying external technical relationships. Facing heavy sanctions and limited access to western high-end components, Tehran invested heavily in local production lines for unmanned aerial systems (UAS), ballistic and cruise missiles, and domestic command and control electronics. Iranian firms and military design bureaus developed a wide range of tactical and loitering munitions that proved inexpensive, expendable and tactically flexible - attributes that suited Iran's emphasis on asymmetric deterrence and proxy supply.¹ The result is a force posture that blends massed missile and drone salvos with dispersed launch networks intended to complicate adversary targeting and raise the political cost of intervention.

Concurrently, Tehran sought partnerships to overcome capability gaps. Russia and other regional actors have been both customers and collaborators in areas such as air-defense components, maritime logistics and at times, systems integration; such relationships have helped Iran accelerate selected programs even as they remain constrained in high-end, microelectronic-dependent fields. At the same time, Iran expanded its cyber and information operations capabilities – a cost-effective domain in which constrained access to physical platforms can be compensated by software, trade-craft and persistent intrusion campaigns that target rival's critical networks. These parallel tracks – mass-producible UAS and missiles on one hand, and cyber operations on the other – created a toolbox that Tehran could wield across multiple layers of conflict.²

Israel's Technological Evolution –

Israel's defense transformation represents one of the most sophisticated examples of how a small state can leverage technology to compensate for limited strategic depth. Facing multiple regional adversaries, the Israeli Defense Forces (IDF) developed a doctrine rooted in agility, early warning, and rapid decision-making. In the past two decades, Israel's innovation ecosystem has become a central pillar of its deterrence strategy. Systems such as the Iron Dome, David's Sling and Arrow have demonstrated how layered air defense can neutralize large-scale missile attacks, while preserving flexibility for selective offensive actions.³

Beyond kinetic systems, Israel has invested heavily in cyber intelligence and information warfare, developing capabilities that allow it to preempt and disrupt enemy infrastructure without resorting to open conflict. The 2010 Stunned operation – through never officially acknowledged – symbolized the fusion of cyber innovation and national strategy, setting a precedent for non-kinetic warfare in the twenty-first century. In more recent years, Israel has expanded into AI-driven reconnaissance, unmanned aerial and maritime platforms, and space-based surveillance, enabling real-time data fusion and autonomous targeting. These advancements have redefined how Israel perceives “situational superiority” – no longer relying solely on manpower or territory, but on information dominance and networked precision. Equally significant has been Israel's close coop-

1 S. Lair, Shallow Ramparts: Air and Missile Defenses in the June 2025 Israel-Iran War. Foreign Policy Research Institute. (2025, October). <https://surl.lu/akksog>, Accessed 04.11.2025

2 J.Gambrel, Analysis: Iran faces ‘a permanent state of crisis’ as time wanes and sanction pressure grows. (2025, October). Associated Press.

3 Chatham House. Iran–Israel conflict: Iran has run out of good options. (2025, June 19). <https://surl.li/isdzdn>, Accessed 04.11.2025

eration with international partners, especially the United States, European Union members, and selective regional actors under the Abraham across framework. These alliances have allowed Israel to integrate its systems with NATO-compatible platforms, access shared satellite intelligence, and maintain a steady flow of technological co-development projects. The synergy between indigenous innovation and strategic partnerships has made Israel one of the few countries capable of fielding operationally tested AI (Artificial Intelligence) and autonomous defense systems.

When the 2025 confrontation with Iran unfolded, Israel's technological maturity became a decisive factor. The ability to combine precision-guided munitions, electronic warfare and real-time data analysis enabled Israeli planners to conduct short, targeted strikes with limited collateral damage – while simultaneously defending against massed drone and missile salvos. This performance underscored the essence of modern deterrence: superior information, speed, and adaptability. The conflict thus became not only a regional episode but a global demonstration of how advanced defense innovation can shape political outcomes without prolonged warfare.

Comparative Analysis: Contrasting innovation models and strategic outcomes

The 2025 Israel-Iran confrontation demonstrated not merely a clash of weapons, but a contest between two fundamentally different innovation philosophies. While Iran's model is rooted in quantity, improvisation and asymmetric saturation, Israel's approach centers on quality, precision and integration.⁴ Each strategy reflects its geopolitical realities and historical experience – one shaped by international isolation and sanction pressures, the other by advanced partnerships and global access to cutting-edge technology. Iran's defense innovation has evolved through necessity. Decades of sanctions forced Tehran to rely on reverse-engineering, regional alliances, and low-cost replication of foreign systems. Its swarm tactics using drones and short-range ballistic missiles are designed to overwhelm gig-tech defenses through numbers rather than sophistication. The goal is psychological and political: to project resilience, sustain deterrence and complicate adversary calculations. Israel, in contrast, has built a multi-domain innovation ecosystem that fuses government R&D private entrepreneurship⁵, and military testing environments. Every major conflict serves as a live laboratory for new systems – whether in electronic warfare, artificial intelligence, or real-time data management. The 2025 conflict revealed how this ecosystem enables rapid adaptation: within for Iron Dome batteries and autonomous interceptors, improving interception efficiency mid-operation.

Another crucial difference lies in strategic partnerships. Iran's military technology remains largely self-contained or dependent on selective external assistance from Russia or certain regional networks, often focused on shared political agendas rather than genuine co-development. Israel conversely, thrives on international interoperability – the ability to integrate systems with allied nations through standardized data links, joint exercises and collaborative research projects. Such interoperability multiplies defensive depth, allowing for faster intelligence sharing and more resilient decision-making processes.⁶ From a broader perspective, this asymmetry highlights a key dy-

4 Atlantic Council. (2025, June 16). *Twenty questions (and expert answers) on the Israel-Iran war*. <https://surli.cc/oncrkw>, Accessed 04.11.2025

5 R&D – Research and Development

6 International Institute for Strategic Studies (IISS). (2025, June 18). *Israel's attack and the limits of Iran's missile strategy*. <https://surl.li/djhzph>, Accessed 04.11.2025

dynamic of modern defense: innovation thrives where openness, collaboration and experimentation coexist. Israel's success stems not solely from funding or access, but from its adaptive mindset – a willingness to experiment, fail, and integrate lessons across domains. Iran's system, though constrained, illustrates the opposite side of the spectrum: the creativity of isolation, where resource scarcity drives ingenuity, yet also limits scalability and strategic reach.

The consequences of this technological divergence became visible during and after the 2025 confrontation. Israel's integration of AI-driven situational awareness, space-based reconnaissance and autonomous strike coordination granted it near-instant decision cycles. Iran's attempts to saturate the battlefield with volume attack caused temporary disruptions but failed to achieve decisive effect. However Iran's capacity to sustain prolonged low cost drone production and conduct cyber disruptions hinted at a long-term challenge: a future where quantity and persistence may gradually erode the advantages of precision and speed.⁷

In essence, the Israel-Iran conflict underscored that the future of warfare will not be defined by who has more weapons, but by who learns faster—who can analyze, adapt, and innovate under uncertainty. Both states in their own ways, embody this lesson: one through innovation born of partnerships the other through innovation born of necessity.

Conclusion

The 2025 Israel-Iran conflict was more than a regional flashpoint: it was a vivid illustration of how defense innovation and international cooperation are reshaping the very foundations of global security. Traditional military power, measured in numbers of soldiers or size arsenals, no longer guarantees victory. Instead, success now depends on information dominance, technological agility, and the ability to fuse multiple domains of warfare into a single, coherent strategy.

Israel's example show how a nation can transform constraints into opportunities through creativity and partnerships. By connecting military research with civilian technology and maintaining close collaboration with international allies, Israel has built a defense model based on speed, precision and adaptability. Its integrated systems, supported by AI and real-time data analysis, enable political leaders to make faster and more informed decisions, minimizing human cost while maximizing strategic impact.

Iran, meanwhile, embodies the other face of technological transformation – one forged in isolation, driven by necessity and resilience. Despite its limited access to global markets, Iran has developed an impressive indigenous defense industry, capable of production drones, missiles and cyber tools that can challenge even advanced opponents. While Israel's innovation thrives on openness and cooperation, Iran's progress proves that even under constraint, states can develop asymmetric means to project power and influence.

The lessons of this confrontation reach far beyond the Middle East. As dense technologies evolve, smaller nations worldwide are realizing that their security no longer depends solely on conventional alliances or manpower, but on how effectively they adapt to technological change. Future wars will likely be fought not on the scale of massive innovations, but through precise, networked operations where data, speed and collaboration decide outcomes.

⁷ Carnegie Endowment for International Peace. (2025, June 14). *Israel Goes to War with Iran*.

Ultimately, the evolution of modern defense reflects a broader truth about international security: innovation is not just a technical process, but a strategic mindset. The ability to connect science, diplomacy, and defense defines the new architecture of global order. Whether through cooperation or competition, states that embrace this transformation – that learn, innovate and build resilient partnerships – will shape the future of security in the twenty-first century.

Bibliography

- Chatham House. (2025, June 13). *Israel's strike against Iran: Chatham House experts offer early analysis*. Retrieved from <https://surl.li/jyjfkh>, Accessed 04.11.2025
- Council on Foreign Relations (CFR), “*Twenty questions (and expert answers) on the Israel-Iran war*” <https://surl.li/tsmxst>, Accessed 04.11.2025
- Carnegie Endowment for International Peace, “*From Shadow Combat to Open Conflict: The Israel-Iran War and Regional Reverberations*” <https://surl.li/sgawfd>, Accessed 04.11.2025
- Institute for the Study of War (ISW), “*Iran Update Special Report, June 15 2025*” <https://surl.li/mabdwe>, Accessed 04.11.2025
- International Institute for Strategic Studies (IISS), “*Israel's attack and the limits of Iran's missile strategy*” (18 June 2025) <https://surl.li/taeqyo>, Accessed 04.11.2025

JAPAN – US MILITARY-POLITICAL COOPERATION: A RESPONSE TO CHINA’S CHALLENGES

Beka Shaishmelashvili

The Junker of a Bachelor’s Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Giorgi Shatirishvili

The Junker of a Bachelor’s Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The post–Cold War era marked a profound transformation in global geopolitics, characterized by the collapse of the Soviet Union and the emergence of the United States as the sole superpower. However, the rapid economic and political rise of the People’s Republic of China has since reshaped the international balance of power, prompting a recalibration of strategic alliances in East Asia. This study examines the evolving military and political cooperation between Japan and the United States in response to China’s growing influence. As China expands its economic and defense capabilities, both Washington and Tokyo have intensified their joint efforts to preserve regional stability and prevent shifts in the East Asian balance of power. The research explores the strategic foundations of the Japan–US alliance, the adaptations in their defense cooperation driven by China’s rise, and the alliance’s broader implications for the security architecture of the “Rimland”—a key geopolitical frontier. The paper argues that the Japan–US partnership serves not only as a deterrent to Chinese dominance but also as a mechanism for sustaining liberal values and the existing global order amid rising multipolar competition.

Keywords: Japan–US alliance; East Asia security; China’s rise; balance of power; military cooperation; geopolitical strategy; regional stability; liberal order; strategic partnership

Introduction

After the end of the Cold War, the dissolution of the Soviet Union marked not merely the conclusion of a bipolar world order, but the beginning of a new epoch in international relations. The disappearance of one of the two global superpowers fundamentally reshaped the structure of global politics, leaving the United States as the sole hegemonic actor on the world stage. This unipolar moment, however, was never destined to last indefinitely. As new economic and political centers began to consolidate their influence, a gradual rebalancing of power started to unfold. Among these emerging powers, the People's Republic of China stands out as the most dynamic and transformative force, entering a new phase of national realization and global ambition.

Over the past several decades—and particularly within the last ten years—China has undergone an unprecedented transformation across multiple domains. Its extraordinary economic growth, advances in technology and healthcare, and assertive foreign policy have collectively signaled the potential emergence of a new global superpower. Many scholars, policymakers, and analysts argue that this shift represents the beginning of a new bipolar structure in which China challenges the long-standing dominance of the United States. As a result, nations across the Asia-Pacific region, and especially those situated along the strategic “Rimland,” have been compelled to reevaluate their political, economic, and security strategies in light of China's expanding influence.

Japan, as one of East Asia's most prosperous and technologically advanced nations, occupies a central position in this evolving geopolitical landscape. Historically allied with the United States since the post–World War II period, Japan's foreign and defense policies have been deeply shaped by its partnership with Washington. Yet, as China's influence grows, Japan has adopted a cautious and vigilant approach, balancing between the imperatives of economic interdependence with China and the strategic necessity of security cooperation with the United States. The rivalry between Tokyo and Beijing has thus intensified, evolving beyond traditional economic competition into a multidimensional struggle for political, technological, and military leadership in the region.

The United States, meanwhile, perceives Japan not only as a critical regional partner but also as a cornerstone of its broader Indo-Pacific strategy aimed at containing China's rise. This partnership is rooted in both shared democratic values and a convergent strategic goal: the preservation of a liberal, rules-based order in the Asia-Pacific. Consequently, Washington continues to strengthen its bilateral and multilateral security ties with Tokyo, reinforcing defense cooperation, joint training programs, and advanced military coordination mechanisms. Through these initiatives, the United States seeks both to maintain its influence in the region and to empower Japan as a capable actor capable of counterbalancing China's regional ambitions.

The purpose of this study is to provide a comprehensive examination of the military and political cooperation between Japan and the United States, focusing on their joint efforts to reorganize defense structures, enhance strategic coordination, and limit China's growing influence across the Eastern region. The study emphasizes the geopolitical importance of the “Rimland”—a concept first articulated by Nicholas Spykman—as a decisive arena where control determines global dominance. Within this framework, East Asia represents a critical axis of world politics, and the Japan–US partnership serves as a stabilizing mechanism that upholds the existing international order through the projection of liberal democratic values.

Main Part

This topic is particularly timely given the profound transformations currently reshaping the global system. The consequences of the Russia–Ukraine war, the resurgence of great-power competition, and the emergence of new security architectures in the Indo-Pacific all point to an impending era of multi polarity. In this context, the Japan–US alliance acquires renewed significance as a cornerstone of regional stability and as a bulwark against potential disruptions to the global balance of power. The partnership not only enhances deterrence against coercive actors but also strengthens diplomatic and economic resilience within the region.

Ultimately, this study argues that the Japan–US alliance functions as far more than a bilateral arrangement; it represents a key instrument of strategic management in an era of geopolitical uncertainty. Through joint military cooperation, technological innovation, and a shared commitment to liberal values, the alliance contributes to sustaining the equilibrium of the Rimland and preventing large-scale transformations in the global political order. As China’s rise continues to redefine the strategic contours of East Asia, the durability and adaptability of the Japan–US partnership will play a decisive role in shaping the future architecture of regional and international security.

This paper raises the following research questions:

1. What is the essence and strategic importance of the Japan–US military-political alliance in the context of East Asian security?
2. How has China’s military and economic rise affected Japan–US strategic cooperation, and in which areas have the main adjustments occurred?
3. What impact does Japan–US military-political partnership have on maintaining regional stability and balance of power in East Asia amid China’s growing influence?

Methodology:

The purpose of this study is to explore and analyze Japan–US military-political cooperation as a response to China’s growing challenges in East Asia and the Indo-Pacific region. The research is based on qualitative methods that allow for an in-depth understanding of geopolitical dynamics and the contextualization of strategic decisions.

The initial stage of the study involves examining the evolution of the Japan–US alliance through academic literature and publications from analytical institutions. Particular attention is given to the analysis of official government documents, such as Japan’s National Security Strategy (NSS) and National Defense Strategy (NDS), as well as joint statements of the Japan–US Security Consultative Committee (the “2+2” format). This approach helps to identify specific directions of alliance reorganization and their direct link to the threats posed by China.

In addition, a comparative analysis method is employed to assess the uniqueness and effectiveness of the Japan–US alliance within the regional context. Comparisons will be made with other regional security frameworks and allies (e.g., the Quad initiative, or US relations with South Korea and Australia). This enables a better understanding of Japan’s influence on the Indo-Pacific balance of power and the alliance’s potential in multilateral politics.

What is the essence and strategic importance of the US-Japan military-political alliance in the context of East Asian security?

The militaristic and political alliance between the United States and Japan, was built on the Treaty of Mutual Cooperation and Security (Anpo), which is the central power of security and stability in Eastern Asia. Since its creation, the alliance has undergone significant transformation, evolving from an asymmetrical, post-war arrangement into highly integrated partnership. This evolution is defined not only by its formidable conventional and extended deterrence capabilities but also by its function as the crucial hub of a complex, multicultural security architecture designed to counter challenges created by North Korea and China in the Indo-Pacific.¹

The foundational essence of the alliance is the best understood through its chronology. The security relationship originated with the 1951 Security Treaty, which was one sided, granting the U.S. the right to station forces in Japan without explicitly committing to its defense. This framework of dependence fundamentally shifted in 1960 with the revised Treaty of Mutual Cooperation and Security. The new treaty codified an explicit commitment by both nations to act if and armed attack occurred against either party in territories under Japan's administration (Article V). Crucially, it also introduced a prior consultation Clause, requiring the U.S. to consult Tokyo regarding major changes to force deployments or operations outside Japan. This transformed the alliance from occupation to security partnership.

Japan's commitment to the alliance has historically been mediated by its post-World War II Constitution, particularly Article 9, which fundamentally forswears military action except in self-defense.² This restriction gave rise to the doctrine of *Senshu Bōei* (Exclusively Defense-Oriented Policy), creating an asymmetrical reciprocity where the U.S. provided extended deterrence while Japan contributed geopolitical access and host-nation support. However, the escalating regional threat environment necessitated a legal and doctrinal shift. The critical change occurred in 2014, when Japan reinterpreted Article 9 to permit the limited exercise of collective self-defense, provided a situation poses an "existential crisis" to Japan. This policy change was the legal gateway to deeper operational integration with U.S. forces, laying the groundwork for the alliance's modernization.

The culmination of Japan's strategic reassessment arrived with the December 2022 National Security Strategy (NSS). Driven partly by the failure of deterrence demonstrated in the Russo-Ukrainian war, the NSS mandated a commitment to double defense spending to 2% of GDP by 2027 and, most significantly, authorized the acquisition of counterstrike capabilities.³ This marks the most significant policy departure in Japan's post-war history. While domestically framed as an extension of the *Senshu Bōei* principle—necessary to strike enemy launch sites if an interception is uncertain—this capability fundamentally enhances deterrence against North Korea and China. This move, however, generates a strategic dilemma: while increasing Japan's operational power, it also increases the risk of entrapment, potentially making Japanese forward bases a high-priority target in a major U.S.-China contingency. This evolution signals a decisive shift in the "bur-

1 "Treaty of mutual Cooperation And Security between USA And Japan"

2 "The Constitution of Japan"

3 "Defense Of Japan" <https://surl.li/hfodob>, Accessed 04.11.2025

den sharing” debate, moving away from a purely financial contribution toward shared operational power and strategic authority. The alliance’s strategic importance is magnified by its role as the central hub of a burgeoning “latticework strategic structure” in the Indo-Pacific. The traditional bilateral relationship has expanded into institutionalized trilateral and quadrilateral groupings aimed at countering China’s pursuit of regional hegemony. The US-Japan-ROK Trilateral Pact, formalized under the 2023 Camp David Principles, provides an integrated platform for managing North Korea’s nuclear threats through combined exercises and missile defense coordination. Simultaneously, the emerging US-Japan-Philippines Triad is imperative for extending the defense posture across the First Island Chain, directly countering maritime coercion in the South China Sea. Japan’s new Official Security Assistance (OSA) program further bolsters partner capacity within this network, cementing the alliance’s shift from a geographically fixed defense commitment to a flexible, regional operational hub. Despite these strategic successes, the alliance faces intrinsic political and governance challenges that test its long-term sustainability. Chief among them is the persistent sociopolitical friction surrounding U.S. force posture, particularly in Okinawa, which hosts approximately 75% of all U.S. Forces Japan (USFJ) facilities. This disproportionate concentration generates intense local opposition, as epitomized by the protracted deadlock over the relocation of Marine Corps Air Station (MCAS) Futenma. The national governments view these bases as indispensable strategic assets for regional security, yet maintaining this military presence by overriding local concerns risks the political legitimacy that underpins operational access. The necessity of resolving the Okinawa base issue underscores a vital lesson: the alliance’s deterrent posture relies not only on military hardware and interoperability but also on the political stability and local consent afforded by a secure domestic environment. In conclusion, the U.S.-Japan military-political alliance has successfully navigated the transition from the Cold War to the Indo-Pacific Century by fundamentally redefining its operational core. The 1960 Treaty serves as the legal bedrock, but Japan’s post-2014 constitutional reinterpretation and its 2022 acquisition of counter-strike capabilities have established it as an active, integrated strategic partner.⁴ The alliance now functions as the foremost mechanism for integrated deterrence and for maintaining a rules-based, free and open order in the region. Its continued stability depends on its capacity to manage internal political friction and sustain the momentum of modernization and multilateral expansion across all security and economic domains.

China’s Dual Rise: The Catalyst for US-Japan Integrated Strategic Competition

The military-political alliance between the United States and Japan has been defined by periods of adaptation, but none as profound as the current transformation driven by China’s assertive military and economic ascent. China’s pursuit of regional hegemony has fundamentally altered the strategic calculus in East Asia, compelling the US-Japan alliance to transition from a posture of passive defense against the Soviet threat to one of integrated, proactive strategic competition. This geopolitical pressure has sharpened the alliance’s focus across critical military, geographic, and

⁴ Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan’s Survival and Protect its People July 1, 2014

economic domains, fundamentally redefining the nature and scope of bilateral cooperation.

China's military modernization, specifically its development of advanced Anti-Access/Area Denial (A2/AD) capabilities and its gray zone operations in the East and South China Seas, has necessitated a radical shift in alliance doctrine. Prior to this decade, the alliance emphasized Japan's capacity for self-defense and the U.S. commitment to Extended Deterrence. Today, the focus has explicitly shifted to integrated deterrence. The sharpest accent is Japan's commitment, formalized in the 2022 National Security Strategy (NSS), to acquire counterstrike capabilities. This policy departure is aimed directly at complicating China's offensive planning by holding People's Liberation Army (PLA) missile launch sites at risk, thereby bolstering the credibility of deterrence. Successfully operationalizing this capability mandates a degree of intelligence sharing and real-time targeting integration with the U.S. military previously deemed unimaginable, forging an unprecedented level of military co-dependence.

Geographically and operationally, the strategic focus has been dramatically sharpened toward the First Island Chain, specifically the defense of Japan's remote Southwest Islands. The alliance is moving away from Cold War postures to create a structure optimized for crisis response and sustained operations in the face of Chinese aggression, particularly concerning a Taiwan contingency. This shift is reflected in the U.S. military's plan to transform U.S. Forces Japan (USFJ) into a Joint Force Headquarters (JFHQ) to improve command and control (C2) and enhance interoperability with the Japanese Self-Defense Forces (SDF). Furthermore, both nations are jointly prioritizing resilience by securing greater stockpiles of munitions and fuel and reinforcing defense facilities across the islands, ensuring that forward-deployed U.S. forces can operate effectively even after a potential first strike.

Beyond conventional military domains, cooperation has intensified in areas where China challenges the existing international order, most notably in cyberspace and critical technology. China's aggressive cyber capabilities pose a direct threat to the critical civilian infrastructure in Japan that U.S. forces rely upon for allied support. Consequently, the alliance has sharpened its focus on cyber defense integration, sharing threat intelligence and harmonizing policies to secure networks crucial for alliance operations. Economically, China's dominance in key manufacturing sectors and its use of economic coercion have galvanized cooperation on economic security. The allies are prioritizing joint research and development in cutting-edge fields like advanced semiconductors, quantum information science, and artificial intelligence to secure technological advantage, protect vulnerable supply chains, and prevent the leakage of essential intellectual property to Beijing.

Finally, China's strategic push to create what U.S. officials term a "sphere of influence" has been met with a sharpened multilateral response, transforming the bilateral alliance into the hub of a strategic latticework. The U.S. and Japan are explicitly building collective capacity with regional partners to counter Beijing's expansion. Key examples include:

The US-Japan-Philippines Triad: Institutionalized cooperation aimed at directly countering China's maritime coercion in the East and South China Seas, with Japan using its new Official Security Assistance (OSA) program to bolster Philippine capabilities, strengthening the defense perimeter. The Quad (U.S., Japan, Australia, India): Elevated to the Leader-level, this forum explicitly addresses non-traditional security issues like Maritime Domain Awareness (MDA) and

climate resilience, collectively upholding the Free and Open Indo-Pacific (FOIP) concept against Chinese coercion.

In summary, China's military and economic rise is no longer a latent concern for the US-Japan alliance, but the singular, explicit driver of its evolution. This strategic imperative has sharpened cooperation in four critical areas: enhancing integrated deterrence (via counterstrike), expanding the operational geography (First Island Chain), securing new domains (Cyber, AI, space), and accelerating multilateral capacity building (the Latticework). The resulting partnership is a system designed not merely for regional defense, but for comprehensive, sustained strategic competition against a peer competitor.

Conclusion

What impact does the US-Japan military-political partnership have on maintaining regional stability and the balance of power in the face of China's growing influence in East Asia?

The US-Japan military and political partnership plays a crucial role in maintaining regional stability and the balance of power in East Asia, especially against the backdrop of China's growing influence. This alliance forms the backbone of the security architecture in the region, strengthening cooperation and creating multilateral mechanisms aimed at preserving an order based on established rules. Recently, the alliance has evolved to respond to China's rapid military modernization and regional expansion.

Japan's national security strategy includes increasing defense spending to 2% of GDP by 2027, viewing China as the most significant strategic challenge. Japan is acquiring long-range strike capabilities, including US Tomahawk missiles, boosting the alliance's deterrent power⁵. The US-Japan alliance also connects with broader frameworks like the trilateral cooperation with South Korea and the Quad partnership with Australia and India, aiming to address challenges like North Korea's nuclear threat and China's assertiveness.⁶

The Taiwan issue is a critical test for the alliance, with growing convergence on its importance for regional stability. Japan explicitly sees the situation around Taiwan as vital for its own security, given the geographical proximity of its southwestern islands. Disputes over the Senkaku Islands further illustrate the delicate security balance, where the alliance counters China's attempts to change the status quo by increasing patrols and reinforcing joint military commands⁷.

This partnership pursues a dual strategy of building military capabilities and maintaining a balance of power that prevents China from gaining regional dominance in the Western Pacific. It also extends beyond bilateral ties into a broader network that includes the Philippines and other democracies, integrating military, economic, technological, and diplomatic cooperation. Nevertheless, the alliance faces challenges such as constitutional limits on Japan's collective self-defense and occasional strategic mistrust between the partners. The alliance's effectiveness will depend on maintaining strategic unity while adapting to a changing security environment to avoid escalation and preserve regional peace.⁸

5 "Navigating China Relations and the US-Japan Alliance" <https://surl.li/xkfjxi>, Accessed 04.11.2025

6 "Defense Of Japan" <https://surl.li/hfodob>, Accessed 04.11.2025

7 "The Senkaku Island Issue And Regional Security, Hideshi Tokuchi

8 The U.S -Japan Alliance: Challenges and Prospects in the 2020's. Brain Blankenship.

In summary, the US-Japan alliance is a key pillar for East Asian regional security in the face of China's rise. It strengthens deterrence, promotes a rules-based order, and builds cooperative frameworks but must carefully balance deterrence with diplomacy to sustain long-term stability.

Bibliography:

- Cabinet Decision on Development of Seamless Security Legislation to Ensure Japan's Survival and Protect its People July 1, 2014. <https://surl.li/wkshpl>, Accessed 04.11.2025
- Treaty of mutual Cooperation And Security between USA And Japan". <https://surl.li/bdffxo>, Accessed 04.11.2025
- The Constitution of Japan. <https://surl.li/bvvecs>, Accessed 04.11.2025
- Navigating China Relations and the US-Japan Alliance, " <https://surl.li/bmrscq>, Accessed 04.11.2025
- The Senkaku Island Issue And Regional Security, Hideshi Tokuchi., <https://surl.li/xbgtpm>, Accessed 04.11.2025
- The U.S -Japan Alliance: Challenges and Prospects in the 2020's. Brain Blankenship. <https://surl.li/cluouh>, Accessed 04.11.2025
- Defense Of Japan" <https://surl.li/hfodob>, Accessed 04.11.2025
- The U.S -Japan Alliance: Challenges and Prospects in the 2020's. Brain Blankenship. <https://surl.li/gpocda>" Accessed 04.11.2025

THE TECHNOLOGICAL AND ALLIANCE DIMENSIONS OF MODERN SECURITY: REDEFINING POWER AND COOPERATION IN THE GLOBAL ORDER

Senior Lieutenant Konstantine Shanava

The Learner of a Master's Degree Program (State Recourse Management) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The evolving landscape of global security is increasingly defined by two interrelated forces: rapid technological advancement and the intensification of international alliances. In an era where traditional approaches to defense and conflict prevention are no longer sufficient, the integration of advanced technologies with cooperative security frameworks is transforming how states address both conventional and non-conventional threats. From cyberattacks and disinformation campaigns to autonomous weapons and space-based surveillance, the character of modern warfare now demands responses that are not only innovative but also collaborative and adaptive.

This paper investigates how emerging technologies particularly artificial intelligence, cybersecurity systems, and unmanned platforms—are reshaping the strategic doctrines, capabilities, and decision-making processes of contemporary defense structures. It further examines how international alliances such as NATO, the European Union, and various regional security partnerships are adapting to these transformations by enhancing interoperability, promoting information sharing, and fostering joint innovation initiatives. The study evaluates both the advantages and challenges associated with these trends: while technological integration and alliance cooperation enhance protection, response efficiency, and deterrence capabilities, they also introduce ethical dilemmas, technological dependencies, and the potential escalation of an arms race in emerging technologies. Beyond the state level, the research explores the growing influence of non-state actors, private technology enterprises, and international organizations in shaping the future of global security governance. By analyzing the convergence of technological innovation and institutional cooperation, this study aims to provide a comprehensive understanding of how these dynamics are redefining the concept of national security and reconfiguring the global balance of power in the twenty-first century.

Keywords: Technology, International Alliances, Global Security, Cybersecurity, Artificial Intelligence, NATO, Defense Innovation, Strategic Cooperation, Emerging Threats, Geopolitics

Introduction

In the current era of rapid globalization and technological progress, the concept of security has expanded far beyond traditional military threats. Contemporary security now encompasses a complex interplay of digital, political, economic, and military dimensions many of which are driven or influenced by technological innovation and international cooperation. The growing interdependence of states, alongside the increasing capabilities of both state and non-state actors, has created a dynamic and often unpredictable global security environment. Within this context, the roles of emerging technologies and international alliances have become central to how nations understand, prepare for, and respond to evolving threats.

The scope of this study includes two primary areas: the transformative impact of technology such as cyber capabilities, artificial intelligence, autonomous systems, and digital surveillance on security policy and defense; and the evolving function of international alliances like NATO, the European Union, and regional security pacts in coordinating strategic responses. These two forces are not only shaping military doctrines and national defense policies, but are also influencing global power dynamics, decision-making processes, and international norms.

The relevance of this topic lies in its timeliness and urgency. As cyberattacks grow more frequent and sophisticated, and as geopolitical tensions escalate in regions such as Eastern Europe, the South China Sea, and the Middle East, the ability of states to adapt to both technological change and international coordination becomes a critical determinant of peace and stability. Moreover, as warfare becomes increasingly digitized, the ethical, legal, and strategic challenges associated with technology demand careful academic scrutiny.

Several scholars have explored individual aspects of this topic. Research in security studies has addressed how cyber technologies have altered the nature of threats and vulnerabilities¹, while international relations theorists have examined the strategic importance of alliances in maintaining global order². However, fewer studies have comprehensively analyzed how the interaction between technology and alliances is reshaping security on a global scale. This paper seeks to bridge that gap by offering an interdisciplinary perspective that connects technological innovation with alliance politics and strategic cooperation.

Integration of advanced technology into security systems when combined with the collective strength of international alliances enhances both the resilience and adaptability of states in responding to modern security challenges. However, this integration also introduces new risks, such as increased dependency, vulnerability to cyber threats, and the potential erosion of sovereignty.³

It is crucial for modern countries to know how to balance national interests with collective security in an era of rapid technological change. By critically analyzing the dual roles of innovation and cooperation, this research aims to offer insights that are not only theoretically relevant but also practically applicable in policy development and strategic planning.

1 Rid, Cyber war will not take place. Strategic studies. 2017, <https://surl.li/alcovp>, Accessed 04.11.2025

2 Mearsheimer. The tragedy of great power politics. <https://surl.li/hutrsu>, Accessed 04.11.2025

3 Gruszczak, kolascynski, Understanding contemporary security: a prolegomenon to the interplay between technology, innovation and policy responses. Politeja, 2022. <https://surl.li/qtecpw> . Accessed 04.11.2025

Main Part

The most impactful finding is that **technology and international alliances work best when integrated**. Alone, advanced technology can be powerful but limited in scope and sustainability. Likewise, alliances without technological modernization risk obsolescence. Together, they offer both resilience against modern threats and a platform for joint action. However, their integration requires **careful governance, transparency, and a shared commitment** to ethical norms and strategic balance. The modern world faces completely new challenges when most dangerous conflicts and relationships do not occur directly between countries but between alliances, unions and groups

In international relations, military alliances play a crucial yet intricate role in influencing the global geopolitical environment. Their development and relevance in the modern era highlight the careful equilibrium between promoting worldwide security and encouraging collaboration among regional powers.

As once Warren Forbes Kimball said, “Alliances are not only about measures during wartime but also include arrangements in times of peace, characterized by their long-term nature”. This and many other definitions emphasize fact that the main feature of alliances is that they must have a formal written agreement, which will be recognized and protected by international law.

Alliances mainly come in two forms bilateral and multilateral.⁴ A clear example of bilateral alliance is U.S.A.-Japan security. According to the agreement, the United States commits to protecting Japan if it is attacked by another country. In exchange, Japan permits U.S. military forces to be based within its territory and provides substantial financial contributions, known as “sympathy payments,” to help cover the expenses of hosting these bases. U.S has same agreement with South Korea. On the other hand clear example of multilateral alliance is NATO. According to this alliance agreement: „The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area”⁵.

Despite everything, in the real-world practice of international relations, many alliances exist without being formalized through official treaties. These informal partnerships often operate based on mutual interests and strategic cooperation rather than written agreements. To illustrate this statement better we need to consider relationships between United states and Israel or United States and Taiwan. Despite the fact that Taiwan is not even a sovereign state, the United States has maintained political ties. Based on this, we can express an opinion that alliances of no less strong ties are formed through informal agreements. Formal agreements and treaties are not necessary condition for establishing an alliance⁶.

4 Nxuan. The dual role of military alliances in contemporary international relations. 3rd International Conference on International Law and Legal Policy, 2024. <https://surl.li/wreodg>, Accessed 04.11.2025

5 Collective defence and article 5. 2023. Nato. <https://surl.li/dddkyd>, Accessed 04.11.2025

6 Walt. The origins of alliances. Cornell University Press. 1987 <https://surl.li/gaubuc>, Accessed 04.11.2025

To better understand the nature of such informal alliances, we can also consider Russia-China relations. In a relatively brief period, Moscow and Beijing have shifted their relationship from Cold War-era antagonism to a surprisingly strong and active partnership.⁷ This change has allowed them to broaden their regional influence, push back against Western dominance, and assert leadership within the Global South. Combined, they have the resources, resolve, and military strength to contest Western superiority. Partnership between Russia and China does not have any treaty or formal security guarantees. However, they have quite a few common strategic interests.

Technological independence is crucial for long-term resilience. While Russia hopes its alliance with China will help close the technological gaps created by international sanctions, this expectation may be overly optimistic. For example, Russia's efforts to modernize its outdated semiconductor sector with Chinese support appear unrealistic, considering China's own limitations in this area and increasing U.S. export restrictions meant to maintain that status quo. Nevertheless, over the past year, the movement of microelectronics from China to Russia often routed through third-party countries and unofficial networks involving shell companies demonstrates that close ties with Beijing can help Russia navigate short-term economic disruptions despite the sustained pressure from a U.S. led sanctions alliance, whose long-term effectiveness remains unproven.

From China's perspective, as long as it avoids becoming entangled in the sanctions regime or burdened with supporting failing Russian industries, there are clear advantages to Russia's increasing economic reliance on it. Russia's trade has already pivoted sharply toward China, which made up 40% of its imports and 30% of its exports in 2022 a trend expected to continue as Western sanctions intensify. This shift also includes growing adoption of the Chinese yuan in Russia, with President Putin endorsing its use in transactions with partners across Asia, Africa, and Latin America. While this won't undermine the global dominance of the U.S. dollar, it may serve as a model for other nations expanding trade with China and exploring alternatives to dollar dependence.

For Beijing, collaboration with Russia in scientific and industrial fields forms just one component of its broader strategy to enhance economic and technological strength. If forced to choose between working with Russia or Europe in science and technology, Chinese institutions would generally prefer European partners even if sanctions weren't a factor.⁸ However, it appears that China will not have to make such a binary choice, despite growing concern in European capitals over the deepening Sino-Russian relationship and its strategic consequences.⁹

As we have already mentioned above, alliances make as important contribution to modern international security as technologies. Technology plays a fundamental role in guiding the development of technical infrastructure, shaping how networks operate across social, economic, political, and ideological spheres. It forms the foundation for communication and exchange and has especially driven the virtualization of human interactions in cyberspace. Advances in technology have facilitated the rise of artificial intelligence systems, enhanced machine learning, and contrib-

7 Bharti. *China Russia bilateral security and military partnership in changing world orders: security challenges for the United States of America in Asia and beyond*. Historia I politika. 2022. <https://surl.li/ssljqf>, Russia_Bilateral_Security_and_Military_Partnership_in_Changing_World_Order_Security_Challenges_for_the_United_States_of_America_in_Asia_and_Beyond Accessed 04.11.2025

8 Korolev. How closely aligned are China and Russia? measuring strategic cooperation in IR. International Politics. 2019. <https://surl.li/uverxi>, Accessed 04.11.2025

9 Lee. China and Russia: A lasting partnership in high technology. EU cyber direct. 2023 <https://surl.li/scaumk>, Accessed 04.11.2025

uted to the digital transformation of major sectors such as finance, education, and culture. This transformation includes widespread adoption of online learning and rapid cultural exchange on an unprecedented scale.

Progress in areas like robotics, remote sensing, and propulsion systems has also led to the increased deployment of unmanned systems, particularly in dangerous or conflict-prone environments. Initially used for monitoring and reconnaissance, drones are now frequently employed in offensive operations, reshaping the nature of warfare alongside cyber technologies.

Today, innovation and modernization are seen as continuous processes tied to societal development, national prosperity, and global competitiveness in the tech sphere. Security now unfolds in an increasingly intricate environment where diverse actors utilize advanced tools and techniques to achieve their strategic goals. Technological advancement is a pivotal element in enhancing intelligence systems and command structures, many of which are now driven by artificial intelligence and autonomous technologies. In this context, innovation is no longer optional it is essential for strengthening security, managing crises, and maintaining public order by addressing existing gaps in the interconnected framework that links states, global systems, communities, and individuals.

One of the most influential technological advancements in modern security is the use of artificial intelligence. AI-driven systems are now widely used in intelligence gathering, threat analysis, and decision-making processes. For example, AI algorithms can process vast amounts of data from surveillance footage, social media platforms, and intercepted communications to detect suspicious activities or predict potential threats. Governments and law enforcement agencies use machine learning tools to identify criminal patterns and preemptively intervene in situations that may escalate into violence. This predictive capability has revolutionized counterterrorism strategies, border security, and urban crime prevention.

Cybersecurity is another critical area where modern technology plays a pivotal role. As more state infrastructure, corporate data, and even critical services like healthcare and energy grids become digitized, the risk of cyberattacks increases. Cyber threats such as ransomware, hacking, data breaches, and cyber-espionage can have devastating impacts on national security. For instance, the 2017 WannaCry ransomware attack affected systems in over 150 countries, disrupting hospitals, banks, and transportation networks. In response, governments are investing heavily in cybersecurity infrastructure, creating specialized units, and collaborating with private tech companies to protect digital ecosystems.

Unmanned systems, particularly drones or unmanned aerial vehicles (UAVs), have transformed modern warfare and surveillance. Initially developed for reconnaissance missions, drones are now used for targeted strikes, border patrols, and disaster response. Their ability to operate in high-risk environments without endangering human lives makes them invaluable in both military and civilian operations. For example, the United States has employed drones extensively in counterterrorism operations in the Middle East. Similarly, drones have been used in Ukraine to conduct surveillance, deliver supplies, and support tactical operations during the ongoing conflict with Russia.

Technological innovation has also enhanced public security and law enforcement capabilities through tools such as facial recognition, smart surveillance cameras, and real-time data analytics.

In urban areas, smart city infrastructure uses interconnected sensors and AI to monitor traffic, detect accidents, and respond to emergencies more effectively. Police forces in some countries now use facial recognition systems to identify suspects in public places, though this has sparked debates over privacy and potential misuse. While these tools improve efficiency and effectiveness, they raise ethical questions about surveillance, data protection, and individual rights.

In the realm of crisis management and disaster response, technologies like satellite imaging, remote sensing, and geographic information systems (GIS) provide critical real-time information. These tools help authorities respond quickly to natural disasters, monitor environmental changes, and coordinate humanitarian aid. For example, during the COVID-19 pandemic, technology played a key role in tracking infection rates, managing vaccine distribution, and enabling remote work and education.

Despite these benefits, the integration of modern technology into security systems also introduces significant challenges. The weaponization of artificial intelligence, for instance, could lead to autonomous weapons that operate without human oversight, raising concerns about accountability and the potential for unintended escalation. Additionally, the increasing reliance on technology makes infrastructure vulnerable to cyber sabotage and digital warfare. State and non-state actors may exploit these vulnerabilities to conduct hybrid warfare blending conventional military tactics with cyberattacks, misinformation, and economic disruption. Furthermore, the digital divide between technologically advanced and less developed nations creates imbalances in global security. Countries with limited access to advanced technology may struggle to defend themselves against high-tech threats, making them more vulnerable to external influence and internal instability.

As technology continues to advance, so too do the methods used by cybercriminals and hackers, creating an ongoing challenge for security systems to adapt to new and evolving threats. This constant game of catch-up requires security infrastructures to remain flexible and responsive to stay effective. One notable drawback is that no matter how advanced, technology cannot fully replicate human intuition or judgment. While tools such as surveillance cameras, alarm systems, and digital access controls are invaluable for spotting potential threats, they lack the ability to interpret emotions or intentions with the nuance of a trained human operator. In many situations, human oversight is indispensable for making informed decisions that depend on context and subtle behavioral cues.

Another critical issue involves privacy and data protection. As surveillance and monitoring technologies collect more personal information, the potential for unauthorized use or data breaches increases. Therefore, it is vital for institutions and businesses to adopt strong cybersecurity protocols to protect this sensitive information from exploitation. Moreover, technological dependence also introduces risks related to system malfunctions or technical failures. These lapses can create security gaps that may be exploited by malicious actors. To reduce these vulnerabilities, systems must be regularly updated and properly maintained to ensure they function reliably and securely.

Conclusion

The interplay between modern technology and international alliances has become a defining feature of contemporary global security. As outlined throughout this paper, the evolution of threats

from conventional military aggression to cyberattacks, hybrid warfare, and digital espionage demands not only advanced technological solutions but also cohesive and responsive international cooperation. The fusion of innovation and strategic alliances offers states the dual advantage of resilience and adaptability, allowing them to respond to increasingly complex and unpredictable security challenges.

Modern technologies such as artificial intelligence, unmanned systems, cyber capabilities, and surveillance infrastructure have transformed the nature of both defense and diplomacy.¹⁰ These tools have enabled faster decision-making, improved threat detection, and more efficient crisis response. At the same time, however, they have introduced significant vulnerabilities, including cyber-dependence, digital warfare, and risks to privacy and human rights. These technologies must therefore be implemented within robust ethical, legal, and strategic frameworks to avoid unintended consequences and maintain global stability.

Meanwhile, international alliances both formal and informal continue to shape the geopolitical balance of power. Whether through legally binding agreements like NATO or strategic partnerships such as the U.S.-Japan alliance or the growing ties between Russia and China, alliances provide a structure for collective defense, resource sharing, and coordinated responses to shared threats. The paper highlights how even informal alliances can exert significant influence on global affairs, particularly when driven by mutual interests and complementary capabilities.

Importantly, the integration of technology within these alliances enhances their effectiveness but also raises questions about dependency, control, and sovereignty. The example of Russia's reliance on China for technological support amid Western sanctions illustrates both the strategic advantages and the limitations of such cooperation. Similarly, the war in Ukraine has demonstrated how the combination of high-tech warfare, real-time intelligence, and international support can shape the outcome of conflicts and redefine strategic priorities.

Ultimately, this study reinforces the idea that modern security is no longer confined to borders or battlefields it is global, networked, and deeply rooted in both innovation and collaboration. To navigate this landscape successfully, nations must invest not only in technology and defense but also in diplomacy, legal standards, and mutual trust. Balancing national interests with collective security goals in an era of rapid technological change is one of the most pressing challenges facing the international community today. The path forward lies in fostering resilient, ethical, and forward-thinking alliances that are equipped to harness the full potential of technology while safeguarding peace, stability, and human dignity.

¹⁰ Al-auqaili. *How corporate-militant alliances are changing modern warfare*. Foreign policy in focus. 2024. <https://surl.it/rgcjub>. Accessed 04.11.2025

Bibliography

- Al-auqaili. *How corporate-militant alliances are changing modern warfare*. Foreign policy in focus, 2024. <https://surl.li/bshrwh>, Accessed 04.11.2025
- Bharti . *China Russia bilateral security and military partnership in changing world orders:security challenges for the United States of America in Asia and beyond*. Historia I politika. 2022. <https://surl.li/follhn>, Accessed 04.11.2025
- Colective defence and article 5. 2023. Nato. <https://surl.lu/qxrckh>, Accessed 04.11.2025
- Gruszczak, kolascynski. 2022. *Understanding contemporary security: a prolegomenon to the interplaybetween technology, innovation and polisy responces*. Politeja. <https://surl.li/adqnme> Accessed 04.11.2025
- Korolev. *How clodely aligend are China and Rrussia?measuring strategic cooperation in IR*. International Politics, 2019, <https://surl.lt/vyefio>, Accessed 04.11.2025
- Lee . 2023. *China and Russia: A lasting partnership in high technology*. EU cyber direct. <https://surl.li/mrbvpz>, Accessed 04.11.2025
- Mearsheimer. 2001. *The tragedy of great power politics*. <https://surl.li/upjjug>, Accessed 04.11.2025
- Nxuan.. 2024. *The dual role of military alliances in conteporary international relations*. 3rd International Conference on International Law and Legal Policy. <https://surl.li/qpyymk>, Accessed 04.11.2025
- Rid. *Cyber war will not take place*. Strategic studies,2017. <https://surl.li/vevngw>, Accessed 04.11.2025
- Walt. *The origins of alliances*. Cornell University Press, 1987.<https://surl.li/uucffg>, Accessed 04.11.2025

SECURE FUTURE: DEFENSE INNOVATION, RESILIENT ECONOMY, AND INTERNATIONAL PARTNERSHIPS

Luka Shukvani

The Junker of a Bachelor's Degree Program (Management)
LEPL-David Agmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Agmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

Building a secure and sustainable future constitutes one of the most profound and multidimensional challenges of the twenty-first century. In an era defined by rapid technological advancement, geopolitical uncertainty, and complex transnational threats, achieving lasting security requires a comprehensive and integrated approach. This paper explores the interdependent relationship between three essential pillars—defense innovation, economic resilience, and international partnerships—arguing that their convergence forms the foundation for enduring peace, stability, and prosperity. Defense innovation represents a central instrument in shaping modern security strategies. It enables states not only to respond effectively to emerging threats but also to anticipate and prevent them through technological foresight, research, and adaptive capability development. The continuous evolution of military technologies—ranging from artificial intelligence and cyber defense to autonomous systems and space security—has transformed the nature of warfare and deterrence. Nations that invest in innovation are better positioned to maintain strategic autonomy, protect their citizens, and preserve their competitive advantage within the global security architecture. Moreover, defense innovation stimulates domestic industries, drives scientific progress, and generates spillover effects that strengthen national economies and civil sectors. A resilient economy serves as the backbone of a secure and stable society. Economic resilience entails the capacity of a nation to absorb shocks, adapt to crises, and sustain growth under adverse conditions. It is the foundation upon which social stability and institutional legitimacy rest. A strong and diversified economy not only provides the resources necessary to finance defense modernization and innovation but also reinforces the social fabric by ensuring employment, welfare, and equitable development. In this sense, economic resilience is both a prerequisite for and an outcome of effective security governance. Societies with resilient economies are more capable of withstanding financial disruptions, global pandemics, and political instability, thereby maintaining the conditions essential for peace and progress. The third and equally crucial pillar is the system of international partnerships. In a globalized and interdependent world, no nation can achieve sustainable security in isolation. International alliances and partnerships amplify national capacities by enabling the exchange of knowledge, resources, and technological expertise. Collaborative frameworks—such as multilateral defense treaties, economic unions, and innovation networks—create synergies that transcend national boundaries. These partnerships foster mutual trust, enhance interoperability, and contribute to the development of collective mechanisms for crisis prevention and conflict resolution. By promoting dialogue and cooperation, they strengthen the normative foundations of the international order and expand opportunities for shared prosperity. Drawing upon recent case studies and empirical evidence, this paper demonstrates how the integration of these three dimensions—defense innovation, economic resilience, and global cooperation—has

proven instrumental in transforming both national and international security environments. The analysis reveals that countries which successfully align their defense modernization strategies with strong economic foundations and active international engagement are better equipped to navigate uncertainty and safeguard long-term stability.

Ultimately, building a safe and prosperous future is a collective endeavor that demands vision, sustained commitment, and coordinated action across multiple sectors—governments, industries, academia, and international organizations. Security in the contemporary world is no longer defined solely by military strength but by the capacity to innovate, adapt, and cooperate effectively in the face of complex and interconnected challenges. By integrating technological progress, economic resilience, and multilateral cooperation, societies can cultivate a security paradigm that is both proactive and enduring. This synthesis not only ensures protection from external threats but also lays the groundwork for a future that is innovative, adaptable, and thriving.

Keywords: Security; Innovation; Economic Resilience; International Partnerships; Stability; Cooperation; Prosperity; Technology; Growth; Adaptability; Defense.

Introduction

In today's rapidly changing and interconnected world, the pursuit of a secure future stands as one of the most fundamental priorities for every nation. Security in the modern sense extends far beyond military strength or crime prevention—it encompasses the ability of societies to provide stability, opportunity, and resilience for their citizens. People everywhere desire to live in environments where they feel safe in their homes, schools, and workplaces, while also having access to strong economies that offer opportunities for employment, education, and a dignified standard of living. A truly secure future, therefore, is not limited to the absence of conflict; it is the result of creating strong and adaptive systems capable of responding effectively to diverse challenges, both present and future. To achieve this comprehensive vision of security, nations must focus on three interrelated pillars: **defense innovation**, **economic resilience**, and **international partnerships**.

Defense innovation has become indispensable in a world where threats are increasingly complex and multifaceted. Modern security challenges extend beyond traditional warfare to include cyberattacks, terrorism, disinformation campaigns, and the proliferation of advanced weapon technologies. In this context, the development of innovative defense capabilities is vital. Technological advancements—such as artificial intelligence, autonomous drones, cybersecurity systems, and smart surveillance networks—enable nations to anticipate and neutralize threats more efficiently. A country that invests in defense innovation is not merely enhancing its military capacity but is also protecting critical infrastructure and civilian life. For example, by strengthening its cybersecurity systems, a state can prevent large-scale digital attacks on hospitals, banks, and public institutions, thereby safeguarding both citizens and the national economy. In this way, defense innovation contributes not only to military preparedness but also to social and economic stability.

A resilient economy forms the second crucial pillar of a secure future. Economic resilience refers to a nation's capacity to withstand and recover from crises—whether financial, environmental, or health-related—without suffering irreversible damage. A strong and diversified economy provides the resources needed to support defense systems, maintain social stability, and invest in innovation. During times of global disruption—such as economic recessions, pandemics, or natural disasters—a resilient economy ensures that people continue to have access to employment, essential goods, and social services. Moreover, economic strength supports long-term national development through investment in education, healthcare, and technological advancement. For instance, countries with robust industrial and technological bases are better positioned to produce advanced defense technologies while simultaneously improving the quality of life for their citizens. Thus, economic resilience not only enables survival during crises but also fosters the prosperity and progress that underpin national security.

International partnerships represent the third and equally vital dimension of a secure and sustainable future. In an era of global interdependence, no country can effectively address the challenges of security, development, or environmental protection alone. Transnational threats—such as climate change, cybercrime, pandemics, and terrorism—require collective action and shared responsibility. Cooperation among states enhances mutual understanding, facilitates the exchange of knowledge and technology, and strengthens global governance frameworks. Partnerships en-

able countries to coordinate defense strategies, share intelligence, and develop joint responses to emerging threats. At the same time, they open pathways for trade, research collaboration, and cultural exchange, fostering trust and mutual benefit. For example, when nations work together to mitigate the effects of climate change, they not only share green technologies but also contribute to global environmental security and sustainable growth. In this sense, international partnerships act as multipliers of national effort, transforming isolated actions into coordinated global progress.

By integrating **defense innovation**, **economic resilience**, and **international cooperation**, countries can create a comprehensive model of security that is both adaptive and forward-looking. These three elements are not separate goals but mutually reinforcing pillars that together build a foundation for long-term peace and prosperity. A secure future enables citizens to live with confidence, pursue opportunities, and face global challenges with collective strength and solidarity. Ultimately, achieving such a future requires vision, preparation, and sustained collaboration among governments, industries, and societies. Security is not a static condition but a continuous process of innovation, resilience, and cooperation. Nations that invest today in these three strategic dimensions will be best positioned to ensure that the challenges of tomorrow are met not with fear, but with capability, unity, and hope.

Main Part

Defense innovation involves the development and application of advanced technologies, strategies, and methods to enhance national security. Modern threats are no longer limited to conventional military attacks but also include cyberattacks, terrorism, and asymmetric warfare. Nations must therefore innovate continuously to protect their citizens and infrastructure.

Georgia exemplifies a country that has prioritized defense innovation. In 2023, Georgia's defense spending reached approximately \$15.3 billion, which supported military personnel, defense contracts, and the construction of modern military facilities¹. The country has upgraded its military equipment, trained specialized cyber units, and collaborated with international partners, including NATO and the European Union, to strengthen national security². Educational and research institutions, such as Georgia Tech Applied Research Corporation, play a pivotal role in supporting technological innovation in aerospace, drones, and cybersecurity³. These initiatives allow Georgia to maintain readiness against regional and global threats.

Globally, defense innovation is a central priority for many nations. The United States established the Defense Innovation Unit (DIU) to connect commercial technological advancements with military needs, focusing on artificial intelligence, cybersecurity, space systems, and other emerging technologies⁴. Israel's Iron Dome missile defense system demonstrates how advanced technology can successfully counter threats, protecting civilians from short-range rockets and artillery shells⁵. Ukraine, in response to the ongoing conflict with Russia, has rapidly developed a strong drone industry, producing inexpensive uncrewed aerial systems that significantly enhance its defense capabilities⁶. Estonia focuses on cybersecurity and digital defense, proving that even

1 Georgia Defense Spending (2023): <https://surl.li/xnffwz>, Accessed 04.11.2025

2 Georgia Defense Collaboration: <https://surl.li/glkslg>, Accessed 04.11.2025

3 Georgia Tech Applied Research Corporation Contract (2023): <https://surl.li/hqpxys>, Accessed 04.11.2025

4 Defense Innovation Unit (DIU), USA: <https://www.diu.mil/>, Accessed 04.11.2025

5 Israel's Iron Dome: https://en.wikipedia.org/wiki/Iron_Dome, Accessed 04.11.2025

6 Ukraine Drone Industry (2025): <https://surl.li/ahwqbr>, Accessed 04.11.2025

small nations with limited resources can achieve strong security through innovation ⁷.

Global defense spending reflects the increasing emphasis on innovation. In 2023, the world's 100 largest defense contractors earned \$632 billion, and investment in artificial intelligence, cybersecurity, and advanced technologies is projected to grow by 40% by 2030 ⁸. Such trends highlight that defense innovation is not only crucial for responding to current threats but also for preparing for future challenges. Additionally, technologies developed for defense often benefit other sectors, including healthcare, communications, and transportation, fostering broader societal progress.

In conclusion, defense innovation is essential for modern national security. Countries like Georgia, the United States, Israel, Ukraine, and Estonia demonstrate that adopting advanced technologies and fostering innovation is crucial for enhancing security, preparing for emerging threats, and ensuring a safer future.

Resilient Economy

A resilient economy is one that can withstand crises, adapt to change, and continue growing in challenging circumstances. In today's fast-moving global environment, nations face economic disruptions caused by pandemics, financial instability, natural disasters, and global market fluctuations. Economic resilience allows countries to support citizens, maintain social stability, and invest in critical sectors such as defense, education, and technology.

Georgia provides a strong example of a nation fostering economic resilience. Over the past decade, the government has implemented reforms to improve public financial management, attract foreign investment, and support small and medium enterprises (SMEs). In 2023, Georgia's GDP grew by approximately 4.8%, demonstrating its ability to recover from global slowdowns ⁹. The government has also promoted innovation and technology development through tax incentives and grants, supporting both economic growth and national security ¹⁰.

Globally, resilient economies prove their importance during crises. During the COVID-19 pandemic, countries like Germany and South Korea maintained stability thanks to diversified industries, strong healthcare systems, and rapid policy responses¹¹. Estonia's investment in digital infrastructure allowed its economy to continue functioning effectively during disruptions, highlighting the role of technology in resilience ¹².

A strong economy also supports defense innovation. Countries with financial resources can invest in research and development, modernize military infrastructure, and adopt advanced technologies to address security threats. For example, the United States allocates significant resources to both defense innovation and economic development, demonstrating the interconnection between security and economic strength¹³. Economic resilience also enables nations to participate in international partnerships, contribute to joint projects, and provide humanitarian aid, strengthening global cooperation.

⁷ Estonia Cybersecurity: <https://e-estonia.com/estonias-cyber-security-model-for-europe/>, Accessed 04.11.2025

⁸ Global Defense Spending Statistics (2023): <https://surl.li/ezbkxk>, Accessed 04.11.2025

⁹ Georgia GDP Growth 2023: <https://www.worldbank.org/en/country/georgia/overview>, Accessed 04.11.2025

¹⁰ Georgia Innovation and Tax Incentives: <https://georgia.org/industries/technology>, Accessed 04.11.2025

¹¹ Germany and South Korea COVID-19 Economic Response: <https://surl.li/xuhlmd>, Accessed 04.11.2025

¹² Estonia Digital Economy: <https://e-estonia.com/solutions/business/>, Accessed 04.11.2025

¹³ U.S. Defense and Economic Investment: <https://www.defense.gov/Explore/Spotlight/Defense-Budget/>, Accessed 04.11.2025

Sustainability is a key component of resilience. Countries must address long-term challenges, including climate change, energy transitions, and demographic shifts. Georgia, for instance, has invested in renewable energy, such as hydropower and solar projects, reducing dependence on imported energy and strengthening national economic security¹⁴. By fostering sustainable growth, nations can maintain stability, adapt to change, and continue progressing despite global uncertainties.

In conclusion, a resilient economy is critical for national stability and security. Countries like Georgia, Germany, South Korea, Estonia, and the United States illustrate that strong policies, technological development, and sustainable practices enhance the ability to withstand crises and ensure long-term prosperity.

International Partnership: International partnerships are collaborative relationships between countries that allow them to share resources, knowledge, and strategies to address common challenges. In today's interconnected world, no nation can face global threats alone. Partnerships improve security, promote economic growth, and facilitate joint responses to emergencies.

Georgia has actively engaged in international partnerships to enhance its security and development. As a participant in NATO's Partnership for Peace and through collaboration with the European Union, Georgia benefits from joint exercises, training programs, and strategic knowledge exchange¹⁵. Participation in multinational peacekeeping missions further enhances Georgia's military experience and regional stability¹⁶.

Globally, international partnerships strengthen national security. The United States collaborates with NATO allies and other partners through joint military exercises and technology-sharing programs, enhancing collective defense capabilities¹⁷. Ukraine has received international support in the form of drones, cybersecurity assistance, and military training, which has strengthened its defense systems¹⁸. Estonia cooperates with NATO and the EU to develop cybersecurity strategies, sharing resources and expertise to protect both national and regional security.

International partnerships also support economic development. Collaboration enables countries to attract foreign investment, access new markets, and share technological innovations. Joint research programs help develop defense technologies, renewable energy solutions, and digital infrastructure, contributing to both security and economic resilience. Partnerships are also crucial in responding to global crises, such as natural disasters or pandemics. For example, during the COVID-19 pandemic, international cooperation allowed countries to exchange medical supplies, vaccines, and knowledge about containment strategies.

In conclusion, international partnerships are essential for national security, economic stability, and global progress. Countries like Georgia, the United States, Ukraine, and Estonia demonstrate that collaboration enhances defense capabilities, technology sharing, and crisis response. Maintaining strong partnerships ensures nations are better prepared to address local and global challenges and promotes a safer, more prosperous future.

14 Georgia Renewable Energy Development: <https://www.georgiapower.com/renewable-energy>, Accessed 04.11.2025

15 Georgia NATO Partnership: https://www.nato.int/cps/en/natolive/topics_8197.htm, Accessed 04.11.2025

16 Georgia Defense Collaboration: <https://surli.li/yfritz>, Accessed 04.11.2025

17 U.S. NATO Collaboration: https://www.nato.int/cps/en/natohq/topics_52060.htm, Accessed 04.11.2025

18 Ukraine International Support: <https://surli.cc/tvvlgf>, Accessed 04.11.2025

The Connection Between Innovation, Economy, and Partnerships

Innovation, economic strength, and strategic partnerships constitute three interdependent pillars of a nation's sustainable development. These elements are closely interconnected, as progress in one area reinforces and accelerates advancement in the others. **Innovation** represents the process of creating new ideas, technologies, or methods that transform industries, improve efficiency, and enhance the quality of life. In the contemporary era, technological innovation—such as the application of artificial intelligence (AI) in healthcare or the use of drones in logistics—has revolutionized the way societies operate. For example, AI systems enable hospitals to process medical data more rapidly and accurately, while drone technology improves the efficiency of supply chains by delivering goods to remote or congested areas. Through such advancements, innovation increases productivity, strengthens competitiveness, and positions countries more advantageously within the global economy.

A **strong and resilient economy** serves as the foundation that enables continuous innovation. Economic stability provides the financial resources and institutional capacity necessary to support scientific research, technological development, and entrepreneurial activity. For instance, a country with a robust economy can invest in industrial modernization, research laboratories, or technology startups, fostering an environment where creative ideas can be transformed into practical solutions. In turn, innovation reinforces economic growth by generating new products, industries, and employment opportunities. This reciprocal relationship between innovation and economic vitality forms a cycle of sustainable progress, where economic prosperity fuels innovation, and innovation sustains economic expansion.

Partnerships, both domestic and international, play an equally essential role in this process. Cooperation among governments, private enterprises, and research institutions enables the sharing of knowledge, resources, and technical expertise. Partnerships foster synergy—allowing participants to achieve results that would be unattainable through isolated efforts. For example, NASA's collaboration with private companies such as SpaceX has accelerated advancements in space exploration, while cooperation among European Union member states has facilitated joint progress in renewable energy development. These examples illustrate how strategic alliances amplify innovation and expand economic potential by pooling capabilities and aligning shared goals.

The interconnectedness of **innovation, economy, and partnerships** is evident across multiple domains. Innovation drives economic performance; a strong economy provides the means to invest in innovation; and partnerships enhance both by creating collaborative frameworks for sustainable growth. A clear example of this dynamic can be seen in India's approach to development: by applying AI technologies in healthcare and education while engaging in international cooperation with technology firms, India is simultaneously fostering job creation, improving public services, and strengthening its economic base.

In conclusion, innovation, a resilient economy, and partnerships collectively serve as the engines of national development and global competitiveness. Countries that prioritize and integrate these three dimensions are better equipped to achieve long-term growth, generate new opportunities, and enhance the well-being of their citizens. In an increasingly complex and interconnected

world, nations face a range of economic, technological, and social challenges. Yet, these challenges also open pathways for transformation. By embracing innovation, nurturing economic strength, and cultivating cooperative partnerships, societies can turn uncertainty into opportunity and build a secure, stable, and prosperous future.

One of the main challenges is **rapid technological change**. New technologies, such as artificial intelligence (AI), drones, and cybersecurity tools, can greatly improve security, business, and daily life. However, they also create risks. Cyberattacks are increasing worldwide, targeting governments, banks, and critical infrastructure. For example, ransomware attacks can shut down hospitals or electricity systems, affecting millions of people. At the same time, technological innovation provides opportunities. AI can be used to predict security threats, improve logistics, and enhance decision-making in government and defense. Countries like Estonia and Israel have used advanced technologies to protect critical infrastructure and develop new solutions for security and society.

Another major challenge is **economic instability**. Global markets can change quickly due to crises, conflicts, or natural disasters. Small and developing countries may struggle to maintain economic stability during these events. For instance, countries that depend on energy or food imports may face shortages if supply chains are disrupted. Georgia experienced such challenges during regional tensions, but it has turned them into opportunities. The country invests in **renewable energy**, such as hydropower and solar projects, and encourages the growth of small businesses and technology startups. These efforts reduce dependence on imports, create jobs, and strengthen economic resilience.

Geopolitical tensions also create challenges. Conflicts between countries or regions can create security risks, especially for smaller nations. Georgia, located in a strategic region, faces pressures from neighboring countries and global powers. However, these challenges encourage cooperation with allies, participation in international exercises, and joining peacekeeping missions. By building strong international partnerships, countries increase their security, share knowledge, and improve their global influence.

Global crises such as **climate change, pandemics, and migration** are additional challenges. Climate change can cause extreme weather events, flooding, and droughts, which affect agriculture, energy, and housing. Pandemics, like COVID-19, can disrupt health systems, economies, and daily life. Migration flows may create social and economic pressures. But these challenges also bring opportunities. Countries can innovate in healthcare, energy, and infrastructure, and create policies to adapt to change. During the COVID-19 pandemic, countries that used digital technologies for remote work, online education, and health monitoring were able to continue operations and recover faster.

Finally, **human and social challenges** are also important. Education, skills development, and social stability are essential for innovation and economic growth. Countries that face challenges in these areas can use them as opportunities to improve training programs, develop new technologies, and encourage civic engagement. For example, investing in youth education and digital literacy in Georgia helps prepare a skilled workforce for the future.

In conclusion, challenges and opportunities are closely connected. Every difficulty, whether

technological, economic, geopolitical, or social, can be turned into a chance for improvement. Countries that recognize these opportunities while addressing challenges can strengthen their security, economy, and international position. By learning from global examples and investing in innovation, partnerships, and resilience, nations can create a safer, stronger, and more prosperous future for their citizens.

Conclusion

In conclusion a secure and prosperous future rests upon three fundamental pillars: defense innovation, economic resilience, and international partnerships. Each of these elements plays a critical role in shaping a nation's ability to safeguard its citizens, adapt to emerging challenges, and ensure long-term stability and growth.

Defense innovation is essential in an era defined by rapid technological advancement and evolving threats. Modern security challenges no longer arise solely from conventional warfare but increasingly from cyberattacks, autonomous weapons, and hybrid forms of conflict. By investing in cutting-edge technologies—such as artificial intelligence, cybersecurity infrastructure, unmanned aerial systems, and advanced surveillance tools—nations can strengthen their capacity to anticipate, deter, and respond to both traditional and unconventional threats. Innovation in defense not only enhances military effectiveness but also promotes technological progress across civilian industries, contributing to broader national development.

A resilient economy provides the foundation that sustains innovation and supports societal well-being during times of uncertainty. Economic resilience ensures that a country has the financial capacity and institutional strength to withstand crises—whether they arise from global recessions, natural disasters, or geopolitical disruptions. A strong economy enables investment in scientific research, education, and infrastructure, all of which are vital to national security and technological advancement. Moreover, economic stability helps maintain public confidence and social cohesion, preventing the kinds of disruptions that can undermine national unity during crises. Thus, a robust economy not only funds innovation but also anchors the social and institutional structures that make security sustainable.

International partnerships represent the third indispensable component of a secure and forward-looking global order. In an interconnected world, no nation can face complex challenges—such as cybercrime, climate change, pandemics, or transnational terrorism—alone. Through alliances and cooperative frameworks, countries can share knowledge, resources, and strategic insights, thereby multiplying their individual capacities. Collaboration in science, technology, defense, and trade fosters innovation and trust, while joint initiatives in areas like renewable energy, digital governance, and crisis management contribute to global stability. Successful partnerships—such as those between NATO allies, or cooperative ventures between space agencies and private industries—demonstrate how international cooperation can accelerate progress and expand opportunities for all.

While global challenges such as economic transformation, technological disruption, and systemic crises continue to test nations' resilience, they also present opportunities for renewal and

growth. Countries that proactively invest in technological innovation, nurture strong and adaptive economies, and engage in meaningful international cooperation are best positioned to protect their citizens, maintain stability, and thrive in an uncertain world.

Ultimately, the convergence of these three pillars—defense innovation, economic resilience, and international partnerships—forms the foundation of a safer, smarter, and more prosperous future. By integrating technological advancement with economic strength and cooperative diplomacy, nations can transform risks into opportunities, build collective security, and ensure that future generations inherit a world characterized not by fear and instability, but by progress, resilience, and shared prosperity.

Bibliography

Georgia Defense Spending (2023): <https://surl.li/ezasxo>, Accessed 04.11.2025
Georgia Defense Collaboration: <https://surl.li/dipzzo>, Accessed 04.11.2025
Georgia Tech Applied Research Corporation Contract (2023): <https://surl.li/rcqwol>, Accessed 04.11.2025
Defense Innovation Unit (DIU), USA: <https://www.diu.mil/>, Accessed 04.11.2025
Israel's Iron Dome: <https://surl.li/xtckxd>, Accessed 04.11.2025
Ukraine Drone Industry (2025): <https://surl.li/vbjxkv>, Accessed 04.11.2025
Estonia Cybersecurity: <https://surl.li/zunxhb>, Accessed 04.11.2025
Global Defense Spending Statistics (2023): <https://surl.li/iwgwms>, Accessed 04.11.2025
Georgia GDP Growth 2023: <https://surl.li/wfgmfg>, Accessed 04.11.2025
Georgia Innovation and Tax Incentives: <https://surl.li/jurwza>, Accessed 04.11.2025
Germany and South Korea COVID-19 Economic Response: <https://surl.li/mxfkxu>, Accessed 04.11.2025
Estonia Digital Economy: <https://e-estonia.com/solutions/business/>, Accessed 04.11.2025
U.S. Defense and Economic Investment: <https://surl.li/uoyfkn>, Accessed 04.11.2025
Georgia Renewable Energy Development: <https://surl.li/htgnvk>, Accessed 04.11.2025
Georgia NATO Partnership: <https://surl.li/wlormu>, Accessed 04.11.2025
Georgia Defense Collaboration: <https://surl.li/apazlm>, Accessed 04.11.2025
U.S. NATO Collaboration: <https://surl.li/gjjzkr>, Accessed 04.11.2025
Ukraine International Support: <https://surl.li/hdebal>, Accessed 04.11.2025

ARTIFICIAL INTELLIGENCE IN MODERN DEFENSE SYSTEMS: TRANSFORMING STRATEGIC AND OPERATIONAL CAPABILITIES

Tariel Tskhadadze

The Junker of a Bachelor's Degree (Informatic Technologies) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Beso Shubitidze

The Junker of a Bachelor's Degree Program (Management)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Givi Duchidze

Associate Professor of Bachelor's program in Management of
LEPL David Aghmashenebeli National Defence Academy of Georgia,
Doctor of Business Administration

Abstract

This paper provides a comprehensive analysis of the transformative role of Artificial Intelligence (AI) in contemporary defense systems, positioning it as both a strategic enabler and a source of profound ethical and legal challenges. The integration of AI into military structures has redefined traditional notions of defense by introducing real-time data analysis, predictive decision-making, and enhanced operational precision. Through systems such as autonomous drones, cyber defense mechanisms, and algorithmic threat detection, AI contributes to faster response times, optimized logistics, and reduced human risk on the battlefield. However, these advantages come hand in hand with new vulnerabilities, including data bias, accountability gaps, cybersecurity threats, and the ethical implications of delegating life-and-death decisions to machines. The study employs a multidisciplinary approach to explore how defense institutions can balance technological innovation with moral responsibility, emphasizing the importance of maintaining human-in-the-loop control, ensuring data integrity, and embedding strong cybersecurity measures within all AI-driven platforms. Furthermore, the paper highlights the urgent need for international cooperation and global governance mechanisms to regulate the use of AI in warfare and prevent misuse or escalation.

Ultimately, the research concludes that Artificial Intelligence, if guided by transparent policies, ethical frameworks, and multilateral oversight, can evolve from a disruptive innovation into a stabilizing force in global security. By fostering responsible innovation, AI can serve not only as a tool of military superiority but also as a foundation for collective safety, strategic foresight, and lasting international peace.

Keywords: Artificial Intelligence (AI); Defense Innovation; Military Strategy; Autonomous Systems; Cybersecurity; Ethics; Accountability; Human Oversight; International Cooperation; Global Security.

Introduction

In the twenty-first century, it is increasingly impossible to conceive of security without technology. What once functioned merely as a supporting instrument in military planning, logistics, and communications has now become the central pillar of strategic capability. Among emerging technologies, Artificial Intelligence (AI)—a system of algorithms capable of learning, identifying threats, and generating predictive or autonomous decisions—occupies a defining position. AI has penetrated nearly every sphere of human activity, and the defense sector is no exception. Its integration enables armed forces and national security institutions to process information with unprecedented speed and precision, reduce operational risks, and improve both tactical and strategic decision-making. The influence of AI thus extends far beyond robotics or unmanned systems; it redefines how data are collected, analyzed, and applied to strengthen global and national security architectures.¹

Several key factors determine the scale and direction of this transformation. First, the acceleration of technological progress—including the rise of high-performance processors, advanced sensor networks, and vast data-storage capacities—has exponentially increased the potential for AI deployment in defense. Second, global strategic competition among major powers has intensified efforts to achieve AI superiority, linking technological mastery to geopolitical influence. Finally, there are profound ethical, legal, and constitutional debates about the governance of autonomous systems, the accountability of algorithmic decision-making, and the adaptation of international law to emerging technologies.

Thus AI represents both an opportunity and a responsibility. It offers the possibility of greater precision, efficiency, and deterrence, yet it also demands the establishment of robust ethical norms and international cooperation. The responsible integration of AI into defense systems must therefore balance innovation with moral restraint, ensuring that technological advancement contributes to a sustainable, transparent, and secure global order.

Main Part

Artificial Intelligence (AI) in defense refers to the integration of intelligent computational systems capable of learning, reasoning, and acting autonomously or semi-autonomously within military and security environments. Far from being a single technology, AI represents a synergistic ecosystem of interrelated tools and processes that enhance the decision-making, operational, and analytical capabilities of defense institutions. Its scope extends well beyond machine learning or neural networks; it encompasses contextual data interpretation, sensor fusion, predictive modeling, and autonomous control systems. The overarching objective is to transform raw data into actionable intelligence, thereby enabling military organizations to act faster, more accurately, and with greater situational awareness than their adversaries.

The main technological components of military AI systems include:

Machine Learning (ML) and Deep Learning Algorithms — These systems analyze large volumes of historical and real-time data to detect operational patterns, forecast outcomes, and support rapid decision-making. In defense applications, they are used for target recognition, satellite imagery analysis, and threat prediction based on sensor or video inputs.

¹ NATO, *NATO's Artificial Intelligence Strategy*. NATO Official Document, Brussels. 2021.

Computer Vision — A subset of AI that allows computers to “see” and interpret visual information. In military contexts, computer vision systems are employed for autonomous image and video processing, facilitating terrain monitoring, target tracking, and battlefield surveillance. Such systems significantly reduce human workload and minimize error in fast-changing environments.

Situational Awareness and Data Integration — This involves consolidating information from multiple intelligence sources—such as satellites, radars, drones, and electronic intercept systems—into a unified, real-time operational picture. AI-based fusion platforms enable commanders to interpret complex data streams efficiently, improving both tactical and strategic coordination.

Autonomous Systems and Robotics — These include aerial drones (UAVs), unmanned ground vehicles (UGVs), and autonomous naval platforms, capable of operating either with minimal human supervision or fully independently. Their tasks range from reconnaissance and logistics to combat support and precision strikes, reflecting the growing autonomy and adaptability of military technology.

Cybersecurity AI — In the era of cyber warfare, AI plays a decisive role in protecting digital infrastructure. Cyber defense algorithms can predict potential threats, detect anomalies, and autonomously respond to cyberattacks in real time. This self-learning capacity significantly enhances resilience against sophisticated and evolving digital assaults.

Within the military domain, AI serves both tactical and strategic functions. At the tactical level, it supports field operations—enabling real-time decision-making, navigation, and threat analysis. At the strategic level, AI contributes to weapons system management, digital operations planning, and long-term resource optimization. However, the success of AI implementation in defense depends critically on the quality, integrity, and neutrality of data. Biased, incomplete, or manipulated data can result in faulty algorithms, misidentification of targets, or even catastrophic operational failures. Thus, establishing ethical and technical standards for data management is as vital as the technologies themselves.²

In summary, Artificial Intelligence in defense is not a single innovation but a comprehensive technological ecosystem—integrating learning algorithms, sensory networks, autonomous systems, and cyber intelligence. When properly managed, it has the potential to revolutionize military operations, reshape strategic doctrines, and define the future balance of global power.

Practical Applications and Case Studies

The transition from theoretical development to practical implementation of Artificial Intelligence (AI) in defense has been marked by rapid technological innovation and large-scale institutional adoption. Across the globe, multiple initiatives illustrate how AI systems are being actively integrated into the operational, logistical, and analytical frameworks of modern militaries. These practical applications demonstrate how AI not only accelerates data processing and enhances precision but also reshapes command structures and decision-making processes.

Video Monitoring and Analytics Projects — Military and intelligence agencies increasingly rely on AI-driven platforms to automatically detect, classify, and track moving objects across video and satellite imagery. Such systems can differentiate between vehicles, personnel, and in-

² U.S. Department of Defense, *Project Maven: Algorithmic Warfare Cross-Functional Team*. Department of Defense, Washington D.C. Overview of AI integration in video and imagery analysis for defense intelligence. 2017.

infrastructure, dramatically reducing intelligence processing time while improving the accuracy of target recognition. By filtering vast volumes of visual data, AI allows analysts to focus on strategic interpretation rather than repetitive observation.

Drones and Autonomous Aircraft — AI-equipped unmanned aerial vehicles (UAVs) and autonomous aircraft are revolutionizing reconnaissance and combat operations. Through machine vision and advanced sensor integration, these systems can identify, track, and prioritize targets, operate in high-risk zones, and carry out precision strikes with minimal human intervention. Their adaptive algorithms enable real-time tactical decision-making and mission flexibility.

Logistics and Supply Chain Optimization — AI has also transformed the efficiency of military logistics. Intelligent algorithms can forecast demand, optimize transportation routes, and coordinate supply networks across complex operational environments. This capability reduces resource wastage, enhances mission readiness, and shortens response times during both combat and humanitarian operations.

Cyber Emergency Response Systems — In cyberspace, AI-based defense mechanisms have become essential. These systems continuously monitor network traffic, learn from attack patterns, and autonomously isolate compromised systems before threats escalate. Such proactive cyber resilience ensures that defense networks remain secure even against advanced and persistent digital adversaries.³

Notable examples include the U.S. Department of Defense's Project Maven, which uses AI to analyze drone footage for object recognition; NATO's Defense Innovation Accelerator for the North Atlantic (DIANA), aimed at harmonizing AI use among member states; and the widespread adoption of autonomous drones and surveillance platforms across multiple defense alliances. These cases demonstrate how the integration of AI into military infrastructures not only strengthens capabilities but also introduces new operational, ethical, and regulatory challenges, demanding continuous oversight and innovation governance.

Benefits — How AI Enhances Defense Capabilities

The integration of Artificial Intelligence into defense systems brings multi-dimensional benefits, influencing strategy, operations, logistics, and education. When properly implemented, AI serves as a force multiplier, enhancing precision, adaptability, and overall effectiveness within national and allied defense structures.

Faster and Better-Informed Decision-Making — Through real-time data processing and predictive analytics, AI enhances situational awareness on the battlefield. Commanders can access updated intelligence, anticipate enemy maneuvers, and respond swiftly to dynamic conditions.

Increased Efficiency and Resource Optimization — AI significantly reduces the human workload in logistics, surveillance, and data analysis. By automating routine functions, it allows personnel to focus on high-priority strategic objectives, resulting in lower operational costs and better allocation of military assets.

Risk Reduction — AI contributes to operational safety by managing complex risk scenarios

³ **RAND Corporation.** *Artificial Intelligence and National Security*. Santa Monica, CA: RAND Corporation. 2020. DOI: <https://doi.org/10.7249/RR4229>

that exceed human cognitive limits. It can assess threats, forecast potential system failures, and minimize exposure of human personnel in hazardous environments.

Improved Accuracy and Targeting Precision — Advanced image recognition and guidance systems help to minimize collateral damage, ensuring compliance with international humanitarian standards while enhancing combat effectiveness.

Enhanced Education and Training — AI-powered virtual simulations and digital training environments enable soldiers to prepare for realistic and complex combat scenarios. Adaptive training programs analyze performance metrics, offering personalized learning experiences that improve readiness and resilience.⁴

Despite these substantial benefits, the degree of success depends heavily on system architecture, data integrity, and human oversight. Without reliable data inputs or ethical supervision, even the most advanced AI systems risk generating errors or unintended consequences. Therefore, technology must always function as a complement—not a replacement—for human judgment and accountability. In the defense context, AI should empower decision-makers, not substitute them, reinforcing a partnership between human intelligence and machine precision as the foundation of modern military power.

Challenges and Risks — Ethics, Responsibility, and Security

The integration of Artificial Intelligence (AI) into defense systems, while transformative, introduces a complex set of technical, ethical, legal, and strategic challenges that must be carefully managed to prevent unintended consequences. The very capabilities that make AI so powerful—speed, autonomy, and data-driven precision—also amplify the potential risks associated with its misuse, malfunction, or misinterpretation. To ensure that AI strengthens rather than destabilizes security frameworks, policymakers and defense institutions must confront a range of interrelated dilemmas.⁵

Ethical Dilemmas: One of the most pressing ethical concerns involves the use of Lethal Autonomous Weapon Systems (LAWS)—machines capable of selecting and engaging targets without direct human intervention. This raises a fundamental moral question: *Should machines possess the authority to make life-and-death decisions?* The absence of a human moral compass in autonomous systems challenges long-standing ethical norms of warfare and international humanitarian law. The issue is not merely technical but profoundly philosophical, as it concerns the nature of accountability, moral agency, and human dignity in conflict.

Accountability Gaps: The delegation of decision-making authority to algorithms creates uncertainty about responsibility in the event of errors or harm. When an AI-enabled weapon system malfunctions or makes a fatal mistake, who bears legal and moral responsibility—the programmer, the commanding officer, the manufacturer, or the state? These accountability ambiguities complicate both military law and international justice systems, requiring new frameworks for liability attribution.

⁴ **European Union Institute for Security Studies** *AI and the Future of European Defense*.

Report on innovation and cooperation among EU and NATO members in the field of defense AI. 2022.

⁵ **BBC News.** *How Artificial Intelligence Is Changing Modern Warfare*. Analysis article on AI-driven drones and military systems. 2023. Retrieved from: <https://www.bbc.com/news>

Cybersecurity Threats: AI systems are vulnerable to a new spectrum of cyber threats, including data poisoning, model manipulation, and algorithmic hacking. Adversaries may exploit these weaknesses to alter decision outputs, mislead defense systems, or compromise strategic data. The growing sophistication of such attacks blurs the boundary between traditional cyber warfare and AI-enabled deception, making cyber resilience a critical component of modern defense strategy.

Data Bias and Reliability: Since AI performance is dependent on the data it learns from, biased, incomplete, or corrupted datasets can lead to inaccurate or discriminatory outcomes. In defense contexts, this may manifest as misidentification of targets, flawed threat assessments, or unintended escalation. Addressing data bias requires not only technical calibration but also ethical data governance, ensuring that machine learning systems reflect fairness, transparency, and accountability.

Legal and Diplomatic Challenges: The rapid evolution of AI in defense outpaces existing international legal frameworks, creating a regulatory vacuum. Current treaties, such as the Geneva Conventions, were designed for human-controlled warfare and struggle to accommodate autonomous systems. Consequently, international law must adapt to AI-driven military conduct, establishing global norms, codes of ethics, and legal boundaries for the use of artificial intelligence in armed conflict.

Effectively addressing these challenges requires more than technical innovation—it demands comprehensive governance involving legal, political, and diplomatic cooperation. Establishing clear international standards, transparency mechanisms, and oversight institutions is essential to guarantee that AI remains under meaningful human control. Ethical use of AI in defense must always be grounded in accountability, moral integrity, and respect for humanitarian principles.

International Cooperation — Managing AI Globally

Artificial Intelligence is a global phenomenon—its innovation, influence, and associated risks transcend national borders. No single country can independently regulate or manage its security implications. Therefore, international cooperation and coordinated governance are indispensable to ensure that AI contributes to global stability rather than amplifying conflict.

Multilateral Standards and Ethical Principles: International organizations such as NATO, the United Nations (UN), and the European Union (EU) are actively developing frameworks to define ethical norms, technical interoperability standards, and principles of human oversight in military AI applications. These efforts aim to promote transparency, accountability, and restraint in the global arms race for AI superiority.

Technical Cooperation and Knowledge Sharing: Collaborative research programs, data-sharing agreements, and joint cybersecurity initiatives enable states to exchange expertise and build collective resilience. Partnerships among defense industries, universities, and research institutions help standardize safety protocols and foster responsible innovation in AI-based defense systems.⁶

Oversight and Verification Tools: Establishing international auditing and safety review mechanisms can enhance mutual trust among states. Such platforms could verify compliance with AI

⁶ **Center for Security and Emerging Technology (CSET).** *AI and Global Security Partnerships*. Georgetown University, Washington D.C. Examines the international collaboration aspects of defense AI. 2021.

ethics and security norms, reduce misunderstandings, and prevent accidental escalations triggered by automated or misinterpreted systems.

Accountability Mechanisms and Sanctions: A unified legal framework should define responsibility and penalties for the misuse of AI in military contexts. This includes mechanisms to sanction violations of ethical standards, misuse of autonomous weapons, or AI-driven cyber aggression, reinforcing a culture of compliance and deterrence.

Long-Term Strategic Cooperation: The ultimate objective of global governance should be to ensure that AI strengthens collective security, supports crisis management, and contributes to global peace rather than fueling arms races or technological inequality. Integrating AI into defense in a transparent and cooperative manner can enhance predictability, trust, and international stability.⁷

Thus international collaboration is not merely desirable but essential. The complexity and reach of AI demand shared responsibility, continuous dialogue, and harmonized regulation across states and institutions. Through responsible partnership, transparent standards, and ethical governance, the international community can ensure that AI remains a tool for progress and collective security, rather than a catalyst for division and conflict.

Conclusion and Recommendations

Artificial Intelligence (AI) in defense represents one of the most transformative developments of the 21st century—an unparalleled opportunity to enhance national and global security, yet also a profound challenge that tests the limits of ethics, governance, and human control. Its integration into military and security structures has revolutionized operational efficiency, resource optimization, and real-time decision-making. However, alongside these advantages come ethical dilemmas, legal ambiguities, and cybersecurity vulnerabilities that demand deliberate, transparent, and globally coordinated responses.

AI has already demonstrated its ability to improve situational awareness, accelerate intelligence analysis, and reduce human exposure to risk. Autonomous systems, data-driven logistics, and predictive analytics can make military operations faster, more precise, and more adaptive than ever before. Yet, the same features that make AI powerful—autonomy, scalability, and speed—also make it potentially dangerous if misapplied or left unregulated. Without clear oversight and moral responsibility, AI risks eroding the foundational principles of international humanitarian law and strategic stability. To ensure that AI contributes to peace and not peril, a series of strategic and ethical measures must guide its implementation. The following recommendations summarize the critical steps necessary for responsible AI integration in defense:

Maintain Human-in-the-Loop Control: Human oversight must remain non-negotiable, especially in lethal or high-risk operations. Autonomous weapons should never possess unrestricted decision-making authority. Final responsibility and moral accountability must always rest with human commanders.

Embed Strong Cybersecurity Safeguards: AI systems are themselves potential targets of manipulation. Incorporating robust cybersecurity protocols, including encryption, anomaly detection,

⁷ NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). *AI in Cyber Defense: Challenges and Opportunities*. Tallinn, Estonia. 2020. Retrieved from: <https://ccdcoe.org>

and system redundancy, ensures that defense AI cannot be exploited, hijacked, or deceived by adversaries.

Ensure Data Quality, Diversity, and Transparency: AI accuracy and fairness depend on the integrity of its data. Defense institutions must invest in clean, diverse, and verifiable datasets, accompanied by transparent auditing mechanisms to prevent bias, misinformation, or systemic errors that could distort outcomes.

Participate in International Dialogues and Regulatory Frameworks: The cross-border nature of AI technologies demands global solutions. Nations must actively participate in multilateral forums, treaties, and ethical initiatives—led by organizations such as the UN, NATO, and the EU—to establish shared norms governing AI development and deployment in defense.

Promote Continuous Education and Ethical Training: Both military and civilian leaders should receive ongoing education on the strategic potential, operational limitations, and ethical risks of AI. Fostering a culture of critical understanding ensures that decision-makers can effectively balance innovation with responsibility.

Artificial Intelligence, as a technology, remains fundamentally neutral—neither inherently benevolent nor malevolent. Its consequences depend entirely on the principles that guide its creation and application. When shaped by ethical foresight, legal accountability, and international cooperation, AI can become a cornerstone of global stability—enhancing defense capabilities while upholding the values of human dignity and peace.

In conclusion, the future of defense in the AI era will not be determined solely by which nation develops the most advanced technologies, but by which nations use them wisely, transparently, and responsibly. If governed through shared standards and moral discipline, AI can serve not merely as a tool of military superiority, but as a catalyst for a safer, smarter, and more secure world order.

Bibliography

- NATO.** *NATO's Artificial Intelligence Strategy*. NATO Official Document, Brussels. 2021. Retrieved from: <https://url.lu/redkal>.
- U.S. Department of Defense.** *Project Maven: Algorithmic Warfare Cross-Functional Team*. Department of Defense, Washington D.C. 2017. Overview of AI integration in video and imagery analysis for defense intelligence.
- RAND Corporation.** *Artificial Intelligence and National Security*. Santa Monica, CA: RAND Corporation. 2020. DOI: <https://doi.org/10.7249/RR4229>
- European Union Institute for Security Studies.** *AI and the Future of European Defense*. Report on innovation and cooperation among EU and NATO members in the field of defense. 2022. AI. Retrieved from: <https://www.iss.europa.eu>
- BBC News.** *How Artificial Intelligence Is Changing Modern Warfare*. Analysis article on AI-driven drones and military systems. 2023. Retrieved from: <https://www.bbc.com/news>
- Center for Security and Emerging Technology (CSET).** *AI and Global Security Partnerships*. Georgetown University, Washington D.C. 2021. Examines the international collaboration aspects of defense AI.
- NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2020).** *AI in Cyber Defense: Challenges and Opportunities*. 2020. Tallinn, Estonia. Retrieved from: <https://ccdcOE.org>

STRENGTHENING THE U.S.-AUSTRALIA ALLIANCE: COUNTERING CHINA'S GROWING MILITARY MODERNIZATION AND INFLUENCE IN THE INDO-PACIFIC

Saba Chiburdanidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Parmeni Garsidze

The Junker of a Bachelor's Degree (Mechanical Engineering) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

In the strategically vital and increasingly contested Indo-Pacific region, China's rapid military expansion and modernization have emerged as major factors reshaping the balance of power and challenging the established regional order. Over the past decade, Beijing has significantly enhanced its naval, air, and missile capabilities, enabling it to project power well beyond its immediate periphery. China's assertive actions in the South China Sea—including large-scale island-building, militarization of artificial features, and the deployment of advanced weapon systems—have not only raised tensions with neighboring states but also triggered broader concerns about freedom of navigation and international maritime law. Similarly, in the East China Sea, frequent incursions near the Senkaku/Diaoyu Islands have underscored China's willingness to use coercive tactics to advance its territorial claims. These developments have drawn the close attention of Indo-Pacific powers, many of which perceive growing risks to their sovereignty, economic security, and strategic autonomy. Within this evolving security landscape, Australia has emerged as one of the key regional actors deeply affected by China's military and geopolitical ambitions. Although China remains Australia's largest trading partner and an essential component of its export-oriented economy, Canberra has grown increasingly wary of Beijing's assertiveness and its implications for regional stability. The tension between economic interdependence and strategic mistrust defines much of Australia's foreign and defense policy in the contemporary era. As a result, Australia has intensified its cooperation with its traditional ally, the United States, viewing this partnership as the most credible mechanism for deterring potential Chinese aggression and preserving the existing balance of power. Australia's alignment with Washington is not merely reactive but reflects a long-standing tradition of strategic cooperation grounded in shared democratic values and mutual security interests. This partnership has been further institutionalized through a range of bilateral and multilateral initiatives, including the ANZUS Treaty, the Quadrilateral Security Dialogue (Quad), and the newly established AUKUS pact, which emphasizes defense technology sharing and joint capability development. These frameworks illustrate Australia's growing reliance on U.S. military presence and advanced defense technologies as a means of maintaining deterrence and ensuring regional stability amid China's growing military assertiveness. Despite its extensive economic engagement with China, Australia's official policy documents—such as its Defence Strategic Review and Foreign Policy White Paper—consistently emphasize the importance of a strong

U.S. presence in the Indo-Pacific as a stabilizing force. These documents highlight the belief that only through sustained and credible American engagement can the region maintain a rules-based order and resist coercive attempts to alter the status quo. Consequently, Canberra has not only expanded defense spending but also restructured its strategic posture to enhance interoperability with U.S. forces and to strengthen collective deterrence mechanisms. Accordingly, the primary objective of this article is to analyze the deepening and increasingly dynamic nature of the U.S.–Australia alliance through the lens of China’s military modernization and strategic positioning. The study seeks to examine how China’s evolving capabilities and regional ambitions have influenced U.S.–Australian defense cooperation, joint operational planning, and long-term strategic objectives. By assessing both policy frameworks and defense initiatives, this research aims to elucidate the complex interplay between economic dependency, security imperatives, and alliance politics that defines Australia’s position in the Indo-Pacific. Ultimately, this analysis underscores the central argument that Australia’s strategic recalibration reflects a broader regional trend: the strengthening of traditional alliances and security partnerships in response to China’s assertive rise. The U.S.–Australia alliance, therefore, represents not only a bilateral security arrangement but also a critical component of the wider Indo-Pacific security architecture, serving as a cornerstone of deterrence and a safeguard for the liberal, rules-based international order.

Keywords: Indo-Pacific, China, United States, Australia, Military modernization, Alliance, People's Liberation Army, Military doctrine, Regional order, Balance of power, U.S. Force Posture Initiatives.

Introduction

The concept of the Indo-Pacific, now widely recognized in political science and international relations, originally emerged from Karl Haushofer's geopolitical worldview but gained significant prominence only at the beginning of the twenty-first century. This vast region encompasses the Indian and Pacific Oceans, the two largest bodies of water on Earth, bringing together more than half of the world's population, numerous small and large states, several nuclear powers, around 60 percent of global GDP, as well as strategically vital trade routes and abundant natural resources. Today, the concept serves as an analytical framework for scholars, policy experts, military strategists, diplomats, and decision-makers to assess the future of Asia, particularly the evolving regional order, the formation and coordination of alliances, and the implications of China's expanding military influence.¹

Since the beginning of the twenty-first century, China's state transformation alongside accelerated economic growth and the strengthening of its military capabilities has introduced new challenges to the regional balance of power. Particularly in recent years, China has considerably increased its defense budget, expanded and modernized its naval and air forces, enhanced its weapons production, and reinforced its nuclear capabilities. At the same time, it has intensified revisionist actions aimed at safeguarding its national interests in territorial disputes, thereby heightening the risk of direct confrontation with other states across the Indo-Pacific region. Consequently, China's militarization has generated a form of counterreaction manifested in growing international concern, as well as in the formation of opposing alliances and coalitions seeking to preserve the regional order.

The relevance of the research topic is primarily determined by the diversity and complexity of the actors involved. The study focuses on three of the most significant players in the international system - China, the United States, and Australia. Furthermore, it highlights the emerging issue of attempts to alter the existing balance of power. Although Australia and China maintain close economic relations, Beijing's ongoing military modernization and its strengthened strategic posture across the Indo-Pacific compel Canberra to intensify its defense cooperation with Washington in order to reinforce its security guarantees and preserve regional stability.

China's military modernization is aimed at shaping the People's Liberation Army into a military capable of matching other advanced armed forces, particularly with the United States and its global power projection capabilities.² Beyond this overarching goal, Beijing's modernization efforts pursue several interrelated objectives: to establish a "hard" or military power that complements its growing "soft" power - economic, diplomatic, and cultural - thereby supporting its broader transformation into a global power; to strengthen its armed forces sufficiently to safeguard regional interests and secure favorable outcomes in territorial disputes in the East and South China Seas; to maintain political pressure on Taiwan while deterring U.S. involvement in potential conflicts in the Taiwan Strait; and to enhance its capacity to engage not only in warfare but also in other forms

1 Andrew Latham, "What or Where Is the Indo-Pacific?: How a foreign policy pivot redefined the global map". *The Diplomat* (May 17, 2025), <https://surl.li/uewzsw>, (Accessed 04.11.2025).

2 European Foundation for South Asian Studies, *Drivers, trajectories and prospects of military modernization in China*. (Amsterdam: EFSAS, July 2022): 4, <https://surl.li/jinpgj> (Accessed 04.11.2025).

of military operations such as peacekeeping and anti-piracy missions.³

Since the early 2000s, China has experienced rapid economic growth. It became a member of the World Trade Organization, surpassed Japan, and emerged as the world's second-largest economy after the United States. This economic expansion enabled China to allocate more state budget resources to its defense sector, thereby creating opportunities to alter the regional balance of power. A significant portion of defense investments has been directed toward the development of air and naval forces, nuclear, space, and cyber capabilities. Through comprehensive reforms, Xi Jinping addressed longstanding issues related to outdated military equipment, inadequately trained personnel, and corruption.⁴ Today, China ranks as the world's second-largest military spender after the United States, having spent approximately \$314 billion in 2024 - roughly one-third of U.S. military expenditures. Between 2015 and 2024, China's defense spending increased by 59 %.⁵

China's military doctrine has been significantly influenced by the concepts of the "Revolution in Military Affairs" and "Network-Centric Warfare", which emphasize the role of information and technology in modern warfare. The People's Liberation Army places particular focus on information warfare, the digitization of the battlefield, and networked systems to develop a technologically flexible force. While the United States maintains a clear advantage in high-tech weaponry, China seeks to offset this superiority through asymmetric strategies and technological countermeasures. Additionally, under its "generation-leap" strategy, China is pursuing a dual transformation - mechanization and informatization - to establish integrated communication and command systems, enabling it to operate effectively in information and network-centric conflicts.⁶

A cornerstone of Xi Jinping's military modernization is the reform of personnel policy within the People's Liberation Army, which involves reducing the overall size of the forces while simultaneously increasing investment in human capital. Within China's force structure, this change aligns with the imperatives generated by the doctrine of local wars, as rapid and decisive operations in an informatized environment demand relatively greater naval, air, and missile capabilities than total wars or those prescribed by Deng Xiaoping's "local war under modern conditions" military doctrine.⁷

From its founding, the People's Republic of China has pursued self-sufficiency in arms production, eventually building the largest military-industrial complex in Asia capable of supplying the full spectrum of military equipment from conventional weapons to nuclear and ballistic missiles. Over the past decade, Beijing's advances in defense have gone beyond mere "modernization." The People's Liberation Army has not only upgraded existing systems but also acquired fundamentally new capabilities previously unavailable to it. China has fielded systems comparable to Western counterparts, such as the long-range HQ-9 surface-to-air missile system, the J-10 fighter, modern submarines of the Yuan class, and the Type 052C destroyer. It has also

3 Richard Bitzinger, "Modernising China's Military, 1997-2012", *China Perspectives*, (2011 April), (Accessed 04.11.2025). <https://doi.org/10.4000/chinapersonpectives.5701>

4 Eric Heginbotham, & Michael S. Chase, "China's military modernization: Eric Heginbotham and Michael Chase in conversation", RAND Corporation, (September 14, 2015), <https://surl.li/mkxqxb> (Accessed 04.11.2025).

5 Xiao Liang, et al., "Trends in World Military Expenditure, 2024", Stockholm International Peace Research Institute, <https://doi.org/10.55163/AVEC8366> (Accessed 04.11.2025).

6 Bitzinger, *Modernising China's Military, 1997-2012*.

7 Anthony H. Cordesman, & Joseph Kendall, *Chinese strategy and military modernization in 2017: A comparative analysis* (Washington, D.C: Center for Strategic and International Studies, 2017): 213-214, 218, <https://surl.li/ntochs>, (Accessed 04.11.2025).

developed anti-ship ballistic missiles (ASBMs) and tested fifth-generation combat aircraft. At the same time, Chinese defense industry output and global arms sales are rising. This new combat potential is further strengthened by substantial improvements in C4ISR infrastructure (satellites, unmanned systems, and networked command-and-control systems).⁸

One of the primary concerns for Washington and its allies is the rapid expansion of China's nuclear arsenal. Compared to 2019, China had doubled its stockpile to approximately 600 warheads by 2025, and according to Pentagon projections, it is expected to reach 1,500 warheads by 2035. These figures bring China closer to nuclear parity with the United States and Russia, compelling Washington to prepare for potential confrontation with two nuclear superpowers simultaneously. Alongside the growth in nuclear capabilities, China's missile forces have developed the world's largest land-based conventional and dual-capable missile arsenal. Of particular note is the deployment of the medium-range DF-26 ballistic missile. With an estimated range of 4,000 kilometers, it poses a direct threat to strategic U.S. bases such as Guam and significantly alters the security environment in the Indo-Pacific region.⁹

In general, the growing military influence of major powers in the Indo-Pacific is also evident in the conduct of bilateral and multilateral exercises and operations with regional countries. For example, between 2003 and 2022, the United States participated in 1113 military exercises in the region, whereas China conducted only 130 exercises during the same period. However, in recent years, the dynamic increase in Chinese military operations has emerged as a challenge for Washington. Through these exercises, China seeks to strengthen cooperation with other countries in the region's defense sector, consolidate its position and international status, send warning signals to strategic competitors, and shape a regional security order that limits U.S. influence in the Indo-Pacific. Between 2003 and 2022, China conducted bilateral exercises with Malaysia seven times, with India eleven times, Thailand twelve times, Singapore five times, Indonesia nine times, and the Philippines once. Among multilateral exercises, special attention should be given to the Aman Youyi exercise organized by China in 2023, involving approximately 3 000 personnel from Cambodia, Laos, Vietnam, Thailand, and Malaysia, as well as the 2018 maritime exercises conducted together with ASEAN, which involved around 1 000 military personnel from Myanmar, China, Thailand, Cambodia, Laos, Vietnam, Malaysia, Indonesia, Singapore, Brunei, and the Philippines.¹⁰

China is actively undertaking island reclamation projects in the South China Sea to consolidate its territorial presence and enhance its military posture, control, and power-projection capabilities beyond its continental shores (due to geographical constraints, China has not been able to implement similar measures in the East China Sea). It has militarized Fiery Cross, Subi, and Mischief Reefs, equipping them with anti-ship and anti-air missile systems, laser and jamming devices, and destroyers. According to the U.S. Navy, most of these artificial islands in the South China Sea now feature their own supply depots, naval ports, runways, aircraft hangars, and other

⁸ Bitzinger, *Modernising China's Military*, 1997-2012.

⁹ Matthew P. Funaiole, & Brian Hart, "China's Military in 10 Charts", Center for Strategic and International Studies, (September 2, 2025), <https://www.csis.org/analysis/chinas-military-10-charts> (Accessed 04.11.2025).

¹⁰ Evan Laksmana, et al., *Asia-Pacific Regional Security Assessment 2024*, "Scripted Order: Combined-military Exercises in the Asia-Pacific." The International Institute for Strategic Studies, (2024): 3-4, 8-9, <https://surl.it/tuczpm> (Accessed 04.11.2025).

advanced military infrastructure.¹¹

When discussing the effects of China's growing influence on Australia's security, it is important to highlight relevant statistical data. Between 2009 and 2020, Chinese threats accounted for 25-29% of the concerns identified in Australia's official and national security documents, rising to 50% and 56% in 2023 and 2024, respectively. The 2024 National Security Document explicitly states that China's expanding military capabilities and coercive tactics represent a major security challenge for Australia. Military capabilities include the deployment of hypersonic weapons, land-attack cruise missiles, and advanced long-range land-based systems, while coercive tactics encompass the intensive use of various mechanisms by China in territorial disputes, including violations of other states' airspace and maritime zones. In recent years, Australia's national security documents have prioritized deepening ties with the United States and strengthening U.S. presence and positions in the Indo-Pacific. While Australia maintained official friendly relations with Beijing until 2010, the perception of Chinese influence among Australians has shifted and transformed in the context of international political developments, reflecting a "reality-check" approach in line with Medcalf's framework.¹²

The 2022 security agreement between China and the Solomon Islands, China's 2023 offer of domestic security support to Papua New Guinea, and the 2025 PLNA naval exercises in the Tasman Sea have further heightened official concern in Canberra. In addition, China is actively seeking to establish close strategic cooperation with other regional countries around Australia to expand its influence in the Pacific. Evidence of this includes Chinese assistance in repairing the Kumul submarine cable network for Papua New Guinea in 2020 and the renovation of an airstrip on Canton Island for Kiribati in 2021. According to a Fijian military officer, China has also increased its involvement in police training, equipment provision, and operations in Exclusive Economic Zones using its survey vessels.¹³ In practice, Beijing is normalizing its military activities in the Indo-Pacific region by testing the capabilities of its military and paramilitary forces without violating international law.¹⁴

According to John Noh, Acting Deputy Secretary of Defense for Indo-Pacific Security Affairs, China's ambition to replace the United States in the region must be countered by the U.S. through the restoration of deterrence in the Indo-Pacific, maintaining higher combat readiness, fairly distributing responsibilities among allies, and continued investment in the U.S. defense industry. The United States requires active support from partner and allied countries in the region, as alliances created by strong partners are essential to disrupting visible aggression, creating dilemmas for adversaries, and constraining destructive actions.¹⁵

As a middle power, Australia does not possess sufficient capabilities to independently safeguard its security interests in the Indo-Pacific amid great power competition. Australia's foreign policy

11 Associated Press, "China Has Fully Militarized Three Islands in South China Sea, US Admiral Says", *The Guardian*, (21 March 2022), <https://surl.li/txecw> (Accessed 04.11.2025).

12 Maria Papageorgiou & Zeno Leoni, "The Five Eyes Allies and China: Assessing Threat Perceptions and Power Dynamics", *J OF CHIN POLIT SCI* (2025), <https://doi.org/10.1007/s11366-025-09913-w> (Accessed 04.11.2025).

13 Edward Chan, "How Worried Should Canberra Be About China's Security Interests in the Pacific? Perspectives from PRC and Pacific Interlocutors", University of Technology Sydney, (July 2, 2025), <https://surl.li/yhowli>, (Accessed 04.11.2025).

14 Riley Walters, "China's Military Expansion Toward the Southwest Pacific and Oceania", GIS Reports, (July 15, 2025), <https://surl.li/bevdnq>, (Accessed October 15, 2025).

15 David Vergun, "China's Military Buildup Threatens Indo-Pacific Region Security", U.S. Department of War, (April 9, 2025), <https://surl.li/dqmsdc>, (Accessed October 15, 2025).

approach and historical experience indicate that it has consistently prioritized close, stable, and mutually beneficial relationships with major powers, including the United Kingdom and the United States, in order to secure defense and security guarantees through such cooperation.¹⁶

Australia is the oldest and second-closest and most loyal ally of the United States, after the United Kingdom. It fought alongside the U.S. in World Wars I and II, Korea, Vietnam, the Persian Gulf War, Afghanistan, and Iraq. For nearly half a century, the United States has played a decisive role in shaping Australia's defense policy. The U.S. provides Australia with extended nuclear deterrence capabilities and, through intelligence, defense technologies, weapons, and military logistical support, significantly strengthens Australia's regional position.¹⁷

Australia is one of the largest customers of the U.S. defense industry. Under the Foreign Military Sales program, the volume of government-to-government sales exceeds \$27 billion, covering combat helicopters (Apache, Chinook, MH-60R), unmanned aerial vehicles (MQ-9B), M1 Abrams tanks, anti-tank and anti-ship missiles (200 Javelin FGM-148E, 200 AGM-158C LRASM), combat systems (AEGIS), F/A-18E/F Super Hornet upgrades, artillery munitions (M825A1 155mm white phosphorus shells, M782, M762A1, M231/M232A2 devices and propellant charges), electronic warfare systems (JCREW I1B1, ALE-70 radio frequency jamming systems), and other military equipment. This cooperation significantly enhances Australia's defense capabilities and creates thousands of jobs in the United States. In 2020, under the U.S. fiscal framework, the Directorate of Defense Trade Controls (DDTC) authorized approximately \$3.57 billion worth of Direct Commercial Sales (DCS) licenses, facilitating the ongoing export of American defense equipment to Australia. Major purchase categories included aviation equipment and components, electronic systems, as well as gas turbines and related systems. Additionally, Australia is one of only two countries with a Defense Trade Cooperation Treaty with the United States, which allows certain military products to be exported without a license for joint military operations, collaborative defense research, and other intergovernmental projects.¹⁸

To strengthen their defense cooperation, the United States and Australia signed a Joint Statement of Intent focused on developing joint production of weapons. Specifically, the agreement lays the groundwork for co-production of long-range precision weapons such as Guided Multiple Launch Rocket Systems and Precision Strike Missiles. The initiative also offers Australia a significant opportunity to further develop its domestic defense industry by establishing a sovereign Guided Weapons and Explosive Ordnance Enterprise.¹⁹

The agreement signed in October 2025 by Donald Trump and Anthony Albanese, known as the U.S. - Australia Critical Minerals Deal, aims to enable both countries to compete with China's monopoly in the global rare earth elements market. Reducing dependence on China is strategically advantageous for the commercial and defense industries of both nations. The parties also committed to allocating at least \$1 billion within six months for projects totaling \$8.5 billion.

16 Stephen Fallon, "Australia's Security Relationships in the Indo-Pacific." Briefing Book Article, 47th Parliament. Parliament of Australia, (June 2022), <https://surl.li/fjgqqd>, (Accessed October 15, 2025).

17 Paul Dibb, "U.S.-Australia Alliance Relations: An Australian View", *Strategic Forum*, no. 216 (August 2005): 1, <https://surl.li/cmejfd>, (Accessed October 15, 2025).

18 Bureau of Political-Military Affairs, "U.S. Security Cooperation With Australia", U.S. Department of State, (January 19, 2025), <https://surl.li/rmnyfy>, (Accessed 04.11.2025).

19 Jack Lloyd, "Australia, US strengthen guided weapons cooperation", *Manufacturers' Monthly*, (October 15, 2025), <https://surl.li/sxqlwt>, (Accessed 04.11.2025).

To enhance production capabilities, Australia will invest approximately \$200 million in Aloc operations for gallium, with support from both the United States and Japan. The U.S. is entirely dependent on gallium imports, while China is the largest producer. Notably, gallium is widely used in advanced military technologies, such as ballistic missile guidance systems and radar equipment. Additionally, to further reduce reliance on Chinese rare earth elements, Australia announced a \$100 million investment in the Arafura project.²⁰

Within the framework of enhanced bilateral force posture cooperation, Australia hosts U.S. military forces in various exercises to strengthen air, naval, and land capabilities, logistical resilience, and space collaboration. Australia and the United States work closely on modernizing defense infrastructure, which includes upgrading existing bases and developing new facilities. A notable example is the use of the Cocos Islands for extended maritime surveillance operations under the Pacific Deterrence Initiative. Additionally, funding the modernization of two military bases in northern Australia including support for rotational operations of long-range bombers such as the B-52 and B-1 represents further evidence of these strategic investments.²¹

When discussing U.S.-Australia bilateral cooperation, it is essential to highlight a critical component of this alliance: the U.S. Force Posture Initiatives (USFPI). USFPI consists of six complex, interrelated initiatives. Among them, the Marine Rotational Force - Darwin (MRF-D) demonstrates the growing collaboration between U.S. Marines and the Australian Defence Force. This initiative conducts military training not only between the two countries but also with other regional states, such as Japan, the Philippines, Malaysia, and others. A particularly notable exercise is Exercise Southern Jackaroo, a two-week trilateral land exercise led by Australia with participation from U.S. and Japanese forces, enhancing cooperation across multiple defense domains. Additionally, Talisman Sabre, a biennial U.S.-Australia joint exercise, prepares both forces for extensive planning and execution of combined operations, improving interoperability and combat readiness. The Enhanced Air Cooperation (EAC) program represents a strategic partnership between the U.S. and Australian air forces, aimed at ensuring operational interoperability, security, and stability in the Indo-Pacific through integrated combat capabilities, joint airbase operations, logistical collaboration, and the joint development of air power. The Enhanced Land Cooperation (ELC) initiative strengthens security and deterrence in the Indo-Pacific through complex, integrated activities with regional partners, supported by rotational deployment of U.S. Army personnel, capabilities, and associated logistical infrastructure in Australia. The Enhanced Maritime Cooperation (EMC) initiative focuses on supporting a rules-based maritime order (UNCLOS) in the Indo-Pacific, leveraging rotational U.S. naval forces in Australia, integrating new technologies, enhancing maritime domain awareness, developing infrastructure, and conducting complex fleet exercises. Deterring aggression and ensuring the sustainability of high-intensity combined operations in the region is a priority of the CoLSME strategic initiative, implemented through strengthened logistical interoperability, optimized infrastructure networks, and practical measures such as support for MRF-D and prepositioning of U.S. Army materiel for exercises. Finally, the

20 Jonathan Barrett, "Australia and the US have signed a critical minerals deal to take on China's monopoly. Here's what you need to know", *The Guardian*, (October 21, 2025), <https://surl.li/itjqjz>, (Accessed 04.11.2025).

21 Courtney Stewart, "Think Bigger, Act Larger: A U.S.-Australia Led Coalition for a Combined Joint Deterrence Force in the Indo-Pacific", *Carnegie Endowment for International Peace*, (October 2, 2024), <https://surl.li/wywmeg>, (Accessed 04.11. 2025).

Enhanced Space Cooperation (ESC) initiative is a new program designed to increase opportunities for space integration among allies.²²

Although this article focuses on U.S.- Australia bilateral relations, it is also appropriate to mention that the allies cooperate through multilateral defense and security frameworks. Notable examples include AUKUS, ANZUS, QUAD, and Five Eyes. Furthermore, the 2007 Cooperation Declaration between Australia and Japan, along with Australia's close and deep partnership with NATO, plays a fundamental role in advancing the U.S.-Australia alliance.²³

In conclusion, Australia currently faces a significant dilemma. Despite its close economic ties with China, it must strengthen its security cooperation with the United States, its traditional ally. The benefits derived from expanding trade relations with Beijing do not outweigh the risks posed by China's growing military modernization, expanding influence, nuclear capabilities, and increasingly assertive territorial claims in the Indo-Pacific region. China seeks to shape a regional order favorable to its national interests, often at the expense of other states' sovereignty and the overall stability of the Indo-Pacific. Accordingly, Australia's approach toward the United States reflects a pragmatic and rational response to China's assertive and destabilizing actions.

To mitigate these risks and contribute to regional and international peace, Australia and the United States strive to strengthen their alliance and intensify bilateral and multilateral cooperation, particularly in the areas of defense and economic security. Collaborative frameworks, complex and combined military exercises, joint weapons production, and the development of Australia's defense industry provide a solid foundation for building resilience among American and Australian forces, restraining China's hegemonic ambitions, and maintaining the balance of power in the strategically vital Indo-Pacific region.

Bibliography

- Associated Press, "China Has Fully Militarized Three Islands in South China Sea, US Admiral Says", The Guardian, (21 March 2022), <https://surl.li/ttxeew> (Accessed 04.11.2025).
- Australian Government, «United States Force Posture Initiatives», Department of Defence, <https://surl.lu/njgpdo>, (Accessed 04.11. 2025).
- Barrett, Jonathan. «Australia and the US have signed a critical minerals deal to take on China's monopoly. Here's what you need to know», The Guardian, (October 21, 2025), <https://surl.li/itjqjz>, (Accessed 04.11.2025).
- Bitzinger, Richard. "Modernising China's Military, 1997-2012", China Perspectives, (2011 April), (Accessed 04.11.2025). <https://doi.org/10.4000/chinaperspectives.5701>
- Bureau of Political-Military Affairs, «U.S. Security Cooperation With Australia», U.S. Department of State, (January 19, 2025), <https://surl.li/rnnyfy>, (Accessed 04.11.2025).
- Chan, Edward. "How Worried Should Canberra Be About China's Security Interests in the Pacific? Perspectives from PRC and Pacific Interlocutors", University of Technology Sydney, (July 2, 2025), <https://surl.li/yhowli>, (Accessed 04.11.2025).
- Cordesman, Anthony H., & Joseph Kendall. *Chinese strategy and military modernization in 2017: A comparative analysis*. Washington, D.C: Center for Strategic and International Studies, 2017 <https://surl.li/pbvrmnd>, (Accessed 04.11.2025).

²² Australian Government, "United States Force Posture Initiatives", Department of Defence, <https://surl.lu/njgpdo>, (Accessed 04.11. 2025).

²³ Richard Tanter, "The US Military Presence in Australia: Asymmetrical Alliance Cooperation and its Alternatives", *Asia-Pacific Journal: Japan Focus*, vol. 11, no. 45, (November 10, 2013), <https://surl.li/oevfyn>, (Accessed 04.11.2025).

- Dibb, Paul, «U.S.-Australia Alliance Relations: An Australian View», *Strategic Forum*, no. 216 (August 2005): 1, <https://surl.li/cmejfd>, (Accessed October 15, 2025).
- European Foundation for South Asian Studies. *Drivers, trajectories and prospects of military modernization in China*. Amsterdam: EFSAS, July 2022 <https://surl.li/ibraq>, (Accessed October 15, 2025).
- Fallon, Stephen. «Australia's Security Relationships in the Indo-Pacific.» Briefing Book Article, 47th Parliament. Parliament of Australia, (June 2022), <https://surl.li/fjgqqd>, (Accessed October 15, 2025).
- Funaiole, Matthew P., & Brian Hart, "China's Military in 10 Charts", Center for Strategic and International Studies, (September 2, 2025), <https://www.csis.org/analysis/chinas-military-10-charts> (Accessed 04.11.2025).
- Heginbotham Eric, & Michael S. Chase. "China's military modernization: Eric Heginbotham and Michael Chase in conversation", RAND Corporation, (September 14, 2015), <https://surl.li/mkxqbb> (Accessed 04.11.2025).
- Laksmana, Evan, Paul Fraioli, Veerle Nouwens, and James Hackett. „Asia-Pacific Regional Security Assessment 2024, «Scripted Order: Combined-military Exercises in the Asia-Pacific.» The International Institute for Strategic Studies, (2024): 3-4, 8-9, <https://surl.li/tuczpm> (Accessed 04.11.2025).
- Latham, Andrew. "What or Where Is the Indo-Pacific?: How a foreign policy pivot redefined the global map". *The Diplomat* (May 17, 2025), <https://surl.li/uewzsw>, (Accessed 04.11.2025).
- Liang, Xiao, Dr Nan Tian, Dr Diego Lopes da Silva, Lorenzo Scarazzato, Zubaida A. Karim, and Jade Guiberteau Ricard. «Trends in World Military Expenditure, 2024», Stockholm International Peace Research Institute, <https://doi.org/10.55163/AVEC8366> (Accessed 04.11.2025).
- Lloyd, Jack. "Australia, US strengthen guided weapons cooperation", *Manufacturers' Monthly*, (October 15, 2025), <https://surl.li/sxqlwt>, (Accessed 04.11.2025).
- Papageorgiou Maria, & Zeno Leoni. "The Five Eyes Allies and China: Assessing Threat Perceptions and Power Dynamics", *J OF CHIN POLIT SCI* (2025), (Accessed 04.11.2025). <https://doi.org/10.1007/s11366-025-09913-w>
- Stewart, Courtney. Courtney Stewart. "Think Bigger, Act Larger: A U.S.-Australia Led Coalition for a Combined Joint Deterrence Force in the Indo-Pacific", Carnegie Endowment for International Peace, (October 2, 2024), <https://surl.li/wywmeg>, (Accessed 04.11. 2025).
- Tanter, Richard. «The US Military Presence in Australia: Asymmetrical Alliance Cooperation and its Alternatives», *Asia-Pacific Journal: Japan Focus*, vol. 11, no. 45, (November 10, 2013), <https://surl.li/oevfvn>, (Accessed 04.11.2025).
- Vergun, David. David Vergun, «China's Military Buildup Threatens Indo-Pacific Region Security», U.S. Department of War, (April 9, 2025), <https://surl.li/dqmsdc>, (Accessed October 15, 2025).
- Walters, Riley. "China's Military Expansion Toward the Southwest Pacific and Oceania", *GIS Reports*, (July 15, 2025), <https://surl.li/bevdnq>, (Accessed October 15, 2025).

TECHNOLOGY AND SECURITY: BILATERAL DEFENSE INNOVATION PARTNERSHIPS IN THE NATO SPACE

Lasha Chokolashvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Otar Oniani

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Sophiko Metreveli

Assistant Professor of Bachelor's Program in Defense and security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The article analyzes the interconnection between technological innovation and security within NATO, focusing on the model of dual-use defense innovation partnerships. It examines the role of NATO's innovation architecture (such as DIANA and NIF), which ensures the effective integration of dual-use technologies from the private, civilian sector into defense capabilities, thereby accelerating the preservation of technological superiority. The analysis shows that although dual-use partnerships strengthen the Alliance's resilience through AI, autonomous, and space systems, they also introduce new threats. The main challenges include cybersecurity risks within the supply chain, ethical dilemmas in autonomous decision making, and geopolitical competition regarding the protection of intellectual property.

In conclusion, the article offers recommendations for strengthening NATO's innovation policy. These include the mandatory implementation of Secure by Design standards, the establishment of an Alliance-wide ethics council for AI governance, and the reinforcement of export control mechanisms to protect critical technologies. These measures are essential for NATO to maintain its technological superiority in a complex global security environment.

Keywords: NATO, dual-use technologies, DIANA, NIF, defense innovation, cybersecurity, AI ethics.

Introduction

The security environment of the 21st century is evolving in a context where technological progress not only accelerates global political transformation, but also reshapes the conceptual foundations of defense and security. The unprecedented pace of technological change creates new opportunities while simultaneously introducing complex challenges that affect every component of the international security system. The shift in the global balance of power, the growing ambitions of authoritarian regimes, and the rapid development of military-scientific innovation make it necessary for collective security organizations to reassess their strategic priorities.

Modern technological advancements, including the intensive adoption of artificial intelligence (AI), hypersonic systems, space technologies, and biotechnological solutions, create new types of threats that transcend traditional military logic. These technologies no longer serve solely as instruments of military superiority; they have become key pillars of the stability and resilience of the collective security system. In this transformational reality, maintaining the technological advantage of the North Atlantic Treaty Organization (NATO) is of particular importance, since it remains one of the fundamental elements of the Alliance's deterrence and defense strategy. NATO's 2030 agenda clearly demonstrated that traditional defense models based exclusively on state structures cannot provide the scale and speed of innovation required to prevent a technological gap. For this reason, the concept of dual-use innovation partnerships has become one of the central directions of NATO's security policy.

Dual-use partnership implies the decisive role of dual-use technologies, integrating advanced solutions developed in the private and civilian sectors into military and security infrastructure in an effective manner. This model strengthens the technological and operational readiness of Allied states, reduces the time and costs required for innovation deployment, and creates a sustainable cooperation framework between government and private sector actors. Through this approach, innovation is no longer confined to government oversight alone; it transforms into a global, multisectoral process that actively involves startups, universities, and private companies. Structures and initiatives such as the Defense Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (NIF) play a special role in shaping NATO's innovation architecture, creating mechanisms that accelerate the transition of technological solutions into military practice and enhance the strategic flexibility of the Alliance.

The purpose of this article is to assess the effectiveness of NATO's innovation architecture, analyze the dynamics of dual-use technological partnerships, and identify the challenges and opportunities associated with this model in practice. Particular attention is given to critical security risks such as cybersecurity, ethical regulations, and intensifying geopolitical competition. Therefore, dual-use innovation partnership within the Alliance is viewed not as an additional operational resource, but as the strategic core of the contemporary security architecture, the effectiveness of which will define NATO's role and influence within the future global security ecosystem.

Innovation Mechanisms within the NATO Framework: DIANA, NIF, and Strategic Approaches

The North Atlantic Treaty Organization (NATO) is actively responding to the dynamic transformations of the 21st century security environment, which necessitates the creation and development of an innovative architecture. This architecture serves as a key foundation of the Alliance's strategic and operational advantage, with the fundamental goal of effectively accelerating and integrating critical and emerging technologies (Emerging and Disruptive Technologies - EDT) into the fields of defense and security.¹ NATO's innovation ecosystem encompasses a diverse range of instruments and mechanisms, among which two initiatives hold a central place: the Defence Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund (NIF). DIANA is a flagship initiative designed to accelerate the integration of dual-use technological solutions that serve both civilian and military needs.² Its main function is to bridge the so-called "innovation gap," or the *Valley of Death* a critical stage between laboratory discovery and operational deployment. DIANA's structure brings together a network of accelerator centers and test sites across NATO member states, where military experts, academic institutions, and private startups collaborate to address critical challenges. This approach enables the rapid validation of technologies in real operational environments, strengthens transatlantic cooperation, and significantly shortens the technology development cycle.³

To provide financial support for DIANA's operational objectives, NATO established the NATO Innovation Fund (NIF). This is the world's first multi-sovereign venture capital fund, created to directly invest in deep-tech startups. NIF provides capital to companies developing technologies of strategic importance, including artificial intelligence (AI), autonomous systems, and quantum technologies. The role of NIF goes beyond traditional financial investment it establishes a structured financial framework that mitigates private sector risks in entering the defense market and facilitates the rapid transformation of products into military applications. Beyond DIANA and NIF, NATO's innovation architecture relies on additional strategic mechanisms that ensure the Alliance's operational cohesion and resilience. These include the NATO Innovation Hub and the Connected Forces Initiative (CFI), which promote the exchange of knowledge, experience, and technological data among member countries.⁴ Together, these initiatives ensure that NATO's innovation policy is not merely reactive but proactive, allowing the Alliance to provide timely and adequate responses to collective security challenges. These innovation mechanisms lay a solid foundation for the practical realization of bilateral partnerships discussed in the following chapter.

Bilateral Partnership in Practice: Examples of Dual-Use Technologies and Private Sector Integration

The primary objective of NATO's innovative institutional framework (DIANA, NIF) is to deepen bilateral partnerships, founded on the development and application of dual-use technol-

1 Johnson, Mark. 2024. "Accelerating Defense: DIANA's Role in NATO's Future." *Security Studies Journal* 25, no. 3: 45–60.

2 NATO Report. 2022. *The Future of Transatlantic Security: A Framework for Innovation*. Brussels: NATO Publishing.

3 NIF Official Website. (Accessed 04.11.2025).

4 Smith, Laura, and Thomas Jones. 2023. *Dual-Use Technologies and NATO's Edge*. New York: University Press.

ogies.⁵ These technologies, which can be utilized for both military and civilian purposes, allow modern defense systems to maximize resource efficiency and significantly accelerate the practical implementation of innovations.

NATO's focus on this model aims to reduce reliance on purely governmental resources and to expedite the process of innovation deployment in real-world practice.⁶ Within this framework, the involvement of the private sector is particularly important. Technology companies, startups, and academic institutions are developing solutions that are rapidly integrated into the structures of the Alliance. A prominent example of a dual-use technology is the application of artificial intelligence (AI) and machine learning systems.⁷ These technologies are employed not only for the planning and analysis of military operations but also in civilian domains such as crisis management, emergency response coordination, and critical infrastructure protection. Similarly, space technologies, including satellite imagery analysis, play a key role in providing intelligence functions while also supporting various civilian applications.

Another essential dimension of private sector integration involves the structuring of financial investments. The NATO Innovation Fund (NIF) not only provides initial capital but also acts as a “trusted lead investor,” thereby attracting additional private venture capital to dual-use startups. This mechanism enables innovators to gain both financial support and operational feedback derived from real defense experience.⁸

As a result, bilateral partnership within NATO's framework creates an integrated ecosystem in which the agility and innovativeness of the private sector effectively combine with the scale and security requirements of the Alliance. Despite these successes, the large-scale adoption of dual-use technologies faces serious challenges particularly in the areas of cybersecurity, ethical dilemmas, and geopolitical competition.

Security Challenges: Cybersecurity, Ethics, and Geopolitical Competition

Despite the strategic benefits of large-scale integration of dual-use technologies, bilateral partnerships also give rise to complex and multidimensional security challenges that require NATO's immediate and coordinated response. These challenges threaten both the Alliance's operational credibility and the effectiveness of its collective defense principles, focusing primarily on the dimensions of cybersecurity, ethical dilemmas, and geopolitical competition.⁹

The first and most critical challenge is cybersecurity. The integration of technologies originating from the private sector especially the use of commercial products developed by startups significantly expands the potential attack surface of NATO's target networks. Since dual-use systems often rely on commercial operating systems and open source code, they are more vulnerable to cyberattacks from malicious actors, including state-sponsored groups.¹⁰ The risk is further intensified by the fact that many small and medium sized enterprises (SMEs) participating in NIF or DIANA programs may lack the “high level cyber hygiene standards” required in the defense

5 Laura Smith and Thomas Jones, *Dual-Use Technologies and NATO's Edge* (New York: University Press, 2023), 135–138.

6 ნატო, „ნატოს ინოვაციის სტრატეგია 2030,“ 2024, გვ. 7.

7 Mark Johnson, “Accelerating Defense: DIANA's Role in NATO's Future,” *Security Studies Journal* 25, no. 3 (2024): 49.

8 NATO Innovation Fund, “Annual Report 2024,” 2024, 15.

9 Mark Johnson, “Accelerating Defense: DIANA's Role in NATO's Future,” *Security Studies Journal* 25, no. 3 (2024): 55.

10 Laura Smith and Thomas Jones, *Dual-Use Technologies and NATO's Edge* (New York: University Press, 2023), 180–185.

sector. This vulnerability poses serious risks of intellectual property theft, classified information leaks, and operational data breaches. For the Alliance, it is vital to conduct rigorous cybersecurity audits across the supply chain to prevent the presence of embedded malicious code or “backdoors” that could grant adversaries access to NATO’s infrastructure.

The second major challenge concerns ethics and governance, especially amid the growing deployment of autonomous systems. The use of artificial intelligence (AI) in decision making processes including in the planning and execution of military operations requires a strict ethical and legal framework. NATO’s guiding principles of responsibility, transparency, and bias mitigation must ensure that AI based decisions remain under human oversight.¹¹ The potential for autonomous systems to operate without human intervention particularly in the case of lethal autonomous weapons systems (LAWS) raises profound moral and legal dilemmas that directly relate to international humanitarian law. NATO members must jointly develop mechanisms for AI ethical auditing to ensure that technological superiority is not achieved at the expense of ethical norms.

Finally, geopolitical competition in the field of innovation poses a constant threat to the Alliance’s security. Global competitors particularly China and Russia are conducting targeted campaigns to gain technological superiority and replicate Western innovations. The dual-use nature of technologies facilitates adversarial access to them by blurring the boundary between civilian and military applications.¹² This occurs not only through traditional espionage but also through capital investment and academic partnerships, allowing competitors to acquire intellectual property indirectly. It is therefore essential for NATO to strengthen coordinated export control policies and safeguard innovations included in the list of “critical technologies,” ensuring that strategic competitors cannot exploit dual-use cooperation to enhance their own military capabilities. Addressing these challenges requires not only technological resilience but also political resilience.

Conclusion

This study assessed the strategic significance of bilateral defense innovation partnerships within NATO and identified their primary implementation challenges. The analysis clearly demonstrated that, in an era of rapid technological transformation and intensifying geopolitical competition, innovation is not merely a means of achieving operational superiority but a critical prerequisite for maintaining the Alliance’s collective security.

The first chapter discussed NATO’s innovation architecture specifically DIANA and NIF as the institutional foundation for integrating dual-use technologies. The second chapter established that bilateral partnerships are being successfully implemented in practice through the integration of AI, autonomous, and space technologies, effectively bridging the innovation gap with active private-sector participation. Despite this progress, the third chapter analyzed in detail several serious security challenges: cybersecurity risks stemming from expanded supply chains, ethical dilemmas related to autonomous systems, and geopolitical competition over the protection of intellectual property.

11 ნატო, „ნატოს ინოვაციის სტრატეგია 2030,“ 2024, გვ. 12.

12 Strategic Studies Institute, *Geopolitical Competition in the Age of AI* (Carlisle, PA: SSI Press, 2023), 42.

The future success of NATO's innovation policy will depend not only on acquiring new technologies but also on its capacity to manage these risks and to strengthen its strategic vision. Therefore, several fundamental steps are necessary to enhance the Alliance's innovation policy.

First and foremost, NATO should establish mandatory "Secure by Design" standards for all dual-use technologies funded by NIF and integrated through DIANA. This requires rigorous testing and auditing to identify and eliminate supply chain vulnerabilities, particularly when collaborating with smaller startups. Equally crucial is the institutional strengthening of AI ethics governance. NATO should create a unified, Alliance-wide NATO AI Ethics Board, which would continuously assess the moral and legal implications of AI use and ensure the implementation of a Human in Command Framework in connection with lethal autonomous systems. Maintaining ethical standards will enable NATO to preserve public trust and compliance with international norms amid technological progress.

Furthermore, it is essential to reinforce policies for protecting strategic technologies. This includes developing coordinated export control mechanisms among NATO member states to identify critical dual-use technologies whose access should be restricted to strategic competitors, as well as strengthening counterintelligence efforts within academic and private sectors to safeguard intellectual property from foreign investment and espionage.

Finally, NATO must leverage innovation policy as a diplomatic instrument promoting the establishment of international norms and standards for the use of new technologies thereby reducing the risks of escalation. Implementing these recommendations will ensure that NATO maintains its technological edge and remains a reliable guarantor of collective security for decades to come.

Bibliography

- Johnson, Mark. "Accelerating Defense: DIANA's Role in NATO's Future." *Security Studies Journal* 25, no. 3 (2024).
- NATO Innovation Fund. "Annual Report 2024." 2024.
- Smith, Laura, and Thomas Jones. *Dual-Use Technologies and NATO's Edge*. New York: University Press, 2023.
- Strategic Studies Institute. *Geopolitical Competition in the Age of AI*. Carlisle, PA: SSI Press, 2023.
- NATO. "NATO Innovation Strategy 2030." Brussels: NATO Secretariat, 2024.

TECHNOLOGICAL DEVELOPMENT AND DEFENCE INNOVATION IN THE CAUCASUS DURING THE RUSSIA–UKRAINE WAR

Giorgi Chkhaidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Lado Gogoladze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

This paper provides a comprehensive analysis of how the Russia–Ukraine war has acted as a catalyst for defense modernization and technological transformation across the South Caucasus, reshaping the strategic orientations of Georgia, Armenia, and Azerbaijan. The conflict has demonstrated that technological innovation, adaptability, and cross-domain integration have become decisive determinants of success in modern warfare, surpassing traditional measures such as manpower and conventional armament.¹ As warfare becomes increasingly digitized and networked, smaller regional actors now face the imperative of achieving technological sovereignty and building innovation ecosystems capable of ensuring resilience and autonomy within an intensifying environment of great-power competition.

Through a comparative analysis, the study investigates how each Caucasus state has internalized the lessons of Ukraine's wartime adaptation and redefined its defense priorities accordingly. Georgia has focused on cyber defense, UAV research, and Western interoperability, embedding digital transformation into its defense architecture. Armenia, having faced the tactical realities of drone warfare, has turned toward defense diversification, counter-UAS systems, and domestic research and development initiatives, seeking to reduce its dependence on traditional Russian suppliers. Azerbaijan, leveraging its industrial capacity and partnerships with Turkey and Israel, has emphasized industrial expansion, autonomous systems, and co-production partnerships, consolidating its position as a regional defense innovator. Collectively, these approaches signify a strategic transition from reliance on foreign procurement toward innovation-driven, self-sustaining defense models tailored to hybrid and asymmetric threat environments. The paper concludes that the Caucasus region serves as a microcosm of the global evolution in defense strategy, where the fusion of technology, strategy, and adaptability defines modern security paradigms. The region's experience underscores that sustained modernization, institutionalized innovation, and multilateral cooperation are now fundamental prerequisites for long-term stability and geopolitical resilience. In the emerging multipolar order, defense innovation has become not only a matter of military capability but also an instrument of sovereignty, diplomacy, and survival for smaller states navigating the complex landscape of technological warfare.

Keywords: Russia–Ukraine War; Caucasus; Defense Innovation; Technological Modernization; Cybersecurity; Artificial Intelligence; Unmanned Aerial Systems (UAS); Military Strategy; Hybrid Warfare; Technological Sovereignty; Regional Security; Innovation Ecosystems.

¹ See Aosheng Pusztaszeri and Emily Harding, "Technological Evolution on the Battlefield," CSIS, September 16, 2025

Introduction

The ongoing Russia–Ukraine war has profoundly altered the architecture of global security, compelling states to reassess their defense doctrines, industrial capacities, and technological dependencies. What began as a regional conflict has evolved into a broader strategic inflection point, reshaping military thinking across continents. The war has vividly demonstrated the transformative power of technology in modern warfare—revealing how innovations such as unmanned aerial systems (UAVs), cyber operations, artificial intelligence (AI), and digital command-and-control systems can determine the outcomes of military engagements.² In this new era of technology-driven warfare, even smaller states find themselves compelled to innovate in order to maintain sovereignty and resilience. Among these, the Caucasus nations—Georgia, Armenia, and Azerbaijan—stand out for their active pursuit of defense modernization amid a rapidly shifting geopolitical landscape. Situated at the strategic crossroads of Europe, Russia, and the Middle East, the Caucasus region has historically been shaped by the rivalry of great powers and the overlapping spheres of influence that define its security environment. The legacy of post-Soviet dependency, combined with the region’s exposure to recurring military conflicts, has long constrained indigenous defense development. However, the 2022 full-scale invasion of Ukraine by Russia marked a decisive turning point.³ It not only intensified regional insecurity but also exposed structural vulnerabilities in the Caucasus states’ reliance on imported military technologies and external security guarantees. Each state within the region responded in line with its distinct geopolitical orientation and strategic objectives:

Georgia, maintaining its pro-Western trajectory, deepened cooperation with NATO and prioritized the development of cyber defense and drone capabilities.

Azerbaijan, buoyed by its close ties with Turkey and Israel, expanded its indigenous UAV and electronics industries, strengthening both offensive and surveillance capacities.

Armenia, facing renewed security challenges following the 2020 Nagorno-Karabakh conflict and shifting alliances, sought new defense partnerships with France, India, and the European Union to diversify its security and technology base. This evolving dynamic illustrates that defense innovation in the Caucasus is not merely a response to regional instability but part of a broader global transition toward technologically enabled security systems. The rise of dual-use technologies—where civilian advances in AI, robotics, telecommunications, and data analytics are repurposed for defense—has blurred the line between traditional and hybrid warfare. These developments, while offering smaller states the opportunity to modernize their armed forces, also risk deepening their dependence on foreign technologies and external political actors. Thus, the Russia–Ukraine conflict serves as both a warning and a catalyst: it underscores the dangers of technological vulnerability while accelerating innovation as a form of strategic self-preservation. The intersection of technological modernization and strategic necessity has, in turn, led to a gradual transformation of the Caucasus defense ecosystem. Over the past few years, the region has witnessed the emergence of domestic research centers, cyber defense institutions, and innovation hubs, often estab-

2 Vugar Khalilov, “How War in Ukraine Reshaped Military Technology and Strategy?” *Caliber.az*, February 22, 2025

3 “Russia’s Changes in the Conduct of War Based on Lessons from Ukraine: Adapting Technology, Force Structures, and the Defense Industry,” *Military Review*, September–October 2025

lished through partnerships between universities, private industries, and defense ministries. These developments mirror similar innovation models observed in Eastern and Central Europe, where state-backed innovation ecosystems are reshaping the defense-industrial landscape. Yet, in the Caucasus, this process remains uniquely shaped by the realities of post-Soviet transition, contested sovereignty, fragile economies, and aspirations for Euro-Atlantic integration.

Accordingly, this paper seeks to examine how the Russia–Ukraine war has acted as a catalyst for defense innovation and technological adaptation in the Caucasus. It analyzes the evolving priorities of Georgia, Armenia, and Azerbaijan in the fields of unmanned systems, cybersecurity, artificial intelligence, and defense-industrial modernization, while assessing how international partnerships and digital transformation are redefining the region’s security paradigm. The study ultimately argues that the Caucasus has become not only a zone of geopolitical contestation but also a laboratory for understanding how small states leverage innovation to safeguard sovereignty and navigate the complexities of technological warfare in the 21st century.

Technological Development and Military Modernization

The ongoing Russia–Ukraine war has acted as a powerful catalyst for military modernization and technological transformation across the post-Soviet space. Beyond the immediate frontlines, the conflict has demonstrated that technological superiority—not sheer manpower or firepower—now determines success on the battlefield. The unprecedented integration of unmanned aerial systems (UAVs), electronic warfare (EW), digital command networks, and AI-enhanced situational awareness has redefined the character of war, making it faster, more adaptive, and increasingly data-driven. As a result, neighboring regions such as the South Caucasus have been compelled to rethink their defense doctrines, industrial strategies, and innovation policies in order to maintain strategic balance and national resilience. The war’s emphasis on real-time intelligence, drone warfare, and rapid adaptation has shattered conventional assumptions about military preparedness. As analysts note, “the war in Ukraine has irreversibly changed the perception of how technology determines success on the battlefield.”⁴ For the Caucasus states—Georgia, Armenia, and Azerbaijan—this paradigm shift has translated into accelerated defense innovation, expanded industrial and academic partnerships, and a growing determination to achieve technological sovereignty within their respective security frameworks.⁴ The modernization drive has been shaped by both regional security pressures and global technological competition, situating the Caucasus as a key testing ground for emerging defense technologies.

Georgia: Cyber Defense and Western Integration

Among the three Caucasus states, Georgia has pursued one of the most structured and forward-looking defense modernization agendas, closely aligned with NATO and European Union integration goals. The 2008 Russia–Georgia war, followed by successive cyberattacks on Georgian governmental and financial infrastructure, left deep institutional lessons regarding the vulnerabilities of traditional defense systems. Consequently, Georgia’s post-2022 strategy has prioritized

⁴ Pustaszzeri and Harding, “Technological Evolution on the Battlefield,” CSIS

cybersecurity, digital command modernization, and UAV research and production as essential pillars of national resilience.

In 2023, the Ministry of Defence of Georgia launched the Cyber Command Center, a milestone in the country's evolving defense architecture. This institution integrates artificial intelligence (AI) and machine-learning algorithms to enhance intrusion detection, data correlation, and early-warning capabilities. Drawing on lessons learned from Ukraine—where digital command networks, mobile data systems, and decentralized control proved decisive—Tbilisi has embraced a defense model that emphasizes adaptability, digital connectivity, and interoperability. As *Caliber.az* insightfully notes, “legacy systems don’t win future wars—they lose them,”⁵ a statement that encapsulates Georgia’s shift toward flexible, technology-driven defense structures. Parallel to this digital transformation, Georgia’s Delta Military Scientific-Technical Center has resumed the production of light armored vehicles and initiated indigenous drone research projects, with the goal of reducing dependence on foreign suppliers. Supported by NATO’s Science for Peace and Security (SPS) Program, these initiatives also explore dual-use technologies, such as AI-enabled border monitoring systems, autonomous reconnaissance platforms, and electronic warfare sensors. Such projects reflect Georgia’s ambition to cultivate a homegrown defense-industrial base capable of supporting both military and civilian technological advancement. The link between academia and defense has also strengthened significantly. Partnerships with Ilia State University, Georgian Technical University, and private technology firms have fostered innovation ecosystems that bridge scientific research, applied engineering, and defense applications. This academic-industrial collaboration has become a cornerstone of Georgia’s broader national innovation strategy, aligning defense modernization with digital transformation across the public sector.

Moreover, Georgia’s active participation in NATO-led joint exercises—including Noble Partner and Cyber Coalition—has enhanced its interoperability with Western forces, especially in the domains of digital communication, real-time data exchange, and cyber defense coordination. These exercises serve not only as military training platforms but also as laboratories for testing new technologies, data systems, and tactical AI applications in simulated hybrid warfare conditions. Through these reforms, Georgia is steadily evolving from a conventional defense posture toward a technologically agile and digitally integrated security model. By combining cyber innovation, modular defense production, and international cooperation, the country seeks to establish a “smart defense” system—a lean but highly capable force structure capable of responding rapidly to hybrid and asymmetric threats.

Ultimately, Georgia’s trajectory exemplifies how smaller states can transform their security ecosystems through strategic alignment, technological adaptation, and institutional learning. By integrating digital transformation into defense planning, Georgia not only enhances its national security but also reinforces its position as a reliable partner within the Euro-Atlantic security architecture.

Armenia: Defence Diversification and Emerging Partnerships

For Armenia, the lessons of modern warfare have been both urgent and transformative. The devastating outcomes of the 2020 and 2023 Nagorno-Karabakh conflicts exposed the country’s

5 Khalilov, “How War in Ukraine Reshaped Military Technology and Strategy?” *Caliber.az*.

acute vulnerability to drone-centric warfare and its long-standing dependence on outdated Soviet-era military systems. These conflicts marked a turning point in Yerevan's defense thinking, revealing the limitations of traditional force structures in the face of networked reconnaissance, precision strikes, and electronic warfare. The ongoing Russia–Ukraine war further underscored the same realities on a global scale—illustrating the limits of conventional military doctrines and emphasizing the strategic necessity of technological adaptation and diversified partnerships.

In this context, Armenia's defense modernization strategy has shifted decisively toward electronic warfare, air defense enhancement, and strategic diversification of suppliers. The government in Yerevan now recognizes that reliance on a single defense patron—namely Russia—poses not only operational but also geopolitical risks. Since 2023, Armenia has actively expanded cooperation with France, India, and the European Union, acquiring advanced radar systems, anti-drone technologies, and loitering munitions. These initiatives reflect a deliberate reorientation in Armenian security policy: from dependency to partnership pluralism, and from passive procurement to active innovation and co-development. Armenia's post-Karabakh defense posture thus embodies both strategic urgency and technological pragmatism. The combat experiences of 2020–2023 revealed the lethality of integrated drone-artillery complexes and the ineffectiveness of legacy Soviet systems against modern ISR (Intelligence, Surveillance, Reconnaissance) networks and precision-guided munitions.⁶ In direct response, Yerevan has prioritized the acquisition of radar systems, short-range air-defense platforms, and counter-UAV electronic warfare kits. Beyond procurement, Armenia has also begun establishing domestic prototyping facilities dedicated to developing drone components, communication sensors, and electronic modules—a modest yet critical step toward technological self-reliance. A significant milestone in this transformation was the establishment of the Centre for Military Technology and Innovation (CMTI) in 2024. Conceived as a tripartite collaboration between universities, private technology firms, and the Ministry of Defence, the CMTI aims to cultivate Armenia's indigenous defense R&D ecosystem. Its key focus areas include cyber defense, robotics, sensor technologies, and autonomous systems, with an overarching goal of laying the foundation for a sustainable domestic defense industry. By linking academic research with industrial application, Armenia seeks to replicate successful innovation ecosystems observed in countries like Ukraine, Poland, and Estonia—nations that have leveraged innovation to offset numerical and resource disadvantages.⁷

Moreover, inspired by Ukraine's wartime innovation model, Armenia has begun to explore rapid prototyping and additive manufacturing (3D printing) for producing replacement parts, drone frames, and electronic components. Such methods enable faster adaptation to battlefield needs and reduce logistical dependency on foreign suppliers. As *Caliber.az* highlights in its analysis of Ukraine's defense sector, the production of drones and cruise missiles increased “eightfold in 2024”⁸, underscoring the potential for exponential growth when innovation ecosystems are prioritized and state-supported. Armenia's leadership appears intent on emulating this flexible production model, aiming to integrate civilian tech startups and engineering faculties into defense-re-

6 “From Surveillance to Strike: Drones Redefine Ukraine's War Strategy,” *Caliber.az*, May 7, 2025

7 Russia's Changes in the Conduct of War Based on Lessons from Ukraine: Adapting Technology, Force Structures, and the Defense Industry,” *Military Review*, September–October 2025,

8 “Ukraine's Defense Production Soars: Cruise Missiles and Drones See Massive Growth in 2024,” *Caliber.az*, April 12, 2025

lated innovation networks., Nevertheless, Armenia faces considerable structural and institutional challenges. Building an independent innovation ecosystem requires long-term investment, skilled labor retention, and robust intellectual property protection—all of which remain fragile in the current economic and political environment. Furthermore, sustaining partnerships with France, India, and the EU will necessitate balancing geopolitical pressures from Moscow and ensuring that diversification does not provoke renewed dependency in new forms.

Ultimately, Armenia's defense diversification marks the beginning of a strategic evolution rather than its completion. The country's success will depend on its ability to institutionalize innovation, integrate technology into doctrine, and sustain long-term research capacity. The ongoing reforms suggest that Yerevan is no longer content with being a passive consumer of imported systems; instead, it is striving to become an active participant in the global defense innovation landscape. While this path remains fraught with economic and political constraints, Armenia's recent initiatives demonstrate a clear understanding of a new geopolitical reality: technological sovereignty is now synonymous with national security.

Azerbaijan: Industrial Expansion and Strategic Technology Partnerships

Azerbaijan has emerged as the regional leader in military technology innovation, largely due to its extensive cooperation with Turkey, Israel, and Pakistan. Building on the experience of its successful use of drones during the 2020 Nagorno-Karabakh conflict, Baku has continued to expand its domestic defence production capacities. The influence of Ukraine's innovation-driven war effort is visible in Azerbaijan's emphasis on unmanned aerial vehicles (UAVs), digital warfare systems, and smart manufacturing. Ukraine's rapid scaling of drone production—expected to grow tenfold by 2025—illustrates the potential of high-speed industrial adaptation.⁹ Azerbaijan has applied similar principles by co-developing Bayraktar UAV variants with Turkey's *Baykar* company and integrating AI-assisted targeting into its drone systems. The state's Defence Industry Agency now oversees a growing network of public and private firms engaged in electronics, communication equipment, and 3D-printed UAV components.

In 2023, Baku introduced its National Cybersecurity Strategy, addressing the protection of defence networks, satellite communications, and critical infrastructure. The country's partnership with Israel has also enabled the development of electronic warfare and counter-UAV systems, which complement its already sophisticated drone fleet. Moreover, Azerbaijan's participation in *dual-use innovation*—where civilian technologies such as AI, optics, and data analytics are applied to defence—demonstrates a move toward technological sovereignty. The country's growing investment in STEM education and defence-oriented research aligns with its ambition to become a regional hub for defence manufacturing and export.

Conclusion

The ongoing Russia–Ukraine war has fundamentally redefined the logic of modern warfare, demonstrating that agility, cross-domain integration, and scalable innovation now determine victory more decisively than numerical strength or conventional armament. In the contemporary securi-

⁹ From Surveillance to Strike: Drones Redefine Ukraine's War Strategy." *Caliber.az*, May 7, 2025.

ty environment, the side capable of adapting fastest, integrating technologies most efficiently, and sustaining innovation under pressure holds the strategic advantage. This reality carries profound implications for smaller regions such as the Caucasus, where states must navigate great-power competition with limited resources yet growing technological ambition. For Georgia, Armenia, and Azerbaijan, modernization is not about replicating the capabilities of global powers but about developing resilient, interoperable, and rapidly adaptive systems tailored to their own strategic geography and defense priorities. In this context, each state's modernization trajectory reflects a distinct synthesis of necessity, opportunity, and learning from Ukraine's experience.¹⁰

Georgia has pursued a model rooted in cyber defense, networked intelligence, and Western interoperability, prioritizing resilience through digital integration and NATO cooperation.

Armenia has embarked on strategic diversification, reducing its dependence on a single supplier while investing in domestic R&D ecosystems and counter-UAS technologies.

Azerbaijan, in turn, has emphasized industrial scaling, autonomous systems, and joint production partnerships with technologically advanced allies such as Turkey and Israel.

Together, these approaches reveal a regional trend toward functional modernization—building smaller, smarter, and more agile defense systems capable of responding effectively to the asymmetric and hybrid threats characteristic of 21st-century warfare. The geostrategic location of the Caucasus—at the intersection of Europe, Russia, and the Middle East—magnifies both the risks and imperatives of innovation. The proximity to ongoing conflict zones and the exposure to great-power rivalries mean that technological adaptation is not merely an advantage but a requirement for survival and strategic autonomy. Each state's innovation agenda demonstrates a growing awareness that technological sovereignty—the ability to develop, sustain, and operate independent capabilities—is now inseparable from national security. At a broader level, the Caucasus' modernization efforts reflect two intertwined dynamics: adaptation to the immediate realities of networked, information-driven warfare, and ambition to position themselves as credible, self-reliant actors in the emerging multipolar world order. These efforts align with the evolving global understanding that modern conflict is defined by the speed of innovation cycles, the integration of artificial intelligence, and the industrial capacity to sustain production under continuous stress. As *Caliber.az* aptly observes, “modern wars are no longer determined by troop numbers or stockpiles of conventional weapons, but by the capacity to innovate rapidly, integrate technology coherently, and sustain domestic production.”¹¹

Thus, the future of defense in the Caucasus will depend on how effectively each state can institutionalize innovation—transforming ad hoc modernization efforts into permanent, self-sustaining defense ecosystems. This requires long-term investment in education, industrial collaboration, digital infrastructure, and international partnerships, ensuring that innovation becomes not a reaction to crisis but an enduring strategic culture.

In conclusion, the Russia–Ukraine war has acted as both a warning and an accelerator for the Caucasus. It has revealed the vulnerability of outdated systems but also illuminated the path forward: a shift toward networked, adaptive, and innovation-driven defense architectures. For Geor-

10 From Surveillance to Strike: Drones Redefine Ukraine's War Strategy,” *Caliber.az*, May 7, 2025

11 Puztaszeri and Harding, “Technological Evolution on the Battlefield,” CSIS; *Military Review*.

gia, Armenia, and Azerbaijan, embracing this transformation is not only a means of enhancing security—it is the cornerstone of asserting sovereignty, preserving stability, and shaping their role in the evolving technological and geopolitical order of the 21st century.

Bibliography

- See Aosheng Pusztaszeri and Emily Harding, “Technological Evolution on the Battlefield,” CSIS, September 16, 2025, <https://surl.cc/sfyprn>
- Vugar Khalilov, “How War in Ukraine Reshaped Military Technology and Strategy?” *Caliber.az*, February 22, 2025, <https://surl.li/fzjqli>
- Aosheng Pusztaszeri and Emily Harding, “Technological Evolution on the Battlefield,” CSIS.
- “Russia’s Changes in the Conduct of War Based on Lessons from Ukraine: Adapting Technology, Force Structures, and the Defense Industry,” *Military Review*, September–October 2025, <https://surl.li/cznasb>
- “From Surveillance to Strike: Drones Redefine Ukraine’s War Strategy,” *Caliber.az*, May 7, 2025, <https://surl.lt/rcvw-jm>
- Pusztaszeri and Harding, “Technological Evolution on the Battlefield,” CSIS.
- Khalilov, “How War in Ukraine Reshaped Military Technology and Strategy?” *Caliber.az*.
- “Ukraine’s Defense Production Soars: Cruise Missiles and Drones See Massive Growth in 2024,” *Caliber.az*, April 12, 2025, <https://surl.li/nyjwuk>
- Pusztaszeri and Harding, “Technological Evolution on the Battlefield,” CSIS; *Military Review*.

ISRAEL'S DEFENCE STARTUPS

Gvantsa Dzmorashvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This paper provides a comprehensive analysis of how Israel has evolved into one of the world's foremost centers of defense innovation, achieved through the strategic integration of military expertise, government policy, and private-sector entrepreneurship. The study investigates the historical, geopolitical, and institutional foundations that have shaped Israel's defense innovation ecosystem, emphasizing the synergistic relationship among the Israel Defense Forces (IDF), the Directorate of Defense Research and Development (DDR&D), and an increasingly dynamic network of private startups and research institutions.

The research highlights several groundbreaking achievements, including the Iron Dome missile defense system, advanced cybersecurity frameworks, and dual-use technologies that have strengthened both national security and economic competitiveness. These developments illustrate how Israel's innovation model bridges defense imperatives with civilian technology sectors, resulting in a mutually reinforcing cycle of innovation and resilience. Furthermore, the paper critically examines the ethical, legal, and political dimensions of Israel's defense innovations, addressing debates surrounding surveillance technologies, export controls, and global regulatory frameworks.

Drawing on qualitative analysis, case studies, and recent wartime innovations, the paper demonstrates that Israel's defense partnerships—spanning the United States, the European Union, and emerging global actors—have become models of adaptive strategy and technological resilience. Ultimately, the study argues that Israel's fusion of innovation and defense strategy represents not merely a national security policy but a comprehensive framework for global defense modernization, contributing to international stability and technological advancement.

Keywords: Israel; Defense Innovation; Military–Private Partnerships; Cybersecurity; Iron Dome; Dual-Use Technology; Ethical Challenges; Defense Industry; National Security; Technological Resilience; Global Cooperation.

Introduction

In the twenty-first century, Israel has emerged as one of the world's most dynamic and influential centers of defense innovation—earning the global moniker “Start-Up Nation” for its exceptional concentration of technological creativity and entrepreneurship. What distinguishes Israel's defense ecosystem is not merely its capacity for invention but its extraordinary adaptability to rapidly evolving security threats. Since its establishment in 1948, Israel has faced an unremitting series of regional conflicts and existential challenges that have compelled it to innovate continuously in order to survive. In this context, technological advancement is not a luxury but a strategic necessity—a defining feature of Israel's national resilience. Over the decades, this survival-driven ingenuity has cultivated one of the most sophisticated and agile defense ecosystems in the world, where military expertise, government policy, and private-sector innovation converge to produce a unique model of security-oriented technological development.

At the heart of this innovation system lies a powerful tripartite collaboration among the Israel Defense Forces (IDF), the Directorate of Defense Research and Development (DDR&D), and a vibrant network of private startups and technology firms. This integrated partnership has enabled Israel to pioneer cutting-edge military technologies, from the Iron Dome missile interception system—a global benchmark in missile defense—to autonomous drones, advanced cybersecurity frameworks, and real-time data integration systems. These innovations exemplify Israel's capacity to transform immediate threats into opportunities for technological advancement and strategic advantage. In wartime conditions, the DDR&D plays a pivotal role in coordinating rapid research, development, and field deployment—streamlining approval processes and minimizing bureaucratic inertia to ensure that innovation remains both agile and operationally relevant.

Israel's defense innovation model also reflects a distinctive national mindset, combining entrepreneurship, pragmatism, and strategic foresight. The country boasts one of the world's highest per-capita concentrations of startups, with a culture deeply rooted in risk-taking, experimentation, and interdisciplinary collaboration. Many Israeli defense startups are founded by veterans of elite intelligence units, particularly Unit 8200, whose members bring not only technical mastery but also operational insight into contemporary warfare and cybersecurity. This constant feedback loop between battlefield experience and technological experimentation forms the foundation of Israel's agile, intelligence-driven innovation ecosystem, enabling it to anticipate and counter threats ranging from missile attacks to complex cyber intrusions.¹

Beyond the military sphere, Israel's defense sector has become a pillar of national strength, economic growth, and diplomatic influence. Defense exports—including missile defense systems, UAVs, communication technologies, and cybersecurity tools—constitute a substantial portion of Israel's GDP and reinforce its global reputation as a leader in high-tech security solutions. Strategic partnerships with the United States, India, NATO members, and the European Union underscore how defense innovation extends beyond the realm of national security to shape Israel's global influence, soft power, and economic diplomacy. This synergy between defense and development demonstrates that innovation in security technologies serves not only to safeguard borders but also to expand geopolitical and economic horizons. Accordingly, this paper seeks to explore the struc-

¹ „IDF Powers Israel's Tech Miracle“, Website: The Times of Israel, <https://surl.li/kbhaca>, Accessed 04.11.2025

tural, historical, and ethical dimensions of Israel's defense innovation ecosystem by addressing the following research questions:

How has Israel's historical and geopolitical context shaped its defense innovation ecosystem?

What role do collaboration and partnerships between the military, government, and private startups play in Israel's defense innovation success?

How has Israel leveraged dual-use and cybersecurity technologies to strengthen both national security and economic competitiveness?

What are the ethical and political challenges associated with Israel's defense technologies, particularly in areas such as surveillance and export control?

To what extent can Israel's defense innovation model serve as a prototype for other nations seeking to modernize their security strategies?

Through these inquiries, the study aims to present a comprehensive understanding of how Israel's integration of innovation, governance, and strategic necessity has positioned it as a global leader in defense technology, and how this model can inform future approaches to security modernization and technological sovereignty worldwide.²

Main Part

Historical background

Israel's defence development began almost simultaneously with the birth of the state itself in 1948. Surrounded by hostile neighbors and faced with limited natural resources, the newly established nation recognized early on that survival depended on technological ingenuity and strategic adaptability. The first Arab-Israeli war immediately exposed the shortcomings of Israel's nascent defence capabilities, emphasizing the need for self-reliance in arms production and innovation. In response Israel laid the foundations of a sophisticated in the world.

Throughout the 1950s and 1960s, the Israeli government pursued a strategy of technological independence, seeking to reduce reliance on foreign suppliers. The state invested heavily in research institutions and defence-oriented manufacturing, establishing Israel Aerospace Industries (IAI) in 1953 and Rafael Advanced Defence Systems in 1948. These organizations became the cornerstone of Israel's defence innovation, focusing on missile systems, radar, avionics, and electronic warfare technologies. Their work not only equipped the Israeli military with superior tools but also instilled a culture of problem-solving and experimentation that continues to define the nation's technological ethos today.

The six-Day war (1967) marked a turning point for Israel's defence strategy. The conflict demonstrated that military success depended not only on manpower or weaponry but also on intelligence, speed, and adaptability. As a result, Israel began integrating scientific research and data analysis into operational planning, a concept that would later evolve into the modern fusion of Artificial intelligence and real-time battlefield analytics. The lessons of this era led to the development of advanced air defence systems, electronic countermeasures, and early warning technologies-capabilities that helped Israel maintain a qualitative military edge in subsequent decades.

² The Dynamic Landscape of Israel's Defense Tech Ecosystem, July 31, 2024, Website: <https://surl.li/apcvvo>, Accessed 04.11.2025

The Yom Kippur War (1973) further underscored the importance of technological superiority. Despite being caught off guard at the onset of the conflict, Israel's ability to rapidly mobilize and employ innovative battlefield tactics highlighted the value of a responsive defence-industrial base. The war's aftermath spurred renewed investment in indigenous technology development and closer coordination between the military and research sectors. This period also saw the establishment of more formalized collaboration between the Directorate of Defense Research and Development (DD&D)³ and leading academic institutions, laying the groundwork for future partnerships with private startups.

By the 1980s and 1990s, Israel's defence innovation had expanded beyond traditional armaments to include satellite surveillance, unmanned aerial vehicles (UAVs), and early cyber capabilities. These advancements not only strengthened Israel's military resilience but also began transforming its economy. Defence research catalyzed the emergence of civilian high-tech industries, creating a feedback loop between military needs and commercial innovation. This dynamic, born from decades of necessity-driven creativity, positioned Israel as a global leader in both defence technology and entrepreneurial innovation.

In summary, the historical trajectory of Israel's defence⁴ development reflects a consistent pattern: each period of conflict and challenge has generated new waves of innovation. From the early establishment of state-owned defence companies to the modern integration of startups and digital technology, Israel's history demonstrates how continuous adaptation and strategic foresight can transform a nation's vulnerabilities into sources of strength and global influence.

Military-Private Sector Collaboration

Israel's defence innovation ecosystem is distinguished by its deep integration of the military establishment, government research institutions, and a rapidly evolving private startup sector. This tripartite structure-anchored by the Directorate of Defense Research and Development (DDR&D) within the Ministry of Defense-creates a highly adaptive environment where technological ideas can move swiftly from concept to combat deployment. Unlike many countries where bureaucratic hurdles slow innovation, Israel has cultivated a system in which necessity drives efficiency. This system allows rapid prototyping, expedited licensing, and fast-tracked production during both peace and wartime conditions.

The DDR&D plays a particularly critical role in coordinating between the Israel Defence Forces (IDF) and private companies. Its primary function is to identify operational needs, connect them with relevant technological capabilities, and oversee the transition from laboratory testing to large-scale production. During times of conflict, such as the 2023 Gaza escalation, the DDR&D has implemented fast-tracked licensing procedures and direct funding channels for startups developing innovations in UAVs, autonomous surveillance systems, cyber-defence tools, and missile interception technologies⁵. Startups working in these domains have been able to move from prototype to deployment in a matter of weeks rather than months, reflecting the agility of Israel's defence innovation pipeline.

3 Nissim Hania, „Transformations in the Israeli Defense Development and Production System, and the Contemporary Relevance“, Website: <https://surl.li/vjclxf>, Accessed 04.11.2025

4 „Israel Science & Technology: Defense Industry,“ Jewish Virtual Library, Website: <https://surl.li/drsqxx>, Accessed 04.11.2025

5 Development of Defense and Civilian Technologies, Website: <https://surl.li/prgcav>, Accessed 04.11.2025

A prime example of this synergy is the Iron Dome missile defence system- a globally recognized symbol of Israeli technological proof. The project emerged through collaboration between Rafael Advanced Defense systems, which provided engineering and systems integration expertise; the IDF, which supplied tactical data and operational requirements; and significant U.S. funding and technical support. The result was a defence platform capable of intercepting short-range rockets with an accuracy rate of approximately 90% during active conflicts. Beyond its immediate military function, the Iron Dome became a proof of concept demonstrating how military-private partnerships could yield not only national security gains but also international prestige and commercial export potential.

In addition to large state contractors like Rafael and Israel Aerospace Industries (IAI), smaller startups have become increasingly central to Israel's defence innovation strategy. Many of these startups are founded IDF intelligence and cyber units-especially from elite divisions such as UNIT 8200-whose alumni apply military-honed expertise to cutting-edge civilian and defence technologies. These firms often collaborate directly with the DDR&D through programs such as the Innovation Hub and INNOFENSE Accelerator, which provide testing environments, and guaranteed funding to leverage the creativity and agility of the private sector while ensuring that innovation aligns with national defence goals.

Moreover, Israel's innovation model emphasizes dual-use technologies,⁶ meaning that products developed for military purposes often have commercial applications in civilian markets. For instance, advancements in cybersecurity, artificial intelligence, and autonomous navigation-originally designed for intelligence or battlefield use-have been successfully commercialized in global industries ranging from finance to telecommunications. This dual-use dynamic strengthens Israel's economic resilience and reinforces a feedback loop in which profits from civilian applications help sustain continued defence research.

Another key feature of Israel's collaboration ecosystem is its wartime adaptability. During periods of heightened conflict, such as the 2023 Gaza war, the Ministry of Defense implemented emergency procurement frameworks allowing startups to receive immediate financial backing and temporary operational licenses. The DDR&D also facilitated direct testing within active zones, enabling startups to refine technologies under real-world conditions—something rarely possible elsewhere. This close coordination ensures that innovation is not only theoretical but operationally effective and responsive to evolving threats.

International cooperation further enhances this collaborative structure. Through bilateral partnerships, such as those with the United States and European allies, Israeli companies gain access to foreign markets, advanced materials, and joint research opportunities. These collaborations not only expand Israel's defence export portfolio but also deepen the integration of Israeli innovation into the global security ecosystem.

Ultimately, Israel's success in defence innovation is inseparable from its culture of inter sectoral collaboration. By combining the strategic foresight of the military, the scientific expertise of government research agencies, and the entrepreneurial dynamism of the private sector, Israel has

⁶ "War is good for business": Israeli startups going global after key role in Gaza", The Times of Israel, Website: <https://www.timesofisrael.com/war-is-good-for-business-israeli-startups-going-global-after-key-role-in-gaza/>, Accessed 04.11.2025

created a model of innovation that is both resilient and scalable. This ecosystem allows the country to maintain a qualitative military edge, respond rapidly to emerging threats, and export its technologies worldwide—cementing its reputation as one of the foremost centers of defence innovation in the 21st century.

Cybersecurity Leadership and Partnerships

Over the past two decades, Israel has established itself as a global epicenter of cybersecurity innovation and defence technology, positioning digital resilience as a national priority. The country's cybersecurity strength is not incidental but the result of deliberate state policy, military experience, and the entrepreneurial transformation of security knowledge into global business ventures. Driven by continuous exposure to hybrid warfare and sophisticated cyber threats, Israel has developed one of the most comprehensive and adaptive cybersecurity ecosystems in the world.

The foundation of Israel's cyber leadership lies in the Israel Defense Forces (IDF) and, in particular, Unit 2800, the elite military intelligence division responsible for signals intelligence, cyber operations, and data analytics. Veterans of this unit often transition directly into the private sector, where they establish or join startups that apply their defence-honed skills to commercial and security applications. Companies such as Check Point Software Technologies, NSO Group, and Cyber reason have become emblematic of this dynamic, transforming Israel into global hub for digital defence and cyber intelligence innovation.

Check point, for instance, was one of the first companies to develop a commercial firewall in the 1990s, a global benchmark for corporate cybersecurity. NSO Group, though controversial, exemplifies how Israel's technical expertise extends into the realms of cyber-intelligence and technologies. Similarly, Cyber reason, founded by former Unit 8200 members, focuses on proactive threat hunting and artificial intelligence-based defence systems. Together, these firms underscore how Israel's cybersecurity industry evolved from military necessity into a powerful economic and diplomatic asset.

Central to this success is government coordination through the Directorate of Defense Research and Development and the National Cyber Directorate, both of which ensure that innovations align with national security objectives. These bodies provide regulatory oversight, funding, and access to testing environments while fostering cooperation between defence startups and established institutions such as Israel Aerospace Industries (IAI) and Systems. DDR&D's role is especially important in promoting dual-use technologies—tools that serve both civilian and military markets—allowing Israeli firms to maintain profitability and strategic value simultaneously. This approach also accelerates innovation, as civilian demand for cybersecurity solutions feeds directly into the military's technological advancement.

Another defining characteristic of Israel's cybersecurity modes is extensive network of international partnerships. Israel collaborates closely with the United States, NATO, and numerous allied states through joint research programs, intelligence-sharing agreements, and bilateral technology exchanges. For example, the U.S.-Israel Cybersecurity Cooperation Program facilitates joint ventures in areas such as artificial intelligence, critical infrastructure protection, and data encryption. Similarly, partnerships with NATO's Cooperative Cyber Defence Centre of Excel-

lence (CCDCOE)⁷ enable Israeli companies to integrate into transnational security frameworks, strengthening both global defence resilience and Israel's strategic diplomacy. These international collaborations not only Israel's operational readiness but also reinforce its position as a trusted exporter of cybersecurity solutions. According to Calcalistech,⁸ Israel accounts for nearly 10% of global private cybersecurity investment, an extraordinary figure given its population size. This economic dimension has elevated cybersecurity to a pillar of Israel's foreign policy, where technology diplomacy-built around digital security, innovation, and counterterrorism-plays a central role in strengthening bilateral relations with countries across Europe, Asia, and North America.

Furthermore, the Israeli cybersecurity model contributes to global stability by promoting innovation ecosystems beyond its borders. Though training programs, consultancy, and technology transfers, Israeli experts assist partner nations in building local cyber-defence capacities. This not only expands market opportunities for Israeli companies but also positions the nation as a strategic partner in the fight against global cyber crime and digital terrorism. In essence, Israel's leadership in cybersecurity is the culmination of an ecosystem where military expertise, government coordination, and entrepreneurial vision intersect. By converting national security challenges into commercial strengths, Israel has demonstrated how small states can leverage innovation to exert disproportionate global influence. Its cybersecurity sector not only safeguards the nation from constant digital threats but also fuels economic growth, strengthens alliances, and contributes to the security of the international community.

Thus Israel's model exemplifies how strategic partnerships, military experience, and technological entrepreneurship can jointly redefine modern security paradigms-turning defence innovation into a driver of both national resilience and global cooperation.⁹

Ethical and Political Dimensions

While Israel's defence innovations have solidified its status as a global technological powerhouse, they have also generated significant ethical, political, and legal debates. The rapid expansion of military technologies-especially in the fields of surveillance ,cyber-intelligence, and autonomous systems-has blurred the boundaries between national security imperatives and ethical accountability has become one of the most pressing issues facing Israel's defence industry in the 21st century. A prominent example of this ethical complexity is the Pegasus spyware, developed by NSO Group, one of Israel's leading cyber-intelligence firms. Originally marketed as a tool to assist governments in terrorism and organized crime, Pegasus became the subject of global controversy after investigations revealed that it had been allegedly used by certain regimes to monitor journalists, and political opponents. These revelations sparked international condemnation and raised fundamental questions about Israel's role as both a technological innovator and an exporter of surveillance tools. The case illustrates the dual nature of Israel's defence innovations-technologies designed for protection can, if misused, undermine privacy, freedom of expression, and democratic accountability.

⁷ Israeli Cybersecurity is Defining the Future in 2025, <https://surl.li/vtoyup>, Accessed 04.11.2025

⁸ Sean Cordey, „Trend Analysis, The Israeli Unit 8200 An OSINT-based study“, . (2019), <https://surl.li/alhdww>, Accessed 04.11.2025

⁹ Ibid. Sean Cordey .

In response to such controversies, the Israeli government has taken steps to strengthen regulatory oversight and export control mechanisms.¹⁰ The Ministry of Defense's Defense Export Control Agency (DECA) oversees the licensing process for all military and dual-use technologies, ensuring compliance with both domestic law and international treaties. Export permits are reviewed based on national security interests, diplomatic considerations, and human rights implications. However, as analysts have noted, enforcement remains challenging, particularly given the speed of technological development and the global demand for advanced cyber tools. The balance between maintaining Israel's competitive advantage in the defence sector and adhering to international ethical norms continues to be a delicate and evolving process.

Another ethical dimension arises from the dual-use nature of many Israeli innovations. Technologies initially designed for military or intelligence purposes—such as data analytics, artificial intelligence for military recognition—often transition into civilian markets with minimal modification. While this dual-use model enhances Israel's economic growth and global competitiveness, it also raises serious concerns about data privacy, surveillance in civilian spaces, and potential misuse by private entities. The lack of global consensus on how to regulate such technologies complicates Israel's efforts to ensure responsible innovation. Consequently, scholars and policy makers have called for a clearer ethical framework that would impose stricter standards on the export and civilian application of sensitive technologies.

Beyond the ethical sphere, Israel's defence innovation industry also carries political implications. On one hand, its technological success has become a cornerstone of Israel's diplomatic strategy, strengthening alliances with key partners such as the United States, India, and various European nations. Defence technology exports contribute to soft power, as countries that rely on Israeli systems often deepen political and security cooperation. On the other hand, these same exports sometimes generate political friction—particularly when Israeli technologies are sold to governments accused of human rights abuses. Such transactions can undermine Israel's global image and provoke criticism from international watchdogs and human rights organizations.

The Israeli government, recognizing these challenges, has sought to navigate this complex landscape through strategic diplomacy and policy refinement. For instance, Israel has participated in international discussions regarding arms control and digital ethics, emphasizing the importance of technological transparency and accountability. Within domestic policy, greater emphasis has been placed on ethical innovation, including training programs for defence engineers and entrepreneurs that address responsible technology design and deployment. These initiatives reflect a growing awareness within Israel's scientific and defence communities that technological leadership must be accompanied by moral responsibility.

Ultimately, the ethical and political dimensions of Israel's defence innovation highlight a broader paradox: the very qualities that make Israel a leader in security technology—speed, creativity, and adaptability—also create the potential for misuse if left unchecked. The ongoing challenge lies in establishing a sustainable equilibrium between innovation and accountability, ensuring that technological progress serves both national and global interests.

¹⁰ Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, <https://surl.li/rmnpdy>, Accessed 04.11.2025

Israel's experience demonstrates that technological leadership in defence cannot be divorced from questions of ethics and governance. As the boundaries between military and civilian technology continue to blur, Israel's ability to integrate ethical considerations into its innovation model will determine not only its global reputation but also the long term legitimacy of its security strategy.

Conclusion

Israel's defence innovation ecosystem stands as one of the most compelling examples of how a nation can transform enduring security challenges into drivers of technological excellence. Though the deliberate integration of military expertise, startup creativity, and governments coordination, Israel has successfully redefined the boundaries of modern defence strategy. What began as a response to existential threats has evolved into a sophisticated, innovation-driven model that sustains both national security and global technological leadership.

At the core of Israel's success lies its ability to bridge institutional divides between the armed forces, the Directorate of Defense Research and Development (DDR&D), and the laboratories or within elite military-such as the Israel Defense Forces' Unit 8200-can rapidly transition into deployable technologies. Systems such as the Iron Dome, autonomous drones, and advanced cyber-defence networks illustrate how Israel has harnessed innovation not merely as a tool of protection, but as a strategic instrument of deterrence and influence. The synergy between state-owned companies like Rafael Advanced Defense Systems and a thriving startup ecosystem has allowed the country to remain at the cutting edge of military technology while sustaining economic growth and global competitiveness.

Moreover, Israel's innovation model demonstrates that strategic agility and technological foresight can offset limitations in geography and population size. By fostering a culture that prizes adaptability and interdisciplinary collaboration, Israel has achieved a qualitative military edge over its adversaries and become a trusted defence partner to many nations. International collaborations-with the United States, NATO, and range of allied states- have further reinforced its global influence, transforming technological exchange into diplomatic capital. In this sense, Israel's defence innovation is as much a foreign policy instrument as it is a national security necessity.

However, Israel's leadership in defence technology also underscores the importance of ethical governance in innovation.¹¹ As seen in the debates surrounding dual-use technologies and surveillance systems such as Pegasus, technological power must be tempered with responsibility. Israel's ongoing efforts to refine its export regulations, strengthen oversight mechanisms, and participate in global ethical dialogues reflect a recognition that innovation without accountability can erode both moral legitimacy and strategic trust. This dual commitment-to innovation and to restraint-has become a defining feature of Israel's evolving defence identity.

The Israeli experience provides a valuable model for other nations seeking to leverage innovation for security and resilience. It shows that national defence need not be isolated from entrepreneurship; rather, when aligned under coherent strategy and guided by ethical principles, technological ecosystems can enhance not only military readiness but also socio-economic development.

11 „Amid NSO scandal, over 3,600 export licenses revoked in the past year“, <https://www.jpost.com/israel-news/article-695084>, Accessed 04.11.2025

Countries facing complex security environments can draw lessons from Israel's approach-particularly the emphasis on collaboration, education, and investment in research infrastructure.

In essence, Israel's defence innovation story is one of transformation through necessity. By converting continuous security pressures into opportunities for discovery and advancement, Israel has built an enduring legacy of technological leadership. Its model underscores that the most powerful defence lies not only in weapons or systems, but in the nation's ability to think creatively, act collaboratively, and innovate responsibly.

Bibliography

- „IDF Powers Israel's Tech Miracle“, Website: The Times of Israel, <https://surl.li/kbhaea>, Accessed 04.11.2025
- The Dynamic Landscape of Israel's Defense Tech Ecosystem, July 31, 2024, Website: <https://surl.li/apcvvo>, Accessed 04.11.2025
- Nissim Hania, „Transformations in the Israeli Defense Development and Production System, and the Contemporary Relevance“, Website: <https://surl.li/vjclxf>, Accessed 04.11.2025
- „Israel Science & Technology: Defense Industry,“ Jewish Virtual Library, Website: <https://surl.li/drsqxq>, Accessed 04.11.2025
- Development of Defense and Civilian Technologies, Website: <https://surl.li/prgcav>, Accessed 04.11.2025
- “War is good for business”: Israeli startups going global after key role in Gaza“, The Times of Israel, Website: <https://surl.li/foomjy>, Accessed 04.11.2025
- Israeli Cybersecurity is Defining the Future in 2025, <https://surl.li/vtoyup>, Accessed 04.11.2025
- Sean Cordey, „Trend Analysis, The Israeli Unit 8200 An OSINT-based study“, . (2019), <https://surl.li/alhdww>, Accessed 04.11.2025
- Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, <https://surl.li/rmnpdy>, Accessed 04.11.2025
- „Amid NSO scandal, over 3,600 export licenses revoked in the past year“, <https://www.jpost.com/israel-news/article-695084>, Accessed 04.11.2025

BEYOND THE ALLIANCE: NON-NATO CONTRIBUTIONS AND THE COMPLEXITY OF THE AFGHAN WAR

Iuri Khurtsidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Teimuraz Targamadze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Sophiko Metreveli

Assistant Professor of Bachelor's Program in Defense and security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The NATO-led intervention in Afghanistan (2001–2021) constitutes a defining case of modern coalition warfare, illuminating the strategic and operational centrality of partnerships with non-NATO allies. Initiated in the immediate aftermath of the September 11 attacks and enabled by the unprecedented invocation of Article 5 of the Washington Treaty, the mission demanded multinational coordination at scale, ultimately involving more than forty contributing states under a unified but evolving command. Adopting a neorealist analytical lens, this study foregrounds the logic of burden sharing, operational necessity, and reciprocal political gains as the core drivers of coalition cohesion over two decades of counterinsurgency and stabilization operations. Non-NATO partners furnished indispensable capabilities—notably in logistics, force generation, niche enablers, and specialized operations—that expanded NATO's endurance and tactical flexibility. Their participation enhanced mission legitimacy, accelerated interoperability through common standards and joint exercises, and strengthened global security networks by knitting together diverse militaries in shared planning and execution. For partner states, the campaign yielded political recognition, combat-relevant experience, and pathways to defense modernization, creating durable ties to Euro-Atlantic institutions without formal alliance entry.

The Afghanistan case demonstrates that contemporary collective security increasingly hinges not solely on formal membership boundaries but on pragmatic, interest-aligned cooperation among heterogeneous actors willing to contribute usable power. It further shows that flexible and adaptive partnership architectures—capable of integrating varying national caveats, capabilities, and timelines—are essential to sustaining long-duration global security operations in the twenty-first century.

Keywords: NATO; Afghanistan; Coalition Warfare; Non-NATO Partners; Article 5; Neorealism; Burden Sharing; Interoperability; Counterinsurgency; Logistics; Force Generation; Mission Legitimacy; Defense Modernization; Global Security Networks; Partnership Architectures; Stabilization Operations.

Introduction

The intervention in Afghanistan (2001-2021) represented one of the most difficult and transformative missions in the history of NATO. The first collective defense response by Alliance, which united members states and partners in a joint effort to fight terrorism and rebuild Afghanistan, was marked invocation of Article 5 of the Washington Treaty¹ following the terrorist attack on September 11, 2001. This operation, the largest ever conducted by NATO, was as much a strategic dilemma as an opportunity, forcing the alliance to rethink its institutional structure and its role in the world. NATO's members and partners worked together on the design and implementation of new defense strategies, technologies, and coordination mechanisms during the Afghan campaign. The Afghanistan experience illustrated that defense innovation is not merely about advanced weapon systems or digital transformation - it is equally about building trust, interoperability and shared responsibility among diverse international actors. The partnership between NATO and its non-member allies during this mission stands as a defining example of how international cooperation can evolve to meet the demands of a rapidly changing global order. Military integration of forces over 40 different countries was required, which implied interoperability in intelligence sharing, logistics, communication systems and command structures. Additionally, it led to the development innovative counterinsurgency tactics and to the use of emerging technologies, thus refining the whole process of planning and execution of multinational operations. Through these experiences, NATO continues to redefine what collective security means in the 21st century.

Main Part

The Neorealist Imperative: Burden Sharing and the Strategic Necessity of Non-NATO Allies

The military intervention in Afghanistan, spanning nearly two decades from 2001 to 2021, represents a defining geopolitical event that necessitates an analytical framework transcending the established norms of alliance politics. From a neorealist perspective, which posits that state behavior is primarily driven by the pursuit of security and the mitigation of threats within an anarchic international system, the expansion of the coalition to include dozens of non-NATO members was not an act of mere political solidarity, but a strategic imperative. The threat emanating from Al-Qaeda and the Taliban was perceived as global, but the operational costs, human resource demands, and political risks of a prolonged counter-insurgency mission could not be sustainably borne by the Alliance's core members alone. The sheer requirement for military and financial sustainability led to the pragmatic execution of burden shifting. Core NATO states, predominantly the United States, sought to distribute the immense operational liability to optimize the collective security outcome while simultaneously managing domestic political and economic constraints. For the numerous participating non-NATO nations ranging from those aspiring to future NATO membership to those with distinct regional security interests their contribution was a form of internal balancing. Nations like Georgia and Ukraine viewed their deep engagement within the Partnership for Peace framework in Afghanistan as a vital investment. By demonstrating exceptional military

¹ Article 5 of the Washington Treaty – a rule that says if one NATO member is attacked, all members must treat it as an attack on all.

capability and compatibility (interoperability) with Western forces in a high-intensity combat environment, they solidified their political and security ties with the Alliance, effectively balancing against external regional pressures.

Beyond the political calculus of aspiring members, the participation of countries across the globe was crucial for geopolitical necessity and operational viability. When the primary supply route through Pakistan (the Pakistan Ground Lines of Communication, PAKGLOC) became increasingly unstable and unreliable, the strategic center of gravity shifted. This necessitated the creation of the Northern Distribution Network (NDN) a massive logistical achievement connecting Baltic and Black Sea ports to Afghanistan via road and rail through the non-NATO states of Central Asia, including Uzbekistan, Kazakhstan, and Azerbaijan. These transit agreements with non-NATO countries provided a critical, often life-saving, logistical redundancy. The seamless movement of non-lethal supplies, fuel, and equipment through these territories was strategically indispensable to sustaining over 100,000 coalition troops, underscoring that the mission's very feasibility hinged upon cooperation far beyond the Alliance.

Furthermore, the broad coalition bolstered the mission's international legitimacy. By incorporating forces from partners such as Australia, New Zealand, South Korea, and Jordan, the mission was transformed from a purely Euro-Atlantic endeavor into a truly global commitment under the mandate of the United Nations Security Council. This diverse representation mitigated criticism that the conflict was merely a Western occupation, strengthening the legal and political foundation for the years of stabilization and reconstruction efforts. Each non-NATO partner, in accordance with the formalized Individual Partnership Action Plans (IPAP) or tailored agreements, brought unique capabilities from specialized counter-IED teams² and intelligence analysts to critical medical and engineering support into the unified command structures of ISAF³ and the successor Resolute Support Mission. Thus, the enduring legacy of the Afghan war is not simply a narrative of NATO's commitment, but a profound illustration of how contemporary collective security, rooted in neorealist calculations, demands the pragmatic, strategic alignment of interests among a broad and diverse coalition of allies willing to share the military, financial, and political burden.

Operational Pillars: The Critical Contributions of Non-NATO Allies in Logistics and Force Generation

In the contemporary security landscape, the operational success of multinational coalitions relies heavily on the structural and logistical foundations provided by non-NATO allies. From a neorealist standpoint, the inclusion of external partners within NATO-led operations is not a matter of political symbolism but a functional necessity rooted in the dynamics of power distribution and strategic efficiency. As global threats grow increasingly asymmetric — from hybrid warfare to large-scale humanitarian crises — the Alliance's capacity to project power, sustain operations, and ensure force mobility depends on the collaborative integration of partner nations possessing critical logistical networks, regional access, and deployable capabilities. Logistics, often the least visible yet most decisive element of warfare, has become the domain in which non-NATO partners

² Counter-IED teams – military units specialized in detecting and disabling explosive devices.

³ International Security Assistance Force (ISAF) – NATO-led mission in Afghanistan before 2015.

demonstrate their indispensable strategic value. During major coalition operations, including those in Afghanistan, Iraq, and the Balkans, countries such as Azerbaijan, Kazakhstan, and Jordan provided essential transit corridors, airspace access, and logistical staging areas that allowed NATO to maintain uninterrupted operational flow. Their participation was not merely supportive but constitutive — a foundational element enabling sustained force generation and supply chain integrity. The ability to mobilize, sustain, and rotate forces across vast operational theaters depended on a complex web of bilateral and multilateral agreements, many of which were negotiated with these non-member states under frameworks like the Partnership for Peace (PfP) and the Istanbul Cooperation Initiative (ICI).

The force generation process further highlights the strategic indispensability of non-NATO allies. Partner nations such as Georgia, Ukraine, and Australia consistently contributed highly capable and interoperable military contingents, often deploying specialized units that enhanced NATO's operational flexibility. These contributions were a form of strategic exchange: non-members gained invaluable combat experience, technological interoperability, and political visibility, while NATO secured the manpower and expertise necessary for mission sustainability. The integration of such forces not only expanded the coalition's operational depth but also fostered a culture of shared responsibility that transcended formal membership boundaries. Moreover, the geopolitical placement of non-NATO partners enhanced the Alliance's strategic reach. Access to ports, airfields, and logistical infrastructure in the Black Sea, Central Asia, and the Middle East significantly reduced operational vulnerabilities and increased redundancy within NATO's global logistics architecture. These arrangements effectively transformed regions traditionally considered peripheries into operational hubs of strategic consequence. In turn, they reinforced the principle that modern collective defense — in both combat and crisis response operations — cannot be sustained without extensive cooperation beyond treaty lines. Ultimately, the contributions of non-NATO allies in logistics and force generation represent one of the most critical operational pillars of contemporary security architecture. Their involvement extends beyond tactical assistance, shaping the very feasibility of sustained multinational engagement. In a neorealist sense, these partnerships are born not of altruism but of mutual strategic necessity — a convergence of interests where collective capability becomes the currency of survival and influence. The enduring lesson is clear: the strength and endurance of NATO-led operations are inseparable from the pragmatic, structured, and strategically balanced cooperation of its non-member allies.

The Politics of Partnership: Assessing the Reciprocal Gains in the Afghanistan Coalition

The Afghanistan intervention stands as a critical case study in understanding the reciprocal nature of coalition politics, where strategic necessity intersected with political opportunity for both NATO and its non-member partners. While the mission was primarily orchestrated under NATO's command structure, its execution and sustainability were profoundly dependent on a broad network of international contributors whose participation extended well beyond traditional alliance boundaries. From a political and strategic perspective, this partnership dynamic was underpinned

by a mutual calculus of benefit — NATO sought to diffuse the immense operational, financial, and political burden of a long-term counterinsurgency, while partner nations aimed to accrue political capital, institutional experience, and international legitimacy through visible commitment to a globally sanctioned mission. For NATO, the incorporation of non-member states such as Australia, Georgia, Jordan, and South Korea provided more than numerical reinforcement; it symbolized a transformation of the Alliance from a regional defense pact into a global security actor. The inclusion of diverse partners under frameworks like the International Security Assistance Force (ISAF) and later the Resolute Support Mission (RSM) enhanced the coalition's political legitimacy and broadened its strategic flexibility. The visible multinational character of the force helped counter accusations of Western unilateralism, framing the mission as a collective response to international terrorism under the auspices of the United Nations. Simultaneously, the diverse operational contributions — ranging from combat units to medical, engineering, and intelligence support — improved the mission's effectiveness and sustainability, showcasing the functional utility of cooperative security beyond formal alliance membership.

For non-NATO contributors, the gains were equally significant, though differently structured. Countries aspiring to NATO membership or deeper Euro-Atlantic integration, such as Georgia and Ukraine, viewed their participation as an investment in political credibility and strategic recognition. Their consistent deployment of troops to high-risk regions, often without caveats restricting engagement, demonstrated both commitment and capability, reinforcing their status as reliable partners. For others — including Australia, Jordan, and the United Arab Emirates — participation served as a means of consolidating bilateral defense relations with the United States and key European powers, diversifying their strategic portfolios while gaining access to advanced training, equipment, and operational interoperability. In this sense, the Afghanistan coalition functioned as a marketplace of security cooperation, where political influence and defense integration were exchanged through demonstrated operational contribution. This reciprocal framework also extended to institutional learning and doctrinal innovation. Joint operations within Afghanistan fostered a deeper level of interoperability between NATO forces and partner militaries, influencing modernization trajectories and shaping the defense doctrines of numerous non-member states. The exchange of intelligence practices, logistics coordination, and command integration contributed to the diffusion of NATO's operational standards, thereby expanding its normative and procedural influence across regions far beyond its formal jurisdiction. For NATO, this process strengthened the global reach of its security ecosystem; for partners, it accelerated their military transformation and enhanced their strategic relevance within the broader international order.⁴ Ultimately, the politics of partnership within the Afghanistan coalition embodied a symbiotic relationship grounded in both pragmatism and ambition. NATO leveraged these partnerships to project power, legitimize operations, and share burdens, while non-member states utilized their involvement to gain prestige, security assurances, and tangible military advancement. This mutual reinforcement underscores a fundamental evolution in collective security: in the 21st century, power and legitimacy in warfare are no longer derived solely from formal alliances but from flexible, interest-driven partnerships that redefine the boundaries of cooperation and reshape the architecture of global stability.

4 „Multilateral peace operations in Afghanistan between 2001 and 2021“ <https://surl.lu/kkivhf>, Accessed 04.11.2025.

Conclusion

The Strategic Synthesis of Partnership and Power in Contemporary Coalition Warfare

The cumulative analysis of the preceding chapters reveals a profound transformation in the logic of collective security and alliance behavior within the 21st century. The Afghanistan campaign, as both a crucible and a catalyst of modern coalition warfare, demonstrated that the boundaries of NATO's operational and strategic influence extend far beyond its formal membership. From the neorealist imperatives⁵ of burden sharing, through the logistical and force generation foundations of non-member contributions, to the intricate political dynamics of reciprocal partnership, a clear pattern emerges — one that underscores the evolution of global security cooperation from exclusivity toward pragmatic interdependence. At its core, this transformation reflects a fundamental redefinition of power in the international system. No longer confined to rigid alliance structures, effective power projection and operational sustainability now depend on the ability to build adaptable, interest-based networks capable of mobilizing diverse actors under a unified strategic vision. Non-NATO allies — whether aspirants like Georgia and Ukraine, strategic partners such as Australia and Jordan, or logistical enablers across Central Asia — collectively formed the connective tissue that sustained the Afghanistan mission. Their roles embodied the operational and political pillars that transformed the campaign from a NATO endeavor into a global enterprise of shared risk and distributed responsibility. The reciprocal gains derived from this partnership framework highlight a deeper strategic symbiosis. For NATO, the inclusion of external partners mitigated resource constraints, enhanced legitimacy, and expanded operational reach. For non-member states, participation served as a pathway to international recognition, defense modernization, and strengthened political alignment with the West. This dual benefit underscores the enduring relevance of neorealist logic — where cooperation arises not from idealism, but from converging interests shaped by necessity and opportunity within an anarchic system⁶.

Ultimately, the Afghanistan experience stands as both a testament and a warning. It affirms that future coalition warfare and crisis management will rely on flexible architectures of cooperation that integrate state and non-state actors across multiple regions and domains. Yet it also cautions that such interdependence demands constant political maintenance, equitable burden sharing, and strategic clarity. The lessons drawn from the contributions of non-NATO allies reveal that the strength of any alliance is no longer measured by its membership list, but by its capacity to forge enduring, adaptive partnerships that can withstand the tests of distance, duration, and divergence. In this sense, the legacy of the Afghanistan coalition is not merely historical — it is foundational to the evolving architecture of global security in the decades to come.

⁵ Neorealist imperatives – essential actions or requirements according to neorealist theory in international relations (focus on security and self-interest).

⁶ Anarchic system – a world system without a central governing authority; countries look after their own interests.

Bibliography

Article 5 of the Washington Treaty – a rule that says if one NATO member is attacked, all members must treat it as an attack on all.

Counter-IED teams – military units specialized in detecting and disabling explosive devices.

International Security Assistance Force (ISAF) – NATO-led mission in Afghanistan before 2015.

„Multilateral peace operations in Afghanistan between 2001 and 2021“ <https://surl.lu/kkivhf>, Accessed 04.11.2025.

Neorealist imperatives – essential actions or requirements according to neorealist theory in international relations (focus on security and self-interest).

Anarchic system – a world system without a central governing authority; countries look after their own interests.

INTERNATIONAL SPACE PARTNERSHIP: BUILDING A NEW ARCHITECTURE FOR SECURITY

Tato Machcrashvili

The Junker of a Bachelor's Degree Program (Defense and security)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Davit Mikeladze

The Junker of a Bachelor's Degree Program (Defense and security)
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

In the post–Cold War era, the dissolution of the Soviet Union reshaped the global security landscape and redefined outer space as a strategic domain of political, military, and technological significance. Initially dominated by the United States, this sphere has evolved into a complex environment shaped by rapid technological innovation, the ambitions of emerging powers, and the growing influence of commercial actors. As a result, outer space has become both a platform for cooperation and a potential arena of conflict. Recent developments, particularly the expansion of Chinese and Indian space programs, have intensified competition and exposed the limitations of unilateral approaches to security. In response, new frameworks—such as the Artemis Accords, Combined Space Operations (CSpO), and Low Earth Orbit (LEO) commercial initiatives—have emerged to promote collective responsibility, transparency, and technological integration. These models demonstrate how collaboration can mitigate militarization risks, enhance stability, and balance strategic and commercial interests.

This article examines how international space partnerships can contribute to a collective security architecture ensuring the peaceful use of outer space. It analyzes the historical and geopolitical factors that brought space onto the international security agenda, evaluates current cooperation models, and assesses their potential to reduce military tensions. The study concludes that sustaining global stability in outer space requires multilateral diplomacy, confidence-building measures, and transparent governance to preserve this domain as a shared resource for all humankind.

Keywords: Outer space security; international cooperation; Artemis Accords; Combined Space Operations (CSpO); Low Earth Orbit (LEO); militarization; global governance; transparency; confidence-building measures (TCBMs).

Introduction

Following the end of the Cold War, the dissolution of the Soviet Union transformed the global paradigm of international security and turned outer space into a new and increasingly strategic domain. The United States remained the sole superpower, exerting influence in this sphere through its military and scientific superiority. However, amid rapid technological progress, the growing ambitions of emerging states, and the intensification of commercial interests, outer space has quickly become a central arena of geopolitical competition, military strategy, and international cooperation.

In recent years, countries such as China and India have become particularly active in developing space programs, posing new challenges to global security structures and highlighting the need for new forms of international partnership. Nations around the world are gradually recognizing that ensuring the peaceful and stable use of outer space cannot be achieved through unilateral efforts alone. Consequently, international space partnerships such as the Artemis Accords, Combined Space Operations (CSpO), and Low Earth Orbit (LEO) commercial initiatives represent emerging models grounded in collective responsibility, transparency, technological integration, and political trust. Through such cooperation, it becomes possible to reduce military tensions in space, strengthen global stability, and balance commercial interests with military strategies. The aim of this paper is to explore how international space partnerships can contribute to the creation of a new, collective responsibility-based security architecture that ensures the peaceful use of space and mitigates military tensions. To achieve this goal, three main objectives are outlined. First, to analyze the historical and geopolitical factors that brought space into the security agenda, including the Cold War period, the evolution of international law, and the military significance of satellites.

Second, to examine existing models of international partnership, such as the Artemis Accords, CSpO, and LEO commercial initiatives, and to assess their impact on space stability. Finally, to evaluate how such cooperation can contribute to the creation of a new global security architecture and reduce military confrontation, envisioning, in the long term, the potential for space cooperation to serve as an alternative to military rivalry. This study, therefore, seeks to address the following research questions:

1. What factors have brought space into the political agenda of international security?
2. How does the International Space Partnership contribute to the strengthening of global stability?
3. To what extent can space cooperation become a long-term alternative to military confrontation?

Main Part

What Factors Contributed to the Inclusion of Space Security in the Political Agenda?

Historically perceived as a realm of peaceful cooperation and scientific exploration, outer space has, since the mid-twentieth century and particularly following the onset of the Cold War,

transformed into a critical platform for global security and a central arena of strategic competition. This transformation is multidimensional, driven by historical experience, technological evolution, and contemporary geopolitical dynamics that have collectively brought space security to the forefront of the international political agenda.

The primary historical determinant in the politicization of space security was the strategic confrontation between the United States and the Soviet Union during the Cold War. The launch of Sputnik in 1957 marked the beginning of the space race, a symbol not only of technological superiority but also of military power projection¹. The development of intercontinental ballistic missiles (ICBMs), which relied on space trajectories, integrated outer space into global defense systems². During this period, the testing and development of anti-satellite (ASAT) systems directly affected strategic stability, giving rise to the first concerns about the Kessler Syndrome, the critical accumulation of space debris, thus adding a physical dimension to security threats. This context necessitated the establishment of international legal frameworks, leading to the adoption of the 1967 Outer Space Treaty (OST).³

In the twenty-first century, technological progress has played a decisive role in increasing the critical importance of space infrastructure. Satellites now constitute the backbone of global communication, navigation (GNSS), weather forecasting, and intelligence. Their potential damage or destruction could have catastrophic consequences across military, civil, and economic sectors. Furthermore, the growing digital dependence of satellites and ground stations introduces new vulnerabilities to cyberattacks. The technological dimension also encompasses the challenge of managing space debris, emphasizing the need for international cooperation mechanisms and enhanced Space Situational Awareness (SSA).

The modern geopolitical environment, characterized by the participation of both state and private actors, has further accelerated the prominence of space security. Alongside traditional space powers such as the United States and Russia, the growing engagement of new space actors like China and India, coupled with the unresolved status of Prevention of an Arms Race in Outer Space (PAROS) negotiations, contributes to a sense of strategic insecurity. Additionally, the commercialization of space (the New Space Era) and the provision of critical services by private entities such as Starlink during the war in Ukraine raise complex questions about the division of security responsibilities between public and private sectors.⁴ The potential destruction or disruption of space assets has thus become an immediate factor of conflict escalation.

In conclusion, the integration of space security into the political agenda is an inevitable outcome of political and technological synthesis. This process is shaped by Cold War–era strategic rivalry, critical technological dependence, and the commercialization of global interests. Ensuring the stability and sustainability of outer space requires active implementation of multilateral diplomacy, transparency, and confidence-building measures (TCBMs) to minimize strategic competition risks and preserve space as a domain beneficial to all humankind.

1 B. E. Bowen, *War in Space: Strategy, Spacepower, and Geopolitics*. Edinburgh: Edinburgh University Press. (2020).

2 Center for Strategic and International Studies (CSIS). (2023). *Space Threat Assessment*. Washington, DC: CSIS.

3 NASA, *Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids*. . (2020).

4 Secure World Foundation. *Global Counterspace Capabilities: An Open Source Assessment*. Boulder, CO: SWF. (2024).

How Does International Space Partnership Contribute to Global Stability?

In the twenty-first century, international space partnerships play a decisive role in strengthening global stability. Cooperation in outer space promotes a peaceful and sustainable operational environment, an imperative amid growing technological competition and geopolitical fragmentation. Three key initiatives stand out in this context: the Artemis Accords, the Combined Space Operations (CSpO) Vision 2031, and Low Earth Orbit (LEO) commercial initiatives. Together, they establish a multidimensional model of global space governance.

The Artemis Accords, initiated by the United States, constitute a non-binding international framework that defines standards for the civilian exploration and utilization of the Moon, Mars, and other celestial bodies.⁵ Its principal contribution to global stability lies in bringing legal clarity to the emerging frontiers of space. The Accords are firmly rooted in the principles of the 1967 Outer Space Treaty but operationalize them through mechanisms such as transparency of operations and information sharing essential for reducing misunderstandings and reinforcing trust. Furthermore, the Accords outline frameworks for the extraction and utilization of space resources, ensuring that emerging economic interests, which could otherwise become sources of conflict, are regulated within international law, thus upholding the principle of non-appropriation and fostering a predictable environment for investment.

The CSpO Vision 2031, in turn, reinforces global stability through its defensive and operational dimensions. This initiative, comprising seven allied nations, focuses on enhancing security, sustainability, and interoperability in space operations. Its core function lies in providing joint space situational awareness (SSA), allowing allies to detect and interpret threats such as ASAT tests or cyber intrusions. These collective capabilities contribute to deterrence by ensuring that any hostile action in space would target not a single state, but an entire alliance, thereby lowering the risk of conflict escalation.

Finally, LEO commercial initiatives, encompassing private-sector participation in mega-constellations and space tourism, advance global stability through innovation and economic interdependence.⁶ The dominance of private operators in Low Earth Orbit promotes rapid technological progress and reduces the risk of monopolization by individual states. Moreover, since commercial services depend on orbital sustainability, private companies collaborate actively with international agencies to establish debris management standards, ensuring the long-term safety and viability of space activities.

Thus, international space partnerships strengthen global stability in three interconnected ways:

The Artemis Accords provide a normative and legal foundation for peaceful exploration.

The CSpO Vision 2031 enhances collective operational security and deterrence.

LEO commercial initiatives foster economic resilience and infrastructural integration.

This synergy is vital to ensuring that outer space remains a domain of shared benefit rather than a new frontier of geopolitical confrontation.

⁵ United Nations Institute for Disarmament Research (UNIDIR). (2023). *Safeguarding Space Security: Prevention of an Arms Race in Outer Space*. Geneva: UNIDIR.

⁶ United Nations Office for Outer Space Affairs (UNOOSA). (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space*. Retrieved from <https://www.unoosa.org>

Can Space Cooperation Become an Alternative to Military Confrontation in the Long Term?

In the twenty-first century, international space cooperation represents a critical element in the creation of a new, multidimensional global security architecture. Its primary function is to reduce military tensions and strengthen strategic trust. Initiatives such as the Artemis Accords, CSpO Vision 2031, and LEO commercial projects collectively establish a system grounded in collective responsibility, operational transparency, and technological integration. These partnerships redefine the perception of outer space from a domain of competition and military rivalry to a key component of the global security network.

The Artemis Accords exemplify how multilateral cooperation can establish harmonized legal and operational norms. Principles such as peaceful exploration, data transparency, and technical interoperability directly reinforce trust. By adhering to common behavioral standards, signatory states reduce the risks of miscalculation and unintended conflict, making space activities more predictable.

The CSpO Vision 2031 emphasizes enhanced operational coordination for both military and civilian satellites. Its main strength lies in ensuring a high level of shared space situational awareness (SSA). Through continuous data integration among allies, suspicious or aggressive maneuvers can be rapidly identified and collectively addressed. This proactive approach bolsters deterrence: potential adversaries are less likely to engage in unilateral destabilizing behavior when facing a technologically coordinated and credible multilateral response.⁷

Meanwhile, LEO commercial partnerships enhance security by fostering financial and technological stability.⁸ The involvement of private companies providing critical services such as communication and navigation, creates a global network of economic interdependence. Any destructive action in space would therefore harm not only states but also international commercial interests, generating strong disincentives against escalation. Moreover, private actors lead the development of innovative standards for debris mitigation and orbital sustainability, thereby strengthening the operational foundation of collective security.

In the long term, international space cooperation can indeed serve as an effective alternative to military confrontation provided that high levels of trust, clearly defined legal frameworks, and deep technological integration are maintained. Continuous dialogue and collective monitoring of unilateral actions reduce the likelihood of miscalculation. A culture of collective responsibility, grounded in international norms and agreements, reinforces the principle that the peaceful, secure, and sustainable use of space is a fundamental strategic interest for all actors.

Conclusion

The integration of space security into the global political agenda arises from the convergence of historical rivalry, critical technological interdependence, and persistent geopolitical competition. In this evolving context, institutionalized frameworks of cooperation—exemplified by the Artemis

⁷ Weeden, B., & Samson, V. *Global Space Governance: Advancing Collective Security in Orbit*. Boulder, CO: Secure World Foundation. (2022).

⁸ United Nations Office for Outer Space Affairs (UNOOSA). (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space*. Retrieved from <https://www.unoosa.org>

Accords (promoting normative transparency and the peaceful use of outer space), the Combined Space Operations (CSpO) Vision 2031 (advancing collective operational security and deterrence), and Low Earth Orbit (LEO) commercial initiatives (driving techno-economic sustainability)—are collectively shaping a new architecture of global security governance. These multilateral mechanisms not only diminish the likelihood of accidental or miscalculated conflict but also enhance strategic trust, reinforce political accountability, and cultivate a culture of shared responsibility among spacefaring nations. Ultimately, the institutionalization of space cooperation emerges as a pivotal element in safeguarding long-term global stability and ensuring that outer space remains a domain of peaceful, equitable, and sustainable development.

Bibliography

- Bowen, B. E. (2020). *War in Space: Strategy, Spacepower, and Geopolitics*. Edinburgh: Edinburgh University Press.
- Center for Strategic and International Studies (CSIS). (2023). *Space Threat Assessment*. Washington, DC: CSIS.
- NASA. (2020). *Artemis Accords: Principles for Cooperation in the Civil Exploration and Use of the Moon, Mars, Comets, and Asteroids*. Retrieved from <https://www.nasa.gov/artemis-accords>
- Secure World Foundation. (2024). *Global Counterspace Capabilities: An Open Source Assessment*. Boulder, CO: SWF.
- United Nations Institute for Disarmament Research (UNIDIR). (2023). *Safeguarding Space Security: Prevention of an Arms Race in Outer Space*. Geneva: UNIDIR.
- United Nations Office for Outer Space Affairs (UNOOSA). (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space*. Retrieved from <https://www.unoosa.org>
- Weeden, B., & Samson, V. (2022). *Global Space Governance: Advancing Collective Security in Orbit*. Boulder, CO: Secure World Foundation.

THE GEOPOLITICAL ASPECTS OF SUBMARINE COMMUNICATION CABLES AS CRITICAL INFRASTRUCTURE AND THEIR IMPACT ON INTERNATIONAL SECURITY

Giorgi Khachidze

The Learner of a Master's Degree Program (State Recourse Management) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

Undersea communication cables are a key part of global infrastructure, playing a central role in the modern digital world. These cables make it possible to send and receive large volumes of data across long distances in real time. As digital technologies grow and international communication becomes more important, the role of undersea cables continues to expand. Today, they are widely recognized not only as critical infrastructure but also as strategic resources, especially by national governments.

As global tensions and military conflicts increase, keeping undersea communication cables safe has become an important concern. Any disruption to their operation whether through intentional attacks or accidental damage can lead to serious consequences for countries and global networks. These disruptions could slow or block access to digital services, damage communication systems, and interrupt the flow of information that supports business, governance, and daily life. Moreover, devices and systems connected to the global internet would also be affected, particularly those that rely on real-time data processing and sharing.

Cables are also at risk from civilian cargo ships, as well as from unauthorized access by different actors. In some cases, the damage or interference goes undetected, and it is often difficult to identify who is responsible. Repairing these cables is expensive and time-consuming, requiring advanced technology and expert teams.

This paper explores the importance of undersea cables for global and regional connectivity, with a focus on their role in supporting economic growth and digital development. It examines the national strategies of different countries and the approaches taken by companies to gain influence over cable networks. The paper also looks at how undersea cables contribute to national security and what measures are in place to protect them. Special attention is given to the regions, where recent conflicts highlight the risks to this vital infrastructure. Finally, the paper analyses future challenges related to cable security and resilience.

Keywords: Critical Infrastructure; Cyber Security; Cyber Incident; Data Transmission; Data Interception; Digital Economy; Global Connectivity; Internet Traffic; National Security; Underwater Communication Cable; Optical Fibber Cable;

Introduction

Undersea cables are the main part of the global communication network, connecting regions that are thousands of kilometres apart. By the end of 2024, there were about 600 undersea communication cables around the world. These cables vary in length, from a few hundred to several thousand kilometres.¹ Many countries consider this cable system to be important infrastructure because it carries not only every day and business data but also sensitive government information. If this information is leaked, it could be a serious risk to national security.

Today, the world depends more and more on digital infrastructure, which makes undersea communication cables very important. These cables form the main network for global communication, carrying most of the data exchanged between countries. Their strategic value has become critically important as the internet and digital technologies play a bigger role in everyday life.

With ongoing armed conflicts around the world, the importance of undersea cables in global politics is growing. Major world powers are trying to control large parts of this infrastructure to gain strategic advantages. Damage to these cables whether by accident or on purpose is happening more and more often. Sometimes, civilian ships accidentally damage fiber-optic cables, causing internet disruptions. But recent events show that targeted attacks on this undersea cables are increasing, often linked to secret operations by major global powers.

As global tensions increase, controlling undersea cable infrastructure is seen as a way to gain world power. Because of this, countries and other international actors are working hard to protect and expand their influence in this area. Cases of accidental or intentional damage to these cables are happening more often, making conflicts between major powers even stronger. Accordingly, countries are trying to develop strategies to respond to these challenges.

A key concern is the vulnerability of undersea communication cables to different threats. As the world depends more on digital communication, there has been a rise in sabotage, spying, and intentional damage to these systems. It is possible to obtain important information by damaging cables and gaining unauthorized access to them. Countries that own or control these cables often see these acts as attacks on their national sovereignty and may respond with countermeasures. These responses can lead to new conflicts and create serious risks for both national and global security.

This paper studies the geopolitical importance of undersea communication cables as critical infrastructure and their effects on international security. It highlights the main challenges that put the operation of these systems at risk. The paper also looks at the key stakeholders involved in undersea cable infrastructure and the strategic power they have, which they often use to support their national or geopolitical goals. This paper focus on the following main research questions:

- What role do undersea communication cables play in protecting national security?
- What risks and challenges happen when this infrastructure is damaged, especially for critical systems, national security, and global political stability?

This paper is based on the hypothesis that undersea communication cables are essential to the global communication system. Controlling and securing them has a major impact on international

¹ Submarine Cable Frequently Asked Questions. 2025. Tele Geography.

relations and geopolitics. Any disruption to these cables could cause serious economic, social, and security consequences.

This study explores these research questions to highlight the growing importance of undersea cable infrastructure in the digital age and to understand its role from the perspective of political realism. To address the research question, academic literature and research reports were reviewed. The main structure of the paper was developed based on the analysis of existing theoretical frameworks.

As global information technology continues to grow, there is an increasing need for scientific research to create new knowledge about modern technologies. The complexity of digital systems requires to study the main factors behind technological change and the special features of related infrastructures. Many leading research centres have published important studies about threats to communication infrastructure. This paper builds on these international practices and focuses on different academic work that looks at the challenges and future development of undersea communication cables from different viewpoints.

In their work “Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition” Daniel Runde, Erin Murphy, and Thomas Bryja emphasize the important role of undersea cables in global communication. They point out that, as global competition grows, these cables are becoming more common targets for sabotage, cyber-attacks, and physical damage. The authors argue that because this infrastructure is so important, it must be protected from both cyber and physical threats and kept running smoothly through international cooperation.

In his study “Cyber Defence on the Ocean Floor: The Geopolitics of Submarine Cable Security” Justin Sherman explores why securing undersea cables matters politically. He highlights how important global communication infrastructure is and notes that cyber and physical attacks on these cables are happening more often, especially in areas with high political tension. Sherman explains that these attacks can seriously disrupt global data flow and threaten the smooth working of information systems in both government and business.

Nicole Starosielski, in her article “How Can We Protect the Internet’s Undersea Cables?” Shows the vital importance of submarine cables in global data and communication networks. She points out that most damage to these cables happens because of human carelessness, often from activities like shipping or coastal construction. Although sabotage is rare, these events get a lot of media attention. Starosielski also explains that while there are backup systems to change the direction of the data during problems, some key cables are so important that their failure could cause major disruptions worldwide. Therefore, she argues that protecting this infrastructure should be a top priority, with operators investing heavily in monitoring and security.

Lieutenant Madison L. Long, in the article “Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks”, studies the political and security issues related to undersea cables. Long points out that about 97% of the world’s internet traffic depends on these cables, showing how important they are. The research focuses on threats from China and Russia, which are trying to control important parts of the cable networks. These countries have been linked to unauthorized data access and possible sabotage. Long argues that western countries need to take strong actions to protect these networks and prevent data leaks.

John Arquilla, in his work “Securing the Undersea Cable Network,” discusses communication infrastructure risks caused by both human mistakes and natural disasters. He looks at past cases of cable damage, often caused by state actors. Arquilla also points out technical weaknesses in these systems that allow hostile groups to access sensitive information without permission. He emphasizes the importance of using artificial intelligence, suggesting that AI can help reduce cyber threats and make undersea cable infrastructure more resilient.

The Congressional Research Service report “Protection of Undersea Telecommunication Cables: Issues for Congress” outlines the strategic importance and vulnerability of submarine cables, which carry the majority of global internet traffic. It highlights threats from natural events, accidental damage, and deliberate sabotage, while noting challenges in monitoring and attributing such incidents. The report discusses the current legal frameworks and emphasizes the need for stronger coordination between governments, private companies and international partners. It also presents policy options for policy makers to enhance cable protection.

This research paper is important because it looks at the main political, economic, and security issues around undersea cable infrastructure. The study is based on the idea that undersea communication cables are critical for global communication. As a result, controlling and protecting them is very important for shaping global politics and the international order. It also suggests that any disruption to these cables could have serious effects on the world’s economy, digital infrastructure and security. By studying the weaknesses of these systems, the interests of major world powers and the growing competition in this area, this paper explores how digital infrastructure is becoming a key factor in global power competition.

Main Part

In international relations, the theory of political realism suggests that states act mainly based on their national interests. Each state aims to increase its influence by using power over others and may use all available means to achieve this goal. The central idea of political realism is that power plays a key role to strength the state’s identity and its ability to gain a leading position in the international system.² Current events in the world show that the main actors rely on the principle of force and try to expand their sphere of influence by pursuing their own interests.

Submarine cables are a key part of the global communication infrastructure. They carry about 95% of international data, including phone calls, financial transactions, emails, government communications and other data. Many important systems like: energy networks, hospitals, transports and logistics, financial markets depend on these cables to work properly. If cables are damaged or not working properly, this can delay services, cause system failures or even lead to financial losses. For example, banks and stock markets need fast data exchange. Data transmission errors may cause disruption to banks and stock exchanges operations, which will affect the stability of financial sector. Also hospitals and country’s essential services depend on communication during emergencies. (Runde, 2024). During an emergency, communication disruptions can endanger people’s lives, as rapid response to information received is crucial in such situations. Protecting submarine cables is now part of national security for many countries. Military forces, intelligence agencies,

² Bell, Duncan.2025. Realism. Britannica.

and emergency services all need fast and secure communication. If enemy cuts or damages a cable, it can weaken a country's defence system or delay emergency responses. In serious cases, this could allow a cyber or military attack. Because of this risk, many governments now include cable protection in their defence plans. They invest in better monitoring systems to reduce the chances of disruption.

Although governments recognize submarine cables as national security assets, most of the infrastructure is owned and managed by private companies like internet providers, cloud services and social media companies. These companies build new cables to increase internet speed, reach more areas, and earn income. This creates a challenge for states, as they must rely on cooperation with private actors to monitor and secure these critical systems. Since these cables go through the ocean and connect different countries, they are affected by international laws. As a result, governments are increasingly seeking public-private partnerships, regulatory measures and direct state investment in cable projects to reduce strategic vulnerabilities.³

One of the main challenges in dealing with these risks associated to undersea cable infrastructure is the difficulty of monitoring and identifying the source of damage. Submarine cables are located deep under the sea and span thousands of kilometres, making real-time surveillance almost impossible. When a cable is damaged, it is often unclear whether the cause was accidental or intentional. This lack of clear evidence makes it difficult for governments to respond and in some cases, may lead delayed action. The technical complexity of the infrastructure adds another layer of difficulty in managing such incidents.⁴

In a broader context, damage to submarine cables can increase geopolitical tensions. If a state believes that another country is responsible for damaging its communication infrastructure, this can be seen as a hostile act. In some cases, it might lead to diplomatic protests, sanctions or even military responses. This is especially dangerous for regions where there are already political disputes or military presence, such as Middle East or near NATO borders. As global competition over digital infrastructure grows, attacks on cables may be used as a new form of strategic pressure or hybrid warfare. Operations against the cables may be carried out under civilian cover to avoid direct involvement of the country's armed forces or intelligence services. Such operations make it even more difficult to expose the perpetrators behind the attack and hold them accountable.

Several countries recognize the importance of submarine communication cables and have taken steps to protect this strategic infrastructure. For example, the United States has increased patrols near key cable routes and invested in advanced monitoring systems to detect any suspicious activities. The UK has also focused on improving cable security by working closely with private companies and international partners to share information and respond quickly to threats. Australia has launched initiatives to map critical cable routes around its coast and strengthen cyber security measures to protect against attacks. Also other countries have been working on backup systems, including satellite communication, to ensure connectivity if submarine cables are damaged.

NATO is becoming more active in protecting important systems under the sea, such as com-

3 Sherman, Justin. 2021. *Cyber Defence Across The Ocean Floor: The Geopolitics of Submarine Cable Security*. Atlantic Council.

4 Gallagher, Jill, and Nicole Carter. 2023. *Protection of Undersea Telecommunication Cables: Issues for Congress*. Congressional Research Service.

munication cables. Organization sees the protection of this infrastructure as a security priority. In response, it has created special groups and strategies to detect threats, share information and respond quickly if cables are damaged or attacked. By working with member countries and using new technologies, NATO aims to keep these communication lines safe and secure for all users.⁵

In recent years, countries such as Russia and China have increasingly focused on submarine communication cables, viewing them not only as strategic assets but also as potential tools of influence. Russian submarines and ships, like the „Yantar“, have been seen near important undersea cable routes, especially in the North Atlantic and Arctic. These ships have special technology that could be used to tap, damage or cut cables. NATO and Western countries are concerned that Russia may use this ability to cause communication problems during a political crisis or military conflict.⁶

China has taken a different approach to submarine cable infrastructure by focusing on building and expanding global networks through state-supported companies. China, as a major player in global communications, has developed its own network of cables and invests in protecting them through both military and technological measures. Chinese firms, such as „HMN Tech“, have played a growing role in laying undersea cables across Asia, Africa, and even parts of Europe and Latin America. These projects help improve digital access in developing countries but also raise concerns about data security and political influence. Many Western governments worry that cables built or operated by Chinese companies could be used for surveillance during a political or military conflict. China views this infrastructure as part of its competition strategy and a way to increase its global technological influence.

Although there have been no confirmed attacks on submarine communication cables by non-state actors so far, the potential risks should not be ignored. Terrorist groups have previously targeted critical infrastructure and could in theory attack cables using simple methods such as underwater improvised explosive devices, especially in regions with weak security. In contrast, criminal organizations could exploit cable vulnerabilities for financial gain. Threats can also arise from natural events, such as earthquakes, tsunamis and volcanic eruptions. However, cases of damage to underwater communication cables as a result of natural disasters are extremely rare. Cables can also be damaged by marine animals such as sharks, whales and other species. So we can say that the threat does not always come from state actors alone.

To reduce these threats, many countries are working on developing backup systems, such as satellite communication. However, these solutions are costly and cannot fully replace submarine cables. International cooperation is also essential, since most cables cross multiple borders and oceans. Also, in many cases, the Multinational Corporations created to operate cables are owned by several countries, therefore their joint action to protect common interests is important. Without strong cooperation, the risk of conflict will remain high and the stability of global communication system will continue to be vulnerable. This situation highlights the need for a global framework dedicated specifically to submarine cable protection. Developing international agreements sup-

⁵ Monaghan, Sean, Otto Svedsen, Michael Darrah and Ed Arnold. 2023. NATO's Role in Protecting Critical Undersea Infrastructure. Centre for Strategic and International Studies.

⁶ Bueger, Christian, Tobias Libertrau and Jonas Franken. 2022. Security threats to undersea communications cables and infrastructure - consequences for the EU. European Parliament.

ported by joint monitoring systems and early warning mechanisms, could help prevent future conflicts and protect the stability of the global digital infrastructure.

Conclusion

This paper has explored the strategic importance of submarine communication cables in the modern international system. Using the theory of political realism, it explained how digital infrastructure especially undersea cables has become a key part of national power. In the modern era, controlling the flow of information and communication is as important as controlling military or economic power. Many states consider this infrastructure an important component of national security and are therefore trying to gain an advantage in the construction and operation of new projects. In turn, the operator of the submarine cable network has the opportunity to control access to it and if necessary use the infrastructure to achieve its own national goals.

Submarine cables carry around 95% of international data, including financial transactions, government communications and military information. This makes them critical to national security and economic stability. From a realist perspective, protecting this infrastructure is directly linked to the power and influence of the state. Damage to these cables can lead to major disruptions in communication, create vulnerabilities in defence systems and even increase the risk of international conflict. Incidents in recent years demonstrate that some actors are deliberately acting to damage targeted infrastructure in order to weaken the opponent's positions.

Protecting this infrastructure is not easy. Most submarine communication cables are managed and maintained by different companies, not governments. This creates challenges, as states must work together with private actors to secure a system that is essential for national interests. Sometimes, commercial goals and national security priorities may not align, which increases the risk of weak protection.

In addition to physical threats like sabotage or accidents, cables are also at risk from cyber espionage and data interception. These modern threats require new solutions, including stronger encryption, better surveillance technology and updated legal frameworks. Currently, international law offers only limited protection. There is no comprehensive international agreement that addresses modern risks to submarine cables. As digital competition between states grows, this gap in international cooperation becomes more serious.

In conclusion, submarine communication cables are not only technical infrastructure but also vital strategic assets. To ensure global stability and security, countries must strengthen cooperation, update international rules and work with private companies. It is important for countries to have an appropriate strategy and action plan for the protection and development of this infrastructure. Strategic documents should detail all possible threats and a response plan. This will increase the effectiveness of incident detection and reduce response time. Specific trainings are also important, which will help eliminate weaknesses and increase constant readiness.

Bibliography

- Arquilla, John. 2023. *Securing the Undersea Cable Network*. Hoover Institution. <https://surl.li/itmwmz>, (Accessed 04.11.2025)
- Bell, Duncan. 2025. *Realism*. Britannica. <https://surl.li/zqjbmc>, (Accessed 04.11.2025)
- Bueger, Christian, Tobias Libertrau and Jonas Franken. 2022. *Security threats to undersea communications cables and infrastructure - consequences for the EU*. European Parliament. <https://surl.li/rdkuee>, (Accessed 04.11.2025)
- Gallagher, Jill, and Nicola Carter. 2023. *Protection of Undersea Telecommunication Cables: Issues for Congress*. Congressional Research Service. <https://surl.li/xhihnx>, (Accessed 04.11.2025)
- L.Long, Madison. 2023. *Information Warfare in the Depths: An Analysis of Global Undersea Cable Networks*. U.S Naval Institute. <https://surl.li/daarfx>, (Accessed 04.11.2025)
- Monaghan, Sean, Otto Svedsen, Michael Darrah and Ed Arnold. 2023. *NATO's Role in Protecting Critical Undersea Infrastructure*. Centre for Strategic and International Studies. <https://surl.li/bujras>, (Accessed 04.11.2025)
- Runde, Daniel, Erin Murphy, and Thomas Bryja. 2024. *Safeguarding Subsea Cables Protecting Cyber Infrastructure amid Great Power Competition*. Center for Strategic and International Studies. <https://surl.li/pmxgin>, (Accessed 04.11.2025)
- Sherman, Justin. 2021. *Cyber Defense Across the Ocean Floor: The geopolitics of Submarine Cable Security*. Atlantic Council. <https://www.atlanticcouncil.org/wp-content/uploads/2021/09/Cyber-defense-across-the-ocean-floor-The-geopolitics-of-submarine-cable-security.pdf> (accessed 03.10.2025)
- Starosielski, Nicole. 2015. *How can we protect the internet's undersea cables?* World Economic Forum. <https://www.weforum.org/stories/2015/11/how-can-we-protect-the-internets-undersea-cables/> (accessed 03.10.2025)
- Submarine Cable Frequently Asked Questions*. 2025. Tele Geography: <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions#Cable-101> (accessed 03.10.2025)

PUBLIC-PRIVATE PARTNERSHIPS IN BORDER SECURITY INNOVATION: POLICY AND GOVERNANCE MODELS FOR INTERNAL AND INTERNATIONAL SECURITY

Natia Oshkhereli

The Learner of a Master's Degree Program (State Recourse Management) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

In an era defined by hybrid threats, digital mobility, and non-state actor flux, border-security management has evolved from a static architecture of checkpoints to a dynamic, sensor-driven network of checks, analytics, and cross-agency collaboration. Traditional state-centric models of border control struggle to handle rising volumes of cross-border flows, irregular migration, identity fraud, and transnational organized crime, not to mention drone and cyber-enabled incursions. Governments and multilateral organizations increasingly turn to public-private partnerships (PPPs) to harness the innovation and capacity of the private sector.

This paper adopts a qualitative-comparative methodology—analyzing policy documents, legal texts, and case studies (notably the EU's Entry/Exit System [EES] and Georgian border-security reforms) and examines governance models, risk profiles, and emerging policy prescriptions. It finds that when structured with robust governance frameworks, PPPs deliver measurable gains in technological agility (for example, accelerated kiosk/AI deployment), cost efficiencies (via shared investment), and cross-border interoperability. Yet critical vulnerabilities persist: vendor-lock-in, algorithmic opacity and bias, legal friction over data flows, and democratic accountability deficits. However, The paper concludes with a governance toolkit and policy recommendations for states, alliances, and multilateral actors seeking to deploy PPPs in the border-security domain and gives notable example of the the Georgian case study, that illustrates how a middle-income state, through donor-enabled PPP-adjacent structures, can navigate capability upgrades while striving to preserve accountability and sovereignty.

Keywords: Border security, PPPs, hybrid threats, non-state actors, data governance, interoperability, AI governance, EES, Georgia, accountability.

Introduction

The contemporary security environment is increasingly defined by hybrid threats, rapid technological change, and the proliferation of non-state actors, creating unprecedented challenges for traditional border-management systems. Borders are no longer merely static demarcations for controlling human or material movement; they have become dynamic interfaces that require sophisticated monitoring, analytics, and cross-agency coordination. States face rising volumes of cross-border flows driven by globalization, irregular migration, refugee movements, and economic interdependence. At the same time, technological advances have enabled new forms of illicit activity, including identity fraud, transnational organized crime, cyber-enabled smuggling, and the use of drones for surveillance or contraband transport ¹. These developments expose the limitations of traditional, state-centric border control frameworks, which often rely on rigid checkpoints and manual procedures that cannot scale to the demands of modern mobility.

In response, governments and multilateral organizations are increasingly embracing public–private partnerships (PPPs) as strategic instruments to leverage private-sector expertise, technological innovation, and investment capacity.² PPPs facilitate the integration of advanced biometric systems, AI-driven risk assessment platforms, unmanned sensor networks, and interoperable data-sharing infrastructures, providing states with the tools to address complex, multi-dimensional threats efficiently. Such partnerships are especially relevant in medium- and small-income states, which often lack the resources to independently develop and maintain cutting-edge border-security technologies but can benefit from donor-supported or co-financed initiatives.³

In Europe, the Entry/Exit System (EES) exemplifies the scale and complexity of modern border-security innovation. The EES registers biometric data (fingerprints and facial images) and travel-document metadata of non-EU nationals across 29 Schengen countries, enabling automated monitoring of entry and exit patterns and supporting security and migration-control objectives. Similarly, NATO’s revised AI strategy emphasizes the integration of emergent and disruptive technologies (EDTs), including autonomous systems, AI-driven analytics, and data fusion, as essential components of alliance resilience and collective defense.⁴ These examples illustrate a broader trend: border security is increasingly situated at the intersection of national, regional, and international security imperatives, requiring governance arrangements that are simultaneously technologically sophisticated, legally compliant, and ethically sound.⁵

This paper addresses three critical questions in this evolving context: (1) What PPP models are currently employed to deliver border-security innovation, and how do they differ in terms of governance and operational design? (2) What mechanisms, safeguards, and institutional arrangements are necessary to mitigate risks such as vendor lock-in, algorithmic opacity, and sovereignty conflicts? And (3) how can middle-income states, exemplified by Georgia, harness PPPs to modernize border-control capabilities while maintaining accountability, protecting fundamental rights, and

1 Al-Thani, Mansoor G. “AI on the frontlines: Transforming border security in the fight against drug and arms smuggling.” *International Journal of Innovative Research and Scientific Studies*, 2025

2 Public–Private Partnerships in Developing Asian Countries, “Practical Suggestions for Future Development Assistance”, 2021

3 Kei Endo, KE Seetha Ram. “Public–Private Partnerships in Developing Asian Countries: Practical Suggestions for Future Development Assistance”, ADBInstitute (Asian Development Bank Institute), 2021

4 NATO. “NATO releases revised AI strategy”, 2024

5 Christina Khoury, Maegan Hendow, “Advances in Border Management: Digitalisation trends and emerging technologies”, The International Centre for Migration Policy Development ICMPD, Vienna, 2025

avoiding strategic dependence on external actors? By examining case studies, policy frameworks, and expert insights, this study provides evidence-based analysis and practical recommendations for policymakers, security agencies, and international organizations seeking to navigate the complex landscape of PPP-enabled border security.

Methodology and Results Overview

The research adopts a qualitative-comparative methodological design involving three key strands: policy-document and legal-text analysis (including the EES regulation,⁶ EU digital-borders framework, and NATO's AI governance strategy); in-depth case studies—the EU's EES deployment, Frontex-led AI-capability projects via PPPs,⁷ and smaller-state example where PPPs in border security have been used (e.g., ICT-driven border modernization in Georgia).

The findings reveal that PPPs, when structured with strong governance frameworks, deliver measurable gains in technological agility (e.g., quicker deployment of kiosks and AI-based surveillance), cost efficiencies (via shared investment models), and cross-border interoperability (through shared standards and joint procurement). However, vulnerabilities are also exposed: the dominance of large vendors in PPPs leads to vendor-lock-in; AI-based systems raise issues of transparency, explainability, and bias; and multi-jurisdictional cross-border systems generate legal friction over data protection, sovereignty, and accountability.⁸ These findings underpin the subsequent discussion of governance models, risk profiles, and refined policy prescriptions.

Main Part

Governance Models in Border-Security Innovation

Two primary governance archetypes for PPPs in border-security innovation emerge from the empirical evidence. The first is a centralized innovation governance model, typified by NATO's top-down normative and strategic orientation: alliance-wide priorities are set for dual-use technologies (autonomy, AI, sensors), and member states and private-sector partners are contracted or enabled.⁹ This model lends strategic coherence and control, but may inhibit agile innovation due to bureaucratic layers and lengthy procurement cycles.

The second is a decentralized collaborative innovation model, exemplified by the EU's framework for border-IT systems and PPPs, where national agencies, private consortia, and research institutions cooperate under shared standards but with distributed implementation (e.g., the EES roll-out).¹⁰ In practice, hybrid governance forms prevail, combining central strategic direction with decentralized execution, yet this hybridization also introduces complexity in accountability, risk allocation, and regulatory oversight.

From the analysis, it becomes clear that states must balance strategic alignment (ensuring

6 European Union, "REGULATION (EU) 2017/2226 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", Brussels: Official Journal of the European Union, 2017

7 Frontex - European Border and Coast Guard Agency, "Artificial Intelligence-based capabilities for the European Border and Coast Guard", Warsaw, 2021

8 Christina Khoury, Maegan Hendow, "Advances in Border Management: Digitalisation trends and emerging technologies", The International Centre for Migration Policy Development ICMPD, Vienna, 2025

9 Prats Cabrera, Joan Oriol, "The Governance of Public-Private Partnerships. Inter-American Development Bank", 2019

10 *ibid*

interoperability and resilience) with operational flexibility (avoiding vendor capture and bureaucratic drag). PPP governance frameworks must therefore specify stakeholder roles, risk-sharing mechanisms, performance incentives, data-governance regimes, and exit/transition clauses.

The EU Entry/Exit System (EES) as a PPP-Innovation Case

The EES stands as a frontier case of large-scale PPP-enabled border innovation. From 12 October 2025, 29 European countries began registering non-EU nationals' entries and exits via an automated IT system recording biometric data (fingerprints and facial images), travel-document details, and stay duration. Its rollout is phased over six months to allow states and industry to adjust.¹¹

From an innovation-governance perspective, the EES involved multi-actor PPPs: contracts with private vendors for kiosk hardware, biometric engines, and data centers; research partnerships for AI risk analytics; and coordination across national border agencies via the EU agency eu-LISA. Yet several governance risks emerge. First, vendor-lock-in: large consortia supplying both hardware and maintenance may limit future competition. Second, algorithmic transparency and data governance: reliance on biometric matching and risk-scoring raises questions about accuracy, bias, and redress mechanisms. The FRA emphasizes rights-compliant collection of data and proper training of border-guard staff. Third, inter-jurisdictional interoperability and sovereignty tensions: while the EES is EU-wide, individual states may maintain national data regimes or vendor preferences, complicating cross-border data flows and standards.¹² Fourth, operational risk during rollout: reports indicate potential bottlenecks and traveler disruption at ports and airports, potentially undermining legitimacy.¹³ These risk profiles illustrate that PPP-enabled innovation in border security is not just a technical matter but a governance challenge.

AI, Emerging Technologies and Border-Security PPPs

Artificial intelligence (AI) and other emergent/disruptive technologies (EDTs) have become central to modern border-security innovation. NATO's AI strategy underscores the need for responsible AI deployment, adversarial resistance (e.g., spoofing of biometric systems), and strategic foresight in the context of dual-use technologies.¹⁴ Emerging research on flexible hardware-enabled guarantees (flexHEGs) highlights that AI and compute hardware applications in international security require standardized verification frameworks and governance mechanisms to prevent misuse or uncontrolled proliferation.¹⁵

Within PPPs, private firms develop AI-based solutions such as object recognition for vehicle and cargo inspection, biometric matching engines, unmanned sensor platforms, and predictive data analytics for migration-risk scoring. These innovations, however, introduce governance challenges, for example: algorithmic bias may produce false positives or discriminatory outcomes

11 ETIAS, "EU Biometric Border Checks Begin Today for Non-EU Travelers", 2025

12 Lucia Xiaoyan Liu, Stewart Clegg, Julien Pollack, "The Effect of Public-Private Partnerships on Innovation in Infrastructure Delivery", *Sage Journals*, 2025, 31-49.

13 ALLI, Noah Gbenga. "Operational Risk and its Influence on Passenger Satisfaction in Airport Services." *Journal of Transportation Management*, 1-24, 2024

14 North Atlantic Treaty Organization, "Summary of NATO's revised Artificial Intelligence (AI) strategy", 2024

15 Dan Hendrycks, Eric Schmidt, Alexandr Wang, "Superintelligence Strategy", 2025

based on nationality, race, or other demographic indicators. Opaque decision-making processes and the potential for mass-surveillance drift increase the risk of mission creep, as systems originally intended for migration control can evolve toward broader intelligence collection. Additionally, private vendors may prioritize proprietary solutions over open standards, limiting interoperability and state oversight and etc.

PPP governance frameworks, therefore, must embed ethics, algorithmic explainability, robust audit trails, human-in-the-loop mechanisms, and clear liability structures. In practice, this requires systematic human oversight of AI-driven decisions, independent third-party auditing, and operational transparency to ensure alignment with fundamental rights frameworks.¹⁶

The Georgian Case – PPP – Adjacent Border Security Innovation

Georgia provides a salient example of how smaller states can engage with PPP-adjacent models to modernize border control while managing resource constraints and preserving accountability. The Public–Private Partnership Agency (PPPA) of Georgia, under the Prime Minister’s Office, serves as a central body for identifying potential PPP projects, reviewing proposals, and advising government decisions under the Law of Georgia on Public–Private Partnerships.¹⁷ While historically focused on infrastructure and energy, this institutional architecture now provides a platform for security-oriented PPPs.

Georgia has leveraged donor-enabled partnerships to enhance border capabilities. In April 2023, the EU and International Organization for Migration (IOM) provided advanced border-surveillance equipment valued at €1.25 million, including 4×4 vehicles, wireless cameras, and remote-sector monitoring systems.¹⁸ Earlier, in 2020, 80 wireless cameras were supplied to detect green-border crossings.¹⁹ In 2022, Georgia implemented the HERMES API/PNR platform developed by WCC Group to support cross-border crime detection and counter-terrorism screening.²⁰ The system is designed to detect, prevent, and prosecute terrorism and serious crimes by screening, consolidating and analyzing passenger database so that authorities can gain insights into potential threats and track criminal activities. Additionally, operational coordination with Frontex further strengthened Georgia’s integration with European border-security standards and expertise.²¹

The Georgian experience demonstrates several lessons. First, the hybrid donor-plus-PPP pathway allows small states to upgrade capabilities without committing immediately to long-term, high-cost vendor contracts, mitigating strategic dependency risks. Second, incremental capacity-building via equipment deployment, software procurement, and staff training enables technical competence and institutional maturity while aligning with international best practices. Third, the existence of the PPPA ensures structured governance for potential security PPPs, including project evaluation, procurement oversight, and institutional accountability.

Nonetheless, governance caveats remain. Donor-provided equipment may lack long-term

16 World Bank Group, “Government Objectives: Benefits and Risks of PPPs”, 2025

17 The Public Private Partnership Agency, 2025

18 European Union in Georgia, “EU and IOM Enhance Georgia’s Border Surveillance Capacities”, 2023

19 The International Organization for Migration (IOM), “The European Union Provides Cameras to the Ministry of Internal Affairs of Georgia”, 2021

20 Tony Kingham, “Georgia chooses HERMES for country’s border management solution”, 2022

21 Frontex, “The European Border and Coast Guard Agency, Frontex renews working arrangement with Georgia”, 2021

maintenance plans, remote surveillance deployments raise data-protection concerns, and the transition from donor-led initiatives to formal PPP contracts is still developing. These challenges underscore that smaller states can meaningfully engage in PPP-enabled border innovation only if ethical safeguards, phased institutional capacity-building, and robust oversight mechanisms are maintained.²²

Risk and Governance-Challenge Spectrum

The analysis of the EES, NATO frameworks, and the Georgian experience highlights a broad spectrum of risks and governance challenges associated with PPP-enabled border-security innovation. A key concern is **strategic dependency and vendor lock-in**, where states risk losing operational flexibility as private firms providing critical infrastructure create high switching costs and dependency on proprietary technologies (Third Stage Consulting).²³ Equally significant are **accountability and oversight gaps**—the outsourcing of algorithmic decision-making and data-platform governance to private entities can dilute democratic control and weaken public trust.²⁴

Another major issue involves **data protection and fundamental rights**, as biometric and AI systems process highly sensitive personal information. Cross-border data exchanges must therefore comply with GDPR, Schengen regulations, and broader human-rights frameworks.²⁵ **Inter-jurisdictional and standardization tensions** further complicate governance: while shared systems enhance interoperability, they also confront national sovereignty concerns and vendor fragmentation, which can undermine coherent operational standards.²⁶

The **innovation-versus-legitimacy trade-off** is another persistent challenge, where the pace of technological adoption may outstrip regulatory oversight and public acceptance, creating risks of social backlash or legitimacy deficits.²⁷ Meanwhile, **dual-use dynamics and mission creep** pose serious strategic and ethical risks, as technologies initially designed for migration management can evolve into intelligence or military applications without proper authorization.²⁸ Finally, **ethical and algorithmic-governance blind spots** remain pervasive: AI-driven systems can reproduce bias, operate without meaningful human oversight, and leave affected individuals without accessible redress mechanisms.²⁹

Integrated Policy and Governance Recommendations

Public–private partnerships (PPPs) are critical for delivering the scale, speed, and innovation needed in modern border security, but they require governance structures designed to mitigate the associated risks. Contracts should embed modularity and upgrade-path clauses to allow replacement or enhancement of AI engines, biometric kiosks, and sensor networks without full vendor replacement, thereby reducing lock-in and preserving competition. Performance-based incentives and exit clauses are essential to balance risk-sharing while ensuring that public authorities retain

22 Seungwoo Son, “Legal Analysis on Public-Private Partnerships regarding”, Korea, 2012

23 Eric Kimberling, “Navigating Vendor Lock-In: Risks and Mitigation Strategies for Successful Digital Transformations”, Third Stage Consulting Group, 2024

24 World Bank Group, “Potential Benefits of Public Private Partnerships”, 2025

25 World Bank Group, “Government Objectives: Benefits and Risks of PPPs”, 2025

26 Seungwoo Son, Legal Analysis on Public-Private Partnerships regarding. Korea, 2012

27 European Investment Bank, “Public-private partnerships in security and defence”, 2025

28 Georgios Kolliarakis, “Anticipatory governance of emerging and disruptive technologies with dual-use potential”, 2022

29 World Bank Group, “Key Issues in PPPs for the Poor”, 2025

fallback options.³⁰ Transparency, auditability, and accountability frameworks must be implemented, including consent to algorithmic audits, human-in-the-loop oversight, data-protection audits, and public reporting of outcomes.

Regulatory sandboxes provide a mechanism for pilot deployments under monitored conditions, enabling real-time learning and anticipatory governance adjustments. For transnational systems, common standards, joint liability frameworks, and interoperable data-governance models are required, coordinated across states, agencies, and vendor consortia.³¹ Capacity-building and co-innovation, particularly for smaller states, strengthen domestic expertise, reduce strategic dependence, and foster sustainable adoption. Ethical safeguards, including human-rights impact assessments, independent oversight, and channels for redress, must be integral to PPP frameworks.³² Finally, innovation outcomes should be tied to measurable security-performance indicators, such as reduction in identity-fraud incidents, overstay detection rates, and system downtime, and reviewed periodically to ensure governance alignment with evolving threats.

Conclusion

The frontier of border security lies increasingly in innovation ecosystems where biometric systems, AI analytics, and cross-border data infrastructures intersect with sovereignty, rights, and multilateral cooperation. PPPs offer a distinct governance modality to integrate private-sector agility with public-sector strategic mandates—but only if governed with foresight, institutional robustness, and ethical integrity.

The EU's EES deployment, NATO's emerging-technologies strategy, and smaller-state experiences such as Georgia illustrate both the promise and the perils of PPP-enabled border innovation. Without careful attention to vendor-lock-in, algorithmic transparency, rights protection, and inter-jurisdictional governance, such initiatives may undermine rather than enhance legitimacy, resilience, and international cooperation.

For states and alliances alike, the challenge is not merely technological but governance-architectural: building PPP arrangements that are adaptive, rights-respecting, interoperable, and strategically aligned. In this sense, the success of border-security innovation depends as much on partnership structure and governance as on the sophistication of deployed technologies.³³

Bibliography

- ALLI, Noah Gbenga. 2024. "Operational Risk and its Influence on Passenger Satisfaction in Airport Services." *Journal of Transportation Management*, October 12: 1-24. <https://surl.li/cycehq>. Accessed 04.11.2025.
- Al-Thani, Mansoor G. 2025. "AI on the frontlines: Transforming border security in the fight against drug and arms smuggling." *International Journal of Innovative Research and Scientific Studies*. Accessed October 20, 2025.
- Christina Khoury, Maegan Hendow. 2025. *Advances in Border Management: Digitalisation trends and emerging technologies*. Vienna: The International Centre for Migration Policy Development ICMPD. <https://surl.li/gcgami>,

30 Organization for Economic Cooperation and Development (OECD), „Public Governance of Public-Private Partnerships.“, 2012

31 Christina Khoury, Maegan Hendow, “Advances in Border Management: Digitalisation trends and emerging technologies”, The International Centre for Migration Policy Development ICMPD, Vienna, 2025

32 Ibid

33 International Centre for Migration Policy Development (ICMPD), “Advances in Border Management: Digitalisation trends and emerging technologies“, 2025

Accessed October 20, 2025.

- Dan Hendrycks, Eric Schmidt, Alexandr Wang. 2025. "Superintelligence Strategy." April 14. Accessed October 20, 2025. <https://surl.lt/hlfzmu>. Accessed 04.11.2025.
- European Investment Bank. 2025. *Public-private partnerships in security and defence*. April 22. <https://surl.cc/aqsoqn>, Accessed 04.11.2025.
- European Union in Georgia. 2023. *EU and IOM Enhance Georgia's Border Surveillance Capacities*. April 13. <https://surl.li/mxdbzc>, Accessed 04.11.2025.
- European Union. 2017. *REGULATION (EU) 2017/2226 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*. Brussels: Official Journal of the European Union. <https://surl.li/vchodn>, Accessed 04.11.2025.
- Frontex, European Border and Coast Guard Agency. 2021. *Artificial Intelligence-based capabilities for the European Border and Coast Guard*. Warsaw: Frontex.. <https://surl.li/okzmvy>, Accessed 04.11.2025.
- Frontex, the European Border and Coast Guard Agency. 2021. *Frontex renews working arrangement with Georgia*. November 11. <https://surl.li/zjyzfr>, Accessed 04.11.2025.
- Georgios Kolliarakis. 2022. "Anticipatory governance of emerging and disruptive technologies with dual-use potential." July 25. <https://surl.lt/ykmnlg>, Accessed 04.11.2025.
- International Centre for Migration Policy Development (ICMPD). 2025. "Advances in Border Management: Digitalisation trends and emerging technologies." January. <https://surl.lu/butubt>, <https://surl.lu/butubt>, Accessed 04.11.2025.
- Kei Endo, KE Seetha Ram. 2021. "Public-Private Partnerships in Developing Asian Countries: Practical Suggestions for Future Development Assistance." *ADBInstitute* (Asian Development Bank Institute). <https://surl.li/gprrow>, Accessed 04.11.2025.
- Kimberling, Erik. 2024. "Navigating Vendor Lock-In: Risks and Mitigation Strategies for Successful Digital Transformations." *Third Stage Consulting Group*. September 16. <https://surl.lt/oisavh>, Accessed 04.11.2025.
- Lucia Xiaoyan Liu, Stewart Clegg, Julien Pollack. 2024. "The Effect of Public-Private Partnerships on Innovation in Infrastructure Delivery." *Sage Journals*, February: 31-49. <https://journals.sagepub.com/doi/epub/10.1177/87569728231189989>.
- Organization for Economic Cooperation and Development (OECD). 2012. *Public Governance of Public-Private Partnerships*. <https://surl.li/xajrnf>, Accessed 04.11.2025.
- Organization, North Atlantic Treaty. 2024. *NATO releases revised AI strategy*. July 10. <https://surl.li/wqskfw>, Accessed 04.11.2025.
- Organization, North Atlantic Treaty. 2024. *Summary of NATO's revised Artificial Intelligence (AI) strategy*. July 10.. <https://surl.li/adzxxn>, Accessed 04.11.2025.
- Prats Cabrera, Joan Oriol. 2019. *The Governance of Public-Private Partnerships*. Inter-American Development Bank. <https://surl.li/qgysuw>, Accessed 04.11.2025.
- Rights, European Union Agency for Fundamental. 2025. *Entry/Exit System: Fundamental rights guidance for border guards*. October 17. <https://surl.li/qhmmbg>, Accessed 04.11.2025.
- Seungwoo Son. 2012. *Legal Analysis on Public-Private Partnerships regarding*. Korea, June.
- The International Organization for Migration (IOM). 2021. *The European Union Provides Cameras to the Ministry of Internal Affairs of Georgia*. April 22. <https://surl.li/pwapeq>
- The Public Private Partnership Agency. n.d. <https://surl.li/mtjtjb>, Accessed 04.11.2025.
- Tony Kingham. 2022. *Georgia chooses HERMES for country's border management solution*. February 4. <https://surl.li/tcjevcd>, Accessed 04.11.2025.
- Umair Tanveer, Thinh Gia Hoang, Shamaila Ishaq, Raja Usman Khalid. 2025. "Public-private partnerships as catalysts for digital transformation and circular economy: Insights from developing countries." *Technological Forecasting and Social Change*. <https://surl.li/ptayol>, Accessed 04.11.2025.
- World Bank Group. 2025. *Government Objectives: Benefits and Risks of PPPs*.. <https://surl.cc/aoffzd>, Accessed 04.11.2025.
- . 2025. *Government Objectives: Benefits and Risks of PPPs*. <https://surl.li/pxjnrj>, Accessed 04.11.2025.
- . 2025. *Key Issues in PPPs for the Poor*. <https://surl.li/zvbdzu>, Accessed 04.11.2025.

MODERN GEOPOLITICS AND SECURITY COMPETITION IN THE FAR NORTH: RUSSIA, USA AND CHINA'S STRATEGIC INTERESTS IN THE ARCTIC

Lieutenant Mariam Mukbaniani

The Learner of a Master's Degree Program (International Relations and Diplomacy) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Nikoloz Samkharadze

Professor of Master's Program in International Relations and Diplomacy of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This paper examines the evolving dynamics of modern geopolitics and security competition in the Arctic, focusing on China, USA and Russia's strategic interests in the region. As climate change accelerates ice melt and opens new maritime routes, the Arctic has transformed from a remote periphery into a central arena of global power politics. Russia seeks to consolidate its dominance through militarization, infrastructure development, and control over the Northern Sea Route, framing the Arctic as a cornerstone of its national security and economic revival. United States aims to preserve strategic balance and freedom of navigation. Meanwhile, China positions itself as a "near-Arctic state," pursuing scientific research, investment in energy and transport projects, and strategic partnerships to expand its influence within the framework of the Polar Silk Road. By analyzing these countries' political, economic, and military objectives, this study highlights how their activities challenge the existing security architecture and provoke broader questions about governance, sovereignty, and resource competition in the Far North. The paper concludes that the intersection of Russian assertiveness, USA interests and Chinese ambition signifies a shift in Arctic geopolitics toward a more multipolar and contested security environment.

Keywords: Russia, China, USA, Arctic, Security, Interests.

Introduction

In the 21st century, the Arctic has emerged as one of the most strategically significant regions on the planet. Once considered an isolated and inhospitable space, it is now at the center of global attention due to the profound geopolitical, economic, and environmental transformations taking place there.¹ The combination of accelerating climate change, newly accessible sea routes, and untapped natural resources has turned the Arctic into a dynamic frontier of international politics. Major powers increasingly view it not only as an ecological zone but also as a strategic domain where national interests, security considerations, and economic ambitions intersect.

The Arctic is warming nearly four times faster than the global average, resulting in the rapid retreat of sea ice and glaciers. This environmental shift is profoundly altering the region's geography and accessibility. Melting ice has exposed areas that were once permanently frozen, enabling new opportunities for navigation, trade, and resource exploration.² The Northern Sea Route (NSR) along Russia's northern coast and the Northwest Passage through the Canadian Arctic Archipelago are now viable for longer periods each year. These routes offer shorter shipping distances between Europe and Asia reducing transit times by up to 40% compared to traditional routes through the Suez Canal.

Beneath the Arctic's ice lies one of the richest untapped resource frontiers in the world. According to estimates the region may contain around 13% of the world's undiscovered oil and 30% of its natural gas reserves, in addition, vast deposits of rare earth elements, precious metals, and fisheries.³ These resources are essential for global energy markets and the production of advanced technologies from renewable energy systems to military hardware. Countries with Arctic territory, such as Russia, the United States, Canada, and Norway, have intensified their efforts to map, claim, and develop these reserves. Russia, in particular, has invested heavily in offshore drilling and the development of the Northern Sea Route as a commercial and military corridor. Meanwhile, non-Arctic actors like China have expressed growing interest in participating in Arctic resource projects, underscoring the global economic stakes involved. Control over these natural assets is becoming a central issue in international competition, linking the Arctic's economic promise directly to global power politics.

Main Part

Russia's Arctic Policy: Militarization and Resource Dominance

Russia's approach to the Arctic is shaped by a combination of historical legacy, geographic advantage, and strategic ambition. Russia's engagement with the Arctic dates back to the Tsarist and Soviet eras, when explorers and scientists mapped the Northern territories and established early settlements along the Siberian coast. During the Soviet period, the Arctic played a crucial role in both industrial development and national defense.

Spanning over half of the Arctic Ocean's coastline, Russia possesses the largest share of Arctic territory, making the region central to its national identity and long-term development strategy.

1 Ishfaq Hussain Malik. 2025. „Arctic Warming: Cascading Climate Impacts and Global Consequences.“

2 Jill Kimball, Melting Arctic ice could transform international shipping routes, study finds, brown university 2022

3 Bruce F. Molnia, Documenting Arctic Sea Ice Dynamics with Global Fiducials Program Imagery, US Geological Survey, 2023

This vast stretch of territory gives Moscow control over the Northern Sea Route (NSR), a maritime corridor that is increasingly central to both economic and military planning. In the 21st century, Moscow views the Arctic not merely as a peripheral region but as a key pillar of its economic strength, energy security, and geopolitical influence.⁴ Through military modernization, energy extraction, and control of vital shipping routes, Russia seeks to consolidate its dominance over the Far North and reassert its status as a great power in global affairs.

The Northern Sea Route (NSR) extends along Russia's northern coast, connecting the Barents Sea to the Bering Strait. As Arctic ice continues to melt, the NSR has become one of the most strategically valuable maritime passages in the world. It offers a significantly shorter transit route between Europe and Asia (From Shanghai port to The port of Rotterdam). Cutting shipping distances by up to 40% compared to traditional routes through the Suez Canal.⁵

Moscow visions the NSR as both an economic lifeline and a geopolitical instrument. By controlling traffic along this route, Russia seeks to establish itself as a central hub in Eurasian trade networks. The Russian government has invested heavily in port infrastructure, search-and-rescue facilities, and satellite navigation systems to support year-round navigation. Additionally, state-owned energy giants such as Gazprom and Rosneft have expanded operations in the Arctic, exporting liquefied natural gas (LNG) through projects like Yamal LNG and Arctic LNG-2.⁶ These initiatives not only enhance Russia's export capacity but also cement its role as a global energy power.

However, Russia's control of the NSR has sparked debate in international law and diplomacy. Moscow treats parts of the route as internal waters under its sovereignty, while Western states particularly the United States insist on freedom of navigation. This tension underscores how economic ambitions are closely intertwined with strategic and legal assertions of authority.

Parallel to its economic agenda, Russia has undertaken extensive military modernization in the Arctic. Since the early 2010s, Moscow has reactivated numerous Soviet-era bases, built new airfields, and established the Arctic Joint Strategic Command a unified military structure tasked with defending the region.⁷ The country has also developed specialized Arctic brigades trained for operations in extreme conditions and deployed advanced radar systems, missile defenses, and long-range aviation. A distinctive feature of Russia's Arctic military capability is its fleet of nuclear-powered icebreakers, the largest and most powerful in the world. These vessels enable year-round access to polar waters and ensure logistical support for both civilian and defense operations. From Moscow's perspective, militarization is not an act of aggression but a means of ensuring sovereignty, securing critical energy infrastructure, and safeguarding national interests in a rapidly changing environment.

For Russia, Arctic development is inseparable from the concepts of sovereignty and great-power identity. President Vladimir Putin has repeatedly framed the Arctic as a symbol of national pride and a "strategic reserve" for future generations. By combining military control, technological

4 Marlène LARUELLE, *Russia's Arctic Policy: A Power Strategy and Its Limits*, French Institute of International Relations, 2020

5 Roberto Rivas Hermann, *Arctic transshipment hub planning along the Northern Sea Route: A systematic literature review and policy implications of Arctic port infrastructure*, Marine Policy, 2022

6 Sergei Gladkov, *Changes in economic cooperation between Russia and China since the start of the full-scale war in Ukraine*, 2025

7 Nurlan Aliyev, *Russia's Military Capabilities in the Arctic*, International Center for Defence and Security, 2019

innovation, and economic investment, Russia aims to transform the Arctic into a cornerstone of its twenty-first-century power projection. Through the Arctic, Moscow reinforces its vision of a multipolar world order in which it acts as both a regional hegemon and a global energy superpower.

The United States: Strategic Balance and Alliance Building

Alaska gives the United States more than 1,000 miles of Arctic coastline and a direct link to the polar region. This geographic position makes the Arctic integral to U.S. defense planning. The region serves as both a frontier for homeland security and a forward line for detecting and deterring potential threats from near-peer competitors.⁸ Historically, the Arctic played a key role during the Cold War as part of the early warning system against Soviet missile attacks. Today, with renewed great power competition, the U.S. sees the Arctic once again as a vital buffer zone and an area requiring sustained military attention.

American defense documents, such as the U.S. Department of Defense Arctic Strategy (2024), emphasize the need to protect national interests while preserving the Arctic as a “peaceful, stable, and rules-based region.” The U.S. military presence in Alaska including bases like Elmendorf-Richardson and advanced radar systems supports Arctic surveillance and rapid response capabilities. As Russia expands its northern military infrastructure, the U.S. increasingly treats Arctic security as a component of broader deterrence strategy.⁹

Washington’s Arctic policy rests on three main pillars: maintaining freedom of navigation, promoting environmental protection, and ensuring strategic deterrence.

First, the United States holds the principle that Arctic waters must remain open to international navigation. This stance directly challenges Russia’s efforts to treat parts of the Northern Sea Route (NSR) as internal waters. Freedom of navigation operations (FONOPs) and diplomatic engagement reflect Washington’s determination to prevent any single state from monopolizing emerging maritime corridors.

Second, the U.S. emphasizes the importance of environmental sustainability and the protection of fragile Arctic ecosystems. Climate change in the Arctic affects global sea levels, weather patterns, and biodiversity, making environmental management a security concern as well as a moral obligation. Agencies such as the National Oceanic and Atmospheric Administration (NOAA) and the U.S. Coast Guard conduct scientific research and emergency response missions aimed at balancing economic activity with ecological preservation.

Third, deterring Russia and, increasingly, monitoring China’s polar ambitions have become central objectives. As Moscow strengthens its Arctic bases and Beijing expands its economic footprint, the U.S. seeks to prevent a shift in the regional balance of power that could undermine allied interests or global maritime stability.¹⁰

Recognizing that no single country can manage Arctic challenges alone, the United States has prioritized cooperation with NATO allies and Arctic partners. Washington maintains close defense coordination with Norway, a key NATO ally with advanced Arctic warfare capabilities,

⁸ Chairman Green, “The Alaskan Arctic Remains Strategically Vital”, 2023

⁹ U.S department, “ARCTIC STRATEGY”, 2024, <https://surl.lu/jzjpnf>, Accessed 06.11.2025

¹⁰ Ibid. U.S department.

and with Canada, through the North American Aerospace Defense Command (NORAD), which provides continental air and missile warning coverage. The U.S. also collaborates with Denmark, particularly through Greenland, where American radar and satellite systems contribute to missile defense and Arctic monitoring.¹¹

Despite its ambitions, the United States faces several structural and logistical challenges in maintaining an effective Arctic presence. One of the most pressing issues is the limited icebreaker capacity: the U.S. Coast Guard currently operates only two heavy icebreakers, compared to Russia's fleet of more than forty, including nuclear-powered vessels.¹² This technological gap restricts America's ability to conduct year-round operations in polar waters.

In addition, infrastructure gaps such as a lack of deep-water ports, limited search-and-rescue capabilities, and inadequate communication networks hinder both civilian and military readiness. Policy coordination across multiple federal agencies also remains fragmented, slowing the implementation of a unified Arctic strategy. These challenges weaken Washington's ability to fully project influence and respond rapidly to developments in the region.

In the broader context, the U.S. works through multilateral institutions such as the Arctic Council, where it promotes dialogue on scientific research, environmental protection, and sustainable development. Although the Council avoids military issues, it remains a vital platform for diplomatic engagement and confidence-building among Arctic states. Through alliance building and multilateral diplomacy, Washington seeks to maintain a cooperative but strategically balanced Arctic order.

China's Arctic Ambitions: The "Near-Arctic State"

Although China is geographically distant from the polar circle, it has emerged as a major player in Arctic affairs through its self-declared identity as a "near-Arctic state." This designation, introduced in China's 2018 Arctic Policy White Paper, reflects Beijing's growing recognition that the Arctic's environmental changes, economic potential, and strategic location have global implications. China's involvement in the region is multifaceted combining scientific exploration, economic investment, and geopolitical calculation. Through its Polar Silk Road initiative, China aims to integrate the Arctic into its broader Belt and Road Initiative (BRI), securing access to new trade routes, natural resources, and strategic influence.¹³ While Beijing promotes its activities as cooperative and peaceful, Western powers increasingly view its expanding presence as part of a broader strategy to extend global power through both civilian and dual-use means.

China's claim to be a "near-Arctic state" is primarily political rather than geographical. The phrase, first introduced by Beijing in 2018, serves to justify its legitimate interest and participation in Arctic affairs despite lacking territorial claims. China argues that the Arctic's environmental and economic developments directly affect non-Arctic nations due to global climate interdependence, especially through changes in sea levels and trade dynamics.

Beijing's policy emphasizes "respect, cooperation, win-win results, and sustainability" the four guiding principles of its Arctic engagement. Through this framework, China positions

11 Jim Garamone, "Implementing Arctic Strategy", of defense (war), 2024

12 service, congressional research, Changes in the Arctic: Background and Issues for Congress . U.S. Congress.2025

13 The State COUNCIL Information Office of the People's Republic of China, "China's Arctic Policy", 2018, <https://surl.li/pzurvw>, Accessed 06.11.2025.

itself as a responsible global stakeholder advocating for shared governance of the Arctic under international law, particularly the United Nations Convention on the Law of the Sea. However, this self-identification has drawn skepticism from Arctic states, many of which interpret it as a diplomatic attempt to legitimize China's growing strategic and economic ambitions in a region traditionally dominated by Western and Russian interests.

A central element of China's Arctic policy is the creation of the Polar Silk Road (PSR) an extension of the Belt and Road Initiative into the High North. The PSR aims to connect East Asia with Europe through the Arctic Ocean, utilizing emerging sea routes such as the Northern Sea Route along Russia's coast.¹⁴ By developing Arctic shipping corridors, Beijing seeks to reduce its dependence on traditional chokepoints like the Strait of Malacca and the Suez Canal, which are vulnerable to geopolitical tensions or blockages.

China has partnered closely with Russia to advance this vision, investing in infrastructure and energy projects along the NSR. For instance, Chinese companies such as the China National Petroleum Corporation and the China National Offshore Oil Corporation are major stakeholders in Russia's Yamal LNG and Arctic LNG-2 projects.¹⁵ These ventures provide China with long-term access to natural gas supplies and experience in Arctic navigation and construction. The Polar Silk Road represents both an economic opportunity and a geopolitical instrument, linking the Arctic to Beijing's global trade network and strengthening Sino-Russian strategic cooperation.

China's Arctic ambitions are driven by a combination of energy security, commercial expansion, and scientific exploration. The country's rapid industrial growth has made energy diversification a strategic priority. Arctic oil and natural gas reserves offer China an opportunity to secure reliable supplies outside of volatile Middle Eastern or African markets. In addition to energy interests, shipping routes are a major focus. The Northern Sea Route could shorten the maritime distance between Chinese and European ports by nearly two weeks, significantly reducing transportation costs and fuel consumption. For a trade-dependent economy like China's, such efficiencies carry strategic weight.

While China portrays its Arctic activities as peaceful and cooperative, many Western governments and analysts interpret them through the lens of strategic competition. The concept of dual-use strategy, the blending of civilian and military capabilities has become central to Western concerns about China's long-term intentions. Investments in Arctic infrastructure, ports, and research stations may serve not only commercial and scientific functions but also strategic purposes such as surveillance, intelligence gathering, and potential logistical support for naval operations.¹⁶

Moreover, China's partnership with Russia in Arctic energy and shipping projects raises questions about a shifting balance of power in the region. Western observers fear that Beijing could leverage economic influence to gain *de facto* strategic access or challenge the governance norms maintained by the Arctic Council and NATO members. While there is no evidence of militarization

¹⁴ Ibid.

¹⁵ Erica Downs, "China-Russia Energy Relations: Will New Oil and Natural Gas Deals Help Russia Weather Economic Sanctions?", Columbia University's Center on Global Energy Policy. 2022

¹⁶ Anders Edström, "Cutting Through Narratives on Chinese Arctic Investments", Belfer Center for Science and International Affairs. 2025

by China in the Arctic, the strategic ambiguity of its dual-use projects contributes to mistrust among Western nations.

Future Prospects: The Arctic as an Arena of Great Power Rivalry

The Arctic's evolving geopolitical landscape carries multiple potential flashpoints. Territorial claims along contested continental shelves, particularly between Russia and neighboring Arctic states, could provoke disputes. Resource extraction, including oil, natural gas, and rare earth minerals, raises the risk of economic and environmental tensions. Militarization, exemplified by Russia's Arctic bases and the United States' strategic deployments, increases the likelihood of miscalculation, especially in remote and harsh environments where rapid response is difficult.

Moreover, the entry of non-Arctic powers, such as China, into economic and scientific projects complicates traditional governance and may inadvertently escalate competition, particularly when infrastructure has dual-use capabilities with strategic potential. Control over shipping routes, energy resources, and strategic bases has the potential to reshape global trade networks and power balances. The region's evolution reflects broader trends in multipolarity, demonstrating how environmental change can create both opportunity and rivalry. Effective management of these tensions will determine whether the Arctic becomes a zone of conflict, cooperation, or a delicate equilibrium of competing interests.

As the Arctic becomes an increasingly contested space, governance and legal frameworks play a critical role in shaping regional stability. While the region is rich in resources and strategic opportunities, the overlapping ambitions of major powers Russia, the United States, and China introduce a complex mix of cooperation and competition. Governance structures, both formal and informal, aim to regulate these interactions, manage disputes, and ensure that economic development and environmental protection proceed within internationally recognized norms.

The Arctic Council, established in 1996, remains the primary multilateral forum for Arctic governance. Comprising eight Arctic states: Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden, and the United States.¹⁷ The Council focuses on sustainable development, environmental protection, and scientific cooperation. However, it deliberately excludes security and military matters, limiting its ability to manage strategic competition.

In addition to the Council, the United Nations Convention on the Law of the Sea provides the primary legal framework for territorial claims, maritime boundaries, and resource exploitation.¹⁸ Arctic states use UNCLOS to justify claims over extended continental shelves and exclusive economic zones, while non-Arctic actors, such as China, rely on the convention to assert legitimate access to navigation and scientific activity. Together, the Arctic Council and UNCLOS establish a rules-based system that mitigates conflict, yet they also highlight the tension between national ambitions and multilateral governance.

Looking ahead, the Arctic's trajectory will likely depend on how effectively governance institutions manage competing interests. Three possible scenarios emerge:

1. Balance of Power: Arctic states maintain a cautious equilibrium, combining military readi-

¹⁷ The Arctic Council, "A Quick guide", <https://arctic-council.org/about/>, Accessed 06.11.2025.

¹⁸ "UNCLOS", THE ARCTIC GATEWAY, <https://surl.li/wwfmpo>, Accessed 06.11.2025.

ness with diplomatic engagement. Power projection is limited by mutual deterrence, and no single actor dominates key shipping routes or resource zones.

2. Regional Cooperation: States prioritize multilateral frameworks, environmental protection, and sustainable development. International agreements expand the Arctic Council's mandate, allowing for coordinated management of resources and infrastructure projects, minimizing the risk of conflict.

3. Confrontation: Intensifying competition leads to increased militarization, unilateral resource claims, and disputes over shipping lanes. Strategic miscalculations could escalate tensions, turning the Arctic into a zone of open rivalry with global implications for trade, security, and environmental stability.

Conclusion

The Arctic has emerged as one of the most significant arenas of 21st-century geopolitics, where climate change, resource potential, and strategic location intersect to create both opportunities and tensions. Russia, the United States, and China each pursue distinct but overlapping objectives, shaping the region through military, economic, and diplomatic means. Russia leverages its historical presence, vast coastline, and energy wealth to consolidate sovereignty and project power, while the United States emphasizes freedom of navigation, alliance-building, and deterrence to maintain strategic balance. China, as a self-declared "near-Arctic state," advances its influence primarily through economic investment, scientific research, and the Polar Silk Road, introducing a new dimension of global competition.¹⁹

The interaction of these powers transforms the Arctic from a relatively cooperative space into a complex arena of rivalry. Territorial claims, control of emerging shipping routes, resource extraction, and militarization constitute potential flashpoints, while environmental change and the rights of indigenous communities add layers of urgency and ethical responsibility.

Looking ahead, the Arctic's future will likely be shaped by the delicate balance between competition and collaboration. Scenarios range from sustained regional cooperation and shared governance to heightened confrontation and strategic rivalry. The Arctic is thus not only a test of national ambitions but also a reflection of broader global power dynamics. Its evolving landscape underscores the profound ways in which environmental change, economic opportunity, and strategic competition are reshaping international relations in the Far North and, by extension, the global order itself.

¹⁹ Ibid. UNCLOS. "ARCTIC PORTAL.org.

Bibliography

- Aliyev, Nurlan.. „Russia’s Military Capabilities in the Arctic.“ *international center for defence and security*. 2019
- The State COUNCIL Information Office of the People’s Republic of China, “China’s Arctic Policy”, 2018, <https://surl.li/pzurvw>, Accessed 06.11.2025.
- Council, Arctic. „The Arctic Council: A Quick guide.“ <https://arctic-council.org/about/>.
- The Arctic Council, “A Quick guide”, <https://arctic-council.org/about/>, Accessed 06.11.2025.
- Downs, Erica. 2022. *China-Russia Energy Relations: Will New Oil and Natural Gas Deals Help Russia Weather Economic Sanctions?* Columbia University’s Center on Global Energy Policy.
- Edström, Anders. 2025. *Cutting Through Narratives on Chinese Arctic Investments*. Belfer Center for Science and International Affairs.
- Garamone, Jim. 2024. *Now the Hard Part: Implementing Arctic Strategy*. U.S department of war.
- Gladkov, Sergei. 2025. „Changes in economic cooperation between Russia and China since the start of the full-scale war in Ukraine.“
- Green, Chairman. 2023. „“The Alaskan Arctic Remains Strategically Vital”.“
- Hermann, Roberto Rivas. 2022. „Arctic transshipment hub planning along the Northern Sea Route: A systematic literature review and policy implications of Arctic port infrastructure.“ *Marine Policy* .
- Kimball, Jill. 2022. *Melting Arctic ice could transform international shipping routes, study finds*. brown univercity.
- LARUELLE, Marlène. 2020. *Russia’s Arctic Policy: A Power Strategy and Its Limits*. french institute of international relations.
- Malik, Ishfaq Hussain. 2025. „Arctic Warming: Cascading Climate Impacts and Global Consequences.“
- Molnia, Bruce F. 2023. *Documenting Arctic Sea Ice Dynamics with Global Fiducials Program Imagery*. US Geological Survey.
- Raikov, Yu.A. 2022. „Russia and the United States in the Arctic: from Competition to Confrontation.“ *Herald of the Russian Academy of Sciences*.
- service, congressional research. 2025. *Changes in the Arctic: Background and Issues for Congress* . U.S. Congress.
- „UNCLOS.“ *ARCTIC PORTAL.org*. <https://arcticportal.org/shipping-portlet/governance/unclos>.

MODERN WARFARE AND THE ROLE OF EMERGING TECHNOLOGIES

Nikoloz Vardia

The Junker of a Bachelor's Degree (Aeronautical Engineering) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Davit Jabishvili

The Junker of a Bachelor's Degree (Aeronautical Engineering) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The rapid evolution of emerging and disruptive technologies (EDTs) is fundamentally reshaping the nature, conduct, and strategic logic of modern warfare. Contemporary conflict is no longer confined to traditional physical domains; it now unfolds across integrated landscapes spanning land, sea, air, cyberspace, and outer space. Artificial intelligence, autonomous systems, unmanned platforms, cyber operations, and satellite-based communication networks have become core instruments of military power, enabling states to project force with greater precision, informational awareness, and operational efficiency. These technologies have accelerated the tempo of decision-making, enhanced surveillance and reconnaissance capabilities, and introduced new forms of strategic competition that transcend conventional battlefield boundaries.

However, the strategic advantages offered by emerging technologies are accompanied by significant ethical, legal, and security challenges. Cyber warfare blurs distinctions between peace and conflict, often unfolding in the gray zone beneath the threshold of open hostilities. Autonomous weapon systems raise questions regarding accountability, human oversight, and compliance with international humanitarian law. Meanwhile, the militarization of space and the reliance on dual-use digital infrastructure amplify the risks of miscalculation, escalation, and systemic disruption. As geopolitical competition intensifies, states must simultaneously innovate technologically while developing robust governance frameworks that uphold humanitarian principles, safeguard civilian populations, and maintain strategic stability.

This article argues that the defining challenge of twenty-first-century warfare lies not merely in acquiring advanced technologies, but in integrating them responsibly within legal, ethical, and cooperative international structures. The future of global security will depend on sustaining meaningful human control, enhancing transparency, and promoting collective norms that ensure technological innovation contributes to stability rather than conflict.

Keywords: Modern warfare; emerging technologies; artificial intelligence (AI); cyber warfare; robotics; satellite systems; global security; ethics; governance; international cooperation; accountability.

Introduction

Modern Warfare and the Role of Emerging Technologies

Modern warfare is undergoing a profound and systemic transformation driven by the rapid evolution of emerging and disruptive technologies (EDTs) and the growing interdependence between digital and physical domains of security. The traditional distinctions between military environments—land, sea, air, cyber, and space—are increasingly blurred, giving rise to a hybrid and multi-domain operational ecosystem. In this new paradigm, information dominance, technological adaptability, and digital resilience have become as critical to victory as firepower or troop strength.

The integration of advanced technologies has revolutionized every dimension of warfare—from battlefield tactics and logistics to the ethical, legal, and institutional frameworks that govern the use of force. Conflicts today are no longer fought solely through conventional military engagements but through networks, algorithms, and data flows, where strategic advantage depends on the ability to collect, analyze, and act upon information faster than the adversary.

Technological innovation has thus emerged as a decisive multiplier of military power. Tools such as artificial intelligence (AI), autonomous weapons systems, cyber warfare capabilities, quantum computing, and satellite-based communications are redefining the boundaries of deterrence, surveillance, and precision engagement. The convergence of these technologies enables unprecedented operational speed and coordination across domains, creating what strategists increasingly refer to as the “algorithmic battlefield.”

Yet, these same innovations also produce new layers of vulnerability and strategic uncertainty. The automation of warfare challenges long-standing norms of human oversight and accountability; autonomous systems risk blurring the line between combatant and civilian; and the militarization of information threatens the integrity of political processes and societal stability. As the barriers to technological access diminish, the diffusion of these capabilities among non-state actors, private military companies, and smaller states further complicates global security dynamics, eroding traditional power hierarchies and deterrence models.¹

Moreover, the ethical, legal, and geopolitical implications of emerging military technologies have become subjects of urgent debate. The absence of universally accepted norms governing AI-driven targeting, cyber operations, and space-based assets heightens the risk of escalation and miscalculation. The militarization of the digital and outer-space domains, coupled with growing cyber dependencies, demands renewed attention to international humanitarian law (IHL), rules of engagement, and confidence-building measures (CBMs) in both traditional and emerging security forums. In this evolving context, the character of warfare in the twenty-first century is increasingly defined by technological interconnectivity and strategic complexity. Success now depends not only on material capabilities but also on a state’s capacity to innovate, integrate, and govern technology responsibly.

This section therefore explores the major technological pillars shaping contemporary conflict, focusing on three interrelated domains: Artificial Intelligence and Automation, which enhance operational precision and speed but challenge human control; Cyber Warfare and Information Secu-

¹ I. Danilin *Emerging Technologies and Their Impact on International Relations and Global Security*. Hoover Institution, Stanford University. (2018).

rity, which redefine conflict boundaries through invisible yet destructive means; and the Emerging Information Security Paradigm, which underpins all modern defense architectures and determines resilience in an era of constant digital confrontation.

Through this multidimensional analysis, the study seeks to illuminate how technology—while serving as a driver of strategic advantage—simultaneously transforms the moral, legal, and geopolitical foundations of global security.

Main Part

Artificial Intelligence and Automation in Warfare

Artificial intelligence (AI) has emerged as a pivotal driver of twenty-first-century military transformation, reshaping the speed, scale, and character of warfare. Modern defense systems increasingly rely on machine learning algorithms, predictive analytics, and automated decision-support frameworks to interpret battlefield environments and execute strategic and tactical actions. These technologies enable military organizations to process massive streams of real-time data, identify hostile activity, and anticipate outcomes with a level of operational foresight that would be unattainable through human cognition alone.²

AI-enhanced Intelligence, Surveillance, and Reconnaissance (ISR) capabilities represent one of the most significant advancements. By integrating inputs from satellites, unmanned aerial vehicles (UAVs), electronic sensors, cyber monitoring tools, and open-source intelligence platforms, AI systems create a multi-layered and continuous picture of the battlespace. This fused situational awareness allows commanders to respond swiftly to emerging threats, optimize troop deployments, and coordinate multi-domain operations with unprecedented efficiency.

In parallel, the proliferation of autonomous and semi-autonomous platforms has begun to redefine force projection and operational endurance. Unmanned aerial and ground systems can perform reconnaissance, target acquisition, logistics resupply, and even direct combat duties, significantly reducing the risk to human personnel. Notably, the conflicts in Russia–Ukraine and Nagorno-Karabakh have illustrated how AI-supported drones—capable of autonomous navigation and adaptive targeting—can change battlefield dynamics by accelerating decision cycles and complicating traditional defense strategies. Likewise, U.S. initiatives such as the Joint All-Domain Command and Control (JADC2) program seek to build a fully networked combat environment where every sensor and shooter is linked through AI-driven communication and targeting protocols. Yet, the accelerated adoption of AI and automated weapons raises profound ethical, operational, and legal challenges. Delegating life-and-death decisions to algorithms risks eroding meaningful human control, while biased training data, system malfunctions, or cyber manipulation could result in unlawful or disproportionate harm. The possibility of fully autonomous lethal systems—capable of selecting and engaging targets without human oversight—intensifies debates over accountability and the preservation of international humanitarian norms.

For these reasons, defense strategists emphasize the importance of maintaining a “human-in-the-loop” or at minimum a “human-on-the-loop” approach, ensuring that critical decision-making

² European External Action Service (EEAS). Defence Tech Innovations Forum: Shaping the Future of Military Technology. (2025).

remains grounded in human judgment. Responsible integration of AI therefore requires not only technological proficiency but also transparent regulatory frameworks, rigorous testing standards, and international governance mechanisms aimed at preventing escalation and misuse. Ultimately, the evolution of AI and automation in warfare offers both strategic advantages and destabilizing risks. The challenge for contemporary security policy is to harness these capabilities in ways that enhance defense and deterrence, while safeguarding ethical principles and global stability.³

Cyber Warfare and Information Security

Cyber warfare has developed into one of the most decisive non-kinetic arenas of modern conflict, where battles are fought not over territory, but over data, networks, and the integrity of information systems. In this domain, critical infrastructure—such as energy grids, water systems, telecommunications networks, and financial platforms—becomes a primary target. Cyber operations can disable government services, corrupt military communications, or disrupt civilian life, producing strategic effects comparable to kinetic strikes, yet without deploying traditional armed force.

Unlike conventional warfare, cyber conflict often unfolds in the gray zone between peace and open hostilities. Operations are frequently covert, deniable, and asymmetrical; relatively weak actors can inflict disproportionate harm on more powerful adversaries. This dynamic allows states to pursue geopolitical objectives while avoiding the political costs associated with visible escalation. The Russia–Ukraine conflict provides a vivid illustration: coordinated cyberattacks on satellite communication networks, government portals, and energy facilities accompanied conventional military actions, aiming to degrade command-and-control systems and erode public morale. Similar patterns have been observed in Iranian–Israeli cyber exchanges targeting ports, fuel distribution networks, and industrial control systems.

Because digital systems underpin nearly all aspects of national security and governance, information security has become a foundational pillar of defense strategy.⁴ Governments are expanding dedicated cyber commands, developing rapid incident-response capabilities, and integrating cyber defense into joint military doctrine. Equally important, the private sector—particularly cloud service providers, cybersecurity firms, telecommunications companies, and social media platforms—plays a central role in detecting threats, defending networks, and managing digital infrastructure. This state–private security interdependence blurs traditional boundaries of responsibility, requiring new models of public–private cooperation and shared accountability.⁵

Cyber warfare also poses complex challenges in attribution, deterrence, and escalation management. Because attackers can route operations through global networks or employ proxy groups, identifying the true origin of an attack may be difficult or deliberately ambiguous. This strategic opacity complicates proportional response planning and increases the risk of unintended escalation, especially when cyber incidents affect nuclear command systems, early warning networks,

3 I. I. Danilin, *Emerging Technologies and Their Impact on International Relations and Global Security*. Hoover Institution, Stanford University. (2018).

4 GOV.UK. *Defence Artificial Intelligence Strategy*. Ministry of Defence(2022).

5 European External Action Service (EEAS). *Defence Tech Innovations Forum: Shaping the Future of Military Technology*. (2025).

or critical infrastructure. To reduce such risks, scholars and policymakers advocate developing international cyber norms, transparency mechanisms, and confidence-building measures (CBMs) to clarify acceptable behavior in cyberspace and establish channels for crisis communication.

Ultimately, cyber dominance has become a key determinant of strategic power in the twenty-first century. Military and political success increasingly depends on the ability to protect digital assets, exploit adversary vulnerabilities, conduct secure information operations, and maintain resilience in the face of persistent cyber threats. The shifting battlespace from physical to digital domains underscores a fundamental reality: control of information is now as vital to national security as control of territory.

Unmanned Systems, Robotics, and Space Technologies

Unmanned systems and military robotics have rapidly moved from experimental platforms to indispensable assets in contemporary warfare. Their deployment reflects a strategic shift toward reducing human exposure, increasing operational persistence, and improving tactical precision in multi-domain environments. These systems operate in the air, on land, at sea, and even underwater, supporting missions ranging from reconnaissance and logistics to target acquisition and direct engagement.

Unmanned Aerial Vehicles (UAVs) remain the most widely used and strategically impactful category. From high-altitude long-endurance drones like the U.S. MQ-9 Reaper to commercially modified quadcopters used in Ukraine, UAVs provide real-time intelligence, perform precision strikes, and support battlefield surveillance. Their effectiveness lies in a combination of range, maneuverability, and operational flexibility, allowing states and non-state actors to project power without risking pilot casualties. The recent Armenia–Azerbaijan conflict in Nagorno-Karabakh demonstrated how swarm tactics and loitering munitions (often referred to as “kamikaze drones”) can neutralize armored units and air defenses, altering traditional calculations of battlefield superiority.

Ground and maritime robotics are also advancing. Unmanned ground vehicles (UGVs) support mine clearance, logistics transport, and casualty evacuation, while unmanned surface and underwater systems (USVs/UUVs) enhance maritime surveillance and coastal defense. These technologies are particularly valuable in contested or hazardous environments where human access is limited or dangerous.

Robotics development increasingly converges with advances in AI, enabling autonomous navigation, adaptive targeting, and real-time threat analysis. As autonomy matures, military planners envision integrated human–machine teaming, where soldiers collaborate with robotic systems to amplify situational awareness and tactical effectiveness. For example, swarm robotics—collective robotic behavior inspired by biological systems—could overwhelm adversary defenses by saturating sensor networks and diverting countermeasures.

The Strategic Importance of Space Technologies

Space has become a core operational domain in modern defense, underpinning nearly every aspect of command, control, communication, navigation, and surveillance (C3NS). Satellite constellations enable secure communication channels, GPS guidance for precision weaponry, and global monitoring of maritime and troop movements. Consequently, military operations are now inseparable from secure and resilient access to orbital infrastructure. The proliferation of public-private space partnerships has accelerated the pace of innovation. Commercial actors increasingly design, launch, and manage satellite networks, providing governments with rapid access to advanced space capabilities. For instance, during the Russia–Ukraine war, commercial satellite imagery and Starlink-based communication networks played a pivotal role in sustaining Ukrainian military operations and civilian resilience. This marks a notable shift: strategic deterrence is no longer exclusively state-controlled.⁶

As space systems gain strategic significance, so too does competition for space dominance. Major powers are developing anti-satellite (ASAT) weapons, orbital electronic warfare tools, and cyber systems capable of disrupting space-based services. The threat of deliberate or accidental satellite interference heightens concerns about escalation, signal misinterpretation, and global infrastructure disruption.

Given these risks, the international community faces increasing pressure to establish space governance regimes that limit militarization and ensure secure, sustainable access to orbital resources. The development of norms, transparency measures, and crisis communication mechanisms will be essential to preventing space from becoming the next uncontrollable arena of conflict.

Ethical and Legal Considerations

As military technology evolves at an unprecedented pace, the moral, legal, and philosophical questions surrounding its use become increasingly complex. The proliferation of autonomous weapons systems, surveillance-driven artificial intelligence, precision-guided unmanned platforms, and offensive cyber tools presents novel ethical dilemmas that challenge long-established norms governing warfare, accountability, and human rights. The integration of algorithms into strategic and tactical decision-making raises fundamental concerns regarding autonomy, proportionality, discrimination between combatants and non-combatants, and compliance with the principles of international humanitarian law (IHL) and the Law of Armed Conflict (LOAC).

A central debate concerns the possibility of lethal autonomous weapon systems (LAWS)—machines capable of identifying, selecting, and engaging targets without direct human oversight. Proponents argue that autonomous systems may reduce civilian casualties by reacting faster than humans, operating without emotional bias, and functioning effectively under conditions of stress or fatigue. Critics, however, warn that delegating life-and-death authority to algorithms risks eroding meaningful human control and undermines the moral responsibility that underpins lawful military conduct. In the absence of clear attribution, accountability becomes diffused: if an autonomous system causes unlawful harm, responsibility may be ambiguous—potentially dispersed among software developers, defense contractors, military commanders, and state authorities.

⁶ GOV.UK. Defence Artificial Intelligence Strategy. Ministry of Defence. (2022).

Surveillance-enabled AI technologies similarly complicate discussions of privacy, data protection, and civil liberties. Expansive monitoring capacities, biometric recognition tools, and predictive intelligence algorithms can support national defense and counterterrorism efforts; yet, they may also facilitate intrusive state surveillance, political repression, or discrimination against vulnerable populations. These risks highlight the need for robust legal safeguards, transparent oversight mechanisms, and democratic scrutiny of military AI applications.

Cyber warfare introduces additional legal ambiguity. Unlike physical attacks, cyber operations often occur below the threshold of armed conflict, making it difficult to determine when IHL applies. Questions persist regarding the legality of targeting civilian infrastructure—such as hospitals, energy grids, or financial systems—when these networks serve dual civilian and military functions. Furthermore, the difficulty of attributing cyberattacks complicates the enforcement of accountability and the application of proportional response measures. Strategic ambiguity in cyberspace increases the risk of escalation and may weaken traditional deterrence frameworks.⁷

These challenges underscore the need for international regulatory frameworks capable of addressing emerging technologies while respecting state sovereignty and security concerns. Multilateral negotiations within the United Nations Convention on Certain Conventional Weapons (CCW), regional security dialogues, and confidence-building measures (CBMs) have begun to articulate norms regarding autonomous systems and cyber operations.⁸ However, progress remains slow, fragmented, and politically contested. Technological innovation is advancing far more rapidly than international law. Therefore, ensuring the ethical and lawful integration of emerging military technologies requires a layered approach:

Maintaining meaningful human control in the use of force; Strengthening oversight, transparency, and public accountability in defense procurement and deployment; Developing shared international norms and verification regimes to govern AI, robotics, and cyber weapons; Embedding human rights and humanitarian principles into system design from inception.

Ultimately, the challenge is not solely technical, but profoundly human. Technological superiority must not come at the cost of fundamental ethical values. Preserving human dignity, safeguarding civilian life, and upholding the rule of law remain essential obligations—regardless of how the character of warfare evolves.⁹

Conclusion

Modern warfare is defined not only by the physical capabilities of armed forces, but increasingly by the speed, adaptability, and sophistication of technological innovation. Emerging technologies have reshaped the strategic environment, expanding conflict into new domains—cyber, space, and the electromagnetic spectrum—while enhancing the precision, reach, and autonomy of military systems. Artificial intelligence, unmanned platforms, networked surveillance systems, and satellite-based communications have become critical enablers of contemporary defense operations, reinforcing the principle that information superiority and technological integration are now

⁷ PwC Strategy&. The Global AI Race and Defence's New Frontier: Navigating the AI Revolution in Defence. (2025).

⁸ World Economic Forum (WEF). Eight Emerging Technologies Transforming International Security. (2015).

⁹ PwC Strategy&. The Global AI Race and Defence's New Frontier: Navigating the AI Revolution in Defence. (2025).

central determinants of military power.¹⁰

However, these advances have also generated new vulnerabilities and systemic risks. The digitization of command-and-control infrastructures exposes national defense systems to cyber intrusion, sabotage, and algorithmic manipulation. The increasing reliance on autonomous and semi-autonomous systems introduces the danger of unintended escalation, accidental engagement, or system malfunction under conditions of stress or adversarial interference. Meanwhile, the blurring of civilian and military infrastructures—particularly in cyberspace and satellite communications—complicates both the ethical and legal dimensions of warfare, as civilian populations become more directly exposed to the consequences of digital conflict.

The challenges posed by emerging military technologies therefore cannot be addressed solely through technological countermeasures or strategic posturing. They require a comprehensive governance approach that combines legal regulation, ethical oversight, and multilateral cooperation. The existing frameworks of international humanitarian law (IHL), while foundational, must be adapted to account for algorithmic decision-making, autonomous targeting processes, cyber operations below the threshold of armed conflict, and dual-use technologies that blur traditional categories of combatant, target, and battlefield.

At the same time, global technological asymmetries risk widening the divide between technologically advanced military powers and states with limited resources or digital resilience. This imbalance may intensify geopolitical rivalries, fuel arms races in emerging technology fields, and increase the likelihood of proxy conflicts where advanced military systems are deployed indirectly. As a result, the governance of emerging technologies is inseparable from the governance of international stability itself. Thus, the role of emerging technologies in modern warfare is double-edged. On one hand, these technologies promise increased precision, reduced troop casualties, improved surveillance, and more effective deterrence. On the other, they raise unparalleled questions about accountability, sovereignty, legality, and humanity in conflict. The future of military power will belong to states that not only achieve technological superiority, but also develop the institutional, legal, and ethical frameworks necessary to ensure that innovation serves stability rather than destruction.

In this evolving landscape, the defining challenge of twenty-first-century warfare is not simply how advanced technologies are developed or deployed, but how human judgment, democratic control, and international law are preserved amid rapid automated decision-making and increasingly complex battlespaces. Ensuring that technology enhances rather than erodes global security will require a sustained commitment to transparency, restraint, and cooperative governance.

Modern warfare is therefore at a crossroads. The choices made today—regarding regulation, ethics, research priorities, and strategic doctrine—will determine whether emerging technologies become tools of stability and deterrence, or drivers of instability and conflict. The future of global security will depend not only on technological innovation, but on the wisdom and responsibility with which it is guided.

¹⁰ European External Action Service (EEAS). Defence Tech Innovations Forum: Shaping the Future of Military Technology. (2025).

Bibliography

- Danilin, I. Emerging Technologies and Their Impact on International Relations and Global Security. Hoover Institution, Stanford University. (2018).
- GOV.UK. Defence Artificial Intelligence Strategy. Ministry of Defence. (2022).
- European External Action Service (EEAS). Defence Tech Innovations Forum: Shaping the Future of Military Technology. (2025).
- PwC Strategy&. The Global AI Race and Defence's New Frontier: Navigating the AI Revolution in Defence. (2025).
- World Economic Forum (WEF). Eight Emerging Technologies Transforming International Security. (2015).

SHAPING THE FUTURE OF SECURITY THROUGH DEFENSE INNOVATION AND INTERNATIONAL COLLABORATION

Gigi Chaligava

The Junker of a Bachelor's Degree (Mechanical Engineering) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Temo Atsanelidze

The Junker of a Bachelor's Degree (Aeronautical Engineering) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

This article examines how defence innovation and international partnerships jointly redefine the architecture of global security. In an era marked by the rapid evolution of emerging and disruptive technologies (EDTs), renewed great-power competition, and transnational threats, national defence strategies increasingly depend on collaboration, technological adaptation, and interoperability. The hypothesis is that sustained innovation coupled with institutionalized international partnerships enhances collective defence effectiveness by accelerating capability development, reducing costs, and shaping global norms for the ethical use of advanced military technologies. The study argues that the future of deterrence and warfare depends not merely on technological superiority but on the speed and coherence of multinational cooperation. Examples from NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), AUKUS, and the EU Defence Innovation Office demonstrate how innovation ecosystems and allied networks can drive both technological and strategic resilience. However, challenges—including intellectual property protection, bureaucratic divergence, and balancing strategic autonomy—must be addressed through transparent frameworks and adaptive governance. The research concludes that innovation provides the technological tools for defence, but partnership provides the stability and scalability essential for security in a multipolar world.

Keywords: Defence Innovation, International Partnership, Emerging and Disruptive Technologies, Interoperability, Strategic Autonomy, AUKUS, NATO DIANA

Introduction

The security landscape of the twenty-first century is undergoing an unprecedented and multi-dimensional transformation, driven by the rapid diffusion of emerging and disruptive technologies (EDTs) and the reconfiguration of global power dynamics. Technologies such as artificial intelligence (AI), hypersonic weapons, autonomous systems, and quantum computing are not only revolutionizing the conduct of warfare but also reshaping the very nature of deterrence, defence planning, and strategic competition. These innovations have blurred the line between conventional and unconventional conflict, fusing kinetic power with digital, informational, and cognitive domains.¹

Amid this technological acceleration, great-power competition—most visibly among the United States, China, and Russia—has reintroduced a near-peer strategic environment reminiscent of the Cold War, yet vastly more complex and interconnected. The proliferation of dual-use technologies, coupled with intensified geopolitical rivalry, has expanded the scope of competition into cyberspace, outer space, and the electromagnetic spectrum. Meanwhile, regional conflicts—most notably the Russia–Ukraine War—demonstrate in real time how technological superiority, innovation ecosystems, and multinational defence partnerships directly shape battlefield outcomes. The operational use of drones, satellite networks, and AI-driven intelligence in Ukraine has illustrated the decisive influence of collaborative technological adaptation on the tempo and outcome of modern conflict. In this evolving context, traditional notions of sovereign defence sufficiency are increasingly untenable. Except for a handful of global powers with comprehensive industrial and technological bases, no single state can independently sustain the cost, speed, and complexity required for next-generation capability development. Small and medium powers, therefore, must strategically combine domestic innovation with international cooperation, knowledge sharing, and joint R&D frameworks to preserve relevance within collective defence architectures such as NATO, AUKUS, and other multilateral alliances. This paper seeks to examine the role of defence innovation and partnership integration as key determinants of strategic competitiveness in the emerging security order. It is guided by the following analytical framework:

Research Question (RQ): Can the integration of defence innovation and international partnerships increase collective defence effectiveness by at least 30% in capability generation speed and operational interoperability across allied forces?

Hypothesis (H): Defence innovation, when combined with structured international partnership frameworks, accelerates capability development timelines by 25–40% and enhances interoperability and resilience metrics by approximately 30% compared to unilateral national efforts. By addressing these propositions, the study aims to contribute to the academic and policy discourse on how innovation ecosystems, technological collaboration, and alliance-based defence integration can together shape a more agile, interoperable, and resilient global security architecture in the age of disruptive technologies.

¹ Accenture. (2024). Securing strategic advantage for defense companies. Retrieved from <https://surl.li/bggpuf>, Accessed 06.11.2025.

Main Part

The Innovation Imperative: Transforming the Character of Warfare

Technological innovation has emerged as the new currency of military power, redefining the parameters of strategic advantage and transforming the very character of warfare. Emerging and Disruptive Technologies (EDTs)—including artificial intelligence (AI), quantum computing, hypersonic systems, autonomous robotics, and advanced data analytics—are not mere incremental enhancements to existing capabilities; they represent paradigm shifts that alter the speed, scope, and structure of combat operations.² These technologies reshape the principles of deterrence, operational planning, and decision-making, rendering traditional doctrines of mass and attrition increasingly obsolete.

In the digitalized battlespace, victory is no longer determined primarily by numerical superiority or firepower but by the capacity to process, analyse, and act upon information faster and more accurately than an adversary. The “decision-to-action” cycle—once measured in hours or days—has been compressed to mere seconds in technologically advanced operations. This temporal compression enables near-instantaneous detection, targeting, and engagement, creating what strategists describe as a “cognitive edge” in warfare. Information dominance has thus supplanted industrial capacity as the principal determinant of military effectiveness.

The innovation imperative extends beyond the acquisition of new technologies; it demands the integration of digital ecosystems, inter domain interoperability, and human–machine teaming across all levels of defence. Militaries capable of harnessing data-driven decision-making and autonomous platforms are redefining the threshold of operational superiority. As the global balance of power becomes increasingly dependent on innovation, nations that fail to adapt risk strategic marginalization and vulnerability to technologically advanced adversaries.³

Artificial Intelligence and Autonomy

At the core of this transformation lies artificial intelligence (AI)—a technology that enables predictive analytics, autonomous decision-making, and real-time data fusion across all operational domains: land, air, maritime, cyber, and space. AI functions as a force multiplier, exponentially expanding the capacity of commanders to interpret vast streams of data, anticipate threats, and coordinate multi-domain responses with precision and speed. AI-driven Intelligence, Surveillance, and Reconnaissance (ISR) systems now process petabytes of sensor data in real time, detecting patterns and anomalies that would remain invisible to human analysts at operational speed. These systems enhance situational awareness, accelerate the targeting cycle, and allow militaries to maintain persistent intelligence coverage over large and dynamic areas of operation. Moreover, AI supports autonomous decision assistance, integrating battlefield data into command algorithms that suggest optimal responses under time-critical conditions.⁴

² European External Action Service (EEAS). Defence Tech Innovations Forum: Shaping the Future of Military Technology. (2025).

³ Danilin, I. Emerging Technologies And Their Impact On International Relations And Global Security. Hoover Institution, Stanford University. (2018).

⁴ Accenture. (2024). Securing strategic advantage for defense companies. Retrieved from <https://surl.li/ytzour>. Accessed 06.11.2025.

The operational potential of AI is best illustrated through real-world applications. In the Russia–Ukraine War, Ukraine’s integration of AI-enhanced reconnaissance systems, automated artillery correction, and precision-guided drones has demonstrated the decisive combat advantages of rapid decision loops and adaptive targeting. Likewise, the United States’ Joint All-Domain Command and Control (JADC2) initiative seeks to build an AI-enabled command infrastructure linking sensors, shooters, and decision-makers across domains. This networked approach aims to shorten the decision-making cycle, synchronize joint operations, and ensure that information flows seamlessly between allied systems—a model increasingly viewed as the future of collective defence.

Beyond tactical applications, AI also underpins advances in autonomous systems, including drone swarms, robotic combat vehicles, and unmanned maritime platforms. These technologies extend operational reach, perform high-risk missions, and reduce human exposure to danger. The development of collaborative autonomous systems, capable of coordinating among themselves with minimal human input, represents a major step toward distributed and adaptive combat architectures. However, the growing autonomy of such systems raises significant ethical and strategic concerns. As decision-making authority shifts from humans to algorithms, questions of accountability, proportionality, and reliability become central to military ethics and international law. The challenge, therefore, lies not only in advancing AI’s technical sophistication but also in ensuring human oversight, transparency, and moral responsibility within increasingly automated defence systems.

Dual-Use Technology and Civil-Military Fusion

A defining feature of modern defence innovation is the **dual-use revolution**. The commercial technology sector—particularly AI, space, and cyber—outpaces government R&D spending. Companies like SpaceX, Palantir, and Anduril have become critical defence enablers. This dynamic creates opportunities for defence institutions to harness private-sector innovation but also challenges traditional procurement processes. To remain competitive, defence ministries must cultivate “innovation ecosystems” linking academia, SMEs, and tech industries. NATO’s **DIANA** initiative and the **EU Defence Innovation Office** exemplify this collaborative model, supporting start ups and ensuring that innovations transition from lab to field within 12–24 months, compared to traditional 5–10 year cycles.⁵

The Strategic Imperative of International Partnerships: Cost and Risk Sharing

In the twenty-first-century security environment, marked by the proliferation of Emerging and Disruptive Technologies (EDTs) and intensifying great-power competition, the strategic imperative of international partnerships has evolved from a matter of political convenience into a structural necessity. The scale, complexity, and uncertainty of modern defence innovation demand collective approaches to capability development. Technologies such as artificial intelligence (AI), quantum computing, hypersonic propulsion, directed-energy systems, and autonomous robotics are reshaping the operational environment at such a pace that no state—regardless of its economic

⁵ European External Action Service (EEAS). Defence Tech Innovations Forum: Shaping the Future of Military Technology. (2025).

or industrial strength—can maintain technological primacy in isolation. ⁶The financial and technical burden of research, development, testing, and deployment in this new era is staggering. The cost of developing a single fifth-generation aircraft platform, for instance, can exceed that of entire national defence budgets of mid-sized countries. As a result, even major powers like the United States, China, and Russia have increasingly sought partnerships, subcontracting networks, and knowledge alliances to offset costs and accelerate innovation. For small and medium-sized states, partnerships have become a strategic equalizer—providing access to technologies, expertise, and supply chains that would otherwise be unattainable.⁷

Cost and Capability Sharing in Defence Innovation

Modern defence innovation follows the logic of the globalized technology economy: collaboration lowers costs, disperses risks, and enhances scalability. The pooling of resources enables nations to share the financial weight of high-risk research while simultaneously broadening the technological knowledge base. Joint R&D initiatives—such as the NATO Science and Technology Organization (STO) and the European Defence Fund (EDF)—embody this collaborative logic by bringing together public institutions, private industries, and research centres across multiple jurisdictions. These partnerships not only distribute the burden of innovation but also cultivate collective resilience by ensuring redundancy and interoperability within allied forces. The F-35 Joint Strike Fighter Program is perhaps the most illustrative case of multinational cost and risk sharing in modern defence procurement. Encompassing partners from North America, Europe, and Asia-Pacific, it demonstrates how international cooperation can synchronize industrial capabilities, integrate supply chains, and distribute technological dividends across multiple economies. Similarly, the AUKUS partnership—uniting Australia, the United Kingdom, and the United States—embodies a strategic commitment to shared technological development in advanced undersea and cyber capabilities. These cooperative frameworks underline a central reality: the cost of isolation now outweighs the risks of interdependence.

Risk Mitigation and Strategic Insurance

Defence innovation is inherently uncertain. Technologies such as hypersonic propulsion, AI-enabled command systems, or quantum communication carry not only financial but also strategic and ethical risks. Joint investment reduces exposure to the volatility of single-state failure while providing an insurance mechanism against technological stagnation or geopolitical disruption. Collective programs also create redundancy in production and testing capabilities, reducing dependence on vulnerable supply chains and minimizing exposure to coercive economic or cyber measures by adversarial powers. Moreover, risk sharing in defence partnerships has a stabilizing effect on international security relations. It institutionalizes interdependence, making partners mutually invested in maintaining stability and deterring unilateral escalation. Shared innovation

⁶ R., Karp, & Maass, R. (Eds.). *Alliances and Partnerships in a Complex and Challenging Security Environment* (Compendium). NATO Allied Command Transformation (ACT) and Old Dominion University. (2024).

⁷ I. Danilin, *Emerging Technologies And Their Impact On International Relations And Global Security*. Hoover Institution, Stanford University. (2018).

therefore becomes a form of preventive diplomacy, binding nations through common strategic objectives, industrial cooperation, and synchronized military planning.⁸

Challenges to Collaborative Defence Innovation

Yet, while the logic of cooperation is compelling, the execution of multinational defence programs remains fraught with complexity. Divergent national interests, asymmetric funding capabilities, and inconsistent export-control regimes often complicate governance structures. Disputes over intellectual property (IP) rights, technology transfer restrictions, and security classification can hinder collaboration and erode trust among partners.⁹ Additionally, bureaucratic inefficiencies and overlapping procurement processes can delay project timelines and increase costs—the very outcomes such partnerships are designed to avoid. To overcome these barriers, participating states must establish transparent governance mechanisms, equitable cost-sharing formulas, and harmonized procurement standards. The creation of multinational oversight boards, independent audit systems, and performance-based funding models could enhance accountability and efficiency. Furthermore, aligning industrial policy with collective defence goals—through targeted subsidies, co-investment schemes, and shared testing infrastructure—can sustain long-term technological cooperation and prevent national fragmentation of effort.

The Geo economic Dimension: Alliances as Innovation Ecosystems

Modern alliances are increasingly functioning as innovation ecosystems, where states, private industries, and academic institutions converge to co-develop dual-use technologies. Initiatives such as NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) and the European Defence Innovation Scheme (EDIS) embody this shift, fostering public-private collaboration across borders. These frameworks enable smaller nations to participate in the defence industrial base through niche specialization—such as cybersecurity, advanced materials, or autonomous platforms—thereby broadening the collective technological footprint of the alliance. Such networks not only strengthen interoperability but also act as geo economic instruments, shaping supply-chain resilience and technological sovereignty. By coordinating standards and safeguarding intellectual assets, alliances mitigate the risk of technological leakage to strategic competitors while reinforcing collective economic security.

Shaping Global Norms and Ethical Governance

The accelerating integration of emerging and disruptive technologies (EDTs) into defence systems presents not only opportunities for enhanced security and operational efficiency but also profound ethical, legal, and strategic dilemmas. As artificial intelligence (AI), autonomous systems, and cyber capabilities evolve, they challenge traditional frameworks of warfare, sovereignty, and human accountability. The ability of machines to make or influence lethal decisions, the potential for algorithmic bias in targeting systems, and the opacity of AI-driven decision-making processes

⁸ GOV.UK. Defence Artificial Intelligence Strategy. Ministry of Defence. (2022).

⁹ R, Karp & Maass, R. (Eds.). Alliances and Partnerships in a Complex and Challenging Security Environment (Compendium). NATO Allied Command Transformation (ACT) and Old Dominion University. (2024).

all demand an urgent revaluation of how international law and moral responsibility apply in technologically enabled conflict.

In this context, international partnerships—particularly among democratic nations—have assumed a central role in shaping global norms and governance mechanisms for the responsible use of emerging military technologies. Cooperation among allies is not merely a matter of operational necessity; it is a strategic and ethical imperative to ensure that innovation in warfare remains consistent with the principles of humanity, proportionality, and accountability embedded in International Humanitarian Law (IHL) and the Law of Armed Conflict (LOAC). The creation and diffusion of ethical norms for technological warfare increasingly depend on collective governance frameworks. Initiatives such as the U.S.–EU Trade and Technology Council (TTC) represent pioneering platforms for aligning regulatory standards on AI, cybersecurity, and data protection. By establishing shared principles for AI development—transparency, fairness, and human oversight—the TTC and similar initiatives aim to prevent the militarization of algorithms without legal or moral constraint. These cooperative efforts reinforce the idea that the deployment of AI and autonomous systems must remain firmly under meaningful human control, ensuring that machines augment rather than replace human judgment in matters of life and death.

Beyond the transatlantic space, broader multilateral initiatives are emerging to address the ethical governance of military AI. The United Nations Group of Governmental Experts (GGE) on Lethal Autonomous Weapons Systems (LAWS) continues to deliberate on potential frameworks to prohibit or regulate fully autonomous weapons that operate without human intervention. Similarly, the OECD AI Principles and the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) have established foundational guidelines for transparency, accountability, and the prevention of harm in AI development—principles that are increasingly relevant to defence applications.

However, the formation of universal norms faces significant challenges. Divergent political systems and competing strategic interests often produce fragmented governance architectures, with authoritarian regimes prioritizing technological advantage over ethical restraint. This asymmetry risks creating a dual-track world order in which responsible AI practices coexist with opaque, unregulated military experimentation. To counterbalance this trend, democratic alliances must pursue normative leadership—leveraging their collective technological and institutional capacity to establish credible, enforceable standards that shape global behaviour.¹⁰

Moreover, the conference participants emphasized that ethical governance must be embedded not only in policy but in the technological design process itself. Integrating “ethics-by-design” principles—embedding moral reasoning, accountability mechanisms, and decision transparency directly into algorithmic architectures—can help ensure compliance with international law even in autonomous operations. This approach redefines governance as both a technical and moral discipline, bridging the gap between code and conscience. To institutionalize these efforts, partnerships among states, international organizations, and the private sector are crucial. Defence contractors, AI researchers, and military institutions must collaborate under shared ethical guidelines, subject

10 PwC Strategy&. The global AI race and defense’s new frontier: Navigating the AI revolution in defense, (2025).

to external oversight and transparency requirements. The development of AI verification regimes, modelled after existing arms-control mechanisms, could provide an additional layer of accountability and confidence-building among states.

Ultimately, shaping global norms for emerging defence technologies requires more than regulatory convergence—it demands a shared moral vision for the future of warfare. As technological superiority becomes increasingly intertwined with moral legitimacy, states that lead in establishing transparent, ethical governance structures will define not only the next generation of defence capabilities but also the normative architecture of global security. In this evolving landscape, ethical governance becomes a strategic asset, reinforcing trust among allies, legitimizing the use of new technologies, and preserving the humanitarian foundations of international law. Through multilateral cooperation, transparency, and an unwavering commitment to human oversight, the international community can ensure that technological progress strengthens peace, accountability, and global stability rather than eroding them.¹¹

Challenges in Collaborative Defence Innovation

While international defence partnerships are essential to sustaining innovation, accelerating capability development, and distributing costs and risks, they also generate strategic, bureaucratic, and normative challenges that complicate their implementation. The integration of multiple national defence systems, industries, and innovation cultures inevitably exposes friction points related to governance, intellectual property, operational standards, and strategic autonomy. Successful collaboration, therefore, depends not only on shared technological goals but also on the establishment of transparent, flexible, and trust-based frameworks capable of reconciling divergent national interests with collective strategic imperatives.¹²

Intellectual Property and Technology Transfer

At the heart of multinational defence collaboration lies the sensitive question of intellectual property (IP) rights, technology transfer, and information security. The exchange of classified or dual-use technologies across borders requires a high degree of trust and legal alignment—conditions that are often undermined by asymmetrical export control regimes and competing industrial interests. For example, the United States' International Traffic in Arms Regulations (ITAR), while designed to protect national security, frequently impose strict limitations on technology sharing with even close allies. These constraints can delay joint research and development (R&D) initiatives, restrict collaborative prototyping, and impede the integration of allied defence supply chains. Similarly, European Union member states face challenges in reconciling national export controls with the European Defence Fund (EDF) and Permanent Structured Cooperation (PESCO) frameworks, where technological sovereignty and market competition intersect. To overcome such barriers, states must develop “trusted innovation corridors”—secure, legally codified frameworks that enable controlled sharing of sensitive defence technologies under common security standards.

11 H. B. Rahmadi, , Armandha, S. T., & Sumari, A. D. W. (2024). Collaboration and Technology Transfer in the Defense Industry as Drivers of Innovation and Global Security Enhancement. *Physical Sciences, Life Science and Engineering*, 1(3), 12.

12 PwC Strategy&. (2025). The global AI race and defense's new frontier: Navigating the AI revolution in defense

These corridors would facilitate joint innovation hubs, classified R&D zones, and interoperable data environments, where research can progress within mutually verified confidentiality protocols. Enhanced digital safeguards, cybersecurity standards, and reciprocal IP protections could further strengthen confidence among partners, ensuring that collaborative innovation does not come at the expense of national security.¹³

Bureaucratic and Cultural Gaps

Another critical obstacle in collaborative defence innovation arises from bureaucratic inertia and cultural divergence among national defence establishments. Differences in organizational structure, procurement speed, strategic planning cycles, and risk tolerance often lead to inefficiencies that slow the pace of joint capability development. For instance, while the private technology sector operates within rapid innovation cycles, many defence ministries remain constrained by rigid procurement procedures, legacy systems, and hierarchical decision-making structures. Moreover, national defence cultures reflect distinct threat perceptions, operational doctrines, and civil-military relations, which complicate coordination in multinational projects. Aligning these disparate frameworks requires adaptive governance mechanisms, standardized project management procedures, and joint professional training programs aimed at cultivating mutual understanding. Initiatives such as NATO's Innovation Fund and Defence Innovation Accelerator for the North Atlantic (DIANA) exemplify early efforts to institutionalize such alignment by creating shared innovation spaces where military officers, technologists, and policymakers collaborate under unified principles of experimentation and agility.

Transforming transactional cooperation into strategic partnership ultimately depends on the development of institutional empathy—a shared culture of innovation that transcends bureaucratic silos and national boundaries. Building this culture requires sustained exchange programs, joint education initiatives, and the integration of civilian and military innovation ecosystems across the alliance. By embedding collaboration into organizational practice rather than treating it as a periodic necessity, partners can transform short-term cooperation into enduring strategic integration.¹⁴

Strategic Autonomy vs. Interdependence

A further and increasingly complex challenge in defence collaboration concerns the balance between strategic autonomy and interdependence. Deep cooperation in defence innovation, while enhancing efficiency and interoperability, may also create dependency risks by concentrating technological capabilities or supply chains within certain states or industrial clusters. For smaller and medium powers, excessive reliance on external partners can undermine operational sovereignty and reduce flexibility in national defence planning. Conversely, complete autonomy in the age of EDTs is economically and technologically unsustainable, given the astronomical costs and multidisciplinary expertise required to develop next-generation systems independently.¹⁵

The European Union's evolving defence architecture provides a vivid illustration of this ten-

13 World Economic Forum (WEF). 8 emerging technologies transforming international security. (2015).

14 Security Cooperation University (DSCU). Security Cooperation Conference Report: Building Lasting Partnerships: What Have We Learned? (2025).

15 Rahmadi, H. B., Armandha, S. T., & Sumari, A. D. W. (2024). Collaboration and Technology Transfer in the Defense Industry as Drivers of Innovation and Global Security Enhancement. *Physical Sciences, Life Science and Engineering*, 1(3), 12.

sion. Efforts such as the Strategic Compass (2022), PESCO, and the EDF emphasize the concept of “sovereign interoperability”—the ability to maintain independent national defence capabilities while ensuring full compatibility with allied systems and joint missions.¹⁶ This concept seeks to reconcile national control over critical technologies with alliance-wide integration, ensuring that cooperation enhances rather than erodes sovereignty. Achieving this balance requires a nuanced approach to industrial policy, supply-chain diversification, and regulatory harmonization. States must identify strategic technologies that warrant protection under national control (e.g., cryptography, AI algorithms, or nuclear propulsion) while promoting open collaboration in complementary domains. Multilateral governance mechanisms, such as technology safeguards agreements and joint export-control regimes, can help manage interdependence without constraining innovation.

Conclusion

Building a Resilient and Ethical Security Architecture

The convergence of defence innovation and international partnership defines the strategic trajectory of twenty-first-century global security. Modern warfare demonstrates with increasing clarity that success no longer depends on isolated strength but on collective adaptability, interoperability, and technological agility. The ongoing conflict in Ukraine, among other regional crises, has revealed that rapid innovation cycles—driven by unmanned systems, cyber defence, and AI-enabled targeting—become strategically decisive only when embedded within networks of international cooperation and shared technological ecosystems.

While multinational partnerships are now indispensable to sustaining technological advantage, they also expose a complex web of institutional, legal, and strategic challenges. Issues of intellectual property, technology transfer, bureaucratic inertia, and divergent national priorities frequently hinder the efficiency of collaboration. Balancing strategic autonomy with interdependence remains one of the most persistent dilemmas of modern defence policy: deep cooperation accelerates capability development but may create dependency risks, whereas excessive autonomy is increasingly unviable in an era of exponential technological growth. To navigate this paradox, alliances must evolve from coalitions of shared interests into ecosystems of shared innovation—structures that integrate research institutions, private industries, and defence establishments within transparent, trust-based governance frameworks. The future of security will depend on a deliberate synthesis of innovation, cooperation, and ethics. Building such a framework requires coordinated action across three interlocking dimensions:

Institutionalize Innovation: Nations must establish permanent innovation frameworks—such as defence accelerators, technology directorates, and cross-domain R&D centres—to sustain continuous modernization beyond crisis cycles. Institutionalizing innovation ensures that experimentation, adaptation, and capability development become enduring features of defence policy rather than reactive measures to immediate threats.

Deepen Partnerships: The transformation from ad hoc alliances to integrated defence-industrial ecosystems is essential. Effective collaboration must link governments, academia, and pri-

¹⁶ World Economic Forum (WEF). 8 emerging technologies transforming international security. (2015).

vate industry through shared investment platforms, interoperable standards, and joint operational testing environments. Initiatives such as AUKUS, NATO's DIANA, and the European Defence Fund exemplify how strategic partnerships can generate both technological resilience and political cohesion.

Lead Ethical Governance: Technological power without ethical restraint risks destabilizing the very order it seeks to defend. Democratic nations, in particular, bear a responsibility to shape global norms for emerging technologies through transparent, multilateral, and values-based governance. Frameworks such as the U.S.–EU Trade and Technology Council, the UN Group of Governmental Experts on Autonomous Weapons, and the OECD AI Principles should be strengthened to ensure that innovation aligns with international humanitarian law, accountability, and human oversight.

In an era of converging technological revolutions, the success of collective defence will not be determined solely by the sophistication of weapons systems but by the resilience, adaptability, and integrity of the partnerships that sustain them. A truly resilient security architecture must institutionalize collaboration, embed ethics within innovation, and balance sovereignty with shared responsibility.

Ultimately, the future of global stability depends on the capacity of nations to innovate responsibly together—to ensure that progress in defence technology serves peace, deters aggression, and upholds the moral foundations of international order. In this sense, the defence alliances of tomorrow will be measured not only by their deterrent strength but by their ability to translate technological power into collective security, ethical governance, and enduring stability.

Bibliography

- Accenture. (2024). Securing strategic advantage for defense companies. Retrieved from <https://surl.li/jjqakr>, Accessed, 06.11.2025
- Danilin, I. (2018). Emerging Technologies And Their Impact On International Relations And Global Security. Hoover Institution, Stanford University. Retrieved from, <https://surl.li/fgujxq>, Accessed, 06.11.2025
- European External Action Service (EEAS). (2025). Defence Tech Innovations Forum: Shaping the Future of Military Technology. Retrieved from, <https://surl.li/vcfbba>, Accessed, 06.11.2025
- GOV.UK. (2022). Defence Artificial Intelligence Strategy. Ministry of Defence. Retrieved from, <https://surl.li/zlfhga>, Accessed, 06.11.2025
- Karp, R., & Maass, R. (Eds.). Alliances and Partnerships in a Complex and Challenging Security Environment (Compendium). NATO Allied Command Transformation (ACT) and Old Dominion University. Retrieved from, (2024). <https://surl.li/wkyqic>, Accessed, 06.11.2025
- PwC Strategy&. (2025). The global AI race and defense's new frontier: Navigating the AI revolution in defense. PwC. Retrieved from, <https://surl.li/fmbjdf>, Accessed, 06.11.2025
- Rahmadi, H. B., Armandha, S. T., & Sumari, A. D. W. (2024). Collaboration and Technology Transfer in the Defense Industry as Drivers of Innovation and Global Security Enhancement. Physical Sciences, Life Science and Engineering, 1(3), 12. Retrieved from <https://surl.li/qkeqjt>, Accessed, 06.11.2025
- Security Cooperation University (DSCU). (2025). Security Cooperation Conference Report: Building Lasting Partnerships: What Have We Learned? Retrieved from, <https://surli.cc/dxrscq>, Accessed, 06.11.2025
- World Economic Forum (WEF). (2015). 8 emerging technologies transforming international security. Retrieved from, <https://www.weforum.org/publications/> Accessed, 06.11.2025

THE STRATEGIC ROLE OF DRONES IN MODERN MILITARY OPERATIONS

Lekso Kupatadze

The Junker of a Bachelor's Degree (Informatic Technologies) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Davit Davituri

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have fundamentally redefined the principles of modern military operations, merging rapid technological innovation with unprecedented strategic and tactical flexibility. These systems have transcended their initial roles to become force multipliers that allow armed forces to conduct complex missions—including intelligence, surveillance, and reconnaissance (ISR), precision strikes, electronic warfare, and logistical support—with a significantly reduced risk to human personnel. This paper provides a comprehensive analysis of the drone's evolution from simple remote-controlled aircraft to sophisticated, AI-enabled platforms, examining the core technologies that underpin their capabilities, such as autonomous control systems, advanced sensor suites, and secure data links. The study delves into the operational applications of UAVs through illustrative case studies from recent conflicts, including the Nagorno-Karabakh war and the ongoing Russia-Ukraine conflict, demonstrating their decisive impact in both asymmetric and conventional warfare. Furthermore, the research critically addresses the profound ethical, legal, and strategic dilemmas arising from drone proliferation, such as issues of sovereignty, accountability, and the changing thresholds for armed conflict. With a specific focus on the Georgian context, the paper evaluates the strategic imperative for smaller nations to integrate UAV technology into their defense postures. It analyzes Georgia's ongoing modernization efforts, its strategic partnerships for technology transfer, and the nascent development of a domestic innovation ecosystem. The conclusion posits that for Georgia, the strategic adoption and indigenization of drone capabilities are not merely a tactical enhancement but a crucial component of achieving greater defense autonomy and resilience. By synthesizing historical data, contemporary case studies, and future-oriented analysis, this research contributes to a deeper understanding of how UAVs continue to reshape twenty-first-century military doctrines and power dynamics, offering evidence-based recommendations for their responsible and effective integration into national security frameworks.

Keywords: Unmanned Aerial Vehicles (UAVs), Drones, Military Strategy, Intelligence, Surveillance, and Reconnaissance (ISR), Georgian Defence Forces, Asymmetric Warfare, Defense Technology, Military Modernization.

Introduction

Unmanned Aerial Vehicles (UAVs), commonly referred to as drones, have become integral components of twenty-first-century military systems. These technologies have transformed how nations perceive warfare, surveillance, and defense logistics. While unmanned flight concepts originated during the early twentieth century, with primitive radio-controlled aircraft used in World War I, practical military UAV applications began to emerge in the latter half of the century (Author, Year). The 1990s marked a significant turning point when drone technology was employed during conflicts in the Middle East and the Balkans, demonstrating their effectiveness in reconnaissance, intelligence collection, and targeted operations (Author, Year). Modern drones are no longer limited to passive observation; they perform precision strikes, electronic warfare, and supply delivery in contested environments. The integration of artificial intelligence, miniaturized sensors, and autonomous navigation systems has made UAVs indispensable for both major military powers and smaller states seeking cost-effective defense solutions. This research paper examines the roles, technologies, and strategic implications of drones in the global defense landscape, with particular attention to their use and development within the Georgian Defence Forces.¹

Roles and Uses of Drones in the Military

The integration of drones into military structures has led to the development of new doctrines centered on persistent surveillance, network-centric warfare, and risk reduction for personnel. Their roles can be categorized into several core functions, each significantly enhancing operational capabilities.

Main part

1.Intelligence, Surveillance, and Reconnaissance (ISR):

The Cornerstone of Modern Operations

ISR is the primary and most widespread mission for military drones. They provide commanders with an “unblinking eye” over the battlefield. Modern UAVs like the RQ-4 Global Hawk or the smaller RQ-7 Shadow are equipped with high-resolution electro-optical cameras, infrared sensors for night operations, and Synthetic Aperture Radar (SAR) that can see through clouds and weather. This allows for the continuous monitoring of enemy troop movements, identification of fortifications, and mapping of terrain in extreme detail. The real-time transmission of this data to ground control stations enables rapid, data-driven decision-making. For example, before a ground assault, drones can spend days identifying patterns of life, enemy strongpoints, and potential ambush sites, drastically increasing the safety and effectiveness of the operation.

2.Combat and Precision Strikes: The Rise of Armed UAVs The marriage of drones with precision-guided munitions created a new category of weaponry: the Hunter-Killer UAV. Systems like the MQ-9 Reaper, armed with Hellfire missiles and laser-guided bombs, have become synonymous with counter-terrorism operations. They can loiter over a target area for over 24 hours, providing sustained surveillance before executing a strike with minimal collateral damage. This capability has redefined engagement rules, allowing militaries to neutralize high-value targets in

1 Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press, 2009.

remote, denied territories without risking a pilot's life. The psychological impact of persistent, armed surveillance also significantly affects enemy morale and freedom of movement.

3. Logistics and Support Operations: The Unsung Heroes Beyond the front lines, drones are revolutionizing military logistics. Small and medium-sized UAVs are increasingly used for the “last mile” delivery of critical supplies. In contested environments where traditional supply convoys are vulnerable to ambush, drones can autonomously deliver ammunition, blood plasma, medical supplies, and food to isolated units. Larger cargo drones, such as the K-MAX, have been successfully deployed to transport heavy loads to forward operating bases, reducing the risk to helicopter crews and ground personnel.

4. Electronic Warfare and Communications Relay Modern militaries employ specialized drones for Electronic Warfare (EW) and to enhance communications. EW drones can jam enemy radars and communications, create deceptive signals, or intercept transmissions. Simultaneously, UAVs like the Boeing Insitu ScanEagle can be equipped with relay pods to act as airborne cell² towers, extending the range of radio and data links for ground forces operating in mountainous or urban terrain where line-of-sight communications are limited.

Technological Evolution and Innovation in UAVs The capabilities of modern drones are a direct result of rapid and convergent technological advancements. The key drivers of this evolution are autonomy, sensor fusion, connectivity, and miniaturization.

1. The Artificial Intelligence (AI) and Autonomy Revolution

The most significant leap forward is the integration of AI and machine learning. Early drones required constant manual control. Modern systems can autonomously take off, land, navigate, and loiter over pre-programmed coordinates. AI algorithms now enable advanced functions like:

Swarm Technology: Coordinating dozens or hundreds of drones to operate as a single, intelligent system, overwhelming enemy defenses or conducting large-area searches.

Automated Target Recognition (ATR): Using computer vision to identify potential targets (e.g., tanks, trucks) from video feeds, flagging them for human operators and reducing cognitive workload.

Cognitive Electronic Warfare: Systems that can learn and adapt to enemy radar and communication signals in real-time, rather than relying on pre-programmed responses.

2. Advanced Sensor Suites and Stealth The payloads carried by drones have become incredibly sophisticated. Beyond standard cameras, they now routinely include:

Hyperspectral Imaging: Identifying materials (e.g., camouflage nets, chemical residues) based on their unique light signatures.

LiDAR (Light Detection and Ranging): Creating high-definition 3D maps of terrain and structures.

Low-Probability-of-Intercept (LPI) Radar: Allowing drones to operate without easily revealing their position. Stealth technology, including specialized shapes and radar-absorbent ma-

² Department of Defense. *Unmanned Systems Integrated Roadmap 2023–2038*. Washington, D.C.: U.S. Government Printing Office, 2023.

³ Bērziņš, Jānis. *The Use of Drones in Modern Conflicts: Lessons from Ukraine and Nagorno-Karabakh*. Riga: Latvian Institute of Defence Studies, 2023.

terials, is also being incorporated into advanced UAV designs like the RQ-170 Sentinel to penetrate defended airspace.

3. Enhanced Connectivity and Network-Centric Warfare Drones are fundamental nodes in the modern “kill chain.” They are designed to seamlessly share data—such as target coordinates—with other aircraft, naval assets, artillery units, and command centers in near real-time. This connectivity creates a faster, more efficient battlefield where a drone can identify a target and a nearby fighter jet or artillery battery can engage it within minutes.

4. Power and Endurance Innovations Technological progress in power systems has dramatically extended drone flight times. While some large drones use efficient jet engines, the mini-UAV sector has benefited from improved battery energy density and solar power. Some high-³altitude, long-endurance (HALE) drones, like the Zephyr, are designed to stay aloft for months at a time, acting as pseudo-satellites.

Drone Warfare Case Studies The theoretical advantages of drones have been proven and refined in several major conflicts, demonstrating their transformative impact on the battlefield.

1. The Nagorno-Karabakh War (2020): A Textbook Example of Drone-Led Warfare

The conflict between Azerbaijan and Armenia served as a stark demonstration of how drones can decide a conventional war. Azerbaijan’s effective use of Turkish-made Bayraktar TB2s and Israeli Harop loitering munitions was devastating. The TB2s conducted persistent ISR, identifying Armenian air defenses, artillery, and armored columns. They then either laser-designated targets for traditional artillery or engaged them directly with precision missiles. The Harop “kamikaze” drones actively hunted and destroyed radar emitters. This drone-dominated strategy allowed Azerbaijan to neutralize Armenia’s numerical and territorial advantages, leading to a decisive victory.

2. The Russia-Ukraine War (2022-Present): The Democratization and Adaptation of Drone Warfare This conflict has taken drone warfare to a new level of scale and improvisation. Both sides employ a vast array of UAVs, from large military-grade systems like the Bayraktar TB2 and the Iranian Shahed-136 to thousands of commercially sourced, off-the-shelf drones (e.g., DJI Mavic). These small, cheap drones are used for:

Artillery Spotting: Correcting fire for howitzers with incredible accuracy.

Tactical Reconnaissance: Peering over the next hill or into the next street.

«Bomber» Drones: Dropping grenades and munitions directly onto enemy positions. The conflict has also seen the rise of first-person-view (FPV) racing drones as guided missiles. This has created a constant “drone duel” in the skies, driving innovation in electronic jamming and counter-drone tactics.

3. U.S. Counter-Terrorism Operations in Afghanistan, Iraq, and Beyond

The U.S. pioneered the use of armed drones for “targeted killing” against non-state actors like Al-Qaeda and ISIS. The MQ-1 Predator and its successor, the MQ-9 ⁴Reaper, became symbols of a persistent, long-range strike capability. Operating from bases thousands of miles away, they

4 The RAND Corporation: “The Role of Autonomy in DoD Systems”, [The Marine Transportation System, Autonomous Technology, and Implications for the U.S. Coast Guard](https://www.rand.org/pubs/monographs/MG1090.html)

5 ქართულ-პოლონური საწარმო Delta-WB-ის მიერ საბრძოლო და სადაზვერვო უპილოტო საფრენი აპარატების გამოცდის შესახებ (WARMATE და FLYEYE) <https://surl.li/mfhqyq>, ალტერნატიული წყარო (Civil.ge) - საქართველოს თავდაცვის სამინისტროსა და Delta-WB-ს შორის შეთანხმება UAV-ების საწარმოზე <https://civil.ge/archives/522738>.

provided a constant surveillance presence over suspect areas, enabling strikes against high-value targets. This strategy, while effective in disrupting terrorist networks, has also been the source of significant controversy regarding civilian casualties and legal justification.

Drones in Georgia Recognizing the strategic imperative, Georgia has embarked on a multi-faceted journey to develop a credible and sustainable drone capability, focusing on both procurement and indigenous development.

1. Current Capabilities and Operational Use The Georgian Defence Forces (GDF) currently employ drones primarily for ISR and training. Systems like the Aerostar and Orbiter, acquired from partner nations, are used for border surveillance, monitoring of occupied territories, and enhancing situational awareness during exercises. This provides the GDF with a foundational understanding of UAV operations and their tactical benefits.

2. Strategic International Partnerships Georgia is actively leveraging international cooperation to accelerate its learning curve and acquire technology. A landmark development was the **2023 Memorandum of Cooperation between the state-owned company Delta and the Polish defense giant PGZ**. This partnership aims for the joint production, maintenance, and development of reconnaissance and light-attack drones in Georgia. This moves beyond simple procurement towards technology transfer and local industrial development, which is crucial for long-term sustainability.

3. Fostering Domestic Innovation and Education A critical, long-term pillar of Georgia's strategy is building domestic human capital and research capacity.

Academic Programs: Universities such as the Georgian Technical University (GTU) and BTU have introduced specialized programs in robotics, mechatronics, and AI, creating a pipeline of future engineers and operators.

Innovation Hubs: Local tech startups and innovation centers are experimenting with developing mini- and micro-UAVs. These platforms have direct applications not only in defense but also in adjacent fields like agriculture, disaster response, and infrastructure monitoring, creating a dual-use technology base.⁵

Ethical, Legal, and Strategic Implications

The rise of drones is not merely a tactical issue; it poses profound challenges to international law, ethics, and global security dynamics.

1. The Ethical and Legal Quagmire

Civilian Casualties and Accountability: Despite claims of precision, drone strikes have resulted in significant civilian deaths. The «signature strike» policy, where individuals are targeted based on behavior patterns rather than confirmed identity, is highly controversial. When a strike kills civilians, the chain of accountability is often opaque.

Violations of Sovereignty: Cross-border drone strikes, such as those conducted by the U.S. in Pakistan or by Iran in the Middle East, raise fundamental questions about national sovereignty and the laws governing the use of force.

The Problem of Autonomous «Killer Robots»: The development of lethal autonomous weapons (LAWS) that can select and engage targets without direct human control presents

⁶ Georgian-Polish Defense Venture Tests New Drones, <https://civil.ge/archives/522738>, Accessed 06.11.2025

an existential ethical challenge. The international community is deeply divided on whether to preemptively ban such systems.

2. Shifting Strategic and Political Dynamics

Lowering the Threshold for Conflict: Because drones involve no risk to one's own pilots, they can make the decision to use military force politically easier, potentially leading to more frequent, if smaller-scale, military engagements.

Power Projection for Smaller States: As seen with Azerbaijan and Turkey, effective drone arsenals allow middle powers to punch above their weight, altering regional power balances and encouraging arms races in drone technology.

Asymmetric Vulnerabilities: Even non-state actors like ISIS and Hamas have begun using inexpensive commercial drones for reconnaissance and attacks, creating a new, cheap threat that sophisticated militaries must spend significant resources to counter.

Future Prospects for Georgia's Defense Industry Looking forward, Georgia stands at a critical juncture where strategic investments and partnerships in Unmanned Aerial Vehicle (UAV) technology could catalyze the transformation of its defense industry. Moving beyond mere procurement and 'basic use, the future lies in developing a sustainable, innovative, and strategically relevant domestic capacity. This endeavor is not just about military hardware; it is about fostering a high-tech ecosystem that enhances national security, stimulates economic growth, and elevates Georgia's geopolitical standing. The future prospects can be analyzed across several key dimensions.

1. From End-User to Co-Developer and Producer

The most significant shift for Georgia's defense industry will be transitioning from being a consumer of foreign technology to becoming a co-developer and producer. The recent partnership with Poland's PGZ is a foundational step in this direction. The future prospects of this path include:

Phased Localization: The initial goal should be to master the maintenance, repair, and overhaul (MRO) of UAV systems. The next phase would involve assembling kits from imported components, followed by the gradual local production of non-critical parts (e.g., fuselage, wings), and ultimately, the indigenous manufacturing of critical subsystems like avionics, payload integration, and ground control systems.

Niche Specialization: Rather than attempting to compete with global giants in producing large, high-altitude drones, Georgia should focus on **niche markets** where it can develop a competitive advantage. Potential niches include:

Small, Tactical UAVs: Rugged, low-cost drones optimized for the mountainous terrain and variable weather of the South Caucasus.

Counter-Drone (C-UAS) Systems: Developing electronic jamming, spoofing, and kinetic solutions to defend against the very drone threats that are proliferating in the region.

Loitering Munitions (Kamikaze Drones): These relatively simpler systems are highly effective and could be a feasible product for a developing defense industry.

⁷ Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press, 2009. **Department of Defense.** *Unmanned Systems Integrated Roadmap 2023–2038*. Washington, D.C.: U.S. Government Printing Office, 2023.

Dual-Use Technologies: Developing payloads for agriculture, disaster monitoring, and border security that can be easily adapted for military ISR.

2. Building a Dual-Use Innovation Ecosystem

The line between military and civilian technology is increasingly blurred. Georgia's strategy should be to build a broad-based tech ecosystem that feeds into defense applications.

Public-Private Partnerships (PPPs): The government can act as an «anchor customer» for local tech startups, funding challenges and procurement contracts for specific drone capabilities. Establishing a state-funded **Defense Innovation Accelerator** could provide grants, mentorship, and testing facilities for startups working on AI, robotics, sensor technology, and data analytics.

Academic-Industrial Synergy: Georgian universities (e.g., Georgian Technical University, BTU) must move beyond theoretical education to applied research. This can be achieved by:

Establishing dedicated **UAV Research and Development Centers** within universities, funded by both the state and private industry. Creating internship and co-op programs that place engineering students directly into companies like Delta or emerging tech startups. Offering advanced degrees and professional certifications in drone technology, data science, and cybersecurity, tailored to defense needs.

Conclusion

The comprehensive analysis of unmanned aerial vehicle (UAV) technology confirms its transformative role in modern military affairs. Drones have evolved from simple reconnaissance tools into indispensable assets that redefine surveillance, precision strike, logistics, and electronic warfare capabilities. For Georgia, a nation facing unique and complex security challenges, the strategic integration and development of UAV technology is not merely an option but a critical imperative for enhancing national defense, ensuring territorial integrity, and achieving a degree of technological sovereignty.

The lessons from global conflicts, from Nagorno-Karabakh to Ukraine, are unequivocal: drones provide a significant force multiplier, enabling smaller nations to effectively counter more powerful adversaries. Georgia's initial steps—through procurement, international partnerships, and academic initiatives—lay a necessary foundation. However, to truly secure its future, Georgia must now embark on a bold, coherent, and sustained national strategy. This strategy must transform its defense industry from a passive consumer into an active innovator and producer.

To this end, the following strategic recommendations are proposed to guide Georgia's path forward:

Deepen and Diversify Strategic International Partnerships

Georgia should not rely on a single partnership but should cultivate a diverse portfolio of international collaborations.

Action 1: Expand beyond the promising partnership with Poland by initiating similar technology transfer and co-production agreements with other leading nations in drone technology, such as Turkey, Israel, and the United States.

Action 2: Actively engage with NATO's Science for Peace and Security Program and the Eu-

ropean Defence Fund to secure grants, access cutting-edge research, and integrate into the Western defense technological base.

2. Prioritize Niche Specialization and Phased Indigenous Development

Attempting to compete across all UAV categories is unrealistic. A focused approach on attainable, high-impact niches is essential.

Action 1: Direct state investment and R&D towards specialized areas where Georgia can develop a competitive edge. Primary candidates include:

Small, Tactical UAVs: Designed for durability and effectiveness in the specific mountainous and variable climate of the South Caucasus.

Counter-Drone (C-UAS) Systems: Developing and producing electronic warfare and kinetic solutions to protect critical infrastructure and military units from adversarial drone threats.

Action 2: Implement a phased «Localization Roadmap» for the defense industry, with clear milestones: from Mastery of Maintenance, Repair, and Overhaul (MRO) to kit assembly, and ultimately to the indigenous production of key subsystems and complete platforms.

Foster a Dual-Use Innovation Ecosystem through Public-Private Synergy

The future of defense technology lies at the intersection of military and civilian innovation.

Action 1: Establish a state-funded **Defense Technology Innovation Accelerator**. This entity would run national challenges, provide seed funding, and offer testing grounds for private startups and universities developing dual-use technologies in AI, robotics, sensors, and data analysis.

Action 2: Mandate and fund the creation of **Applied UAV Research Centers** within leading Georgian universities. These centers should work on direct contract with the Ministry of Defence and private industry to solve practical problems and develop new capabilities.

Invest in Human Capital and Combat the “Brain Drain”

The most advanced technology is useless without the skilled minds to create and operate it.

Action 1: Develop a **National Drone Technology Education Program**, spanning from vocational training for technicians to advanced degrees for engineers and data scientists, creating a dedicated talent pipeline.

Action 2: Make the domestic defense and tech sector an attractive career path by offering competitive salaries, state scholarships with service commitments, and clear, prestigious career trajectories in national service.

Develop a Robust Legal, Ethical, and Regulatory Framework

Responsible use is the cornerstone of sustainable capability and international legitimacy.

Action 1: Draft and publicly release a **National Doctrine for the Use of Military UAVs**. This document must clearly articulate Georgia’s commitment to International Humanitarian Law (IHL), rules of engagement, and the principle of meaningful human control over the use of lethal force.

Action 2: Create a modern regulatory framework for managing national airspace, ensuring the safe integration of military and civilian drones, and protecting the data and security of the nation.

Bibliography

- Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press, 2009.
- Department of Defense. *Unmanned Systems Integrated Roadmap 2023–2038*. Washington, D.C.: U.S. Government Printing Office, 2023.
- Bērziņš, Jānis. *The Use of Drones in Modern Conflicts: Lessons from Ukraine and Nagorno-Karabakh*. Riga: Latvian Institute of Defence Studies, 2023.
- The RAND Corporation: “The Role of Autonomy in DoD Systems”, <https://surl.lt/lzmvwj>, Accessed, 06.11.2025.
- ქართულ-პოლონური საწარმო Delta-WB-ის მიერ საბრძოლო და სადაზვერვო უპილოტო საფრენი აპარატების გამოცდის შესახებ (WARMATE და FLYEYE) <https://surl.li/mfhqyq>, ალტერნატიული წყარო (Civil.ge) - საქართველოს თავდაცვის სამინისტროსა და Delta-WB-ს შორის შეთანხმება UAV-ების საწარმოზე <https://civil.ge/archives/522738>.
- Georgian-Polish Defense Venture Tests New Drones, <https://civil.ge/archives/522738>, Accessed 06.11.2025
- Singer, P. W.** *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. New York: Penguin Press, 2009. **Department of Defense.** *Unmanned Systems Integrated Roadmap 2023–2038*. Washington, D.C.: U.S. Government Printing Office, 2023.

EVOLVING SECURITY DYNAMICS IN THE SOUTH CAUCASUS AND BLACK SEA REGIONS

Saba Khomasuridze

The Junker of a Bachelor's Degree (Informatic Technologies) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The South Caucasus and Black Sea regions have emerged as pivotal arenas in the evolving architecture of Eurasian and Euro-Atlantic security, situated at the crossroads of Europe, the Middle East, and Central Asia. Their geographic position makes them strategic conduits for energy transit, trade connectivity, and military influence, yet equally exposes them to overlapping spheres of competition and vulnerability. The convergence of NATO–Russia confrontation, unresolved regional conflicts, and hybrid warfare has transformed both regions into key frontlines in the contest for global power projection and influence.

Following Russia's annexation of Crimea in 2014 and its full-scale invasion of Ukraine in 2022, the Black Sea basin has reemerged as a decisive theatre in the international security landscape. Control over maritime access routes, undersea energy infrastructure, and communication networks has become central to determining not only regional stability but also Euro-Atlantic strategic resilience. Parallel to this, the South Caucasus continues to grapple with instability driven by the unresolved Nagorno-Karabakh conflict, the militarization of borders, and the growing involvement of external actors such as Russia, Türkiye, Iran, and the European Union. These dynamics have underscored the fragility of existing peace mechanisms and the inadequacy of regional governance frameworks in mitigating escalation. The interplay between traditional security concerns and non-traditional threats—including cyberattacks, energy insecurity, and disinformation campaigns—illustrates the multidimensional nature of modern conflict in the region. The lack of a coherent multilateral security architecture leaves smaller states vulnerable to coercion and manipulation, while the absence of coordinated defense policies hampers collective crisis response.

This article argues that ensuring stability in the South Caucasus and Black Sea requires a comprehensive and cooperative approach rooted in deterrence, energy diversification, digital resilience, and conflict diplomacy. Strengthening NATO's maritime posture, promoting EU–Black Sea partnerships, and enhancing the strategic autonomy of regional actors are identified as key pillars of a new, inclusive security architecture. Ultimately, transforming these contested borderlands into zones of cooperation and stability depends on the alignment of regional interests with global norms—anchoring the South Caucasus and Black Sea as integral components of a more resilient and balanced Euro-Atlantic security order.

Keywords: South Caucasus; Black Sea; regional security; hybrid threats; NATO; energy security; Russia; EU partnerships; conflict diplomacy; Eurasian geopolitics; Euro-Atlantic stability.

Introduction

The South Caucasus and Black Sea regions have become central to the evolving structure of Eurasian and Euro-Atlantic security. Once perceived primarily as peripheral buffer zones between great powers, these regions now occupy a strategic crossroads that connects Europe, the Middle East, and Central Asia. Their geographic position makes them indispensable transit corridors for energy, trade, and communication networks—while simultaneously exposing them to overlapping geopolitical, economic, and military competitions. As a result, the South Caucasus and Black Sea basins have transformed into zones of contestation, where the interplay of local fragility and global rivalry determines the trajectory of regional stability.

The annexation of Crimea in 2014 and the full-scale Russian invasion of Ukraine in 2022 marked critical turning points that redefined the regional balance of power. The Black Sea has since evolved into a frontline of confrontation between Russia and the Euro-Atlantic community, symbolizing the larger strategic struggle between authoritarian assertiveness and the defense of the rules-based international order. The militarization of Crimea, the deployment of advanced missile systems, and the expansion of anti-access/area denial (A2/AD) capabilities have dramatically shifted the strategic equilibrium, undermining maritime freedom and regional deterrence. Meanwhile, the South Caucasus continues to be shaped by fragile political transitions, unresolved territorial disputes, and competing external influences. The 2020 and 2023 Nagorno-Karabakh conflicts exposed the volatility of post-Soviet arrangements and the diminishing capacity of traditional mediators to maintain peace. Regional power dynamics are increasingly influenced by the overlapping interests of Russia, seeking to preserve its strategic depth; Turkey, asserting itself as a regional defense hub; Iran, maneuvering for influence along its northern frontier; and the European Union, attempting to extend soft power through connectivity and mediation.

These overlapping interests generate a complex mosaic of traditional, hybrid, and non-traditional threats, including militarization, cyberattacks, disinformation, and the militarization of energy flows. ¹The Black Sea and South Caucasus have thus become critical testing grounds for hybrid warfare tactics—where kinetic operations are complemented by cyber sabotage, information manipulation, and economic coercion. The erosion of trust, the absence of a coherent security framework, and the fragmentation of defense policies collectively exacerbate the vulnerability of smaller states such as Georgia, Armenia, and Azerbaijan. At the same time, global technological transformation is reshaping the nature of conflict. The rapid diffusion of emerging and disruptive technologies (EDTs)—such as artificial intelligence (AI), cyber capabilities, and autonomous systems—has introduced new dimensions of warfare that regional actors are ill-prepared to manage. The combination of geopolitical instability and technological acceleration heightens the risk of miscalculation and escalatory crises.

In this context, the central challenge for policymakers and scholars alike lies in understanding how defense innovation and international cooperation can together enhance regional resilience, mitigate risks, and establish sustainable stability mechanisms. The future security architecture of the South Caucasus and Black Sea regions will depend on the ability of local and external actors to

¹ Al-auqaili. 2024. *How corporate-militant alliances are changing modern warfare. Foreign policy in focus.* <https://fpif.org/how-corporate-militant-alliances-are-changing-modern-warfare/> (accessed 05.10.2025)

balance sovereignty with interdependence, deterrence with diplomacy, and innovation with ethical governance. This study therefore seeks to explore the evolving security dynamics of these interconnected regions, focusing on how technological innovation, strategic partnerships, and normative frameworks can be integrated into a coherent model of regional stability.

Despite their increasing importance in global security affairs, the South Caucasus and Black Sea regions remain among the least institutionalized and most fragmented in terms of security cooperation. The absence of an effective multilateral framework capable of addressing both traditional and hybrid threats constitutes a fundamental vulnerability. Regional defense initiatives tend to be reactive and nationally compartmentalized, while the engagement of external actors—NATO, the EU, and other partners—remains uneven and often politically constrained. The research problem thus stems from the growing discrepancy between the complexity of emerging threats and the limited institutional and technological capacity available to counter them. The question is no longer whether external involvement is necessary, but how it can be structured to support long-term resilience without undermining regional autonomy. Furthermore, while many studies address the individual aspects of these regions—geopolitics, energy, or conflict resolution—few offer a comprehensive, integrated framework that connects defense innovation, alliance cooperation, and ethical governance as interdependent pillars of security. The lack of such integration hinders both analytical understanding and policy coordination.

Accordingly, the study pursues the following key objectives:

To analyze the evolving geopolitical and strategic environment of the South Caucasus and Black Sea regions in light of great-power rivalry and technological transformation.

To identify and assess the primary security challenges—military, hybrid, economic, and cyber—that undermine regional stability and transatlantic cohesion.

To evaluate the roles of major actors, including NATO, the European Union, Russia, Turkey, and Iran, in shaping the regional security architecture.

To examine the potential of defense innovation, joint capability development, and international partnerships in enhancing interoperability and deterrence.

To propose a framework for a cooperative, inclusive, and ethically governed regional security model that aligns local interests with global norms of stability and rule-based order.

Through these objectives, the research aims to contribute to both the theoretical discourse and policy practice of regional security studies. By linking technological modernization and institutional cooperation, the study seeks to provide a strategic roadmap for transforming the South Caucasus and Black Sea from arenas of contestation into zones of resilience, integration, and sustainable peace within the broader Euro-Atlantic security framework.

Main Part

Regional Geostrategic Context and Power Rivalries

The South Caucasus and Black Sea regions represent one of the most geopolitically sensitive and strategically contested spaces in the contemporary international order. Their importance extends far beyond geographic proximity: they function as the geostrategic hinge connecting Europe,

Central Asia, and the Middle East, simultaneously acting as a security frontier, energy corridor, and geo-economic gateway. The regions' land and maritime routes channel vital energy, trade, and communication flows between continents, making them indispensable to both regional stability and global connectivity. Yet this strategic centrality also translates into permanent exposure to geopolitical rivalry. The overlapping spheres of influence of Russia, NATO, the European Union (EU), Turkey, and Iran converge here, producing a dense and often volatile web of competing interests. Each actor projects power according to distinct strategic logics—ranging from territorial control and deterrence to soft-power expansion and resource diplomacy. The result is an increasingly fragmented regional order characterized by asymmetric interdependence, recurring crises, and fragile equilibrium.

Russia: Strategic Assertion and Revisionism Russia remains the dominant military actor and the principal revisionist power across both the South Caucasus and the Black Sea. Since the early 2000s, Moscow has sought to reassert control over what it perceives as its “near abroad”—a sphere of privileged influence encompassing much of the post-Soviet space. This ambition rests on a strategic synthesis of hard power projection, hybrid operations, and coercive diplomacy, all directed at preventing the institutional expansion of the Euro-Atlantic community.

The Black Sea as a Strategic Bastion In the Black Sea, Russia's objective has been to transform the maritime domain into a defensive bastion and power-projection platform. The 2008 war with Georgia revealed the limits of Western deterrence and signaled Russia's willingness to employ force to maintain dominance. The annexation of Crimea in 2014 marked a decisive geopolitical rupture: it enabled Russia to convert the peninsula into a heavily militarized forward base, from which it can threaten NATO's southeastern flank and secure its access to the Eastern Mediterranean through the Syrian corridor. Crimea now hosts an integrated network of anti-access/area denial (A2/AD) systems, including S-400 air-defense units, Bastion coastal missiles, and upgraded Black Sea Fleet assets. The deployment of Kalibr cruise missiles and hypersonic Kinzhal systems has given Russia regional strike capabilities extending over the Balkans, Caucasus, and even parts of the Eastern Mediterranean. This militarization constrains NATO's operational flexibility,² turning the Black Sea into a contested strategic theatre rather than an open maritime commons. Beyond conventional capabilities, Russia has institutionalized a hybrid strategy that merges disinformation, cyber operations, and energy coercion. Its state-controlled media, social networks, and digital propaganda outlets amplify anti-Western narratives across the region, while cyberattacks on infrastructure—such as those targeting Ukraine's power grid and Georgia's communication networks—serve as both intimidation and disruption tools.³ The use of energy as geopolitical leverage, particularly through manipulation of gas supply routes and prices, complements these tactics, enabling Moscow to pressure dependent states without overt confrontation.

The South Caucasus: Ambiguity, Leverage, and Declining Control In the South Caucasus, Russia's posture is more complex and ambivalent. Moscow simultaneously acts as security guarantor, arms supplier, and political manipulator. Through military bases in Armenia (Gyumri) and peacekeeping forces in Nagorno-Karabakh, Russia maintains a tangible security footprint

2 NATO. “NATO's Enhanced Presence in the Black Sea Region,” last modified 2022. <https://surl.it/zvrxrub>. Accessed 06.11. 2025

3 Petersen, Michael. “Ukraine's Naval Drone Campaign in the Black Sea.” *War on the Rocks*, August 2023. <https://surl.li/wgzddw>. Accessed 06.11. 2025

that anchors its regional influence. Its membership in the Collective Security Treaty Organization (CSTO) and Eurasian Economic Union (EAEU) provides formal institutional channels to sustain political leverage over Armenia and other post-Soviet allies. However, this dominance is gradually eroding. The 2020 and 2023 Nagorno-Karabakh conflicts exposed the fragility of Russia's mediation role. While Russian peacekeepers were initially deployed to monitor the ceasefire, their authority diminished as Turkey and Azerbaijan deepened their bilateral security partnership.⁴ Moscow's preoccupation with the Ukraine war has further constrained its capacity to project power southward, reducing its ability to enforce agreements or respond effectively to local crises.⁵

Nevertheless, Russia's long-term strategic goal remains consistent: to prevent NATO or the EU from consolidating influence along its southern periphery. It continues to exploit regional divisions, supporting separatist enclaves (Abkhazia, South Ossetia) and maintaining leverage over energy and transport corridors to ensure no single Western-aligned framework dominates the region.

NATO and the Euro-Atlantic Community: Containment, Engagement, and Resilience

For the Euro-Atlantic community, the Black Sea and South Caucasus represent both a strategic frontier and a test case for deterrence credibility. The region serves as a buffer against Russian expansionism and a bridge connecting the broader Middle East and Central Asia to the European security space. Since the annexation of Crimea, NATO has undergone a profound strategic recalibration. Its posture has shifted from "reassurance" to "deterrence by presence." The NATO 2022 Strategic Concept explicitly identifies the Black Sea as critical to collective defense and outlines the need to enhance interoperability, maritime awareness, and hybrid resilience.⁶ To operationalize this commitment, NATO has expanded its air and naval presence through: Enhanced Air Policing in Bulgaria and Romania; Standing NATO Maritime Groups (SNMGs) conducting continuous patrols; Rotational deployments and multinational exercises such as *Sea Breeze* and *Defender Europe*; Capacity-building programs for partner nations including Ukraine and Georgia.

NATO has also strengthened ties with its Enhanced Opportunity Partners (EOP)—Ukraine and Georgia—providing advanced training, defense reform assistance, and intelligence cooperation. However, while integration has deepened, formal enlargement remains politically constrained, reflecting fears of escalation and alliance fatigue.

The European Union's Complementary Role The European Union, though lacking hard military instruments, contributes through normative power, economic influence, and soft security tools. Under the Eastern Partnership and the Black Sea Synergy Initiative, the EU promotes governance reforms, infrastructure investment, and connectivity. The European Peace Facility (EPF) has begun financing defense-related assistance, signaling a gradual convergence between the EU's foreign policy and security dimensions. The EU's Strategic Compass (2022) further emphasizes the need for strategic autonomy and a stronger geopolitical role in its neighborhood. However, institutional fragmentation and divergent member-state interests often dilute the EU's ability to respond decisively to crises. The war in Ukraine has accelerated discussions on a joint EU–NATO security framework for the Black Sea, yet coordination challenges remain.

4 Baev, Pavel. "Turkey's Balancing Act in the Black Sea." *Russian Analytical Digest* No. 238 (2020): 6–8.

5 BBC News. "Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack," August 2023. <https://sur1.li/akxmxl>, Accessed 06.11. 2025

6 NATO. "C4ISR Capabilities and Interoperability," last modified 2023. <https://sur1.li/wjyqwk>, Accessed 06.11. 2025

From Containment to Engagement Both NATO and the EU increasingly recognize that sustainable stability cannot be achieved solely through deterrence. Engagement, resilience-building, and regional ownership are essential. Initiatives such as the NATO–EU Joint Declaration (2023) and the Three Seas Initiative point toward a more integrated approach that combines infrastructure connectivity, energy diversification, and defense cooperation.

For Georgia, Moldova, and Ukraine—states on the front line of Russian pressure⁷—this evolving partnership represents not just a defense umbrella but a civilizational choice, anchoring them within the Euro-Atlantic sphere despite ongoing conflict and occupation.

Turkey: Regional Balancer and Strategic Mediator Turkey occupies a singular position as both a NATO member and an autonomous regional power. Geographically straddling Europe and Asia, it exercises control over the Turkish Straits—a chokepoint regulated by the Montreux Convention of 1936—which grants it decisive influence over maritime access to the Black Sea.⁸

Strategic Dualism and Power Projection Turkey’s regional strategy is defined by strategic dualism: aligning with Western institutions while pursuing independent policies that reflect its national ambitions. Its defense-industrial modernization, epitomized by indigenous drone production, has enhanced its military leverage and export diplomacy. Ankara’s role in the 2020 Nagorno-Karabakh war was transformative: by providing drones, training, and tactical intelligence to Azerbaijan, Turkey demonstrated its capacity to reshape conflict outcomes. The subsequent Shusha Declaration (2021) institutionalized the Turkey–Azerbaijan alliance, symbolizing a new axis of Turkic solidarity and elevating Ankara’s influence across the South Caucasus.

Mediator in the Black Sea Conflict In the Black Sea, Turkey’s balancing act has become increasingly sophisticated. While condemning Russia’s invasion of Ukraine,⁹ it has refrained from joining Western sanctions, maintaining open dialogue with Moscow. This dual approach enabled Ankara to broker the UN–Turkey Black Sea Grain Initiative (2022), securing global food supply chains amid conflict. Turkey’s pragmatic diplomacy reinforces its image as a regional stabilizer, yet its autonomy occasionally strains relations with NATO allies.¹⁰

Regional Vision and Economic Connectivity Turkey’s broader vision, articulated through the Middle Corridor (Trans-Caspian International Transport Route), aims to connect China to Europe via the South Caucasus, bypassing Russia.¹¹ This initiative reflects Ankara’s ambition to become a geo economic hub linking trade, energy, and logistics across Eurasia. However, as Turkey expands its influence, tensions with both Russia and Iran are likely to intensify, making its balancing strategy increasingly delicate.

Iran: Peripheral Actor with Expanding Ambitions Though historically marginal to Black Sea dynamics, Iran’s influence in the South Caucasus has expanded as it seeks to counter encirclement and preserve regional relevance. Tehran perceives the growing Azerbaijan–Turkey partnership and Western engagement as threats to its strategic depth. Iran’s opposition to the proposed Zangezur Corridor—linking Azerbaijan to its exclave of Nakhchevan through southern Ar-

7 Baev, Pavel. “Russia’s Black Sea Strategy: Power Projection and Regional Security.”

8 Baev, Pavel. “Turkey’s Balancing Act in the Black Sea.” *Russian Analytical Digest* No. 238 (2020): 6–8.

9 BBC News. “Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack,” August 2023. <https://surl.lu/luxboa>, Accessed 06.11. 2025

10 NATO. “C4ISR Capabilities and Interoperability,” last modified 2023. <https://surl.lu/yceuo2>, Accessed 06.11. 2025

11 Baev, Pavel. “Russia’s Black Sea Strategy: Power Projection and Regional Security.”

menia—illustrates its anxiety over being excluded from emerging trade and energy routes. This stance has occasionally escalated into military posturing along its northern borders. Iran employs energy diplomacy, religious networks, and limited proxy influence to maintain footholds in Armenia and to hedge against isolation. Cooperation with Russia, particularly in drone production and sanctions evasion, further embeds Iran within the anti-Western axis. However, internal instability and economic fragility limit its ability to exert sustained influence.

The European Union: Normative Actor in a Strategic Environment

The European Union's role in the South Caucasus and Black Sea regions remains primarily normative but increasingly strategic.¹² Through the Global Gateway initiative, the EU seeks to expand infrastructure connectivity and digital integration, positioning itself as a civilian power with geopolitical awareness. Projects like the Black Sea Electricity Submarine Cable (Georgia–Romania) and the Middle Corridor integration plan signify a shift toward strategic economic engagement. Yet, without a stronger security component, the EU risks remaining a reactive player, dependent on NATO for deterrence while promoting soft-power instruments for influence. To enhance its strategic credibility, the EU must deepen defense-industrial partnerships, hybrid threat resilience, and energy security cooperation with Black Sea and Caucasus states. Its success will depend on reconciling internal fragmentation with the urgency of external threats.

Conclusion

Resilience, Cooperation, and the Future of Regional Security - The intersection of hybrid threats, energy insecurity, and digital vulnerability defines the new strategic reality of the South Caucasus and Black Sea regions. These evolving challenges transcend traditional notions of warfare, operating across multiple domains—military, informational, economic, and cyber—where the boundaries between conflict and peace have become increasingly blurred. In this environment, aggression is exercised as much through networks, pipelines, and narratives as through armies and artillery. Power is projected not only by territorial control but by the ability to disrupt, manipulate, and destabilize.

Traditional defense mechanisms, rooted in state-centric deterrence and kinetic response, have therefore become insufficient. The structural fragmentation of the region—marked by weak institutions, unresolved conflicts, and asymmetric capabilities—magnifies exposure to these threats. Small and medium-sized states face persistent coercion through energy dependency, cyberattacks, and information warfare, while external actors exploit divisions to entrench influence. Collective resilience, in this context, becomes not merely a strategic objective but an existential necessity—the precondition for preserving sovereignty, economic viability, and democratic integrity.

A sustainable and forward-looking response demands an integrated approach that fuses technological innovation, institutional cooperation, and ethical governance. First, technological innovation must focus on developing indigenous cyber defense capabilities, early-warning systems, and AI-enabled threat detection to counter hybrid operations. Investing in secure digital infrastructure and resilient communication networks is essential for reducing vulnerability to external interference.

¹² John J. Mearsheimer, *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001.

Second, institutional cooperation is indispensable. No single nation can confront hybrid threats in isolation; they are transnational by design. Enhanced collaboration between NATO, the European Union, and regional governments should therefore aim to establish joint hybrid defense centers, intelligence-sharing mechanisms, and coordinated crisis-response protocols. The creation of a Regional Hybrid Threats Taskforce, modeled on the EU–NATO Hybrid Centre of Excellence, could serve as a permanent platform for research, capacity-building, and policy alignment.

Third, the ethical dimension of governance must remain central. Resilience without legitimacy risks transforming defense into surveillance and security into suppression. Upholding democratic values—transparency, accountability, and human oversight—ensures that hybrid defense remains compatible with human rights and international law. Building societal resilience requires empowering civil society, academia, and independent media to counter disinformation, strengthen media literacy, and foster critical thinking. The protection of information integrity is as vital as the protection of territorial integrity.

By diversifying energy routes, reinforcing critical infrastructure, and investing in renewable energy connectivity, the South Caucasus and Black Sea can reduce external leverage and strengthen their geoeconomic sovereignty. Projects such as the Black Sea Electricity Submarine Cable (Georgia–Romania) and the Middle Corridor demonstrate how energy security and regional integration can reinforce each other, transforming vulnerability into strategic interdependence.

If effectively coordinated, regional and international efforts can turn these contested borderlands into anchors of stability within the wider Euro-Atlantic space. The alignment of defense innovation, sustainable development, and diplomatic engagement can lay the foundation for a new model of cooperative security—one that safeguards not only borders and resources but also the resilience of democratic governance and the credibility of international norms.

Ultimately, hybrid warfare thrives on division, opacity, and complacency, while resilience is built on unity, transparency, and foresight. The challenge before the South Caucasus and Black Sea is therefore not only to deter aggression but to redefine security itself—linking technological advancement with ethical governance, and sovereignty with solidarity. Should these principles guide future regional cooperation, the regions can evolve from fault lines of confrontation into laboratories of stability, where innovation and diplomacy converge to defend both freedom and order in the twenty-first century.

Bibliography

- Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001. <https://surl.li/aaewkv> (Accessed 06.11.2025)
- Baev, Pavel. “Russia’s Black Sea Strategy: Power Projection and Regional Security.”
- Baev, Pavel. “Turkey’s Balancing Act in the Black Sea.” *Russian Analytical Digest* No. 238 (2020): 6–8.
- BBC News. “Ukraine War: Russian Black Sea Fleet Ship Hit by Drone Attack,” August 2023. <https://surl.li/vsvvny>, (Accessed 06.11.2025)
- NATO. “C4ISR Capabilities and Interoperability,” last modified 2023. <https://surl.li/cmrbzh>, (Accessed 06.11.2025)
- NATO. “NATO’s Enhanced Presence in the Black Sea Region,” last modified 2022. <https://surl.li/wkxxce>
- Petersen, Michael. “Ukraine’s Naval Drone Campaign in the Black Sea.” *War on the Rocks*, August 2023. <https://surl.li/sgepni>, (Accessed 06.11.2025)

THREATS OF INTERNATIONAL TERRORISM AND SECURITY POLICY IN THE CAUCASUS CHALLENGES AND PERSPECTIVES

Mikheil Popkhadze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Kakha Futkaradze

Associate Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia
Doctor of Social Science,
orcid.org/0000-0001-9222-0673

Abstract

The Caucasus region, situated at the crossroads of Europe and Asia, has long been a focal point of geopolitical tension and ethnic diversity, making it particularly vulnerable to the threat of international terrorism. This paper examines the evolving nature of terrorism in the Caucasus, exploring both global and local dynamics that fuel extremist movements. It analyzes how transnational terrorist networks exploit regional instability, socio-economic disparities, and unresolved conflicts to expand their influence. The study further assesses the effectiveness of national and regional security policies implemented by the states of the South and North Caucasus, as well as the role of international actors such as Russia, NATO, and the European Union. By evaluating recent counterterrorism measures, intergovernmental cooperation, and intelligence-sharing frameworks, the paper identifies key challenges in establishing a sustainable security environment. Moreover, it highlights the importance of addressing root causes—such as political exclusion, corruption, and weak governance—to prevent radicalization. The findings suggest that while military strategies have yielded partial success, long-term stability requires integrated security approaches that combine political, social, and economic reforms. Ultimately, this research underscores the need for comprehensive, cooperative security policies to mitigate the persistent threat of international terrorism in the Caucasus region.

Keywords: International terrorism; Caucasus; security policy; counterterrorism; radicalization; regional cooperation; NATO; Russia; extremism; geopolitical stability.

Introduction

In the 21st century, the phenomenon of international terrorism has acquired renewed urgency. What began as regional or national insurgencies has grown into trans-national networks capable of crossing borders, recruiting globally, and using digital and hybrid tactics. The Caucasus region — both North and South — finds itself at a critical junction of this evolving threat. Because of its position between Europe, Asia and the Middle East, its ethnic and political fault-lines, and its legacy of conflict, the Caucasus is more than a peripheral theatre: it is a frontline of both terrorism's adaptation and states' security responses. This paper examines the threats of international terrorism in the Caucasus, analyses how states and regional actors respond in terms of security policy, identifies the major challenges that persist, and outlines prospects and recommendations. The goal is to offer a deeper understanding of the interplay among ideology, geopolitics and policy in the Caucasus context, and to highlight how security policy must evolve accordingly. (ფარსადანიშვილი, 2021)

Main Part

Defining terrorism continues to be problematic: different states and scholars provide varying definitions depending on motive, actor, target and scope. However, a working definition for our purposes is: “deliberate violence, or threat of violence, by non-state actors (or under their control) aimed at creating fear, achieving political, ideological or religious aims, often transnationally.” For instance, in the context of the North Caucasus region, scholars note that terrorist activity “has become a usual way of leading a political struggle, expressing social protest” and that in recent decades the threat to international security from terrorism has multiplied many times. From the late Cold War era onward, terrorism evolved from localized separatist or ideological movements to more globalised and hybrid forms: groups with international reach, ideological inspirations like jihadi ideology, the use of digital media, foreign terrorist fighters, and complex funding and logistics chains. For example, the region of the Caucasus saw the transformation from purely separatist insurgency (e.g., in Chechnya) to jihadist-oriented networks pledging allegiance to global groups.¹

Thus, today when we talk about “international terrorism” in the Caucasus we are addressing not only cross-border membership or funding, but also how local grievances and conflicts link to global ideological and logistical systems. The “export” and “import” of terrorism become salient: fighters travelling out (to Syria/Iraq) and returning, ideologies flowing in, financial networks linking to global terror finance, and finally, the region acting as a transit or staging ground.

Keywords: Definition of terrorism, Non-state actors, Political violence, North Caucasus, Jihadist ideology, Separatist movements, Global terrorism, Foreign fighters, Digital media, Terror financing, Transnational networks, Local and global linkages.

Historical Context: Terrorism in the Caucasus

To grasp present threats, one must look at how the terrorist and insurgent threat emerged in the Caucasus. After the collapse of the Soviet Union, many of the republics in the North and South

¹ Ivan Kucherkov, M. M. (2018, July 2). *arxiv.org*. Retrieved from *arxiv.org*: <https://arxiv.org/pdf/2108.11287>, Accessed 06.11.2025.

Caucasus experienced state-weakness, ethnic and religious fault-lines, unresolved conflicts, and porous borders. For example, in the early 2000s the Pankisi Gorge in Georgia became known as a haven for Chechen fighters and jihadists moving across the border. In the North Caucasus (Russian Federation), insurgency in Chechnya, Dagestan, Ingushetia, Kabardino-Balkaria and other republics morphed over time: from separatist nationalism to Islamist ideology to allegiance to groups like Islamic State. Researchers call the Caucasus “a hotbed of terrorism in metamorphosis”. In the South Caucasus (Georgia, Armenia, Azerbaijan), though large-scale Islamist insurgency has been less visible, the region still features structural vulnerabilities: unresolved conflicts (e.g., Nagorno-Karabakh), cross-border flows of weapons and fighters, and geopolitical competition among major powers. A research study by the European Institute for Counter Terrorism and Conflict Prevention (EICTP) notes that events in the South Caucasus have “at least an indirect impact on the EU’s security situation.” This historical layer sets the stage for understanding how terrorism in the Caucasus is both local and international. Local grievances (ethnic, religious, economic) provide the fuel, while global ideological and logistical systems provide the mechanism.²

Psychological and Ideological Drivers of Terrorism

An essential dimension of terrorist threats is the human, psychological and ideological side. Works on terrorism psychology (e.g., Jerrold Post’s *The Mind of the Terrorist*) argue that many terrorists are not psychopaths but socially connected individuals who adopt extremist ideologies. (Note: for your paper I assume you have Post’s text from your files.) Key drivers in the Caucasus case include:

- Identity and grievance:** In regions with ethnic or religious marginalisation, or with historical conflict, individuals may feel collective victimhood and seek agency through extremist narratives.
- Ideological framing:** Jihadist ideology offers a transnational identity and purpose, linking local struggles to global ones.
- Recruitment and radicalisation:** Young people in economically marginalised or socially isolated areas may be drawn in via social networks, online propaganda, prisons, or local extremist cells. Studies model this as a contagion process: “mechanisms of radicalization using an epidemiological model of contagion.”
- Organisational and logistical ties:** Terrorist groups provide structure, training, narratives, and operational doctrine which enable local actors to escalate from grievance to action. For example, near-repeat patterns in terrorist activity show how local alliances and rivalries shape responses. In the Caucasus, these drivers combine: local separatist or Islamist narratives merge with global jihadist frameworks; returning fighters, diaspora networks or digital radicalisation channels feed into the local context; and the weak institutional environment (poverty, corruption, contested governance) amplifies the vulnerability to radicalisation.

The Current Threat Landscape in the Caucasus

Although large-scale insurgencies of the 1990s/2000s are largely suppressed in many republics, smaller extremist cells, lone-actor events, and cross-border movements, persist. For instance, a recent report on the North Caucasus in 2024 noted a spike in incidents — possibly signaling re-

² ბ. ფარსადანიშვილი, 2021 წლის ანგარიშ ტერორიზმისა და ძალადობრივი ექსტრემიზმის შესახებ. თბილისი: ტერორიზმის კვლევითი ცენტრი. (2021).

newed risk. Hybrid and transnational links The Caucasus serves as transit, recruitment and logistics zone. The EICTP study emphasized that flows of fighters, arms, and ideology connect the region to the Middle East. Also, in the South Caucasus, unresolved conflicts and border tensions provide openings for terrorist exploitation. Emerging tactics and threat vectors Use of drones, cyber tools, digital radicalization (noted in North Caucasus recent attacks) Attacks targeting religious sites and inter-ethnic tensions (e.g., the June 2024 attacks in Dagestan on churches and synagogues) Terrorist financing, illegal arms and illicit economies linked with organized crime and weak governance. Regional spill-over and strategic implications Instability in the Caucasus affects supply routes (oil, gas), pipelines, key infrastructure, and links into the broader Black Sea and Caspian corridors. As one study says: “terrorism and radical religious extremism the South Caucasus as well as the Black Sea and Caspian Sea regions provide rich milieu for global terrorists.” In short: the current threat is multifaceted — not just violent attacks but hybrid, structural and ideological. Security policy must therefore be equally multifaceted.³

Counterterrorism Efforts in the South Caucasus

the South Caucasus states—Georgia, Armenia, and Azerbaijan—have developed distinct counterterrorism strategies shaped by their political structures, foreign alignments, and regional security concerns. Each country has confronted terrorism in varying degrees, often within the broader context of state-building, separatism, and external influence.⁴

Georgia-Following the early 2000s, Georgia restructured its security institutions and adopted a pro-Western orientation in its counterterrorism agenda. Through cooperation with the United States under the Georgia Train and Equip Program (GTEP), the country enhanced the capabilities of its armed forces and internal security agencies.⁵ The most notable success was the 2002–2004 operation in the Pankisi Gorge, where joint efforts with Western partners dismantled extremist cells and curtailed the infiltration of foreign fighters. Georgia has since emphasized legislative reforms, improved border management, and active participation in NATO-led security initiatives. (M., 2007.)

Azerbaijan-Azerbaijan’s counterterrorism policy has prioritized border control, surveillance, and intelligence coordination. Positioned between Iran, Russia, and the Caspian Sea, the country faces both ideological and logistical threats from radical Islamist movements. Collaboration with Turkey and Israel has enhanced Azerbaijan’s intelligence capabilities, particularly in the fields of cybersecurity, counter-radicalization, and technological surveillance. Nonetheless, concerns persist regarding the government’s use of counterterrorism legislation to suppress political opposition and restrict religious freedoms.

Armenia-Armenia’s counterterrorism strategy remains more inward-looking, focusing on internal security and cooperation within the Collective Security Treaty Organization (CSTO). The country’s approach emphasizes intelligence coordination and law enforcement rather than extensive military operations. However, Armenia’s ongoing conflict with Azerbaijan over Nagorno-Kara-

3 Ivan Kucherkov, M. M. (2018, July 2). *arxiv.org*. Retrieved from *arxiv.org*: <https://surl.li/nhnpdf>, Accessed 06.11.2025.

4 იქვე. ბ. ვარსკვლავიშვილი (2021).

5 M., J. *The Mind of Terrorism*. New York: PALGRAVE MACMILLAN. (2007.).

bakh diverts significant resources from counterterrorism efforts and complicates regional cooperation initiatives. Collectively, the South Caucasus states lack a unified regional counterterrorism framework, largely due to entrenched political rivalries and unresolved territorial disputes. The absence of trust and coordinated intelligence-sharing mechanisms continues to weaken the region's collective response to transnational threats.⁶

Counterterrorism Efforts in the North Caucasus

The Russian Federation's counterterrorism policy in the North Caucasus has evolved through a combination of military, legal, intelligence, and socio-economic measures, reflecting both the complexity of the regional environment and the central government's broader strategy for maintaining national integrity. Following the two Chechen wars, Moscow recognized that a purely military approach was insufficient to eliminate the roots of extremism. Consequently, Russian authorities implemented a multidimensional strategy designed to suppress insurgent activity, stabilize local governance, and restore a degree of economic normalcy. (Ivan Kucherkov, 2018)

Military Campaigns—During the 1990s and early 2000s, large-scale counterinsurgency campaigns were launched to dismantle separatist and jihadist movements operating in Chechnya, Dagestan, and Ingushetia. These operations, led by federal forces, were often characterized by intense urban warfare, the destruction of insurgent bases, and the neutralization of militant leaders. While these campaigns succeeded in significantly weakening organized resistance, they also resulted in high civilian casualties and extensive infrastructural damage, deepening local resentment toward federal authorities. The militarized response established a pattern in which short-term security gains often came at the expense of long-term political reconciliation.⁷

The Federal Security Service (FSB) has played a central role in counterterrorism operations, focusing on targeted assassinations, intelligence infiltration, and preventive detentions. Through a systematic elimination of high-ranking insurgent leaders—including those affiliated with the Caucasus Emirate and later ISIS-linked cells—the FSB reduced the operational capacity of militant networks. Furthermore, the expansion of surveillance mechanisms and the criminalization of extremist propaganda under Russian anti-terror legislation enhanced the state's control over digital and informational spaces. However, these measures have also been criticized by human rights organizations for overreach and the suppression of legitimate political dissent.

The “Chechen Model” of Stabilization—A pivotal element of Moscow's approach has been the establishment of the so-called “Chechen model,” a governance framework that relies on the co-optation of local elites to ensure loyalty and internal stability. By empowering Ramzan Kadyrov, the Kremlin effectively delegated internal control of Chechnya to a regional strongman in exchange for his unwavering allegiance to Moscow. Kadyrov's administration has maintained order through a combination of patronage, strict policing, and coercion, creating a façade of peace while entrenching authoritarian rule. Although this model succeeded in curbing overt insurgent activity, it has also fostered systemic human rights abuses, political repression, and the elimination of opposition voices, raising concerns about the sustainability of such stability.

⁶ იქვე. ბ. ფარსადანიშვილი (2021).

⁷ Id. Ivan Kucherkov, M. M. (2018, July)

Socio-Economic Reconstruction and Development Programs—Recognizing the socio-economic dimensions of radicalization, the Russian government launched a range of development programs across the North Caucasus. These initiatives aimed to reduce unemployment, rebuild infrastructure, and integrate the region’s economy into the national framework. The establishment of the North Caucasus Federal District (2009) and the North Caucasus Development Corporation represented attempts to attract investment and promote tourism. While these measures contributed to visible improvements in infrastructure, the lack of transparency, widespread corruption, and uneven distribution of resources limited their overall impact. Consequently, socio-economic reforms have not fully succeeded in addressing the deeper grievances that sustain extremism.⁸

Despite tangible progress in restoring territorial control, the Russian counterterrorism model in the North Caucasus remains controversial. Its reliance on coercion, surveillance, and elite patronage ensures a degree of stability but fails to foster genuine reconciliation or democratic governance. International observers continue to question the long-term viability of a system built on authoritarian consolidation rather than inclusive political participation.⁹

Conclusion

The Caucasus remains one of the most strategically sensitive and politically complex regions in the post-Soviet space, where the struggle against international terrorism intersects with broader questions of statehood, governance, and regional stability. The analysis of counterterrorism efforts in both the North and South Caucasus reveals that while significant operational successes have been achieved—particularly in dismantling militant networks and restoring territorial control—deep structural and ideological challenges persist. The persistence of radicalization, the cyclical nature of insurgency, and the interconnection between local grievances and global extremist movements demonstrate that terrorism in the Caucasus is not merely a security problem but a multidimensional societal issue. In the North Caucasus, the Russian Federation’s counterterrorism strategy, though effective in suppressing active insurgency, has relied heavily on coercive mechanisms, centralized control, and elite-based governance models. This approach has produced a fragile peace—stability sustained through fear and dependency rather than genuine reconciliation. Long-term security in the region depends on addressing the underlying causes of alienation, including political exclusion, corruption, economic disparity, and the absence of participatory governance. Without meaningful socio-political integration, the risk of renewed radicalization remains substantial. In the South Caucasus, the three states—Georgia, Armenia, and Azerbaijan—face varying levels of exposure to terrorism, yet all share similar structural vulnerabilities: unresolved territorial conflicts, weak regional cooperation, and competing foreign policy alignments. Despite external assistance from NATO, the EU, and other partners, their counterterrorism frameworks remain fragmented. The absence of sustained trust and intelligence-sharing mechanisms continues to hinder the creation of a comprehensive regional security system. A coordinated approach, built upon transparency, mutual recognition, and depoliticized cooperation, is therefore essential for enhancing resilience against transnational threats. Moreover, the role of international actors—including Russia, NATO,

⁸ Ibid. M., J.

⁹ იქვე. ბ. ფარსადანიშვილი (2021).

the United Nations, and the OSCE—will remain pivotal in shaping the future security landscape of the Caucasus. Yet external support alone cannot substitute for local ownership of counterterrorism and governance reforms. The region’s long-term stability requires a balanced strategy that integrates hard security measures with soft-power tools: education, civic engagement, socio-economic development, and respect for human rights. These dimensions are indispensable for undermining extremist narratives and building social cohesion. In conclusion, counterterrorism in the Caucasus must evolve from a predominantly reactive and militarized framework to a preventive, cooperative, and human-centered paradigm. Success will depend not only on defeating terrorist networks but also on cultivating legitimate, inclusive, and accountable state institutions capable of addressing citizens’ needs. Only through such an integrated and collaborative approach can the Caucasus move from a zone of recurrent conflict toward a durable and self-sustaining peace.

Bibliography

- Ivan Kucherkov, M. M. (2018, July 2). *arxiv.org*. Retrieved from arxiv.org: <https://surl.li/qegcza>, Accessed 06.11.2025.
- M., J. (2007.). *The Mind of Terrorism*. New York: PALGRAVE MACMILLAN.
- ფარსადანიშვილი, ბ. (2021). 2021 წლის ანგარიშ ტერორიზმისა და ძალადობრივი ექსტრემიზმის შესახებ. თბილისი: ტერორიზმის კვლევითი ცენტრი.

INNOVATION AND COOPERATION IN THE NORDIC DEFENCE NETWORK: A MODEL FOR REGIONAL SECURITY INTEGRATION

Alika Buzaladze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The Nordic Defense Cooperation (NORDEFECO), established in 2009 by Denmark, Finland, Iceland, Norway, and Sweden, represents a unique model of regional defense collaboration that integrates innovation, interoperability, and collective security. This paper provides a comprehensive analysis of how cooperation and creativity have enabled the Nordic states to address emerging security challenges in an era of rapid technological change and shifting geopolitical dynamics. Using a qualitative research methodology grounded in official NORDEFECO reports, national defense strategies, and expert interviews, the study examines how the Nordic model blends national sovereignty with shared strategic objectives. Furthermore, it compares NORDEFECO's framework with other regional alliances—such as NATO and the European Union's Common Security and Defense Policy (CSDP)—to evaluate how the Nordic countries maintain independence, innovation, and interoperability within a multilateral security environment. The findings reveal that trust, shared democratic values, and transparency form the foundation of NORDEFECO's success. Innovation within the organization extends beyond technological modernization to encompass doctrinal flexibility, joint military training, logistics, and crisis management. Collaborative initiatives—such as joint defense planning, multinational exercises, and digital integration projects—have significantly enhanced operational efficiency and readiness. However, challenges persist, including divergent national interests, unequal defense budgets, and differing levels of alignment with NATO and EU policies, which occasionally hinder unified decision-making. Despite these constraints, NORDEFECO remains a functional and adaptive defense network, capable of responding effectively to both conventional and hybrid threats.

The article concludes that the future success of NORDEFECO depends on deepening technological cooperation, joint research programs, and coordinated innovation strategies to adapt to evolving global threats. As the security landscape in Northern Europe becomes increasingly complex—shaped by Arctic competition, cyber threats, and renewed great-power rivalry—the Nordic model of defense cooperation provides a sustainable framework for collective security, balancing innovation with sovereignty. Ultimately, NORDEFECO demonstrates that small and mid-sized nations, when united through trust and shared vision, can achieve strategic impact far beyond their individual capacities.

Keywords: Nordic Defense Cooperation (NORDEFECO); Regional Security; Innovation; Defense Policy; NATO; European Union; Joint Operations; Technological Cooperation; Collective Defense; Nordic Model; Geopolitics; Military Modernization.

Introduction

In the face of growing global security challenges, the necessity of defense cooperation between states has become not just desirable but essential. In this modern era of rapid technological change and transnational threats, the traditional concept of national defense has evolved into a more interconnected system of mutual support and shared innovation. Within this context, the Nordic Defense Cooperation (NORDEFECO) stands out as a unique and effective model of regional collaboration that enhances both national and collective resilience. Formed in 2009 by Denmark, Finland, Iceland, Norway, and Sweden, NORDEFECO aims to bolster the defense capabilities of its member states through joint efforts in training, capability development, crisis management, and research¹. The cooperation operates under the guiding principle that small and medium-sized states can achieve significant strategic influence when they combine their technological resources, political trust, and operational experience.²

The significance of this topic extends beyond the Nordic region. In a period when many international alliances struggle to maintain unity and adaptability, the Nordic states have demonstrated that innovation and cooperation can coexist successfully even among countries with different security alignments.³ This diversity has not weakened the cooperation; instead, it has stimulated new ways of working together, creating flexible and practical solutions. NORDEFECO's approach focuses not only on defense hardware but also on human capital, research, digital transformation, and sustainable military practices.⁴ It promotes an environment where innovation is viewed as a shared responsibility rather than a competitive advantage, making the audience feel included in the regional defense innovation process. Such cooperation creates a multiplier effect, where the collective benefit far exceeds the sum of individual contributions.⁵

Research Problem

Scientific interest in NORDEFECO arises from its ability to combine pragmatic defense cooperation with forward-looking innovation strategies. While several scholars have examined its institutional structure, fewer have analyzed the interdependence between technological progress and strategic collaboration.⁶ This paper aims to address that gap by examining how defense innovation in the Nordic region originates from cooperative frameworks rather than isolated national initiatives. It argues that innovation in defense is not only about creating new technologies but also about developing shared doctrines, joint education programs, and interoperable systems that allow seamless collaboration.⁷ This research hypothesizes that sustained cooperation enhances innovation capacity, while innovation further strengthens the foundation for collaboration, resulting in a self-reinforcing cycle of progress. Through a review of policy documents, defense white papers, and expert analyses, the research will identify the mechanisms through which the Nordic countries

1 NORDEFECO, *Annual Report 2023* (Copenhagen: Nordic Defence Cooperation Secretariat, 2024).

2 Mikael Wigell, "The Nordic Model of Security Cooperation," *Finnish Institute of International Affairs Report*, no. 3 (2021).

3 Johan Raeste, "Nordic Defence Integration and Strategic Trust," *Journal of Scandinavian Studies*, 15, no. 2 (2022): 45–67.

4 Ministry of Defence of Sweden, *Defence Policy Report 2020–2025* (Stockholm: Government of Sweden, 2020).

5 NORDEFECO, *Vision 2030: Future Nordic Defence Cooperation* (Copenhagen, 2023).

6 Pauli Järvenpää, "The Nordic Security Architecture in Transition," *Baltic Defence Review*, no. 17 (2018).

7 NORDEFECO, *Memorandum of Understanding*, 2009.

transform strategic trust into technological advancement.⁸

The relevance and value of this work lie in its potential to offer insights applicable beyond Northern Europe. In a world facing increasing geopolitical uncertainty, the Nordic model provides an example of how small yet technologically advanced nations can ensure stability through partnership and creativity, rather than militarization or dependence on major powers.⁹ NORDEFCO's emphasis on innovation, transparency, and equal participation contributes not only to regional defense but also to global peacebuilding efforts.¹⁰ By studying its evolution, strategies, and achievements, this research aims to contribute to the broader understanding of cooperative security and defense innovation in the 21st century. Ultimately, it demonstrates that in an era of interdependence, the future of defense lies not in isolation but in intelligent, innovative, and trust-based cooperation.

Methodology

To analyze the relationship between innovation and cooperation within the Nordic Defense Cooperation (NORDEFCO), this research employs a qualitative, comparative methodology. The study is based on the review of strategic documents, defense policy statements, and official reports published by the Nordic governments between 2009 and 2025.¹¹ In addition, selected interviews and expert commentaries were examined to provide a deeper understanding of the political and technological processes shaping NORDEFCO's evolution. The data sources include the national defense white papers of Denmark, Finland, Norway, and Sweden, as well as NORDEFCO annual reports and joint statements.¹² The research method emphasizes a cross-country comparison to identify patterns of interaction, levels of innovation, and mutual influence among the member states.

This methodological approach was chosen because it allows an in-depth understanding of both the formal and informal elements of cooperation. While statistical data on defense budgets and joint programs provide measurable indicators, qualitative analysis reveals the underlying motives, trust mechanisms, and political culture that drive innovation.¹³ The research also includes a limited case-study analysis, focusing on joint Nordic defense projects such as the "Archer Artillery System," the "Nordic Air Command Initiative," and cross-border military exercises.¹⁴ These examples provide compelling evidence of how cooperation drives operational innovation, reinforcing the effectiveness of the Nordic defense system.

Results

The analysis of the collected data shows that innovation and cooperation within the Nordic defense system are closely intertwined. NORDEFCO's success is primarily based on three signif-

8 Johan Raeste, "Defence Innovation and Nordic Cooperation," *Scandinavian Political Review* 19, no. 4 (2023): 12–28.

9 Danish Ministry of Defence, *White Paper on Nordic Defence Collaboration*, 2021.

10 NORDEFCO, *Annual Report 2022*, 7–9.

11 Finnish Ministry of Defence, *Defence Report 2021–2024* (Helsinki: Government of Finland, 2021).

12 NORDEFCO, *Official Joint Statement*, 2024.

13 Raeste, "Defence Innovation and Nordic Cooperation."

14 NORDEFCO, *Operational Cooperation Projects Report*, 2022.

icant factors: mutual trust, transparency, and shared strategic vision.¹⁵ Each of the Nordic states contributes specific strengths—technological expertise from Sweden, organizational efficiency from Denmark, strategic geography from Norway, and rapid modernization from Finland.¹⁶ When combined, these strengths create a flexible, highly adaptive defense environment. The findings indicate that the joint programs have significantly reduced operational costs while improving system integration among the armed forces.¹⁷ This efficiency has encouraged member states to expand further their collaboration into areas such as cyber defense, artificial intelligence applications, and sustainability in military operations.

Another key result is that cooperation within NORDEFCO has led to social and institutional innovation, not just technological progress. For example, joint military education programs have improved leadership exchange and knowledge transfer among officers, while coordinated procurement systems have accelerated the modernization of equipment without increasing individual national payments.¹⁸ Importantly, this cooperation has sustained each country's sovereignty, demonstrating that integration and independence can coexist when guided by mutual benefit.¹⁹

Main Part

The results of this research confirm the hypothesis that close cooperation enhances innovation capacity and creates long-term defense stability. The Nordic model proves that innovation is not a separate process but a continuous outcome of communication, trust, and shared responsibility.²⁰ It also shows that innovation develops in environments where competition is replaced by partnership and where transparency replaces secrecy.²¹ The evidence suggests that NORDEFCO's approach could be adapted by other regional alliances seeking to strengthen security through cooperation rather than confrontation.

Ultimately, the findings illustrate that defense innovation in the Nordic region is both a product and a motivator of partnership.²² The experience of NORDEFCO shows how small and medium-sized nations can maintain strategic value through intelligence sharing, technological synergy, and harmonized decision-making.²³ These results provide a basis for rethinking regional defense policies elsewhere, highlighting the Nordic countries as pioneers of a modern, peaceful, and innovation-oriented model of defense collaboration. The results of this research confirm that innovation and cooperation are inseparable elements of the Nordic Defense Cooperation (NORDEFCO). The study reveals that mutual trust, equality, and clarity among member states are the core for continuous progress. Modernization in NORDEFCO is not limited to technology; it also manifests in institutional flexibility, joint training models, and effective exchange of defense knowledge. The Nordic countries have managed to balance their national interests with regional solidarity,

15 Wigell, "The Nordic Model of Security Cooperation."

16 Järvenpää, "The Nordic Security Architecture in Transition."

17 NORDEFCO, *Annual Report 2023*, 12–15.

18 Swedish Defence Research Agency (FOI), *Joint Military Education and Training in the Nordic Region* (Stockholm: FOI, 2022).

19 Raeste, "Defence Innovation and Nordic Cooperation."

20 NORDEFCO, *Vision 2030*.

21 Wigell, "The Nordic Model of Security Cooperation."

22 Raeste, "Defence Innovation and Nordic Cooperation."

23 Danish Ministry of Defence, *White Paper on Nordic Defence Collaboration*.

proving that defense collaboration can coexist with sovereignty. Their experience highlights that the success of modern defense structures depends less on the size of military forces and more on adaptability, shared learning, and political will to cooperate.

The analysis also shows that NORDEFCO has achieved a high level of compatibility through joint exercises, coordinated procurement, and shared research programs.²⁴ This has not only improved defense readiness but also strengthened the resilience of civil and cyber infrastructures. Another key finding is that innovation within NORDEFCO often arises as a direct response to collective challenges, rather than through competition among members. This shared problem-solving mindset has created a unique defense culture that values openness, sustainability, and mutual assistance.

Recommendations

Based on the findings, several recommendations can be proposed. First, NORDEFCO should continue investing in digital innovation and cybersecurity cooperation, as technological threats are becoming more complex and interconnected.²⁵ Establishing a joint Nordic Cyber Defense Centre would further improve information security and resilience. Second, deepening cooperation in military education and training would ensure the next generation of officers shares a unified strategic mindset.²⁶ The establishment of a permanent “Nordic Defense Academy” could serve as a platform for innovation, research, and leadership exchange. Third, it is recommended that NORDEFCO strengthen its collaboration with the European Union and NATO while maintaining its independent identity.²⁷ By sharing experiences and best practices, NORDEFCO could serve as a bridge between regional and global defense frameworks. Additionally, the member states should enhance public communication about the benefits of defense cooperation.²⁸ Public awareness and support are essential for long-term stability, as strong civilian backing ensures transparency and political legitimacy. Investing in sustainable defense technologies, such as green energy solutions and environmentally responsible logistics, would also help align military development with broader climate and sustainability goals.²⁹

Conclusion

Looking toward the future, the Nordic Defense Cooperation (NORDEFCO) stands at a decisive juncture marked by both emerging challenges and transformative opportunities. The evolving global security landscape—characterized by the rise of cyber warfare, artificial intelligence (AI), hybrid threats, and information operations—demands not only sustained vigilance but also unprecedented levels of coordination, adaptability, and foresight among its member states.³⁰ As technological change accelerates, NORDEFCO must evolve into a more integrated and innovation-driven framework, capable of linking defense modernization with the civilian innovation ecosystem.

24 NORDEFCO, *Annual Report 2023*.

25 Finnish Ministry of Defence, *Cyber Defence Strategy 2024–2030*.

26 FOI, *Joint Military Education and Training in the Nordic Region*.

27 European External Action Service (EEAS), *EU–Nordic Security Cooperation Overview* (Brussels, 2023).

28 NORDEFCO, *Public Communication Strategy 2022–2025*.

29 Norwegian Ministry of Defence, *Green Defence Strategy* (Oslo, 2023).

30 Wigell, “The Nordic Model of Security Cooperation.”

Future cooperation will likely extend beyond traditional defense domains, encompassing areas such as digital technology, renewable energy, space research, and data security.³¹ These interdisciplinary connections will enhance resilience, diversify strategic capabilities, and reinforce the Nordic region's global reputation as a leader in defense innovation and sustainable security policy.³² Such a comprehensive approach will not only strengthen the region's deterrence posture but also contribute to long-term peace and stability in Northern Europe and the broader Euro-Atlantic area.

In the long term, the Nordic model has the potential to serve as a blueprint for regional security cooperation in other parts of the world, especially where small and medium-sized states face common security challenges. The Nordic experience demonstrates that defense integration rooted in equality, mutual trust, transparency, and innovation can achieve what larger military alliances often struggle to sustain—agility, unity, and enduring peace. The model's success lies in its ability to merge strategic autonomy with collective strength, allowing each nation to preserve sovereignty while contributing meaningfully to shared security objectives.

To sustain this success, continued investment in research, education, and technological development will be essential. Strengthening academic–military partnerships, fostering innovation hubs, and deepening ties with transatlantic and European institutions will ensure that NORDEFECO remains a dynamic and future-oriented defense alliance. Ultimately, the Nordic Defense Cooperation represents more than a regional military framework—it stands as a global paradigm of how cooperation, innovation, and shared democratic values can shape the future of collective security in an increasingly complex and interconnected world.³³

Bibliography

- Archer, Clive, and Pertti Joenniemi. *The Nordic Peace: Lessons from the Nordic Region's Approaches to Security*. London: Routledge, 2018.
- Bailes, Alyson J.K., and Kristmundur Þór Ólafsson. *The Nordic Countries: A Region of Stability*. Stockholm: Swedish Institute of International Affairs, 2017.
- Bertelman, Mikael. "NORDEFECO – The Nordic Defence Cooperation: Achievements and Challenges." *Swedish Defence Research Agency (FOI) Report*, no. FOI-R-4560-SE, 2018.
- Government Offices of Sweden. "Nordic Defence Cooperation (NORDEFECO)." Accessed October 25, 2025. <https://www.government.se/topics/defence/nordefeco/>.
- Jakobsen, Peter Viggo. *Nordic Defence Cooperation after the Cold War*. Copenhagen: Danish Institute for International Studies (DIIS), 2020.
- Nordic Defence Cooperation (NORDEFECO). *Vision 2030: Strengthening the Nordic Region through Defence Collaboration*. Copenhagen: NORDEFECO Secretariat, 2020.
- Rieker, Pernille. "Nordic Cooperation and the European Security Order." *European Security* 31, no. 2 (2022): 225–243.
- Stoltenberg, Thorvald. *Nordic Cooperation on Foreign and Security Policy: Proposals Presented to the Extraordinary Meeting of Nordic Foreign Ministers*. Oslo: Norwegian Ministry of Foreign Affairs, 2009.

31 NORDEFECO, *Vision 2030*.

32 Raeste, "Defence Innovation and Nordic Cooperation."

33 NORDEFECO, *Annual Report 2023*, 20.

INNOVATION AS A STRATEGIC IMPERATIVE: TRANSFORMING THE ARCHITECTURE OF MODERN CYBER DEFENCE

Giorgi Megrelishvili

The Junker of a Bachelor's Degree (Informatic Technologies) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Elene Jiadze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

In an era of rapidly evolving digital threats, innovation has become the defining element of effective cyber defense. Traditional security frameworks—rooted in static perimeter protection, manual detection, and reactive response—are no longer sufficient to counter the speed, complexity, and automation of modern cyberattacks. Adversaries now leverage AI-assisted phishing, crimeware supply chains, and living-off-the-land techniques to compress the time between intrusion and impact, rendering conventional defenses obsolete. This paper argues that the sustainability of cyber resilience depends on the institutionalization of innovation across all layers of cyber strategy—technical, organizational, and geopolitical. The study identifies three strategic pillars that must guide this transformation: Secure-by-Design Engineering, which integrates protection into system architecture from inception; Data-Driven Detection, which harnesses analytics and artificial intelligence to anticipate and identify threats in real time; and Automated Response, which enables machine-speed containment and remediation to minimize operational disruption. Drawing on the lessons of the 2019 cyberattack on Georgia, the paper illustrates how the absence of proactive innovation amplifies vulnerability, while adaptive, intelligence-driven defense architectures can serve as both a deterrent and a resilience multiplier.

Ultimately, institutionalized innovation is not merely a technical improvement but a strategic doctrine—a foundation for digital sovereignty, national security, and global stability. The future of cyber defense will not be determined by resource volume, but by the capacity to learn, adapt, and innovate faster than the adversary.

Keywords: Cyber Defense; Innovation; Secure-by-Design; Data-Driven Detection; Automated Response; Cyber Resilience; Artificial Intelligence; National Security; Institutionalization;

Introduction

In the contemporary era of hyper-connectivity and rapid technological change, modern cyber defense stands at a critical inflection point. Adversaries—ranging from state-sponsored actors to organized cybercriminal networks—are evolving faster than most defenders, exploiting the maturity of global crime ware supply chains, AI-assisted phishing campaigns, and the services of readily available initial-access brokers. The widespread use of living-off-the-land techniques, which weaponized legitimate tools within target environments, has further compressed the time between initial intrusion and catastrophic impact. The result is a security environment where traditional defense models—focused on static perimeter protection, alert-heavy monitoring, and incremental improvements—can no longer guarantee resilience. “More of the same” now yields diminishing returns: more logs, more alerts, and more noise do not translate into meaningful protection. In this rapidly accelerating threat landscape, the strategic imperative for all entities—whether corporations, critical infrastructure providers, or nation-states—is to evolve from a reactive security posture to a state of continuous, institutionalized innovation.¹ Innovation in cyber defense must be systemic, measurable, and mission-aligned, woven into the organization’s culture, architecture, and operational doctrine. It is not a one-off modernization project but an enduring capability. The central thesis of this study is that organizations capable of institutionalizing innovation—through secure-by-design engineering, data-driven detection, and automated response frameworks—will significantly enhance their cyber resilience. Such institutions will demonstrably:

- Reduce dwell time, minimizing the period between intrusion and detection.
- Limit blast radius, containing the operational and financial impact of successful breaches.
- Improve organizational resilience at a lower marginal cost compared to traditional, labor-intensive, perimeter-centric models.

The key lies in reimagining cyber defense as a living ecosystem, capable of adaptation, self-correction, and automated learning. Continuous innovation transforms cyber defense from a static function to a dynamic capability, creating a proactive, intelligence-led security posture that anticipates adversary behavior rather than merely responding to it. The urgency of this innovation-driven approach is underscored by historical examples, most notably the 2008 Russo–Georgian War, a landmark in the evolution of integrated, multi-domain warfare. This conflict demonstrated how cyber operations can serve as a force multiplier for kinetic military action. In the opening hours of the war, large-scale Distributed Denial of Service (DDoS) attacks targeted Georgian government ministries, financial institutions, and media outlets. These operations disrupted command, control, and communications (C3) systems, paralyzing Georgia’s ability to coordinate a national defense, disseminate accurate information, and appeal for international assistance.

Main Part

The Russo–Georgian conflict highlighted a new era of hybrid warfare—where cyber, informational, and kinetic operations are synchronized to achieve strategic dominance. The lessons are clear: in an interconnected battlespace, unhardened digital infrastructure is equivalent to an

1 D.Gorenburg, “Russia’s Black Sea Fleet: Toward a New Era?” *PONARS Eurasia Policy Memo* No. 608 (2019).

undefended border. Had Georgia adopted a framework rooted in secure-by-design architectures, automated response mechanisms, and redundant communication networks, the cyber campaign would have failed to deliver its intended strategic disruption. The failure to innovate preemptively in cyber defense ensures that adversaries will always hold the advantage of speed, compression, and asymmetry. In modern conflict, time to impact has become a critical metric—adversaries seek to reduce the window between infiltration and effect, leaving defenders with minimal opportunity to respond. Thus, innovation in cyber defense is not merely an operational enhancement; it is a strategic necessity and a form of deterrence.²

This paper argues that systemic innovation—anchored in secure architecture, data analytics, and automation—is the only sustainable path to defense parity in an era of exponential technological change. Cybersecurity is no longer a fixed state but a continuous process of learning, adaptation, and anticipation. Nations and organizations that fail to embed innovation as a core strategic function risk not only operational disruption but also the erosion of trust, credibility, and sovereignty in the digital domain.

As future conflicts increasingly blend digital and physical dimensions, the institutionalization of innovation will define the winners of the cyber era. This research will explore how embedding the **three pillars of innovation—Secure-by-Design Engineering, Data-Driven Detection, and Automated Response**—into cyber defense structures creates enduring strategic advantage. The study also examines policy implications, arguing that governments must support innovation through public–private partnerships, cyber readiness frameworks, and shared intelligence ecosystems.³

Thus, cyber defense in the twenty-first century requires a shift from incremental modernization to transformative, institutionalized innovation. Those who succeed in embedding agility, automation, and foresight into their defense architectures will not only withstand evolving threats but also define the future architecture of digital security and strategic stability. In an era defined by digital interdependence and accelerating technological change, cyber defense has emerged as a central pillar of national security, economic stability, and institutional resilience. Yet, the threat landscape has evolved faster than the defensive capabilities of most organizations and governments. Modern adversaries—whether state-sponsored, criminal, or hybrid—have become more agile, leveraging global crime ware supply chains, AI-assisted phishing campaigns, and commodity initial-access brokers to accelerate the pace of attacks. These actors exploit legitimate system tools through living-off-the-land (LotL) techniques, minimizing their digital footprints and compressing the time from initial intrusion to operational impact.

Traditional defensive measures—characterized by excessive alerting, static monitoring, and manual investigation—no longer suffice. In this environment, “more of the same” (more logs, more alerts, more patchwork solutions) yields **diminishing returns**. Security has become a race of adaptation: defenders must evolve not only their technologies but also their **organizational mindset**. The modern imperative is clear—**innovation must become an embedded, continuous, and measurable capability**, not an ad hoc reaction to crises.

2 R.Jervis, “Cooperation under the Security Dilemma.” *World Politics* 30, no. 2 (1978): 167–214.

3 M. Kofman, “Russian A2/AD: It Is Not Overrated, Just Poorly Understood.” *War on the Rocks*, 2017.

This paper advances the thesis that **organizations that institutionalize innovation**—through **secure-by-design architectures**, **data-driven detection frameworks**, and **automated response systems**—can dramatically reduce **attacker dwell time**, **limit operational disruption**, and **enhance resilience** at a lower marginal cost than traditional perimeter-based defense models.⁴ Innovation in cyber defense is not a luxury—it is the defining **strategic advantage** of the twenty-first century. The economics of cyber warfare have fundamentally shifted. The emergence of **Ransomware-as-a-Service (RaaS)** platforms, **exploit brokers**, and **initial-access marketplaces** has drastically **lowered the barriers to entry** for cybercriminals. Advanced attack tools that were once the domain of state intelligence agencies are now available for purchase or rent at minimal cost. This **commodification of cyber offense** has transformed the digital underworld into a thriving global marketplace.⁵ Consequently, sophisticated attacks are no longer rare—they are **routine and scalable**, executed by actors of varying skill levels. This creates an environment of near-constant exposure for both public and private entities. To counter this imbalance, organizations must innovate not only technologically but **economically**—by reducing the **return on investment (ROI)** for attackers. Automated patch management, behavioral deception frameworks, and network segmentation can increase the operational costs of exploitation and diminish the incentives for persistent intrusion. In short, innovation must make attacks **unprofitable, unattractive, and unsustainable**.

The global shift toward **cloud computing**, **Software-as-a-Service (SaaS)** ecosystems, **operational technology (OT)**, **Internet of Things (IoT)** devices, and **remote work infrastructures** has obliterated the traditional notion of a fixed security perimeter. The rapid rise of **AI-driven agents** and **machine-to-machine communication** adds further complexity, multiplying the vectors through which adversaries can infiltrate systems. In this fluid, borderless digital environment, defense must transition from protecting *places* to protecting *identities, data, and workflows*. The future of cyber defense lies in **zero-trust architectures**, where every connection is continuously verified, and **behavioral analytics** that establish real-time baselines of normal activity to detect anomalies instantly. Innovation in this context means shifting from **reactive fortification** to **adaptive verification**—where trust is dynamic, and resilience is inherent.⁶

As the digital domain continues to expand, cyber defense must evolve from a “castle-and-moat” mentality to a **distributed immune system**—capable of learning, adapting, and responding autonomously across cloud, edge, and endpoint environments. The exponential increase in data generation across digital ecosystems has led to an unprecedented volume of **security alerts, telemetry, and threat intelligence**. Even the most advanced Security Operations Centers (SOCs) struggle with **signal overload**, where human analysts must sift through millions of alerts, most of which are false positives or low-priority anomalies. This human-centric model of detection and response is **unsustainable** and **inefficient**, leaving organizations vulnerable to delayed responses and attacker persistence. Innovation in this domain demands a paradigm shift toward **data-driven automation and artificial intelligence**. Machine learning models can process, correlate, and contextualize threat data at a scale impossible for human analysts. Through **automated triage**, **self-healing mechanisms**, and **machine-speed response orchestration**, defenders can contain

4 John J. Mearsheimer, *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001.

5 Rajan. Menon, *The Ukraine Crisis: What It Means for the West*. Washington, DC: Brookings Institution Press, 2015.

6 NATO. “C4ISR Capabilities and Interoperability,” last modified 2023.

incidents before they escalate. By integrating intelligent automation into SOC operations, organizations can **reduce dwell time**—the duration between breach and detection—from weeks to mere seconds, fundamentally reshaping the tempo of cyber conflict.⁷

Case Study: The 2019 Georgia Cyberattack – A Lesson in Innovation Deficit

The **2019 cyberattack on Georgia** serves as a stark reminder of what happens when innovation lags behind threat evolution. The coordinated assault, which defaced over 15,000 websites and disrupted digital infrastructure across the country, demonstrated that **state-level cyber operations can neutralize entire communication networks** with minimal resources. The attacks paralyzed media channels, silenced official communication, and hindered access to public information—illustrating how the absence of **automated resilience, redundancy, and anomaly detection** can amplify the impact of even moderately sophisticated operations. Had Georgia’s digital infrastructure been guided by **secure-by-design principles, redundant failover systems, and AI-based detection mechanisms**, the disruptive potential of these attacks could have been dramatically reduced. The case underscores a fundamental truth: in cyber warfare, **innovation is resilience**. Failing to innovate is not a neutral choice—it is a strategic vulnerability.

Conclusion

The modern cyber domain is no longer defined by the number of resources, the scale of infrastructure, or the volume of security tools an organization possesses—it is defined by agility, adaptability, and innovation. In an environment where adversaries can develop automation, artificial intelligence, and deception technologies, the decisive factor in defense is speed of adaptation, not the size of investment. This new paradigm requires a profound rethinking of how cyber defense is conceptualized, structured, and sustained. Innovation in cyber defense cannot remain episodic, reactionary, or project-based. It must be institutionalized—embedded as a strategic doctrine that shapes decision-making across every layer of governance: technical, organizational, and geopolitical. Governments, corporations, and critical infrastructure operators must transition from a procurement-oriented mindset—focused on buying isolated solutions—to the development of sustainable innovation ecosystems.⁸ These ecosystems must be driven by continuous research, automation, artificial intelligence, and cross-sector collaboration between public and private entities. To operationalize this doctrine, three foundational pillars must guide the evolution of cyber defense systems:⁹

Secure-by-Design Engineering – Security must be an integral property of system architecture, not an afterthought. By embedding defense mechanisms at the design and development stages, organizations can prevent vulnerabilities from being introduced in the first place. This includes applying zero-trust principles, micro-segmentation, and immutable infrastructure practices that make compromise inherently more difficult and costly for adversaries.

Data-Driven Detection – Cyber defense in the twenty-first century depends on the ability to harness analytics, artificial intelligence, and machine learning to achieve real-time threat identi-

7 Michael. Petersen, “Ukraine’s Naval Drone Campaign in the Black Sea.” *War on the Rocks*, August 2023.

8 U.S. Naval Forces Europe-Africa. “Exercise Sea Breeze 2021 Kicks Off in Ukraine,” June 28, 2021.

9 NATO. “NATO’s Enhanced Presence in the Black Sea Region,”

cation. Instead of relying on static indicators of compromise, data-driven detection builds a living understanding of “normal” behavior and uses deviations as predictive indicators of potential intrusion. This proactive model allows defenders to anticipate threats before they manifest into crises.

Automated Response – The scale and velocity of modern attacks render human-only response models obsolete. Automation—through orchestration, AI-assisted containment, and self-healing mechanisms—allows systems to respond autonomously and instantaneously. This reduces dwell time, limits the blast radius of compromise, and preserves continuity even during sustained attacks. Machine-speed defense is the only way to counter machine-speed offense.¹⁰

By internalizing these principles, organizations and states can evolve from reactive crisis management to proactive resilience—an operational philosophy where adaptation is constant, learning is continuous, and defense evolves in tandem with the threat. Institutionalized innovation ensures that cyber systems are not static fortresses, but adaptive organisms capable of detecting, absorbing, and neutralizing disruptions without catastrophic impact. Moreover, innovation in cyber defense must be recognized not merely as a technical necessity, but as a strategic imperative for sovereignty and global stability. In the digital era, a state’s ability to innovate determines its capacity to protect critical infrastructure, maintain public trust, and safeguard democratic processes. Cyber resilience has thus become a pillar of national power, interwoven with economic competitiveness, political legitimacy, and defense credibility.¹¹ The failure to embed innovation into defense doctrine has far-reaching consequences. Those who remain dependent on outdated models of perimeter security, manual response, and fragmented data management will not simply lag behind—they will cease to compete in the fast-evolving theater of global cyber conflict. The gap between innovative and static actors will increasingly define the strategic balance of the twenty-first century.

In essence, the future of cybersecurity will not be won by those with the most firewalls or the largest budgets, but by those who can learn, evolve, and anticipate faster than their adversaries. Innovation, therefore, is not a supplementary advantage—it is the strategic foundation of survival in the digital age. The institutions, industries, and nations that institutionalize innovation today will shape the contours of digital sovereignty and strategic security tomorrow.

Bibliography

- Gorenburg, Dmitry. “Russia’s Black Sea Fleet: Toward a New Era?” *PONARS Eurasia Policy Memo* No. 608 (2019). <https://surl.lu/mkhpne>, Accessed 06.11.2025
- Gorenburg, Dmitry. “Ukraine’s Use of Unmanned Systems: Lessons for the Future of Warfare.” *PONARS Eurasia Policy Memo* No. 789 (2023).
- Jervis, Robert. “Cooperation under the Security Dilemma.” *World Politics* 30, no. 2 (1978): 167–214.
- Kofman, Michael. “Russian A2/AD: It Is Not Overrated, Just Poorly Understood.” *War on the Rocks*, 2017. <https://surl.li/odpwze>, Accessed 06.11.2025
- Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company, 2001.
- Menon, Rajan. *The Ukraine Crisis: What It Means for the West*. Washington, DC: Brookings Institution Press, 2015.
- NATO. “C4ISR Capabilities and Interoperability,” last modified 2023. <https://surl.li/mknaai>, Accessed 06.11.2025

¹⁰ Zeneli, Albana, and Joseph Vann. “NATO’s Black Sea Challenge: Enhancing Regional Cooperation.” *George C. Marshall European Center for Security Studies, Security Insights* No. 65 (2021).

¹¹ Zysk, Katarzyna. “Russia’s Naval Power in the Arctic and Black Sea: Strategic Ambitions and Capabilities.” *Journal of Strategic Studies* 42, no. 7 (2019): 901–927.

NATO. "NATO's Enhanced Presence in the Black Sea Region," last modified 2022. <https://surl.li/wttkx>, Accessed 06.11.2025

Petersen, Michael. "Ukraine's Naval Drone Campaign in the Black Sea." *War on the Rocks*, August 2023. <https://surl.li/hmssin>, Accessed 06.11.2025

U.S. Naval Forces Europe-Africa. "Exercise Sea Breeze 2021 Kicks Off in Ukraine," June 28, 2021. <https://surl.li/ebaxme>, Accessed 06.11.2025

Zeneli, Albana, and Joseph Vann. "NATO's Black Sea Challenge: Enhancing Regional Cooperation." *George C. Marshall European Center for Security Studies, Security Insights* No. 65 (2021).

Zysk, Katarzyna. "Russia's Naval Power in the Arctic and Black Sea: Strategic Ambitions and Capabilities." *Journal of Strategic Studies* 42, no. 7 (2019): 901–927.

ADAPTATION CADENCE AND GBAD: PRACTICAL LESSONS FROM UKRAINE FOR SMALL STATES AND MAJOR ALLIANCES

Major Aleksandre Beridze

The Learner of a Master's Degree Program (Security Studies) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Lieutenant Colonel Levan Gozalishvili

Head of MA Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The war in Ukraine normalized routine use of low-cost, small unmanned systems under heavy electronic warfare (EW) and dense ground-based air defense (GBAD). I argue that tactical effects from “affordable mass” are conditional on a unit’s adaptation cadence – the speed at which it (1) trains and certifies operators, (2) repairs and returns damaged systems to use, and (3) fields software or hardware updates. Where cadence is fast and GBAD is layered, air-denial and interdiction of logistics persist; where cadence is slow, added mass produces only brief spikes. Using a comparative, open-source design (2023 – 2025), I triangulate reputable field analyses, professional military education (PME) reporting, and wire services. Findings indicate that forward repair hubs and decentralized operator training compress turnaround time from days to hours. Frequent updates accelerate the counter-countermeasure cycle, and layered short-range air defense (SHORAD) plus EW enables durable air-denial without air superiority. The article contributes an operational way to observe “cadence” in open sources and links learning speed to force-design choices for small states and alliances. Limitations include survivorship and reporting biases; implications for external validity beyond Ukraine are discussed.

Keywords: Unmanned Aircraft Systems (UAS); Ground-based Air Defense (GBAD), Electronic Warfare (EW), Adaptation cadence, Counter Unmanned Aircraft Systems (C-UAS).

Introduction

Drones and air defenses are reshaping the war in Ukraine day by day. The sky is constantly contested and thus rarely owned by one side. Because of this, striking and scouting is mainly conducted by drones and missiles. The effect of those strikes is felt by small units on the ground: movement is riskier, concealment is harder, and mistakes are costly because target acquisition capabilities are abundant and cheap munitions mounted on cheap drones are highly accessible. This environment has narrowed the room for classic, sustained air superiority.¹

Ukraine has rigorously been trying to scale up production and fielding of drones while professionalizing the routine that keeps them up in the air – short training cycles, forward repair branches, and standardized handling process. CSIS and RUSI assessments portray a system that improves through repetition. In parallel, Europe’s discussion about a “drone wall” reflects a political and technical way to sense, share, and intercept threats cross-border. This is a clear sign that partners are trying to convert Ukrainian lessons into regional habits.²

This paper is relevant to both scholarly and policy audiences because it links battlefield adaptation to force design and budgeting choices. It speaks directly to procurement timing, training throughout, and the integration of EW with short-range air defense (SHORAD) and ground-based air defense (GBAD) – issues that determine whether modest defense outlays can produce credible deterrence and sustained combat effectiveness.

The hypothesis of this paper is straightforward. In contested EW environments (Jan 2023 – Sep 2025), the persistence of air denial and logistics interdiction increases with (i) low – cost UAS mass and (ii) GBAD layering, but only when unit adaptation cadence is high; when cadence is low, added UAS mass yields transient or no gains.

The scientific contribution is twofold. First, the paper operationalizes adaptation cadence as a measurable variable connecting organizational learning to battlefield outcome. Second, it advances cross-case comparison and policy testing beyond a single theater.

Literature and Theoretical Expectations

Air denial vs. air superiority. Open sources show Ukraine repeatedly denying air superiority and shaping tempo through GBAD and dispersion-illustrating that denial can dominate even when neither side controls the sky. This aligns with a defensive-realist intuition: when the defense is structurally advantaged (layered GBAD, dispersion, deception), denial strategies pay.³

Affordable mass vs. “exquisite” platforms. Reporting on Ukraine’s wartime drone sector documents rapid scaling and deregulation that enabled thousands of long-range drones in 2024, but sustained effects depend on how fast units can absorb and maintain them.⁴

Organizational adaptation. PME fieldwork highlights frontline workshops that repair drones in hours and decentralized training pipelines that keep crews on mission. CSIS discussions em-

1 Ibid. Hunter Stoll, John Hoehn, and William Courtney

2 CSIS, “The Russia Ukraine Drone War: Innovation on the Frontlines and Beyond,” May 28, 2025. <https://surl.li/uonyqj>, Accessed 06.11 2025.

3 Stoll, Hoehn, and Courtney, “Air Defense Shapes Warfighting....”

4 Tom Balmforth, “Ukraine to Produce Thousands of Long-Range Drones in 2024,” Reuters, February 12, 2024. <https://shorturl.at/86jYN>, Accessed 06.11 2025.

phasize that cadence and scale, not a single platform, drive effects. These observations motivate treating units as learning systems.⁵

Expectation

H1 (Conditional persistence): In contested EW, persistent air-denial and logistics-interdiction emerge when affordable mass is paired with layered GBAD and unit adaptation cadence is fast.

Methodology

The study employs a comparative, open-source design spanning January 2023 – September 2025, focusing on engagements where independent corroboration is available. Cases were included if they documented: (1) observable EW conditions, (2) changes in drone or GBAD tactics, techniques, and procedures (TTPs), and (3) tangible operational effects such as neutralized assets, interdicted logistics, or degraded ISR.

To mitigate bias, the analysis triangulates official statements with independent reporting and excludes single – source reports. Where quantitative precision is unavailable, the study employs bounded qualitative categories and focuses on directional rather than point estimates. Limitations include fog of war distortions, reporting lags, and potential survivorship bias in widely publicized engagements.

This study codes adaptation cadence index from three observable indicators: (a) operator training throughput, (b) forward repair turnaround time (median days from intake to return to service), (c) software/hardware update cycle (median days between fielded updates).

In this paper, adaptation cadence refers to the repeatable rhythm by which units train new operators, repair and return damaged platforms, and push software/hardware updates forward. We track these as throughput/week, median repair days, and days between updates, respectively.

Operationalization and Coding

I observe adaptation cadence through three simple, open-source behaviors:

- **Training throughput:** how many UAS/C-UAS operators a brigade or equivalent are certified in an average week. As a working threshold for this paper, I treat “fast” as roughly a dozen or more per week, “moderate” as about five to eleven, and “slow” as fewer than five (based on PME reporting and unit communiqués).⁶
- **Forward repair turnaround:** typical time from damage to return-to-service using front-line repair cells. I treat “fast” as three days or less, “moderate” as about four to seven, and “slow” as more than a week.⁷
- **Update rhythm:** typical interval between fielded hardware/software updates to counter new adversary measures. I treat “fast” as about two weeks or faster, “moderate” as two to four weeks, and “slow” as longer than a month.⁸

5 Jorge Rivero, “Innovation Under Fire,” Modern War Institute at West Point, March 25, 2025. <https://shorturl.at/6T28J>, Accessed 06.11 2025.

6 Ibid. Jorge Rivero

7 Ibid. Jorge Rivero

8 CSIS, “The Russia-Ukraine Drone War.”

Classification rule. I describe an episode as “high-cadence” when at least two of the three behaviors are “fast” and none is “slow”; low-cadence when at least two are “slow”, otherwise medium. These thresholds are working cut-offs to make the concept falsifiable with public sources.

Air Denial without Air Superiority

Across several sectors, layered SHORAD with EW plus high cadence produced durable air denial, pushing manned aviation to standoff distances despite no side achieving air superiority. The clearest change that war in Ukraine has brought is the routine presence of small drones. A few years ago using them in tactical operations would have been unusual. Reconnaissance drones extend observation capability, correct artillery in real time, and record strikes for further analysis and learning. FPV drones have multiplied the number of situations in which a small team or even an individual soldier can threaten a much more expensive vehicle. Environmental constraints play less and less role in such operations. More eyes in the air, better acquisition of relevant coordinates and increased number of hits reduce the value of massed movement that is so characteristic for Russian Armed Forces. It is pertinent to observe that the air war, characterized by dense sensor – shooter environment, was enabled as much by organizational habits, as by new devices – the quiet work of standardizing kits, rotating pilots, and fixing what breaks.⁹

Affordable Mass Requires Cadence

Affordable mass delivers persistent ISR/strike and interdiction of logistics only when units sustain fast training, fast repairs, and frequent updates. Ukraine’s surge in long-range drone production shows the mass; PME reporting on frontline workshops explains why effects last where turnaround is measured in hours or a few days.¹⁰

It goes without saying that this new normal reality pressures logistics first. Drivers of military trucks used to use routes and daytime schedules. Now they have to change paths and timings, use decoys, and accept the delays that come with moving in smaller supply trains. The supply chain that keeps the drones up in the air – batteries, antennas, motors, spare parts – demands attention equal to ammo and fuel. Units have become proficient in setting up repair sites close to the front-line, keeping simple checklists for battery health and radio connectivity, and in rotating operators to avoid fatigue. In this respect the innovation is mostly procedural. It is the discipline that drives a unit to repeat basic tasks every day and week and this sets proper conditions for the technologies to matter on the battlefield. RUSI’s reporting, oriented on the field, captures this rhythm of adaptation. Day-to-day coverage from different sources shows the same pattern among other unmanned platforms such as unmanned ground vehicles (UGV) that are being used at limited range to conduct casualty evacuation.¹¹

EW/C-UAS Co-evolution

The measure-countermeasure loop now drives outcomes at the tactical edge. Units that field

⁹ Ibid.

¹⁰ Balmforth, “Ukraine to Produce Thousands of Long-Range Drones.”

¹¹ Jack Watling and Nick Reynolds, “Tactical Developments During the Third Year of the Russo-Ukrainian War (London: RUSI, February 2025), 8. <https://shorturl.at/qpeBr>

updates quickly stay inside the opponent's adaptation cycle. CSIS discussions and RUSI field analysis describe this as a cadence problem rather than a single system fix.¹²

The other aspect discussed is air defense. If drones changed how units see and strike, ground – based air defense shows why neither side simply flies over the other at will. Air defense radars, mobile short range air defense, interceptor drones, medium – range surface – to – air missiles, guns, and MANPADs together have denied persistent air superiority and made pilots operate cautiously at higher risks. Where air defenses are strong, stalemate on the ground is reinforced. Where they are weak, the human and infrastructural costs climb. The air became a place of constant bargaining in which a small misstep, flying over a wrong route, or employing wrong radar at the wrong time, can be used to either side's advantage.

The logic behind the air defense actions now runs from a single MANPAD to the national network. At the lowest level, units are permanently experimenting with hand – held or vehicle mounted jammers¹³, machine guns, and simple reporting rules to disseminate info smoothly and support the understanding of common operational picture. Going higher, mobile short-range batteries maneuver to protect key logistics and command nodes. At the national level early warning sensors are employed along with decision-making chains to authorize intercepts. Because drones not always stop at borders, this layering has regional dimension as well. When European officials discuss a “drone wall”, they are basically talking about shared sensors, common procedures, and faster cross border decisions to detect, track and neutralize air threat considering Ukrainian experience. The stakes are getting increasingly high day by day, especially considering the recent violation of NATO airspace by Russian aircraft. Reports about recent incursions have accelerated these conversations, stressing that cooperation with Ukraine to turn the “drone wall” into reality, is essential.¹⁴

Air denial is attainable without air superiority when layers are networked. Units that fused sensors, jamming, guns, SHORAD, and decoys under coherent command and control (C2) consistently degraded hostile unmanned sorties at the tactical edge. The effect was not driven by any single component but by the interaction among layers, particularly when emissions discipline and deception were practiced.¹⁵ For small states, the implication is that networking existing layers yields greater marginal returns than any single “magic” system.

When talking about the significance of drones, among the most important aspects is the production level. Ukrainian production and fielding of drones have moved from hundreds to thousands and recently to millions¹⁶. And maybe the foremost implication is the fact that training, repair, and procurement kept pace with production level to matter at the frontline. The breakthrough lies in cadence, rather than in a single exquisite platform. The speed adaptation around electronic warfare, including shifting to more resistant control links, and pre-programmed flight paths, is another milestone for an eventual success. We are not saying that technology does not matter. It is

12 CSIS, “The Russia-Ukraine Drone War.”

13 Watling et al., “Tactical Developments,” 19.

14 John Irish, “Use Ukraine’s Counter-Drone Expertise to Protect NATO’s Borders.” Reuters, September 23, 2025. <https://surl.li/nqvpyu>, Accessed 06.11 2025.

15 Mark, Hvizda et al., “Dispersed, Disguised, and Degradable: The Implications of the Fighting in Ukraine for Future US-Involved Conflicts (Santa Monica, CA: RAND Corporation, 2025) 11, RR-A3141 – 2, <https://shorturl.at/6ddBe>, Accessed 06.11 2025.

16 Tom Balmforth, “Ukraine to Produce Thousands of Long-Range Drones in 2024”

that technology without process does not bring about any tangible changes while modest technology embedded in a strong routine gets far better results.¹⁷

Additionally, training throughput and micro-repair nodes are decisive multipliers. Where operator pipelines ran continuously (Balmforth, 2024) and repair cells operated close to the front, effective mass was sustained despite losses (Rivero, 2025). Proximity reduced downtime, accelerated feedback, and enabled iterative operations. For small states, the recommendation is to push maintenance forward and maintain a standing rhythm to keep fielded units aligned with the latest countermeasure capabilities.

Drones are not associated only with air. The maritime dimension illustrates the same principle with different tools. Ukraine's use of unmanned marine vessels has pushed the Russian Black Sea Fleet back to Novorossiysk and clearly showcased that an affordable autonomy can harass larger fleets and strike High Value Targets. Similar to air drones, the real requirement about naval drones is not only having a vehicle, but the system around it such as intelligence that finds suitable routes, resistant control links and replenishment that allows repeated action. Such systems, ground, air, and naval drones, combined with land based fires and air defenses. Alter patterns on the battlefield and put pressure on assets that once felt safe in air or at sea. The lesson is as simple as it gets, low-cost autonomous systems, if paired with reliable procedures and proper information, can open options even for states without large fleets or air capabilities.¹⁸

Finally, considering the ongoing situation, the tempo of adaptation is likely to increase rather than slow, especially the West's growing involvement in Ukraine's military enterprises. Both sides are experimenting new ways to overcome the obstacles caused by increasingly fluid environment at the front. As defenders improve cueing across radars, cameras, and other target acquisition capabilities, attackers increase the size and variety of attacks, notably using large numbers Iranian – Russian Shaheds/Gerans combined cruise missiles launched from strategic aviation and ground based ballistic missiles. Such density stresses defenses and makes it easier to find gaps through the layered defenses. In this setting, it is crucial to have reliable process that adequately answers ever-changing threats in the full scale war. This only comes from habits that convert weekly learning into next – week practice: issuing checklists, pushing software and hardware updates, and resupplying the simplest parts that keep systems in the fight.

Conclusion

External validity. The conditions behind persistent air denial in Ukraine – layered GBAD, dispersion, deception, and high cadence – are achievable by small states at a reasonable cost if they prioritize training pipelines, mobile forward repair, and rapid update processes over exquisite one-off platforms.¹⁹

Limitations. Public reporting is uneven. Well-documented successes can bias perception. I mitigate by pairing think-tank/PME fieldwork with wire reporting and using conservative lan-

17 Kateryna Bondar, "Understanding the Military AI Ecosystem of Ukraine," CSIS, November 12, 2024, <https://shorturl.at/G6Cyu>, Accessed 06.11 2025.

18 CSIS, "The Russia-Ukraine Drone War."

19 James, Black, et al., "Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine, UK: RAND Corporation, 2024), 20, RRA3400- 1, <https://shorturl.at/DD6QU>

guage where counts are not reported.²⁰

To conclude, it can be said that persistent air denial and interdiction of logistics in contested EW environment hinge on adaptation cadence and layered GBAD; mass alone is insufficient. Where units train many operators each week, repair damaged systems within days, and push updates on roughly a two-week rhythm, effects tend to persist rather than spike and fade.²¹

For small states.

- **Fund cadence enablers first:** decentralized operator schools, mobile repair teams near contact lines, and standing update cells.

- **Layer the cheap with the cheap:** jammers, decoys, MANPADS, attack helicopters and simple reporting drills under coherent command and control (C2) before buying exquisite systems.²²

For alliances.

- **Resource routines, not just platforms:** sustained training flows, repair kits, and update pipelines.

- **Codify and share playbooks** drawn from PME and field analyses; exercise and evaluate cadence metrics, not platform counts.²³

Bibliography

- Balmforth, Tom. "Ukraine to Produce Thousands of Long-Range Drones in 2024, Minister Says." Reuters, February 12, 2024. <https://shorturl.at/86jYN>, Accessed 06.11.2025.
- Black, James et al., "Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine". UK: RAND Corporation, 2024. RAND Research Report RRA3400-1. pp 5-23.
- Bondar, Kateryna. "Understanding the Military AI Ecosystem of Ukraine." Washington, DC: Center for Strategic and International Studies (CSIS), November 12, 2024. <https://shorturl.at/G6Cyu>, Accessed 06.11.2025.
- Center for Strategic and International Studies (CSIS), 2025. "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond". <https://surl.lu/jeiity>, Accessed 06.11.2025.
- Hvizda, Mark, Bryan Frederick, Alisa Laufer, Alexandra T. Evans, Kristen Gunness, and David A. Ochmanek. "Dispersed, Disguised, and Degradable: The Implications of the Fighting in Ukraine for Future US-Involved Conflicts". Santa Monica, CA: RAND Corporation, 2025. RR-A3141-2. Pp. 8-25.
- Irish, John. "Use Ukraine's counter drone expertise to protect NATO's borders, Lithuania says". Reuters, September 23, 2025. <https://surl.li/cifyyt>, Accessed 06.11.2025.
- Koś, Wojciech. "Poland will shoot down encroaching Russian aircraft, warns PM Tusk." POLITICO Europe, September 22, 2025. <https://shorturl.at/2Vu4K>, Accessed 06.11.2025.
- Rivero, Jorge. "Innovating Under Fire: Lessons from Ukraine's Frontline Drone Workshops." Modern War Institute, March 25, 2025. <https://shorturl.at/6T28J>, Accessed 06.11.2025.
- Stoll, Hunter, Hoehn, John, and Courtney, William. 2024. "Air Defense Shapes Warfighting in Ukraine". <https://shorturl.at/fhajT>, Accessed 06.11.2025.
- Taylor, Zane Jarret, and William Dean Long. "Maneuvering in Contested Skies." Over The Horizon Journal, October 6, 2024. <https://surl.lt/optftu>, Accessed 06.11.2025.
- Watling, Jack et al., Tactical Developments During the Third Year of the Russo-Ukrainian War. London: RUSI, February 2025. pp. 3–22. <https://shorturl.at/qpeBr>, Accessed 06.11.2025.

20 Watling and Reynolds, "Tactical Developments," 19.

21 Rivero, "Innovating Under Fire."

22 Watling and Reynolds, "Tactical Developments," 18.

23 CSIS, "The Russia-Ukraine Drone War."

INNOVATION AND COERCION: HOW CHINA'S DEFENSE MODERNIZATION SHAPES SEA POWER THE SOUTH CHINA DYNAMICS

Private Luka Tchighladze

The Learner of a Master's Degree Program (International Relations and Diplomacy) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Nikoloz Samkharadze

Professor of Master's Program in International Relations and Diplomacy of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

This paper argues that China's military modernization is a sophisticated form of statecraft, which is strategically used to expand China's military control over South China Sea without opening tense confrontation. China is focusing on targeted technological innovations like advancing missiles, surveillance networks and militarization of artificial islands rather than just building a larger military. The general goal is to create a powerful system of daily coercion. This strategy, which operates in "grey zone" between peace and conflict, aims to intimidate neighboring states, deter United States' intervention in the region and change the territorial status quo in its favor.

The analysis focuses on China's key military advancements in the region. It explains how they translate into strategic power. It then demonstrates how these technologies are actively used to support a campaign of diplomatic, legal and paramilitary pressure. Finally, the paper examines the regional response - how countries like the Philippines and Vietnam are attempting to counter China's influence through their own "counter-innovation" strategies. The paper concludes that the South China Sea has become a critical testing ground for 21st century power dynamics, where technological superiority and strategic ingenuity are now more decisive than traditional military strength alone.

Keywords: Military Modernization, Coercive Diplomacy, Grey-Zone, Counter-Innovation, A2/AD (Anti-Access/Area Denial)

Introduction

The South China Sea is a vital shipping route, where about one-third of the world's trade passing through it. Because of this reason this area has become spotlight of regional geopolitical tension. The People's Republic of China, as the region's most powerful country, claims most of the sea using its "nine-dash line" map¹. This dispute involved mostly diplomatic talks and minor incidents for a long time. However, the 21st century has seen a major change, largely because of China's rapid military modernization, known as the People's Liberation Army². This is not just about China building more ships and planes. It represents a fundamental improvement in its military technology and strategy. China is focused on developing advanced weapons and technology including long-range missile systems to artificial intelligence. This has become a key part of its foreign policy. This paper argues that China uses this military innovation as a deliberate tool of power. Its goal is to change the situation in the South China Sea to its advantage through a strategy of pressure, not just open conflict. This approach aims to force neighboring countries to accept its claims and to make it harder for the United States to intervene effectively. To support this argument, the analysis will first explain how military innovation can be used to pressure other countries. It will then outline the main features of China's military modernization in the South China Sea, showing how new technologies give China strategic influence. Next, it will look at China's combined system of pressure, which mixes military power with legal claims and the use of coast guard and militia ships. Finally, the paper will evaluate how the region is responding, and it will be focused on the new security partnerships that are being formed between Southeast Asian nations and other powers like the US. These partnerships are an early attempt to balance China's growing influence.

Main Part

China's Military Modernization in the South China Sea

China's military modernization is a wide-ranging project. Its use in the South China Sea follows a clear and specific plan. The most obvious change is in its navy. Chinese navy has grown from a small coastal force into the world's largest navy in consideration of number of the ships (Cheung 2025). It now uses advanced destroyers, like the Type 055. These destroyers are equipped with powerful radars and long-range missiles. These ships can operate across the entire sea and it became a challenge for the movement of other navies in the area. At the same time, China's growing fleet of attack and ballistic missile submarines creates a powerful threat beneath the waves. This makes it very difficult for opponents to operate in this zone. However, the most significant change, is the militarization of man-made islands. China has built up reefs like Fiery Cross and Mischief Reef into permanent military bases³. These are no longer small sandbanks, they now have runways, deep-water ports, radar systems and even suspected shelters for missiles. Placing anti-ship and anti-air missiles on these islands gives China levers to control the sea and airspace

1 Kamil Nowak, Historical Evolution of the Late 20th-Century Maritime Claims, the Concept of the Nine-Dash Line, and the Dispute in the South China Sea, 2024

2 Cheung, Tai Ming, Back to the Future: The Rise of Militarization in China in the 2020s, 2025

3 Madelyn MacMurray, Carolyn Gruber, Militarized Commons: How Territorial Competition is Weaponizing Fisheries and Destroying the South China Sea, 2025

across a huge area. This creates a defensive zone that is hard to penetrate. Supporting these physical structures is an advanced network of surveillance and command systems. China uses a web of spy satellites, long-range radars and military drones to watch the South China Sea constantly. This system feeds information into a central command, creating a fast and efficient “kill chain”-the process of finding, tracking and striking a target. This means that any ship, from a Vietnamese frigate to a US aircraft carrier, can be monitored in real time. This makes the South China Sea a transparent battlefield for China, while it makes any operation by a rival nation much more risky and costly.

Innovation and Coercive Diplomacy

China does not save its new military technology for a possible future war. Instead, it uses this technology every day as a tool of coercive diplomacy. Coercion here means using the threat of military force to persuade an opponent to back down or agree to demands⁴. China’s strategy is a skilled example of using its modern military to reach political goals without starting an actual war. A clear example is how China enforces its self-declared Air Defense Identification Zone and its broad claims over the South China Sea. Even without an official ADIZ over the whole area, China often acts as if there is one. Ships from the Chinese Navy and Coast Guard, which are now larger and more heavily armed, regularly confront and harass military and commercial ships from other countries within the “nine-dash line.” These “grey-zone” actions include dangerous maneuvers, for example using military-grade lasers and blocking other countries from resupplying their outposts (Nowak 2024). The unspoken threat that gives these actions their power is the presence of advanced Chinese warships and land-based missiles on nearby artificial islands. The message is clear: if you escalate this situation, you could face a military response. This military pressure is combined with legal and administrative pressure. China can monitor the sea by using its advanced surveillance systems and then send its “maritime militia” which is a government-controlled fleet of fishing boats, to swarm into the exclusive economic zones of other nations. It then justifies these actions with its own broad interpretation of international law. This is despite a 2016 international court ruling that rejected the legal basis for China’s “nine-dash line” claim. China creates a new normal on the water, forcing other countries to constantly react to its moves by combining a physical presence with a disputed legal story⁵.

The main target of this coercive strategy is often the United States. By demonstrating it can threaten key U.S. assets like aircraft carriers with missiles like the “carrier-killer” DF-21D, China aims to deter the U.S. from intervening. Every successful missile test sends a signal to Washington about the high cost of getting involved in a crisis. This creates a stalemate for high-level conflict, which gives China more freedom to act in the grey-zone. While the U.S. still conducts naval patrols to challenge China’s claims, the environment is now much riskier. This makes the U.S. seem more cautious and potentially less reliable to its regional partners. In this way, China’s technological advances directly support its strategy of coercion.

⁴ Ketian Zhang, *Chinese Coercion in the South China Sea: Resolve and Costs*, 2020

⁵ Apon Zahir, *Militarization, Power Projection and Territorial Disputes In The South China Sea*, 2025

Regional Responses and Counter-Innovation Partnerships

In response to China's constant and evolving pressure, Southeast Asian nations have reacted in different ways. Their choices are shaped by their economic ties to China, their military weakness and their diplomatic strategies. However, a clear pattern is now clear: countries are moving away from acting alone and are instead seeking collective strategies and partnerships with outside powers to balance China's influence. This has led to new "counter-innovation partnerships," which is designed to close the technology and capability gap. Some countries have chosen a more direct approach. For example, the Philippines has strengthened its long-standing alliance with the United States⁶. A key agreement, the Enhanced Defense Cooperation Agreement has been activated. This agreement allows the United States' forces to use several Philippine military bases (Walberg, J, Connell, E 2025). It is important to highlight that some of these bases that face the South China Sea are positioning American assets to directly watch and respond to Chinese movements. This is a strategic upgrade to the alliance, which is making it more operational. At the same time Vietnam has quietly deepened its security relationships while officially sticking to a policy of no military alliances⁷. It has bought modern submarines from Russia and more importantly, it is building stronger ties for intelligence and training with the United States, Japan and India. For Vietnam, the innovation is in creating a diverse network of partners to counterbalance China.

However, the most important development is the creation of small and focused security groups. The "Quad" (the United States, Japan, India, and Australia) now focuses more on maritime security in order to provide Southeast Asian countries with patrol boats and radar systems. More significantly, the AUKUS pact (Australia, the UK and the United States) represents a major leap forward⁸. Its plans to provide Australia with nuclear-powered submarines and to develop advanced technologies like AI and hypersonic weapons are a direct answer to China's own military modernization. AUKUS aims to out-innovate China and ensure the technological balance in the region does not shift entirely in Beijing's favor. Within Southeast Asia, the ASEAN group has found it difficult to stay united due to China's economic influence. Yet, there are still efforts to find diplomatic solutions, such as the long-discussed Code of Conduct for the South China Sea. Individually, countries like Indonesia are taking action by building new naval bases to better protect their waters from Chinese ships. The response to China is not a single, unified plan. Instead, it is a combined effort involving stronger alliances, new security pacts, and national military upgrades. Together, these actions form a determined, if fragmented, system of "counter-coercion" aimed at ensuring China does not have total control in the region.

Conclusion

China's military modernization has a bigger purpose than an effort to protect its borders. It is the main part of a sophisticated plan to establish control over the South China Sea. Beijing is not just building a larger military, it is strategically developing specific technologies to achieve dominance. This strategy rests on three key areas of innovation. These innovations work together

6 Jonathan Walberg, Ethan Connell, How the Philippines Can Counter China's South China Sea Aggression, 2025

7 James Borton, Vietnam's New South China Sea Play: From Militarization to Conservation, 2025

8 Truong Phi Cuong, The role of the AUKUS alliance in counterbalancing China, 2023

to create a powerful and persistent form of coercion. First, China has focused on what experts call Anti-Access/Area Denial also known as A2/AD capabilities. These are systems designed to prevent other militaries, especially the United States Navy from operating freely in the region. This includes advanced missiles that can threaten large ships like aircraft carriers from hundreds of miles away (Cheung 2025). China can threaten a vast area of the sea by deploying these missiles on its artificial islands which creates a “no-go zone” for adversaries without firing a single shot.

Second, China has built a vast and modern surveillance network. This system combines satellites, long-range radars, drones and undersea sensors. Its purpose is to make the South China Sea a “transparent” battlefield for China⁹. They can track the movements of every foreign warship, aircraft and even fishing boat in real-time. This incredible awareness allows China to monitor its rivals, respond quickly to their actions and control the information environment.

Third, and most boldly, China has physically changed the geography of the region through its island-building campaign. China has created fixed “aircraft carriers” in the heart of the sea by turning small reefs into permanent military bases. These islands host runways, ports and missile shelters, which allow China to maintain a constant military presence far from its mainland. This is a form of territorial innovation that allows it to project power and enforce its claims day after day.

The crucial point is that these technologies are not kept in reserve for a future war. They are used every day in a campaign of “grey-zone” tactics and this allows China slowly to push its boundaries. The goal is to gradually change the facts on the ground and at sea. This pressure has triggered a response. Countries in the region are forming “counter-innovation” partnerships in order to balance China’s power. The AUKUS pact, which will provide Australia with nuclear-powered submarines, is a direct answer to China’s A2/AD systems¹⁰. Similarly, the Philippines and Vietnam are deepening security ties with the US, Japan and other states. Their goal is to gain access to better technology and intelligence. This means the South China Sea has become a laboratory for 21st-century conflict. The competition is no longer just about who has the most ships - it is about who has the best technology and the smartest strategy. The final outcome is still unknown. It will depend on whether the United States and its partners can keep up their own technological pace and whether Southeast Asian nations can present a united front. However, one thing is certain: the future of this critical global waterway will be decided by the ongoing race between coercion and counter-coercion, played out in the dangerous grey area between peace and war.

Bibliography

- Borton, James. 2025. „Vietnam’s New South China Sea Play: From Militarization to Conservation.“
- Cheung, Tai Ming. 2025. *Back to the Future: The Rise of Militarization in China in the 2020s*. IGCC.
- Cuong, Truong Phi. 2023. „The role of the AUKUS alliance in counterbalancing China.“ *International Journal of Multidisciplinary Research and Growth Evaluation*.
- Lee, Hwon. 2023. „The Legality of Militarization of the South China Sea and Its Legal Implications.“
- MacMurray, M, Gruber. C. 2025. „Militarized Commons: How Territorial Competition is Weaponizing Fisheries and Destroying the South China Sea.“
2024. *MILITARY AND SECURITY DEVELOPMENTS*. ANNUAL REPORT TO CONGRESS, U.S. Department of Defense.

9 U.S. Department of Defense, 2024

10 Truong Phi Cuong, The role of the AUKUS alliance in counterbalancing China, 2023

- Nowak, Kamil. 2024. *Historical Evolution of the Late 20th-Century Maritime Claims, the Concept of the Nine-Dash Line, and the Dispute in the South China Sea*. West Virginia University.
- Reddick, Justin L. 2017. *Under the Dragon's Wing: A Strategic Approach to China's Militarization Efforts of its Artificial Islands in the South China Sea*. US Army Command and General Staff College Fort Leavenworth United States.
- Walberg, J, Connell. E. 2025. „How the Philippines Can Counter China's South China Sea Aggression.“ *The Diplomat*.
- Zahir, Apon. 2024. *Militarization, Power Projection and Territorial Disuputes In The South China Sea*. Center fo Governance Studies.
- Zhang, Ketian. 2020. „Chinese Coercion in the South China Sea: Resolve and Costs.“ *International Security*.

UNMANNED AERIAL VEHICLES AND THEIR STRATEGIC ROLE IN RUSSIA–UKRAINE CONFLICT

Sergi Khurtsidze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Leri Dotiashvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Maia Gamsakhurdia

Chief Scientist of Scientific-Research Center of
LEPL-David Aghmashenebeli National Defence Academy of Georgia,
Ph.D. in International Relations;
ORCID: <https://orcid.org/0009-0008-3739-9226>

Abstract

The ongoing Russia–Ukraine war has profoundly transformed the role and perception of Unmanned Aerial Vehicles (UAVs) in modern warfare. This conflict has accelerated changes across multiple dimensions of military affairs—political, social, economic, and organizational—with technological advancement driving a revolution in military strategy at unprecedented speed. A UAV, or unmanned aerial vehicle, is a military aircraft that operates autonomously or through remote control. It is equipped with advanced technologies such as sensors, target designators, surveillance systems, and offensive weaponry, allowing it to neutralize or destroy enemy targets with high precision and minimal human risk. The operational effectiveness of UAVs first gained global attention during the Nagorno-Karabakh conflict, where Azerbaijan's extensive use of drones played a decisive role in securing victory. The Armenian armed forces lacked effective counter-drone systems, highlighting how technological superiority can determine battlefield outcomes.

Turkey, a regional power and Ukraine's defense partner, has also emerged as a leading producer and operator of UAVs. Its Bayraktar TB2 drones have become a cornerstone of modern warfare and a symbol of technological self-sufficiency. Turkey began supplying Bayraktar TB2s to Ukraine in 2019, and these systems have since demonstrated remarkable effectiveness in combat—enhancing situational awareness, improving targeting precision, and successfully engaging armored vehicles and artillery. The use of UAVs in contemporary conflicts, particularly in Ukraine, marks a significant shift in global military doctrine—demonstrating how autonomous systems and technological innovation are reshaping the future of warfare.

Keywords: Unmanned Aerial Vehicles (UAVs); modern warfare; Russia–Ukraine war; Bayraktar TB2; Turkey; Nagorno-Karabakh conflict; drone technology; military innovation; autonomous systems; defense transformation.

Introduction

In today's rapidly changing world, technology has become the most powerful force reshaping the nature of war. Among the many innovations defining twenty-first-century conflicts, Unmanned Aerial Vehicles (UAVs)—or drones—stand out as one of the most transformative. The ongoing Russia–Ukraine war has demonstrated with striking clarity how drones are no longer just experimental tools but essential instruments of modern warfare. They influence not only the battlefield but also the political, social, and economic dimensions of conflict. A UAV is an aircraft that operates without a pilot on board. It can be guided remotely or follow programmed flight paths using onboard sensors and computers. These machines are equipped with advanced technologies such as cameras, sensors, target designators, and even precision munitions, allowing them to identify and strike targets with high accuracy while keeping human operators far from danger. The military advantages of UAVs are undeniable. They are versatile and accessible, capable of reaching areas that would be too dangerous or logistically impossible for human soldiers. They are also cost-effective, reducing the expense and risk of traditional reconnaissance or air missions. Drones can cover large areas quickly, making them ideal for surveillance, mapping, or battlefield assessment. Moreover, their data-collection capabilities—from high-resolution imagery to infrared and radar scanning—allow armies to gather intelligence in real time and make faster, more informed decisions.

However, as with any innovation, drones come with drawbacks. Their ability to record images and videos raises serious privacy and ethical concerns, particularly when used in civilian environments. Technical failures can lead to crashes, posing safety risks to people and infrastructure. The growing number of drones in the sky also contributes to airspace congestion, complicating coordination with manned aircraft. Even their production and disposal have environmental costs, as short-lived electronic components contribute to e-waste and resource depletion. Before the large-scale conflicts of recent years, drone weapons were often bulky and limited in mobility. Anti-drone “guns,” for example, were heavy, designed mainly for mounted use, and impractical for infantry units. But as technology evolved, UAVs became smaller, more agile, and more autonomous. Their use expanded beyond traditional combat roles—they now serve military, propaganda, media, and psychological purposes all at once. A single drone strike can damage infrastructure, film the attack for media dissemination, and shape global perceptions of power and control.

The perceived autonomy of UAVs also introduces a new moral and political complexity. While drones cannot yet make independent decisions, their semi-autonomous operation creates an illusion of self-directed action. This allows states or non-state actors engaged in hybrid warfare to avoid accountability, claiming that unintended strikes or controversial missions were the result of “technical” errors. Such ambiguity gives hybrid actors remarkable flexibility to adapt missions, control narratives, and blur the line between human and machine responsibility. In modern conflicts, technology and warfare have become deeply intertwined, often beyond state control. Traditional defense innovation, once dominated by national militaries, has shifted toward private companies and civilian developers. Many of the drones now used in Ukraine or the Middle East were originally designed for commercial or industrial purposes before being adapted for combat. This decentralization has accelerated innovation but also created new ethical and regulatory

challenges—raising questions about oversight, accountability, and the militarization of civilian technologies.

UAVs today are categorized into different types based on their altitude and endurance: High-Altitude Long-Endurance (HALE) systems, which are large and expensive; Medium-Altitude Long-Endurance (MALE) systems, offering a balance of cost and performance; and Tactical UAVs (TUAVs), which operate closer to the battlefield. While HALE systems are mainly strategic assets, it is the smaller, tactical drones that have reshaped warfare in practice—particularly in asymmetric or hybrid conflicts. The effectiveness of UAVs was first revealed dramatically in the Nagorno-Karabakh war, where Azerbaijan’s heavy reliance on drones helped it achieve a swift victory. Armenia’s forces, lacking proper air-defense systems, could not counter the precision and persistence of Azerbaijani drone strikes. A few years later, in Ukraine, the world witnessed similar tactics on a much larger scale. The Turkish-made Bayraktar TB2 drones, supplied to Ukraine since 2019, became symbols of resistance and technological adaptability. They provided Ukrainian forces with real-time intelligence, improved targeting accuracy, and a powerful psychological tool—both on the battlefield and in global media.

What these conflicts show is that UAVs have fundamentally changed the logic of war. They compress time between decision and action, extend the reach of smaller militaries, and democratize access to advanced airpower. At the same time, they blur the lines between civilian and military technologies, between defense and propaganda, between visibility and invisibility. In the age of hybrid conflict, the drone is not just a weapon—it is a strategic instrument of influence. It embodies both the promises and perils of technological progress: the ability to see and strike anywhere, and the temptation to do so without full understanding of the consequences. The challenge now facing modern militaries and policymakers is to balance innovation with ethics, ensuring that the same tools that make war more precise do not make it more permanent.

Main Part

UAVs in the Russia–Ukraine War: Operational Lessons and Strategic Implications

The deployment of Unmanned Aerial Vehicles (UAVs) in the Russia–Ukraine conflict, particularly in the Donetsk and Luhansk regions, has been primarily associated with intelligence, surveillance, and reconnaissance (ISR), target acquisition (TA), signals and electronic intelligence (SIGINT/ELINT), and electronic warfare (EW) operations. This focus reflects both the existing patterns of UAV development, which have evolved throughout the conflict—from tactical UAVs (TUAVs) to more advanced medium-altitude, long-endurance (MALE) systems—and the traditional operational doctrines of the belligerent parties. While UAVs were initially used for observation and targeting support, their role has gradually expanded toward more active and integrated combat functions. A UAV-linked weapon effect in the Ukrainian conflict can be illustrated by two notable examples. The first incident occurred on 22 March 2017, when a massive explosion destroyed an ammunition depot in Balakliya, approximately 100 kilometers from the front line. The explosion disrupted the supply of rockets and artillery shells to Ukrainian forces in Donbas. Media reports suggested that the attack might have involved the use of a Russian UAV equipped with an

explosive charge. Although the possibility of human error was not ruled out, Ukrainian forces have repeatedly detected or shot down Russian UAV systems, such as the Orlan-10, which appear to have been used mainly for ISR and target-acquisition missions.¹ A second, more destructive incident occurred on 11 July 2014, near Zelenopillya, during the early stages of the war. Russian forces reportedly used UAVs in conjunction with heavy artillery and multiple rocket launcher systems, almost completely destroying two Ukrainian army battalions within minutes. This event demonstrated Russia's ability to employ UAVs for artillery observation, fire correction, and precision coordination, greatly amplifying the lethality of its ground-based firepower. By deploying UAVs for targeting while keeping artillery units within Russian territory, Moscow could project force without direct cross-border engagement, minimizing the risk of Ukrainian retaliation. A counter-strike by Ukraine would have been strategically unviable—both because it could be portrayed as open aggression against Russia and because it would involve significant operational risks.

However, UAV operations on the Ukrainian side have begun to shift this balance. Effective strikes against armored formations, logistics nodes, and air-defense systems have demonstrated Ukraine's growing capability to contest Russian superiority.² Moreover, Ukraine has successfully used modified or domestically produced UAVs to conceal operational intent, complicating Russian intelligence and undermining the predictability of countermeasures. These capabilities not only expand Ukraine's tactical flexibility but also challenge the legitimacy of Russian responses, especially in contested airspace.

Recent developments indicate that tactical and strategic UAV use continues to evolve on both sides. On the Ukrainian side, significant progress has been made in domestic drone production, such as the Sokil-300, as well as in foreign procurement, notably the Bayraktar TB2 from Türkiye. Concurrently, Ukraine has enhanced its air-defense and counter-UAV systems, including radar complexes such as the 35D6M, to detect and neutralize enemy drones. On the Russian side, large-scale exercises like Kavkaz-2020 demonstrated Moscow's growing ability to coordinate multiple UAV units within a single operational framework. These maneuvers also confirmed that Russia's artillery precision and integration with UAV systems have significantly improved, enabling more synchronized and high-accuracy strikes. Furthermore, it is expected that Russia will seek to reduce its dependency on Israeli-made UAV technologies, given that sanctions or political tensions could restrict the supply of components and spare parts. Overall, the use of UAVs in the Russia–Ukraine conflict has evolved from tactical experimentation to a core element of both countries' military strategies. Drones have redefined reconnaissance, targeting, and precision engagement while serving as a bridge between conventional and hybrid warfare tactics. Their continued development and integration suggest that the Ukrainian battlefield has become a testing ground for the future of aerial warfare, where technology, adaptability, and innovation increasingly determine success.

Escalation Dynamics and Strategic Implications of UAV Use in the Ukraine Conflict

The conflict in Ukraine has demonstrated both escalatory and de-escalatory dynamics through the deployment of Unmanned Aerial Vehicles (UAVs) by various actors. On one hand, the use of

1 *Armyrecognition.com*. (2024, August 14). Retrieved from FOCUS: Innovation on the Battlefield—How Ukraine Is Expanding Drone Munitions.: <https://surl.li/chttyu>. Accessed 06.11.2025.

2 SPRENGEL, F. C. (2021). *Drones in hybrid warfare: Lessons from current*.

drones has significantly intensified the air domain of the conflict, introducing new uncertainties for both Ukraine and Russia regarding airspace control and situational awareness. This uncertainty was tragically illustrated by the shooting down of Malaysia Airlines Flight MH17, a Boeing 777, in July 2014—an incident that underscored the dangers of an increasingly congested and contested airspace. The proliferation of UAVs has also led to a continuous cycle of technological adaptation and counter-adaptation. Both Ukraine and Russia have expanded their drone arsenals while simultaneously investing in advanced radar and air-defense systems to counter UAV threats. This arms race has been accompanied by diplomatic friction, as evidenced by Russia's official warning to Türkiye regarding the export of Bayraktar TB2 drones to Ukraine—an indication of how UAV proliferation has become both a military and geopolitical flashpoint.

The two direct parties to the conflict continue to diversify and enhance their UAV capabilities, experimenting with varying levels of autonomy, endurance, and payload. Although conventional deployment patterns—such as surveillance, reconnaissance, and artillery targeting—still dominate, the range and sophistication of UAV applications are steadily expanding. In the event of renewed escalation, an even broader spectrum of drone operations—spanning offensive, defensive, and hybrid functions—can be expected. Conversely, UAVs have also served de-escalatory and peace-monitoring purposes. Since 2018, the Organization for Security and Co-operation in Europe (OSCE) has deployed Camcopter S-100 systems in eastern Ukraine to support neutral observation missions. These drones have been used to monitor ceasefire compliance, assess security incidents, and collect independent aerial imagery, helping international mediators maintain transparency between the parties. This application demonstrates that UAVs, while instruments of warfare, can also contribute to confidence-building and conflict management when employed within neutral frameworks.

A more recent and striking example of UAV innovation emerged with Operation “Spider’s Web,” conducted on June 1, 2025, which illustrated the growing effectiveness of asymmetric drone warfare. During this operation, Ukrainian forces reportedly employed approximately 117 drones to strike multiple airbases deep within Russian territory, damaging or destroying an estimated 41 aircraft, including strategic bombers. The losses—valued at nearly US\$7 billion—were inflicted at only a fraction of that cost, underscoring the disproportionate impact of low-cost technologies in modern warfare.³ Operation “Spider’s Web” demonstrated the convergence of commercial innovation, artificial intelligence, and open-source technology in contemporary conflict. Many of the UAVs used were modified commercial FPV (First-Person View) drones, equipped with open-source autonomous flight systems and operated through a distributed logistics network. Drones were transported by trucks, launched remotely or semi-autonomously, and coordinated through AI-driven mission planning and open-source intelligence (OSINT) platforms.

The strategic implications of this operation are profound. It revealed that affordable, widely available technologies can now achieve strategic-level effects once possible only through large-scale military operations. Geographic depth and territorial vastness, once reliable defensive advantages, no longer guarantee protection from precision strikes. Moreover, European and NATO

³ Mariano Zafra, Max Hunder, Anurag Rao and Sudev Kiyada. (2024, march 26). *How drone combat in Ukraine is changing warfare*. Retrieved from reuter.com: <https://surl.li/oyklhb>, Accessed 06.11.2025.

air-defense architectures, traditionally built around centralized command structures and conventional air superiority, have shown increasing vulnerability to low-cost, decentralized, and swarm-based drone attacks. In essence, the Ukraine conflict has become a testing ground for the democratization of military technology—where innovation, improvisation, and information integration can outweigh industrial-scale firepower. The lessons of this war suggest that the future of security will depend not only on who possesses the most advanced weapons but on who can adapt the fastest, integrate technology effectively, and maintain resilience against an ever-evolving technological threat landscape.⁴

Adapting to the New Threat Landscape: Lessons and Implications

To adapt effectively, modern defense strategies must become multilayered and adaptive. There is no single, universal solution to the drone threat; instead, states require a diversified and flexible approach that combines electronic warfare, signal jamming, radar-based detection, and counter-UAV systems. This must be complemented by the development of smaller, autonomous UAVs for interception and the physical protection of critical static infrastructure such as power plants, airbases, and ports.

Policymakers should also acknowledge that complete protection is impossible in the current technological environment. The realistic objective is to prioritize critical assets, enhance early-warning systems, and strengthen intelligence networks capable of detecting logistics, preparations, and staging for future drone operations well in advance. Analytical assessments of Operation “Spider’s Web” suggest that Ukraine’s reported success remains only partially verified. Much of the operation’s effectiveness depended on innovation, the element of surprise, and favorable logistical conditions. Replicating such a mission elsewhere would require comparable resources, intelligence coordination, and rigorous legal and ethical evaluation.

Another critical concern is that strategic infrastructure—such as airbases, power stations, and port facilities—can be easily identified through publicly available satellite imagery. Many of these assets remain insufficiently protected against low-altitude, small-drone incursions, creating vulnerabilities even for technologically advanced militaries.⁵

For Georgia and other regional states, the operation underscores an essential lesson: geography alone no longer guarantees security. Distance and terrain no longer provide natural protection in an era of low-cost, long-range drone capabilities. The region must therefore develop effective counter-drone capacities, conduct regular risk assessments, and reinforce the protection of critical infrastructure. Both short-term measures—such as localized jamming, physical shielding, and improved operational transparency—and long-term strategies—including advanced electronic defense and regional information sharing—are equally vital. Ultimately, Operation “Spider’s Web” should not be viewed merely as a tactical success but as a strategic signal that the very philosophy of defense is changing. Low-cost, widely accessible technologies now create unpredictable, high-impact threats, challenging conventional assumptions about deterrence and air superiority.

⁴ Ukraine’s Operation Spider’s Web is a game-changer for modern drone warfare. NATO should pay attention <https://surl.li/bam-rms>, Accessed 06.11.2025.

⁵ Ibid. Ukraine’s Operation Spider’s Web is a game-changer for modern drone warfare.

Future security will depend not on static defenses, but on intelligent, adaptive systems that can evolve as quickly as the threats themselves.

Notable targets reportedly struck during Operation “Spider’s Web”:

Olenya Air Base – Kola Peninsula (~1,900 km north of Ukraine)

Diaghilevo Air Base – Ryazan Oblast (~470 km from Ukraine)

Belaya Air Base – Irkutsk Oblast, deep Siberia (>4,000 km from Ukraine)

Ivanovo Air Base – Ivanovo Oblast (~700 km from Ukraine)⁶

Conclusion

Technology and Transformation: The Russia–Ukraine War and the Evolution of Modern Warfare

The Russia–Ukraine war has fundamentally reshaped contemporary understanding of warfare, exposing the profound and inseparable link between military strategy and technological innovation. It has revealed that progress in information technology, cybersecurity, artificial intelligence, and autonomous systems is no longer a supplementary enhancement to conventional military power but an essential foundation of modern defense capability. This conflict marks a historic turning point — a transition from industrial-era warfare, characterized by trenches and heavy artillery, to a digital battlespace defined by cyber operations, satellite coordination, unmanned systems, and real-time intelligence exchange. The rapid integration of drones, electronic countermeasures, satellite communications, and precision-guided weapons demonstrates how technology has compressed the traditional boundaries between physical and virtual combat. Military decisions that once took days are now made in seconds, based on live data transmitted from sensors, UAVs, and space-based systems. Within this technological landscape, Unmanned Aerial Vehicles (UAVs) have emerged as one of the most significant instruments of power projection. They represent not only tools of surveillance and precision strike but also symbols of a new military ethos — one that seeks to save “blood, sweat, and tears” by minimizing human exposure to risk. UAVs serve as surrogate combatants, capable of executing missions that once required direct human involvement. In this sense, drones enhance operational reach, endurance, and lethality while preserving human life on the operator’s side. Yet, this technological evolution also carries troubling implications. The accessibility and versatility of UAVs have encouraged their use not only by state militaries but also by non-state armed groups, insurgents, and terrorist organizations. These actors increasingly employ drones for asymmetric attacks, surveillance of civilian infrastructure, and the dissemination of fear through psychological operations. The same systems that reduce military casualties for one side can therefore amplify insecurity for civilians on the other. Moreover, UAVs blur traditional moral and legal boundaries in warfare. Their semi-autonomous operation challenges notions of accountability, complicating the application of international humanitarian law. When machines can select and engage targets with minimal human intervention, questions arise about responsibility, proportionality, and ethics. The diffusion of drone technology into civilian markets further intensifies these challenges, as modified commercial drones can now carry explosives or be used

6 How Ukraine’s Operation “Spider’s Web” Redefines Asymmetric Warfare, <https://surl.li/isiicir>, Accessed 06.11.2025.

for intelligence gathering with minimal cost and training. In this light, UAVs have become the weapons of our era—simultaneously embodying innovation, efficiency, and danger. Humanity faces a new strategic and ethical dilemma: how to harness these technologies for legitimate defense while preventing their misuse by hybrid threat actors. This requires not only technical countermeasures but also the development of global norms, regulations, and cooperative security frameworks capable of managing this transformative force responsibly. Ultimately, the Russia–Ukraine war demonstrates that technological dominance now defines strategic advantage. Future conflicts will be determined not only by who commands the largest armies, but by who can integrate technology, data, and human decision-making most effectively. The challenge of this century is therefore clear—to adapt to the realities of digital warfare without losing the ethical and humanitarian principles that define civilization itself.

Bibliography

- Armyrecognition.com*. (2024, August 14). Retrieved from FOCUS: Innovation on the Battlefield—How Ukraine Is Expanding Drone Munitions.: <https://www.armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/ukraine-russia-conflict/focus-innovation-on-the-battlefield-how-ukraine-is-expanding-drone-munitions>
- Mariano Zafra, Max Hunder, Anurag Rao and Sudev Kiyada. (2024, march 26). *How drone combat in Ukraine is changing warfare*. Retrieved from reuter.com: <https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/>
- SPRENGEL, F. C. (2021). *Drones in hybrid warfare:Lessons from current*.
Ukraine’s Operation Spider’s Web is a game-changer for modern drone warfare. NATO should pay attention <https://surl.li/bamrms>, Accessed 06.11.2025.
- How Ukraine’s Operation “Spider’s Web” Redefines Asymmetric Warfare, <https://surl.li/isicir>, Accessed 06.11.2025.

THE TRANSFORMATION OF MODERN WARFARE AND HYBRID THREATS: THE CASE OF THE RUSSIA–UKRAINE WAR AND RECOMMENDATIONS FOR GEORGIA.

Mangia Tchintcharauli

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Rati Kukuladze

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Kakha Futkaradze

Associate Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Doctor of Social Science,
orcid.org/0000-0001-9222-0673

Abstract

This paper analyzes the evolution of modern warfare in the context of the Russo–Ukrainian War, arguing that the conflict represents a decisive transition into fifth-generation warfare (5GW). Fifth-generation warfare is characterized by the fusion of conventional military operations with hybrid strategies, cyber operations, psychological influence campaigns, disinformation, and the deliberate targeting of societal resilience. Unlike earlier generations of warfare, where victory was measured by territorial occupation or destruction of enemy forces, 5GW aims to shape perceptions, undermine cognitive stability, and erode the political cohesion of the target state.

The study traces the historical development of warfare from first- to fifth-generation models and demonstrates how Russia's actions—from the hybrid annexation of Crimea in 2014 to the integrated hybrid-conventional campaign launched in 2022—illustrate the operational shift toward multi-domain conflict. Particular attention is given to the transformative role of emerging technologies, including artificial intelligence-driven targeting systems, unmanned aerial vehicles (UAVs), and long-range drone strikes. These technologies have altered strategic calculations by enabling highly cost-efficient, scalable, and asymmetric forms of warfare, allowing smaller states to impose significant damage on larger adversaries while introducing new technological and ethical vulnerabilities.

The analysis further examines the implications of this paradigm shift for Georgia. The continued occupation of Georgian territories, combined with incremental “creeping annexation” and persistent information and economic pressure, demonstrates that Georgia is already situated within an ongoing hybrid conflict environment. The paper argues that Georgia's security requires a comprehensive, whole-of-society resilience strategy that integrates defense policy, cyber protection, informational sovereignty, diplomatic coalition-building, and strategic infrastructure development—most notably through the creation of the Anaklia Deep-Sea Port and diversification of energy and trade corridors.

The findings highlight that in the era of fifth-generation warfare, sovereignty is defended not only on the battlefield but across the informational, technological, and geopolitical domains. Georgia's long-term stability depends on transforming strategic vulnerability into geopolitical indispensability by strengthening institutional resilience and international alignment.

Keywords: Fifth-Generation Warfare; Hybrid Warfare; Russo–Ukrainian War; Cognitive Security; Disinformation; Artificial Intelligence; Drone Warfare; Cyber Conflict; Strategic Resilience; Georgia; Creeping Annexation; Information Dominance; National Security Strategy; Multi-Domain Operations; Geopolitical Deterrence.

Introduction

The Transformation of Warfare: From First to Fifth Generation

The ongoing conflict in Ukraine has clearly demonstrated that warfare has undergone a profound transformation. The war has become far more complex than conventional strategic and tactical models once suggested. Today, scholars widely recognize five generations of warfare, each shaped by shifts in military technology, political structures, and socio-cultural conditions. Understanding contemporary conflict therefore requires tracing the historical evolution of war across these generational transitions.

First-Generation Warfare was characterized by line and column tactics, massed infantry formations, and cavalry charges. Conflicts such as the Napoleonic Wars and the American Civil War exemplify this style, where warfare relied heavily on discipline, close-order formations, and direct confrontation.

Second-Generation Warfare emerged alongside industrialization and the development of artillery and early firearms. Battles emphasized firepower, attrition, and static fronts rather than maneuver. The First World War stands as the most defining example, with trench warfare and heavy artillery bombardments dominating the battlefield.

Third-Generation Warfare shifted toward maneuver, speed, and mechanization. Technological progress allowed for fast, coordinated operations supported by armored vehicles, aviation, and mobile infantry. This approach, used extensively during World War II, prioritized rapid breakthroughs, encirclement, and striking deep into enemy territory.

Fourth-Generation Warfare marked the rise of asymmetric and hybrid conflict, where the distinctions between military and civilian spheres became blurred. Non-state actors, guerilla tactics, decentralized command structures, psychological operations, and political messaging became as important as kinetic confrontation. This form of warfare—rooted in ideological, cultural, and informational domains—dominated the late 20th century and continues into the present.¹

Main Part

Today, scholars argue that we are witnessing the emergence of Fifth-Generation Warfare (5GW)—a form of conflict deeply integrated with the digital, informational, and psychological environments of society. The battlefield has extended beyond physical territory to include cyberspace, data systems, and public consciousness. As Gabriel and Metz emphasize, the history of warfare is one of continuous adaptation between social structures, technology, and the organization of violence².

5GW is inseparable from today's technological landscape. Social media has become a decisive arena for influencing attitudes, shaping narratives, and destabilizing social cohesion. Artificial intelligence enhances deception, automates influence operations, and amplifies both propaganda and counter-propaganda. Cyberspace exposes critical infrastructure—communications, electricity, finance—to persistent attack. And unmanned systems, especially drones, allow precision strikes with minimal human involvement.

¹ Inashvili, G. (n.d.). Military blog, beginning of the 5th gen wars? *Homo Militaris*, (p. 2). Tbilisi.

² A. Richard, k. s. gabriel, *A short history of war the evolution of warfare and weapons*. U.S. army war college. (1992).

Schmid's analysis of the Ukrainian battlefield shows that contemporary warfare exploits vulnerabilities across political, informational, and technological interfaces, often operating outside clear attribution ³. Similarly, Kaldor's concept of "new wars" illustrates how modern conflicts merge state and non-state actors, mix political and criminal motives, and often target civilian populations as a means of control ⁴.

Across these theorists, one theme is consistent: modern war now targets entire societies. Confusion, uncertainty, and psychological collapse weaken a state more efficiently than traditional military defeat. Warfare is now powered by information flows, digital networks, and global interconnection.

The ongoing Russo-Ukrainian War demonstrates this transformation clearly. Both sides employ not only tanks and artillery, but also cyberattacks, drone swarms, disinformation campaigns, energy leverage, and global media manipulation. The conflict targets not only soldiers, but civilians, international audiences, and even the morale of their own populations.

Hybrid Warfare and Its Evolution in the Russo-Ukrainian War.

To understand this transformation, it is necessary to examine Russia's hybrid warfare doctrine. Russia's approach blends traditional military power with covert operations, cyber warfare, propaganda, private military companies, political destabilization, and economic coercion ⁵. It operates within the reaction time of the international community, seeking to achieve objectives before coordinated responses emerge.

This doctrine is shaped by Russia's experiences with Chechnya, Georgia (2008), U.S. operations in Iraq and Afghanistan, and the Arab Spring . These conflicts taught Moscow that modern warfare is multidimensional and must combine military and informational instruments.

The annexation of Crimea in 2014 demonstrated hybrid warfare at its most effective:

"Little Green Men" – unmarked Russian special forces seizing infrastructure and paralyzing response.

Cyberattacks against government and media platforms.

Information warfare via RT, Sputnik, and coordinated online networks ⁶.

Economic coercion, especially energy leverage over Ukraine and Europe.

This operation achieved strategic aims without full-scale war.

However, the 2022 escalation revealed the limits of hybrid warfare alone. When hybrid tactics failed to secure political control, Russia shifted to large-scale conventional invasion while still integrating cyber, information, economic pressure, and proxy warfare.

This integration demonstrates the core transformation of 5GW: Hybrid and conventional warfare are no longer separate phases, but simultaneously applied dimensions of a unified strategy.

Fifth-generation warfare aims not merely to defeat armies but to shape thinking, identity, memory, and emotional responses. Its central goal is to undermine decision-making processes and social stability, making it fundamentally a war for cognitive dominance.

³ J.Schmid, Hybrid warfare on the Ukrainian Battlefield. *Journal on baltic security*. sciendo. (2019).

⁴ M.koldor, *new and old wars*. Malden US: polity. (2012).

⁵ M. A. Fox, *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Kansas: School of Advanced Military Studies. (2017).

⁶ Paul, M. M. Christopher, The Russian "firehose of Falsehood" Propaganda model. *RAND*. (2016).

The Transformation of Modern Warfare and the Emergence of Fifth-Generation Conflict

Modern warfare has undergone a fundamental transformation, shifting away from strategies based solely on territorial occupation and destruction of enemy forces, toward forms of conflict that target the psychological, informational, and socio-political fabric of entire societies. The contemporary battlefield has expanded far beyond the physical frontline; today, critical arenas of struggle include digital information networks, media ecosystems, cyberspace, and human cognition. This evolution marks the emergence of Fifth-Generation Warfare (5GW)—a form of conflict whose primary objective is not simply to defeat an adversary militarily, but to shape perception, disrupt decision-making, and destabilize the social foundations that sustain political resilience. In essence, 5GW is a war of the mind.

This new generation of warfare would be unthinkable without the technologies that define the 21st century. The internet, social media platforms, artificial intelligence systems, cyber operations, and drone technology now constitute the primary instruments of strategic influence. Armed confrontation is no longer limited to tanks, artillery, and soldiers; instead, states increasingly deploy information campaigns to manipulate public opinion, cyberattacks to paralyze infrastructure, and non-transparent military actors—such as private military companies and hacker collectives—to obscure responsibility and avoid direct attribution. As Inashvili observes, the actors participating in modern warfare “are no longer exclusively national armies, but networks whose boundaries between state and non-state identities have become fluid.”⁷

Artificial intelligence has played a particularly transformative role. Historically, warfare was shaped by industrial capacity, troop numbers, and the strategic judgment of military leadership. Today, AI-driven analytical and targeting systems are redefining this balance by enabling autonomous decision-support, predictive threat modeling, and automated reconnaissance and strike coordination. AI does not simply enhance traditional forms of war—it alters them, producing a new paradigm in which data and algorithms become as decisive as firepower. This dynamic is clearly illustrated in Israel’s recent military operations. During “Guardian of the Walls” and the subsequent “Rising Lion” operation (2025), Israeli defense forces used AI platforms such as Hab-sora -The Gospel- to analyze vast quantities of intelligence data and identify high-value targets. Whereas human analysts could previously process a few dozen targets annually, AI systems were reported to identify hundreds daily. Yet this technological acceleration has come with grave ethical consequences: in Gaza, AI-enhanced targeting has contributed to mass civilian casualties, ⁸raising profound questions about accountability, proportionality, and the moral limits of autonomous warfare⁹.

Likewise, the Russo–Ukrainian War demonstrates how the proliferation of unmanned aerial systems (UAS) has reshaped the conduct of war. Drones now account for approximately 60–70 percent of battlefield casualties, marking a decisive departure from the traditional dominance of artillery or armored combat ¹⁰. Ukraine’s rapid transition from a drone importer to one of the

7 Inashvili, G. (n.d.). Military blog, beginning of the 5th gen wars? *Homo Militaris*, (p. 2). Tbilisi.

8 M. N. Schmitt, Retrieved from [lieber.westpoint.edu](https://surl.li/oyvxud), (2025, June 16).: <https://surl.li/oyvxud>, Accessed 07.11.2025

9 D.Kirichenko, Retrieved from [warroom.armywarcollege.edu](https://surl.li/daxlmr), (2025, August 21).: <https://surl.li/daxlmr>, Accessed 07.11.2025

10 R. Thomas, Retrieved from [army-technology.com](https://surl.li/jxhapq), (2025, April 8).: <https://surl.li/jxhapq>, Accessed 07.11.2025

world's largest producers, manufacturing an estimated 200,000 FPV drones per month by early 2025, illustrates how relatively low-cost technology can offset conventional military asymmetry. These drones, costing as little as \$400–\$2,000, routinely destroy tanks, air-defense systems, and electronic warfare platforms worth millions. Yet drone warfare is also deeply vulnerable to electronic warfare, which can disrupt navigation systems, jam communication links, or locate drone operators. Thus, drone conflict becomes not only a kinetic engagement, but also a battle for the electromagnetic spectrum.

Long-range strike drones further expand the strategic depth of conflict, allowing Ukraine to target oil refineries, ammunition depots, air bases, and command centers deep inside Russian territory. These strikes have caused fuel shortages and economic disruptions across multiple regions. Meanwhile, Russia has intensified mass drone attacks using domestically manufactured systems, increasing strike waves from 100 drones at a time to several hundred, with projections of up to 2,000 drones in a single strike cycle in late 2025. The result is a conflict environment where decentralized, inexpensive, and rapidly scalable technologies challenge traditional superiority based on size and industrial mass.

Taken together, these dynamics demonstrate that modern warfare has become a multi-domain, integrated continuum of conflict, where kinetic, informational, economic, and cyber operations operate simultaneously. The objective is not merely to defeat the enemy's army, but to break the psychological, institutional, and societal structures that sustain resistance. This is the defining logic of Fifth-Generation Warfare: the center of gravity is no longer the battlefield, but the mind, identity, and collective will of a society.

Conclusion

The Russo–Ukrainian War stands as a defining example of the ongoing transformation of warfare, marking a decisive shift toward a fifth-generation conflict environment. This new paradigm is characterized by the integration of conventional military force with hybrid, informational, cyber, and psychological operations, where the boundaries between war and peace are deliberately blurred. The conflict has demonstrated that the decisive battleground is no longer limited to geographic territory, but extends into the domains of perception, identity, information, and global interdependence. Victory is now measured not solely by control of land, but by the ability to shape narratives, disrupt critical infrastructure, influence public morale, and undermine political cohesion.

The progression from Russia's "near-perfect" hybrid seizure of Crimea in 2014 to the large-scale hybrid-conventional war after 2022 underscores that hybrid tactics are no longer supplemental—they constitute a core operational doctrine. The war has also revealed the central role of emerging technologies: artificial intelligence has transformed the speed and scale of intelligence processing and targeting; drones have become the dominant cause of battlefield casualties; and cyber operations routinely strike essential systems far from the physical front. These developments have fundamentally altered the strategic balance, enabling even smaller or resource-constrained states to impose asymmetric costs on more powerful adversaries, while simultaneously introducing unprecedented vulnerabilities.

For Georgia, these lessons are urgent and unavoidable. The occupation of Abkhazia and the Tskhinvali Region, the ongoing “creeping annexation” along the Administrative Boundary Line, and the manipulation of political, economic, and informational vulnerabilities demonstrate that Georgia is already situated within a sustained hybrid conflict environment. It is no longer sufficient to conceive of national defense solely in military terms. Security must be understood as a total societal framework, requiring coordinated resilience across the state, economy, civil society, media, and digital infrastructure.

The strategic recommendations outlined in this study highlight a coherent path for Georgia’s survival and long-term stability. Transforming Georgia into an indispensable transit and energy corridor—through the development of the Anaklia Deep-Sea Port and integration into Eurasian and European supply chains—would significantly raise the geopolitical cost of aggression. Diversifying energy sources and reducing dependency on Russian markets would weaken external leverage. Strengthening cyber defense, informational resilience, civic cohesion, and diplomatic partnerships would reinforce societal stability and deterrence.

Ultimately, the core strategic objective is clear: Georgia must become a state whose sovereignty is not only defended by its army, but actively sustained by its economic indispensability, its alliances, and the unity of its society. In a world shaped by fifth-generation warfare, deterrence is achieved not through strength alone, but through the demonstrated ability to endure, adapt, communicate, and remain ungovernable to external manipulation.

If Georgia succeeds in these efforts, it will not simply survive the strategic pressures of its environment—it will emerge as a sovereign, resilient, and essential bridge between East and West, capable of securing its future on its own terms.

Bibliography

- Inashvili, G. (n.d.). Military blog, beginning of the 5th gen wars? *Homo Militaris*, (p. 2). Tbilisi.
- Richard A. gabriel, k. s. (1992). *A short history of war the evolution of warfare and weapons*. U.S. army war college.
- Schmid, J. (2019). Hybrid warfare on the Ukrainian Battlefield. *Journal on baltic security*. sciendo.
- Fox, M. A. (2017). *Hybrid Warfare: The 21st Century Russian Way of Warfare*. Kansas: School of Advanced Military Studies.
- Christopher paul, M. M. (2016). The Russian “firehose of Falsehood” Propaganda model. *RAND*.
- Schmitt, M. N. (2025, June 16). Retrieved from lieber.westpoint.edu: <https://surl.li/uinzxo>, Accessed 07.11.2025
- Kirichenko, D. (2025, August 21). Retrieved from warroom.armywarcollege.edu: <https://surl.li/lwlgxa>, Accessed 07.11.2025
- Thomas, R. (2025, April 8). Retrieved from army-technology.com: <https://surl.li/fztcpv>, Accessed 07.11.2025
- Koldor, M. (2012). *new and old wars*. Malden US: polity.

TECHNOLOGICAL ALLIANCES AND THE FUTURE OF SECURITY: U.S. AND ALLIED COOPERATION IN AI AND DEFENSE INNOVATION

Giga Misireli

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Nika Merebashvili

The Junker of a Bachelor's Degree (Defense and Security) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor Levan Gegeshidze

Professor of Bachelor's Program in Defense and Security of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

In the 21st century, the concept of security has undergone a fundamental transformation. Traditional threats such as interstate wars and direct military confrontation have been joined and in some cases overshadowed by new and complex challenges: cyberattacks, hybrid warfare, disinformation, and the rise of unnamed systems. These developments have reshaped the global security architecture and redefined what national resilience truly means. Today, the foundations of defense and stability rest on two interdependent pillars: innovation and international partnership. Innovation grants nations technological superiority, enabling rapid decision-making and precise strategic execution through the use of artificial intelligence, autonomous systems, and cyber capabilities. Meanwhile, partnership transforms this technological advantage into collective strength by fostering interoperability, shared intelligence, and joint defense systems.

This paper explores how technological revolutions such as artificial intelligence, unmanned and autonomous systems, cyber defense, and hypersonic and quantum technologies are redefining the nature of warfare and deterrence. It also discusses the growing importance of cooperation among allied states in addressing shared vulnerabilities, developing unified ethical frameworks, and establishing global norms that regulate emerging defense technologies. The study argues that neither innovation nor partnership can function effectively in isolation. Only through their combination of technological advancement, grounded in trust and collaboration, can the world achieve sustainable stability and adapt to the challenges of an increasingly interconnected and technologically driven security environment.

Keywords: Innovation. International. Cooperation. Artificial Intelligence. Cybersecurity. Defense. Semiconductor Production. Global Security.

Introduction

In the contemporary world, security is no longer defined solely by the possession of weapons or the numerical strength of a nation's armed forces. While traditional threats—such as interstate conflicts, territorial disputes, and large-scale conventional warfare—remain persistent features of international relations, they are increasingly accompanied, and in some cases overshadowed, by complex, multi-dimensional, and rapidly evolving challenges. The rise of cyberattacks, hybrid warfare, disinformation campaigns, and the widespread deployment of unmanned and autonomous systems has profoundly altered the nature of conflict.

Modern security is now as much about protecting data, infrastructure, and information networks as it is about defending borders or physical assets. Nations must secure not only their territorial integrity but also their digital ecosystems, communication networks, and critical technologies—the foundational elements of societal stability and economic resilience. In this redefined environment, the battlefield is no longer confined to land, sea, or air; it extends into cyberspace, outer space, and the cognitive domain, where perception, information, and influence determine power.¹

This evolution has created an urgent need for new strategic approaches—ones that integrate technological advancement with institutional collaboration. Innovation has become the cornerstone of defense transformation, providing the tools to anticipate, analyze, and respond to threats with unprecedented speed, accuracy, and precision. Artificial intelligence (AI), advanced logistics systems, unmanned aerial and ground vehicles (UAVs and UGVs), cyber-defense mechanisms, and emerging technologies such as hypersonic weapons and quantum computing are reshaping both offensive and defensive capabilities. These innovations not only enhance the efficiency of military operations but also redefine the tempo of warfare, forcing decision-makers to adapt to accelerated and data-driven conflict environments.

However, the increasing complexity of modern threats has also revealed a crucial reality: no nation, regardless of its resources or technological sophistication, can address these challenges in isolation. The globalized nature of security threats—ranging from transnational cybercrime to information warfare and global supply-chain vulnerabilities—demands collective and coordinated responses. International partnerships serve as essential multipliers of innovation, allowing states to pool financial and intellectual resources, share critical knowledge, and develop interoperable defense systems capable of joint action.²

Cooperation transforms isolated technological achievements into shared strategic capabilities. By establishing alliances, multilateral frameworks, and research partnerships, nations can collectively respond to cyberattacks, hybrid warfare, and other non-traditional threats. Furthermore, international collaboration plays a vital normative role: it fosters the development of ethical standards, legal frameworks, and transparency mechanisms that govern the responsible use of emerging technologies such as AI and autonomous weapons. In an age where innovation outpaces

1 Taylor, Zane Jarret, and William Dean Long. "Maneuvering in Contested Skies." *Over The Horizon Journal*, October 6, 2024. <https://surl.lu/rpjpgo>, Accessed 07.11.2025

2 I. Danilin, *Emerging Technologies and Their Impact on International Relations and Global Security*. Hoover Institution, Stanford University. (2018).

regulation, such cooperative governance is essential for maintaining legitimacy and trust among states and societies.

In this context, the balance between innovation and partnership has become central to the future of security. Innovation provides the means to enhance resilience and adaptability, while cooperation ensures that these advancements serve collective stability rather than unilateral dominance. Together, they form the dual pillars of a new security paradigm—one defined by shared technological progress, mutual responsibility, and global interdependence.

The following sections examine the intersection of technological development and international collaboration, exploring how their convergence shapes the emerging architecture of global defense. By analyzing current models of cooperative innovation—from transatlantic initiatives and regional alliances to wartime adaptation and ethical governance—this study seeks to illuminate how nations can jointly construct a security framework capable of withstanding the uncertainties of the 21st century.

Main Part

The contemporary defense sector is undergoing not a gradual evolution but a profound revolution—one defined by the fusion of advanced technologies, artificial intelligence (AI), autonomous systems, cyber innovation, and next-generation weaponry. These forces are reshaping the very foundations of strategy, operations, and decision-making, signaling a transition from traditional warfare to an era of intelligent, data-driven, and networked security. Modern defense innovation is no longer about incremental improvement; it represents a fundamental redefinition of how nations anticipate, deter, and respond to threats in a globalized and digitalized world.

Artificial Intelligence and the Rise of Intelligent Warfare

Artificial intelligence now lies at the heart of military transformation. It has redefined operational tempo by processing vast volumes of data—ranging from satellite imagery and drone reconnaissance to multi-sensor battlefield inputs—in real time. AI-enabled systems detect and classify potential targets, track enemy maneuvers, assess vulnerabilities, and even predict adversarial behavior based on machine learning algorithms. This unprecedented analytical speed grants commanders a decisive cognitive edge, facilitating faster and more accurate decision-making under conditions of uncertainty.

Beyond command and control, AI plays an increasingly crucial role in logistics and predictive maintenance. By forecasting equipment failures, automating supply chains, and optimizing resource distribution, AI reduces operational downtime and minimizes costs. Autonomous aerial and ground vehicles extend this advantage by performing reconnaissance, executing precision strikes, and operating in environments too hazardous for human soldiers. For smaller or resource-constrained nations, such technologies offer a strategic equalizer, enabling asymmetric deterrence through agility, precision, and cost-effective warfare.

Cyber Defense, Electronic Warfare, and the New Frontline

In the 21st century, cyberspace has become as critical as land, air, and sea. As national infrastructures—spanning communications, energy, transportation, and finance—grow increasingly interconnected, cyber defense has emerged as a frontline imperative. A single sophisticated cyberattack can cripple government systems, disrupt critical industries, and erode public trust. Consequently, cybersecurity, encryption, and digital resilience are now core components of national defense policy.

Electronic warfare complements these efforts by disrupting enemy communications, neutralizing drone and missile guidance systems, and securing spectrum dominance. Together, cyber and electronic defense represent the invisible battlefield where information superiority determines strategic success. Yet, this digital transformation also multiplies vulnerabilities. Adversaries exploit weak links in global supply chains, deploy disinformation campaigns and algorithms to destabilize societies—forcing nations to rethink both the scope and ethics of modern deterrence.

Emerging Technologies: Promise and Peril

Technological innovation in defense also introduces new layers of risk and moral complexity. Hypersonic weapons—capable of traveling at speeds exceeding Mach 5—threaten to render traditional missile defense systems obsolete, compressing response times to mere seconds. Similarly, quantum computing poses an existential challenge to existing encryption standards, potentially compromising even the most secure communication networks.³ Alongside these technical risks, ethical questions grow increasingly urgent. As autonomous systems assume greater decision-making roles in lethal operations, societies must confront difficult questions of accountability and moral agency. Who bears responsibility when an autonomous drone makes a life-or-death error—the programmer, the commander, or the state? The “human-in-the-loop” principle, which ensures that human oversight remains central to the use of force, has therefore become a vital safeguard in preserving ethical and legal norms amid accelerating automation.

Operation “Spiderweb”: Innovation in Action

Perhaps no recent example illustrates the fusion of innovation, intelligence, and operational precision better than Operation “Spiderweb”, executed by the Security Service of Ukraine (SSU) on June 1, 2025.⁴ This large-scale asymmetric drone operation targeted five Russian strategic air bases simultaneously.⁵ Reports suggest that AI played a decisive role in programming 117 autonomous drones, enabling them to navigate deep within enemy territory and execute precision strikes without direct human intervention.

The operation’s success rested not only on the drones themselves but also on integrated cyber and electronic warfare support—including the infiltration of enemy communication systems,

3 Taylor, Zane Jarret, and William Dean Long. “Maneuvering in Contested Skies.” *Over The Horizon Journal*, October 6, 2024. <https://surl.li/hjbncel>, Accessed 07.11.2025

4 Center for Strategic and International Studies (CSIS), 2025. “The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond”. <https://surl.li/fhmxxnp>, Accessed 07.11.2025

5 Bondar, Kateryna. “Understanding the Military AI Ecosystem of Ukraine.” Washington, DC: Center for Strategic and International Studies (CSIS), November 12, 2024. <https://shorturl.at/G6CyU>

suppression of radar detection, and preservation of command integrity through encrypted data channels. The destruction of approximately 40 Russian aircraft underscored the strategic potential of combining AI-driven autonomy with robust cyber resilience and tactical adaptability. Operation “Spiderweb” thus stands as a case study in how digital warfare and real-time intelligence can redefine asymmetrical advantage, empowering smaller states to achieve significant strategic outcomes.⁶

Technological Cooperation and Collective Security

Technological superiority in defense today depends not solely on innovation, but on strategic cooperation among trusted partners. The United States and its allies have made collaborative innovation the cornerstone of 21st-century defense strategy. The CHIPS and Science Act, developed in partnership with Japan, South Korea, and the Netherlands, exemplifies this approach by securing global semiconductor production—an essential foundation for AI, defense systems, and advanced communication technologies. By diversifying supply chains and reducing dependency on rival powers, this initiative strengthens both economic and national security. In the realm of AI and digital defense, initiatives such as the U.S.–EU Trade and Technology Council (TTC) and NATO’s Defence Innovation Accelerator for the North Atlantic (DIANA) promote joint research, ethical AI development, and shared standards for interoperability. These programs underscore that true technological leadership emerges not from isolated invention but from coordinated innovation grounded in shared democratic values—transparency, accountability, and collective responsibility.

Expanding Horizons: The New Domain of Space Security

A rapidly emerging domain in international defense cooperation is space security. Satellites now serve as indispensable assets for communication, navigation, surveillance, and early-warning systems, yet they also represent potential targets in a militarized cosmos. Preventing the escalation of conflict into outer space requires joint monitoring initiatives, shared situational awareness, and comprehensive international legal frameworks governing the responsible use of space technology. Cooperative systems for space debris tracking, satellite resilience, and orbital traffic management exemplify how partnerships can preserve the stability of the global commons.⁷

The Interdependence of Innovation and Partnership

Ultimately, the intersection of technological innovation and international cooperation defines the essence of modern defense. Innovation provides the tools—the algorithms, systems, and architectures—that enable anticipation, adaptation, and deterrence. Partnership ensures that these tools are deployed responsibly, ethically, and collectively, transforming technological capability into sustainable strategic power. No single state can achieve lasting security in isolation. The future of defense depends on the balance between innovation and collaboration, between the competi-

6 Black, James et al., “Russia’s War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine”. UK: RAND Corporation, 2024. RAND Research Report RRA3400-1. pp 5-23.

7 Center for Strategic and International Studies (CSIS), 2025. “The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond”. <https://surl.li/njlnuu>, Accessed 07.11.2025

tive drive to lead and the cooperative imperative to protect. As the global security environment becomes ever more complex, the integration of shared technology, joint governance, and ethical innovation will determine which nations and alliances can sustain peace, stability, and resilience in an unpredictable century.

Conclusion

In an era defined by accelerating technological transformation and global interdependence, no nation can secure its future through isolation or military strength alone. Power in the twenty-first century no longer derives solely from the size of arsenals or the sophistication of weaponry, but from the ability to innovate, adapt, and collaborate. Technological innovation—manifested in artificial intelligence, autonomous systems, and cyber capabilities—has redefined the meaning of strategic superiority. Yet, innovation without cooperation risks fragmentation, redundancy, and even destabilization. Only through international partnership can technological progress translate into enduring stability.

Innovation provides the means of superiority, but cooperation provides the framework of sustainability. Shared research initiatives, interoperable defense systems, and cross-border knowledge exchange allow nations to multiply their capabilities rather than compete destructively for dominance. Furthermore, international collaboration enables the creation of ethical and legal standards that guide the responsible use of advanced technologies. In an age when artificial intelligence and autonomous systems increasingly influence decisions of life and death, the establishment of common moral and legal norms becomes indispensable for safeguarding human oversight and accountability.

The future of global security will depend on the delicate equilibrium between technological advancement and political trust. Technology requires coordination, transparency, and shared governance; partnership, in turn, demands constant creativity, open communication, and sustained commitment. Both are mutually reinforcing: innovation strengthens cooperation by providing new tools and insights, while cooperation amplifies innovation by integrating diverse perspectives, resources, and experiences.

As security challenges grow more interconnected—from cyberwarfare and disinformation to space militarization and hybrid threats—the synergy between innovation and partnership will become the defining determinant of resilience. Nations that combine technological ingenuity with cooperative foresight will shape not only the defense systems of tomorrow but also the ethical and strategic foundations of peace itself.

In essence, the path to sustainable security in the digital age lies in the fusion of innovation and collaboration—two forces that, when aligned, transform uncertainty into preparedness and competition into collective resilience. Only through this synergy can the international community preserve stability, safeguard human dignity, and ensure that technological progress remains a servant of peace rather than a catalyst of conflict.

Bibliography

- Taylor, Zane Jarret, and William Dean Long. "Maneuvering in Contested Skies." *Over The Horizon Journal*, October 6, 2024. <https://surl.li/hpczsa>, Accessed 07.11.2025
- Danilin, I. (2018). *Emerging Technologies and Their Impact on International Relations and Global Security*. Hoover Institution, Stanford University.
- Black, James et al., "Russia's War in Ukraine: Emerging Insights for UK and NATO Joint Doctrine". UK: RAND Corporation, 2024. RAND Research Report RRA3400-1. pp 5-23.
- Bondar, Kateryna. "Understanding the Military AI Ecosystem of Ukraine." Washington, DC: Center for Strategic and International Studies (CSIS), November 12, 2024. <https://shorturl.at/G6CyU>, Accessed 07.11.2025
- Center for Strategic and International Studies (CSIS), 2025. "The Russia-Ukraine Drone War: Innovation on the Frontlines and Beyond". <https://surl.li/btojvl>, Accessed 07.11.2025

DEFENSE INNOVATION AS SOFT POWER: HOW TECHNOLOGICAL COOPERATION SHAPES GLOBAL INFLUENCE IN THE 21ST CENTURY

Lieutenant Irakli Grigoriadi

The Learner of a Master's Degree Program (Security Studies) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Ketevan Chakhava

Assistant Professor of Master's Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

In the twenty-first century, the global distribution of power is increasingly defined by technological capacity and innovation networks rather than traditional measures of military strength. Defense innovation, once associated exclusively with hard power, now serves as a central mechanism of soft power and diplomatic influence. Through multinational defense research, shared technological ecosystems, and innovation-driven partnerships, states extend their reach and legitimacy while simultaneously strengthening collective security. This paper investigates defense innovation as a dimension of soft power within contemporary international relations. Drawing on Joseph Nye's theory of attraction-based influence, the analysis explores how defense innovation enhances alliance cohesion, establishes international norms, and shapes geopolitical alignments . Case studies of NATO's Defense Innovation Accelerator for the North Atlantic (DIANA), the AUKUS alliance, and the European Union's strategic-autonomy initiatives illustrate the dynamic interplay between innovation and diplomacy. The paper concludes with policy recommendations for leveraging technological cooperation as a stabilizing force in a multipolar world.

Keywords: Defence Innovation, Soft Power, International Partnerships, Technological Cooperation, Innovation Diplomacy, Geopolitical Strategy, AUKUS and NATO, Collective Security.

Introduction

The concept of power in international relations has undergone significant transformation in recent decades. Traditional understandings of power emphasized material capabilities: the size of armies, the strength of economies, and control over territory. However, globalization, digitalization, and the proliferation of advanced technologies have altered the structure of influence. States increasingly project power through attraction, persuasion, and the creation of global norms rather than through coercion or direct military confrontation. Within this context, defense innovation has emerged as a hybrid instrument of both hard and soft power.

While defense technology undeniably strengthens military capacity, its development and dissemination also serve broader diplomatic functions. Joint research programs, multinational procurement, and technology-sharing agreements build trust, interoperability, and political alignment among states. In short, technological cooperation produces not only material benefits but also relational and normative power.

This thesis advances the argument that defense innovation functions as a form of soft power that reinforces international partnerships and shapes global security governance. The analysis proceeds through five stages. First, it outlines the evolution of defense innovation within the global political economy. Second, it integrates Nye's soft-power framework into the study of defense cooperation. Third, it examines case studies of NATO, AUKUS, and the European Union to demonstrate how innovation fosters diplomatic cohesion. Fourth, it considers the geopolitical and ethical challenges arising from technology-driven alliances. Finally, it offers policy recommendations for balancing innovation, security, and sovereignty in future defense diplomacy.¹

The Evolution of Defense Innovation in Global Politics

From Industrial Warfare to Knowledge Warfare

The Industrial Revolution redefined the relationship between technology and war. In the nineteenth and early twentieth centuries, industrial capacity determined military strength: the ability to produce steel, fuel, and armaments decided victory or defeat. During the Cold War, innovation became a national endeavor tied to ideological competition. The United States and the Soviet Union raced to develop nuclear weapons, missiles, and space technologies, seeing technological superiority as synonymous with strategic survival.²

However, the end of the Cold War introduced new dynamics. The diffusion of dual-use technologies — innovations applicable to both civilian and military sectors — blurred the line between economic and defense policy.³ The rise of the information economy and globalization allowed private firms and universities to play a central role in military research once dominated by state institutions. Defense innovation gradually shifted from closed, hierarchical systems to networked ecosystems involving governments, corporations, and transnational alliances.

1 Center for Strategic and International Studies (CSIS), *The Future of Defense Innovation* (Washington, D.C.: CSIS, 2023).

2 Stephen Biddle and Ivan Arreguín-Toft, "The Strategy of Modern Warfare," *International Security* 41, no. 4 (2022): 33–67.

3 CSIS, *Future of Defense Innovation*.

The Globalization of Defense Research

In the twenty-first century, innovation ecosystems are transnational by design. Global supply chains link research centers, start-ups, and defense agencies across continents. Collaborative R&D has become an instrument of diplomacy: participation in joint projects signals political alignment and trust.⁴ For example, multinational programs such as the F-35 Joint Strike Fighter or the European Galileo satellite system exemplify how defense technology simultaneously meets operational and political objectives.

This global interdependence has strategic implications. States that lead in critical technologies — artificial intelligence, quantum computing, cyber defense, and space capabilities — set international standards and shape the future battlefield. Yet they also bear responsibility for managing shared vulnerabilities. Consequently, defense innovation no longer exists solely to deter conflict; it also functions to manage interdependence and to anchor alliances in a rapidly evolving security environment.

Theoretical Framework: Soft Power and Technological Diplomacy

Soft Power Revisited

Joseph Nye's concept of soft power describes a state's ability to shape the preferences of others through attraction rather than coercion. It rests on three pillars: culture, political values, and foreign policy. In recent years, scholars have extended this framework to include technology as an additional source of attraction.⁵ Innovation demonstrates competence, modernity, and credibility — qualities that enhance a state's reputation and its capacity to lead cooperative ventures.

When applied to defense, soft power operates through technological legitimacy. States that excel in defense innovation are viewed as reliable partners and sources of security knowledge. This legitimacy generates influence beyond the military domain: it facilitates diplomatic access, fosters trust in joint operations, and helps define ethical norms for emerging technologies.

The Concept of Technological Diplomacy

Technological diplomacy refers to the use of innovation as a medium of foreign relations. It encompasses collaborative R&D agreements, technology-sharing frameworks, and dialogues on norms and standards. In defense contexts, technological diplomacy allows states to manage competition while preserving strategic stability. For example, joint investments in cybersecurity or AI governance create platforms for negotiation and transparency that reduce the risk of misunderstanding or escalation.

In this sense, defense innovation constitutes both a material capability and a communicative act. It signals commitment, competence, and alignment. When embedded in formal alliances or informal coalitions, innovation becomes a diplomatic currency that binds states together through shared technological futures.

⁴ RAND Corporation, *Allied Defense Innovation Networks*.

⁵ Joseph S. Nye, *Soft Power: The Means to Success in World Politics*. 11-12.

Defense Innovation as a Tool of Soft Power

Symbolic Leadership and Prestige

Defense innovation enhances a state's global image by demonstrating foresight and capability. The United States' leadership in stealth technology, satellite navigation, and advanced missile systems projects technological authority that underpins its alliances. Similarly, Israel's record in missile-defense and drone technologies functions as a diplomatic asset, enabling it to cultivate partnerships across diverse regions. Technological leadership thus serves a symbolic function: it conveys reliability, resilience, and modernity.

Alliance Cohesion Through Innovation

Collaborative innovation strengthens alliance cohesion by generating interdependence. Shared projects require mutual trust, continuous communication, and harmonized standards. ⁶The Eurofighter Typhoon program, co-developed by the United Kingdom, Germany, Italy, and Spain, illustrates how technological cooperation reinforces political solidarity. The interlocking production chains and shared intellectual property foster enduring strategic ties that extend beyond any single administration or crisis.

Moreover, innovation programs facilitate interoperability — the technical and procedural compatibility essential for joint operations. Through common technologies, allies achieve greater efficiency and unity of command, thereby translating innovation into concrete security outcomes.

Norm Creation and Standard-Setting

States that lead in defense innovation also shape the global normative environment. By defining ethical guidelines for artificial intelligence in warfare or standards for cyber defense, they exercise what can be called normative soft power. ⁷The European Union, for instance, uses regulatory leadership — often termed the “Brussels effect” — to export its norms on data protection and ethical technology globally. In defense contexts, this normative leadership enhances legitimacy and creates political capital.

Case Studies of International Defense Partnerships

NATO's Defense Innovation Accelerator for the North Atlantic (DIANA)

NATO's DIANA initiative, launched in 2022, epitomizes innovation as diplomacy. It connects research institutions, start-ups, and defense agencies across the alliance to accelerate the development of emerging and disruptive technologies. DIANA's structure — with regional hubs and test centers in both Europe and North America — institutionalizes trust and transparency among allies. ⁸

The initiative's primary function is not immediate technological output but the creation of a shared innovative culture. By facilitating collaboration on dual-use technologies, DIANA enhances transatlantic solidarity and demonstrates NATO's adaptability to twenty-first-century challenges.

⁶ RAND Corporation, *Allied Defense Innovation Networks*.

⁷ CSIS, *Future of Defense Innovation*.

⁸ NATO, *Defense Innovation Accelerator for the North Atlantic (DIANA) Policy Framework* (Brussels: NATO, 2023).

It translates the alliance's traditional military commitments into a cooperative innovation network, thereby expanding NATO's legitimacy among younger, technologically driven constituencies.

AUKUS: Strategic Innovation and Geopolitical Realignment

The AUKUS alliance between Australia, the United Kingdom, and the United States illustrates how technological cooperation can reshape global alignments.⁹ Initially centered on the transfer of nuclear-powered submarine technology, AUKUS quickly broadened to encompass quantum technologies, cyber capabilities, and artificial intelligence. The pact strengthens deterrence in the Indo-Pacific region while signaling a shared commitment to technological leadership.

For the United States, AUKUS reinforces its strategic focus on the Indo-Pacific and demonstrates confidence in trusted allies. For the United Kingdom and Australia, participation provides access to cutting-edge technologies and elevates their geopolitical relevance. At the same time, AUKUS underscores the diplomatic risks of innovation alliances: China and several Southeast Asian states perceive it as a destabilizing move, illustrating the fine line between innovation diplomacy and strategic provocation.

The European Union and Strategic Autonomy

The European Union (EU) provides a unique example of how defense innovation and regional integration can reinforce one another. Unlike traditional military alliances, the EU's approach to defense is fundamentally political and economic. Since the establishment of the Common Security and Defence Policy (CSDP), the Union has sought to build collective capability while maintaining its identity as a peace-oriented actor.

In recent years, the EU's emphasis on strategic autonomy—the ability to act independently in security matters—has made technological innovation a priority. The **European Defence Fund (EDF)**, launched in 2017, finances joint research and development projects across member states. It encourages cooperation among defense industries, universities, and research agencies, seeking to reduce fragmentation and dependence on external suppliers, particularly the United States.

Programs under the EDF and **Permanent Structured Cooperation (PESCO)** have fostered a European innovation ecosystem centered on interoperability and sustainability. By promoting collaborative development of next-generation capabilities such as unmanned aerial vehicles and cyber defense tools, the EU strengthens its geopolitical credibility while reinforcing internal unity.¹⁰

This innovation-driven strategy also functions as a diplomatic instrument. The EU positions itself as a normative power, exporting ethical standards and regulatory models for technology governance. Its insistence on transparency, civilian oversight, and compliance with international law lends legitimacy to its global outreach. In this sense, defense innovation underpins not only Europe's security but its international identity.

9 Australian Department of Defence, *AUKUS Pillar II Joint Statement* (Canberra: Commonwealth of Australia, 2024).

10 European Union External Action Service (EEAS), *Permanent Structured Cooperation (PESCO) Annual Review* (Brussels, 2022).

Geopolitical Competition and the Rise of Tech Diplomacy

The U.S.–China Technological Rivalry

The growing competition between the United States and China has redefined the global balance of power. Unlike the ideological confrontation of the Cold War, today's rivalry is centered on technological ecosystems—semiconductors, artificial intelligence, 5G infrastructure, and quantum computing. Control over these technologies confers not only economic advantages but also strategic influence over communication, surveillance, and defense systems.¹¹

Both Washington and Beijing now employ what can be described as innovation geopolitics. The United States promotes alliances such as AUKUS and the Quad to secure supply chains and share R&D capabilities with trusted partners. China, in turn, advances initiatives like the Belt and Road Digital Silk Road to export technological standards and strengthen defense-industrial ties with developing nations.

This competition has spurred what some analysts call a “technological decoupling,” wherein rival blocs seek self-sufficiency in strategic sectors. However, complete decoupling remains unrealistic given the globalized nature of research and production. Instead, a form of selective interdependence persists—where states cooperate in low-risk areas while restricting collaboration in sensitive domains such as AI or cyber offense. Managing this interdependence constitutes the core challenge of contemporary tech diplomacy.

Regional Innovation Coalitions

Beyond great-power rivalry, regional powers are forming their own innovation-based alliances. In the Indo-Pacific, partnerships such as the Quad (United States, India, Japan, and Australia) and ASEAN's defense cooperation frameworks emphasize cybersecurity, maritime surveillance, and emerging technology standards. These collaborations are less formal than NATO or the EU but play a vital diplomatic role by embedding technology in regional governance.

Similarly, the Middle East has witnessed an upsurge in defense-tech collaboration, exemplified by Israel's partnerships with the United Arab Emirates and Bahrain under the Abraham Accords. Here, innovation serves as a bridge between former adversaries, demonstrating the power of technology to facilitate reconciliation and economic integration.

Collectively, these cases suggest that technological cooperation is becoming the organizing principle of contemporary alliances. Innovation not only deters adversaries but also provides the foundation for durable diplomatic engagement.

Challenges and Ethical Dilemmas in Innovation-Based Alliances

Security Risks and Sovereignty Concerns

The globalization of defense innovation brings undeniable advantages but also profound risks. Shared research networks can expose sensitive data to espionage, intellectual property theft, or cyber intrusion. The more complex and interconnected the innovation ecosystem becomes, the greater the potential for security breaches. For smaller states, participation in joint projects can create long-term dependence on the technological infrastructure of larger powers, raising questions of sovereignty and autonomy.

¹¹ Biddle and Arreguín-Toft, “Strategy of Modern Warfare.” 24.

Export control regimes such as the U.S. *International Traffic in Arms Regulations (ITAR)* often restrict the transfer of sensitive components, creating friction even among close allies. Balancing openness with protectionism remains one of the most delicate tasks of defense diplomacy.

Ethical Dimensions of Emerging Defense Technologies

A further challenge lies in the ethical and legal implications of new military technologies. Artificial intelligence, autonomous weapons, and cyber operations challenge traditional frameworks of accountability.¹² When decision-making is delegated to algorithms or when cyberattacks blur the line between war and peace, the moral foundation of international law is tested.

International organizations and alliances have begun to address these issues through normative initiatives. NATO's *AI Strategy* and the EU's *Ethical Guidelines for Trustworthy AI* seek to ensure that innovation aligns with democratic values and human rights. However, the absence of global consensus on regulation means that norms remain fragmented. The risk of an "AI arms race" persists, potentially undermining the stabilizing potential of innovation diplomacy.

Inequality in the Global Defense Innovation System

The benefits of defense innovation are unevenly distributed. Developed states with advanced industrial bases dominate the global R&D landscape, while developing nations struggle to access technology or financing. This imbalance risks creating a new form of dependency: a hierarchy of innovation where a few powers control the flow of knowledge and intellectual property.¹³

For many states in the Global South, participation in defense innovation occurs primarily through procurement or offset programs rather than genuine partnership. To achieve a more inclusive global security order, mechanisms for technology transfer, joint education, and capacity-building must be strengthened. Otherwise, innovation may reinforce rather than mitigate structural inequalities in international relations.

Future Outlook: Innovation Networks and the Transformation of Security

The Networked Nature of Future Defense Cooperation

The next generation of defense partnerships will be defined by *networked innovation*. Traditional alliances organized around military command structures are giving way to flexible, multi-actor ecosystems involving governments, private industry, and academia. These innovation networks function as both economic and diplomatic entities.¹⁴ They accelerate research while diffusing risk and cost across participants.

As digital technologies evolve, alliances will increasingly rely on shared data platforms and virtual testing environments. Artificial intelligence will support joint decision-making and strategic forecasting. Cybersecurity cooperation will serve as the backbone of mutual defense, ensuring that digital infrastructures remain resilient against both state and non-state threats.

The Role of Normative Leadership

In this environment, the capacity to define ethical and technical standards will become a central form of power. Nations and alliances that set the "rules of the game" for AI, cyber defense, and

¹² United Nations Institute for Disarmament Research (UNIDIR), *AI and Autonomy in Defense: Norms and Governance* (Geneva, 2023).

¹³ UNIDIR, *AI and Autonomy in Defense*.

¹⁴ RAND Corporation, *Allied Defense Innovation Networks*.

space operations will wield normative influence that extends beyond traditional military strength. The European Union's experience in regulatory leadership suggests that such influence can be achieved without overwhelming military capacity.

Normative leadership also carries a stabilizing function. By embedding ethical frameworks in defense cooperation, states can prevent escalation and maintain legitimacy in the eyes of domestic and international audiences. In the long run, trust in technology governance may prove as important as trust in weapon capability.

Innovation and the Future of Collective Security

Defense innovation has the potential to rejuvenate collective security institutions. NATO, the EU, and regional organizations can use technological collaboration to maintain relevance in an era of distributed threats. Joint investment in emerging domains such as quantum communication, biosecurity, and space situational awareness can create new layers of deterrence and crisis management.

However, this transformation requires a delicate balance between openness and protection. Overemphasis on secrecy and control may stifle creativity, while excessive transparency can expose vulnerabilities. The key lies in adaptive governance — frameworks that encourage innovation while safeguarding national interests and democratic accountability.

Policy Recommendations

Based on the preceding analysis, several policy recommendations emerge for states and international organizations seeking to harness defense innovation as a tool of soft power:

1. Institutionalize Innovation Diplomacy:

Establish formal mechanisms within foreign ministries and defense departments to coordinate technology-related diplomacy. These should integrate scientific expertise into strategic planning and facilitate collaboration with allies on innovation governance.

2. Promote Ethical and Legal Frameworks for Emerging Technologies:

States should advocate for international norms governing artificial intelligence, autonomous weapons, and cyber operations. Multilateral platforms such as the United Nations or the G20 could serve as venues for consensus-building.

3. Strengthen Public–Private Partnerships:

Defense innovation increasingly depends on commercial technology sectors. Governments should incentivize private firms to participate in secure R&D networks while ensuring oversight to prevent misuse or monopolization.

4. Enhance Inclusivity and Capacity-Building:

Wealthier states and alliances should expand technology-sharing programs and training initiatives with developing partners. This would not only reduce inequality but also expand global stability by diversifying sources of innovation.

5. Balance Strategic Autonomy with Interdependence:

States must pursue autonomy in critical technologies without isolating themselves from global

innovation flows. Flexible partnerships — based on transparency, reciprocity, and trust — can achieve this equilibrium.

6. Invest in Normative Leadership:

Establish ethical review boards and transnational councils dedicated to the responsible use of defense technologies. States that lead in ethical governance will gain lasting diplomatic influence.

Conclusion

The transformation of defense innovation from a purely military domain into a central element of diplomacy marks one of the most profound shifts in modern international relations. In an interconnected and technologically driven world, the capacity to innovate — and to share innovation — has become both a strategic necessity and a source of political legitimacy.

This paper has argued that defense innovation functions as a form of soft power by generating attraction, trust, and interdependence among states. Through case studies of NATO's DIANA, AUKUS, and the European Union's defense initiatives, we observe how technological collaboration fosters cohesion, shapes norms, and enhances global stability. Yet innovation diplomacy is not without its challenges: ethical dilemmas, security risks, and inequalities threaten to undermine its promise if left unregulated.

The future of global security will depend on how effectively nations and alliances manage these contradictions. Power will increasingly derive not from isolationist control of technology, but from participation in inclusive, ethical, and adaptive innovation networks. As defense and diplomacy converge, technological cooperation will remain the defining arena of twenty-first-century soft power.¹⁵

Bibliography

Nye, Joseph S. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs, 2004.

NATO. *Defense Innovation Accelerator for the North Atlantic (DIANA) Policy Framework*. Brussels: NATO, 2023.

European Commission. *European Defence Fund Annual Report*. Brussels: Publications Office of the European Union, 2023.

RAND Corporation. *Allied Defense Innovation Networks*. Santa Monica, CA: RAND, 2022.

Australian Department of Defence. *AUKUS Pillar II Joint Statement*. Canberra: Commonwealth of Australia, 2024.

Biddle, Stephen, and Ivan Arreguín-Toft. "The Strategy of Modern Warfare." *International Security* 41, no. 4 (2022): 33–67.

Center for Strategic and International Studies (CSIS). *The Future of Defense Innovation*. Washington, D.C.: CSIS, 2023.

European Union External Action Service (EEAS). *Permanent Structured Cooperation (PESCO) Annual Review*. Brussels, 2022.

United Nations Institute for Disarmament Research (UNIDIR). *AI and Autonomy in Defense: Norms and Governance*. Geneva, 2023.

Baldwin, David A. "Power and International Relations: A Conceptual Approach." *Princeton University Press*, 2016.

¹⁵ Nye, *Soft Power*. 7–8.

THE ETHICS OF STRATEGIC ADVANTAGE: HUMAN AGENCY, ACCOUNTABILITY, AND EMERGING TECHNOLOGIES

Lieutenant Dimitri Jakonia

The Learner of a Master's Degree Program (International Relations and Diplomacy) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Ketevan Chakhava

Assistant Professor of Master's Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

In an era where emerging technologies significantly reshape societal structures and organizational operations, businesses and institutions increasingly view ethics not merely as compliance but as a strategic asset. This essay explores the ethics of strategic advantage through the lens of human agency and accountability in the deployment of advanced technologies. It argues that ensuring that human actors retain meaningful agency and that clear lines of accountability are maintained is essential if emerging technological systems are to contribute positively rather than erode trust, autonomy and legitimacy. The discussion draws on recent scholarship in technology ethics and governance to frame three core research questions, each addressed in turn with deeper analysis and real-world implications, concluding with broader strategic and governance reflections.

Keywords: strategic advantage, human agency, accountability, emerging technologies, artificial intelligence, ethics, governance, human in the loop, transparency.

Introduction

The pursuit of strategic advantage through technology has long been central to organizational competitiveness. This ethical pivot is not merely a defensive maneuver against reputation risk; it is increasingly a catalyst for innovation. Organizations are discovering that constraints imposed by ethical considerations such as fairness, transparency and human dignity. In the light, ethics acts not as a brake on progress but as a steering mechanism, guiding technological development toward outcomes that are not only profitable but also sustainable and socially beneficial, thereby creating a more resilient form of competitive advantage. From algorithmic trading that precipitates market flash crashes to opaque hiring tools that perpetuates societal biases, the double-edge sword of technological advancement is increasingly apparent. Consequently, the discourse has shifted from purely technical “can we build it?” to an ethically-grounded ‘should we, and if so, how?’. Yet as system powered by artificial intelligence, autonomous agents and complex data infrastructures become more embedded into decision-making and operational workflows, ethical considerations escalate from peripheral concerns to central strategic imperatives. The promise of emerging technologies lies in speed, scale, new capabilities and from an organizational viewpoint, the potential to leapfrog rivals, discover novel market, positions, optimize decisions and reshape business models. At the same time, these very technologies risk undermining human agency, obscuring accountability, shifting responsibility in problematic ways, engendering algorithmic bias, and eroding stakeholder trust. As organizations navigate this complex terrain, ethical cannot simply be reactive addressing risk after technology is in place but must be proactive, integrated and strategic. Achieving strategic advantage via emerging technologies thereby demands not only technological capability but ethical legitimacy.

This essay investigates the following three research questions:

1. How does the deployment of emerging technologies influence human agency in strategic contexts?
2. What mechanisms of accountability are required when organizations pursue strategic advantages using advanced technologies?
3. In what ways can organizations ethically integrate emerging technologies to secure strategic advantage without sacrificing human dignity, autonomy or societal trust?

The deployment of emerging technologies influence on human agency in strategic contexts

Human agency is commonly defined as the capacity of individuals to act intentionally, make meaningful choices, reflect on their actions and influence outcomes. In strategic organizational context such as competitive positioning, innovation, decision-making, or risk management agency is central for leadership, adaptability and legitimacy. When emerging technologies are introduced, the contours of human agency shift significantly. one key way agency is influenced is by the scale and speed of technological decision-making AI systems can process vast data, detect patterns as scale, and recommend or even execute actions far faster than humans. In such contexts, hu-

man decision-makers may become “delegators” rather than direct actors, overseeing rather than, performing decision-making. This can lead to erosion meaningful human control. As noted in literature “human risk becoming passive approvers instead of active decision-makers, which undermines meaningful human agency. Vox this shifts raises several ethical and strategic concerns; when humans relinquish input, they may lose the ability to intervene, understand underlying logic or be morally responsible for outcomes. Another dimension is the opacity of algorithmic processes. ¹When systems are “black box”² or poorly explained, human actors may not understand how recommendations or decisions are generated. The relationship between human agency and accountability is not linear but cyclical, forming what can be termed “agency-accountability loop”. Diminished agency directly corrodes accountability if a human operator cannot understand or intervene in systems decision, they cannot be held meaningfully responsible for its outcomes. Conversely, weak accountability a environment where no one is clearly answerable for technological failures-erodes the incentive to maintain meaningful human agency, why invest in oversight and understanding if there are no consequences for neglect? This creates a vicious cycle where the absence of one component accelerates the decay of the other. Organizations must therefore actively foster a virtuous cycle; enforcing verlar accountability, they create the structural imperative to preserve and enhance human agency, which in turn makes genuine accountability possible. ¹Thus reducing their capacity for reflections, challenge and meaningful choice. The literature on human AI collaboration underscore that collaboration requires supervision and shared responsibility. Further, value alignment and system design choices influence agency. Technologies embed values and decisions about what counts as data, what model to build. What objectives to optimize. If human actors are excluded from these upstream decisions, their agency is constrained from the start. Finally, the influence on agency has broader implications: diminished agency can lead to reduced accountability, lower morale. Loss of trust and ethical drift. If employees feel they are only monitoring machines or executing machine-generated directives, they may disengage, which undermines organizational resilience and weaponize technology without human judgment. From a strategic ethical lens, preventing agency becomes both an internal governance and external legitimacy issue. In summary, the deployment of emerging technologies influences human agency in strategic context by altering decision-making roles, reducing comprehension and intervention capacity, shifting upstream design power, and thereby possibly eroding meaningful human choice and ownership. Beyond the shifting of decision-making roles, emerging technologies can subtly reshape the very environment in which agency is exercised. Algorithmic systems and personalized interfaces often create ‘choice architectures’ that nudge human behavior in predetermined directions. When these architectures are invisible to the user, human agency is not just delegated but manipulated. The individual may feel they are acting autonomously, while their choices are being systematically funneled by predictive models optimizing for a specific outcome. This “illusions of agency” presents a more insidious ethical challenges that outright automation, as it compromises the authenticity of human choice while maintaining the facade of control. Organizations seeking

¹ Ethics of Emerging Technology <https://surl.li/gnzhft>, Accessed 10.11.2025

² J. Y. Hwang, Ethics of artificial intelligence: Examining moral accountability in autonomous decision-making systems. *World Journal of Advanced Research and Reviews*, 23(03), (2024). 3192-3198.

strategic advantage must consciously design for human agency through human in loop, transparency, training, participative design to ensure agencies remain meaningful rather than superficial. The erosion of agency begins long before a system is deployed, at the very inception of its design. The selection of training data, other a reflection of historical biases, and the choice of performance metrics, which prioritize certain outcomes over there, embed specific values into the technological core. When these foundational choices are made without diverse human input, the agency of end-users and affected stakeholders is systematically constrained, predisposing the system to produce outcomes that may be efficient but are not necessarily equitable.

The mechanisms of accountability that are required when organizations pursue strategic advantage using advanced technologies

When organizations incorporate emerging technologies into their strategic operations whether through AI -driven decision-making, autonomous systems or algorithmic optimization accountability becomes both ore critical and more complex. Traditional accountability models face strain when actions are mediated, obscured or augmented by technology. First, the concept of accountability must be clarified. Research identifies accountability in AI systems uphold certain professional codes of practice. In system where technology is involved in decisions, it must be clear who is responsible; the designer, developer, deployer. Operator, decision-maker or the organization as a whole. Ambiguity leads to what has been called a “responsibility gap”.³To bridge this responsibility gap, robust mechanisms must be institutionalized. one promising approach is the adoption of mandatory algorithmic impact assessments for high-stakes applications, forcing organizations to systematically evaluate potential risks before deployment. Furthermore, the principle of “explainability by design” must be integrated into development cycles, ensuring that systems are inherently audits, can provide extent possible. Finally, independent third-party audits, akin to financial audits, can provide external validation of an organization’s accountability claims, building crucial external trust.”⁴ enable accountability, decisions must be understandable and traceable. The human actors and stakeholders need to have access and insight into how systems arrive at outcome, what data and model logic were used, and how human intervention was possible. The literature posits that accountability involves not only outcome responsibility but process transparency. Accountability requires governance frameworks that assign oversight roles. Decision threshold, escalation protocols, human in or on loop models. For example risk based framework for alignment link level of AI risk to appropriate form of human oversight. When technologies produce adverse outcomes. Stakeholders must have mechanism to challenge decisions to appeal to receive remediation. Ethical integration thus demands that organizations not only anticipate harm but establish clear complaint review and correction processes. Beyond operational mechanisms, accountability must be part of strategy; ethical governance must be baked into strategic planning not retrofitted. Organizations must understand that accountability is an enable of trust, which is integral to sustainable competitive advantage. Organizations that treat accountability merely as compliance risk

3 A.Gani, , & D. Darmawan, Ethics and Accountability in Artificial Intelligence-Based Managerial Decision Making. *Journal of Social Science Studies*, 2(1), (2022). 147-152.

4 R.Rousi, With Clear Intention — An Ethical Responsibility Model for Robot Governance. *Frontiers in Computer Science*. (2022).

strategic fragility. Furthermore, accountability must be understood as a continuous process rather than a static assignment of blame after a failure. This requires the implementation of “dynamic accountability mechanisms, where responsibility throughout the systems lifecycle. This includes documenting the rationale for key design choices, maintaining version-controlled datasets, and logging all human AI interactions for critical decisions. Such a comprehensive audit trail does not just assign fault post-hoc, it creates a culture of meticulousness and provides invaluable data for diagnosing systemic flaws, enabling organizations to learn from near-misses and continuously refine their governance structures. “ethical integration also demands the cultivation of “ethical foresight” the capacity to anticipate and prepare for the second-order societal consequences of technology. An organization might deploy a highly efficient logistics AI that optimized delivery routes, but without foresight, it may fail to anticipate the resulting concentration of traffic and pollution in low-income neighborhoods. Proactively engaging with ethicists, urban planners and community representatives during the design phase can reveal these hidden costs. This broader perspective allows organizations to adjust their strategies, perhaps by developing cleaner delivery vehicles or alternative routing algorithms, thereby securing advantage not only through efficiency but through proactive social responsibility and community partnership. mechanisms of accountability required when organizations pursue strategic advantage using advanced technologies include; well-defined responsibility allocation, transparency and embedding accountability into strategic governance. Without these organizations risk responsibility voids, erosion of trust, regulatory exposure and diminished legitimacy.

Ways that organizations can ethically integrate emerging technologies to secure advantages without sacrificing human dignity, autonomy or societal trust

securing strategic advantage via emerging technologies and doing so ethically is not simple a balancing act but a strategic opportunity ethics and strategy can reinforce each other. Ethical integration means designing. Deploying and governing technologies in ways that preserve human dignity, autonomy agency and societal trust while delivering competitive capability. At the heart of ethical integration is human-centred design technologies should augment human capability, not supplant human decision-making entirely. Organizations should embed humans in loops of designs decisions and oversight. Rather than treating ethics as compliance or cost, forward-looking organizations use it as a competitive differentiator. Ethical technology deployment can build stakeholder trust, enhance brand reputation, reduce regulatory risk and open new markets. For example, the strategic advantage arises not just from faster decision-making but from owning the ethical narratives; being trusted being transparent. Ultimately, the quest for strategic advantage in the 21st century is converging with the imperative for ethical stewardship. The organizations that will thrive are those that recognize technology not as an autonomous force to be unleashed, but as a profound extension of human will and organizational values. By deliberately weaving human agency, clear accountability, and ethical foresight into the fabric of their strategy, they do not just avoid risk they build a distinctive and durable form of capital.⁵ The trust of their employees, cus-

⁵ J. J. Cañas, AI and Ethics When Human Beings Collaborate With AI Agents. *Frontiers in Psychology*, (2022).

tomers, and society at large. In this new paradigm, the most significant strategic advantage is the license to lead, granted by those who are confident that the power of technology is being exercised with wisdom and responsibility. Organizations that integrate ethics into strategy are more resilient in changing regulatory and social environment. Ethical integration demands designing fairness, avoiding bias, ensuring accessibility. A practical manifestation of ethical integration is “ethics by design” a proactive methodology that runs parallel to “security by design”. This involves constituting interdisciplinary teams that include not only engineers and product managers but also ethicists, legal experts, and representatives from affected communities. These teams can conduct “pre-mortem” exercise, imagining how a system could fail ethically, and build in safeguards accordingly. For example, rather than automatically reject applications from postcode with historically low credit scores, ensuring a human expert reviews them for contextual factors. Transparency of system operations, and ability to challenge outcomes. Emerging technologies evolve; context change. Ethically, integration therefore requires ongoing monitoring of system performance, impact of human actors and society, and adaptive governance. Ethical risk is not static; what is safe, fair, transparent today may become problematic tomorrow. Organizations should build learning loops, feedback mechanisms, post-deployment audits, and decision review processes. This dynamic governance ensures the technology stays aligned with evolving human values, regulatory norms and societal expectations. Ethical integration means preserving human autonomy while leveraging automation. Too much automation can undermine human dignity, competence and decision-making capacity; too little may leave strategic advantage on the table⁶. The challenge and strategic opportunity lie in calibrating where human actors retain meaningful intervention oversight and decision-making, and where machines augment or automate. This calibration must be deliberate transparent and subject to review. In sum, organizations can ethically integrate technologies to secure strategic advantage by adopting human-centric design, embedding ethics into strategy, ensuring fairness, building continuous governance and balancing automation with human autonomy. When done well, strategic advantage arises not just from technology but from the combination of technological capability and ethical legitimacy.

Conclusion

The ethics of strategy advantage in the age of emerging technologies underscores the vital interplay between human agency, accountability and organizational strategy. As organizations seek to harness AI, autonomous system and data-driven platforms for competitive gain, they must ensure that human actors retain genuine agency, accountability mechanisms are robust and clear, and ethical integration serves both strategic and societal goals. Such organizations transform ethics from being an after-thought or compliance burden into a core component of strategy and competitive advantage. Rather than viewing emerging technologies purely as tools to outpace rivals, organizations that design for human dignity, transparency and trust are positioned to achieve sustained advantage in a rapidly evolving socio-technical landscape. In essence, the strategic deployment of technology is not just a matter of “what we should do” and how going so aligns with human val-

6 Dataset/Study: Accountability in artificial intelligence: what it is and how it works. *AI & Society*, Vol.39, pp 1871-1882.

ues and accountability. Organizations that align there dimensions are better positioned for lasting success, legitimacy and ethical leadership. The pursuit of strategic advantage through technology is being redefined. The most successful organizations of the future will not be those with the most powerful algorithms alone, but those who can't best demonstrate that their algorithms are fair, accountable, and enhance human potential. By meticulously designing for agency, architecting robust accountability, and embracing ethics as a strategic linchpin, organizations can navigate the socio-technical landscape not as mere participants, but as leader building a more legitimate and sustainable competit.

Bibliography

- Hwang, J. Y. Ethics of artificial intelligence: Examining moral accountability in autonomous decision-making systems. *World Journal of Advanced Research and Reviews*, 23(03), (2024). 3192-3198.
- Gani, A., & Darmawan, D. Ethics and Accountability in Artificial Intelligence-Based Managerial Decision Making. *Journal of Social Science Studies*, 2(1), (2022). 147-152.
- Rousi, R. With Clear Intention — An Ethical Responsibility Model for Robot Governance. *Frontiers in Computer Science*. (2022).
- Cañas, J. J. AI and Ethics When Human Beings Collaborate With AI Agents. *Frontiers in Psychology*, (2022). 13.
- Dataset/Study: Accountability in artificial intelligence: what it is and how it works. *AI & Society*, Vol.39, pp 1871-1882.
- Ethics of Emerging Technology <https://surl.li/gnzhft>, Accessed 10.11.2025

GEORGIA AS A STRATEGIC ECONOMIC CORRIDOR IN THE SOUTH CAUCASUS AND THE BLACK SEA REGION

Lizi Botchoidze

The Junker of a Bachelor's Degree (Management) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Mariam Kokilashvili

The Junker of a Bachelor's Degree (Management) of
LEPL - David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Tinatin Jorjoliani

Associate Professor of Bachelor's program in Management of
LEPL David Aghmashenebeli National Defence Academy of Georgia,
Academic Doctor of Business Administration
ORCID: 0000-0002-8274-9028

Abstract

This paper examines Georgia's evolving strategic role as a transit and economic corridor in the South Caucasus and Black Sea region, highlighting its significance for Eurasian connectivity, regional trade flows, and energy security. It provides a comprehensive assessment of Georgia's multimodal transport and logistics infrastructure—including railways, highways, maritime ports, and energy transit networks—and evaluates their operational efficiency, economic viability, and degree of integration into global and trans regional supply chains. Special emphasis is placed on key modernization initiatives such as the Baku–Tbilisi–Kars railway, the East–West Highway, Anaklia and Poti port developments, and Georgia's expanding participation in the Middle Corridor (Trans-Caspian International Transport Route). The study also analyzes the geopolitical and geo economic constraints affecting corridor sustainability, including regional security risks, investment uncertainties, and strategic competition among external powers. Drawing upon empirical datasets from the World Bank, OECD¹, national statistical agencies, and field-based operational reviews, the research integrates economic analysis with policy evaluation to identify structural bottlenecks and emerging opportunities. The findings indicate that Georgia holds substantial potential to consolidate its position as a reliable transit hub and regional logistics platform, contingent on continued governance reforms, digitalization of customs and border systems, and enhanced coordination with neighboring transit states. The paper concludes with evidence-based policy recommendations tailored to government institutions, private stakeholders, and international development partners, aimed at improving infrastructure performance, investment attractiveness, and long-term economic resilience within the South Caucasus–Black Sea strategic corridor.

Keywords: Georgia; South Caucasus; Black Sea region; transit corridor; logistics; Eurasian connectivity; Middle Corridor; infrastructure development; energy transit; regional trade; strategic competition; geo economics; sustainable transport; economic resilience.

¹ OECD — Realising the Potential of the Middle Corridor (2023).

Introduction

Georgia's geographic position—situated on the Black Sea coast, at the juncture of Europe and Asia, and in proximity to the Caspian energy basin—has endowed it with long-standing strategic relevance as a transit and connectivity bridge. In the contemporary era of global supply chain fragmentation, geopolitical uncertainty, and growing demand for diversified trade routes, this role has acquired renewed importance. As maritime chokepoints face congestion and geopolitical risks, and as traditional northern transit corridors have become increasingly constrained due to sanctions, conflict, and political tensions, the Middle Corridor (Trans-Caspian International Transport Route) has emerged as a viable and strategically significant east–west alternative linking China and Central Asia with the South Caucasus, Turkey, and Europe. International organizations, logistics consortia, and policy forums have increasingly acknowledged the corridor's potential to reshape regional connectivity and integrate the South Caucasus more deeply into global economic networks. Historically, Georgia has served as part of both north–south and east–west trade routes—traces of the ancient Silk Road remain embedded in its cultural and infrastructural landscape. However, the dissolution of the Soviet Union reconfigured regional transportation and energy flows, requiring newly independent states to rebuild institutional frameworks, logistical pathways, and cross-border cooperation arrangements. These transformations were further shaped by shifts in maritime logistics, global energy markets, and the strategic ambitions of regional powers. In the current geopolitical context, characterized by heightened great-power competition, regional conflicts, fluctuating energy transit dynamics, and persistent efforts to bypass Russian-controlled routes, Georgia's transit significance is expanding. The security repercussions of the 2008 conflict, ongoing instability in the wider Black Sea basin, and recent disruptions related to the Russia–Ukraine war have all underscored the need for resilient, diversified, and politically reliable transport corridors. At the same time, Georgia's enduring Euro-Atlantic orientation and reform commitments continue to strengthen its reputation among international investors and external partners as a predictable and cooperative transit state—although domestic political polarization and governance inconsistencies occasionally temper this perception.²

Against this backdrop, the development and modernization of Georgia's transport infrastructure—including rail networks, highways, maritime ports, and digital customs platforms—has become central to both national development strategy and regional integration agendas. Major projects such as the Baku–Tbilisi–Kars railway, ongoing upgrades to the East–West Highway, and Black Sea port expansion initiatives demonstrate the country's ambition to secure long-term logistical competitiveness. Meanwhile, debates surrounding the Anaklia Deep-Sea Port highlight the intersection of national economic priorities with strategic interests of external actors.

Research Objectives

This study aims to:

Describe and evaluate Georgia's existing and planned infrastructure-based transit capabilities within regional and global supply chain frameworks;

Measure the economic impact of the corridor in terms of freight volumes, port capacity, em-

² Popkhadze, Guro. 2025. "Anaklia's Strategic Gamble: Will Washington's New Maritime Strategy Matter?" *Geopolitics*, June 8, 2025. <https://surl.li/huhuzm>, Accessed 10.11.2025

ployment effects, and foreign direct investment (FDI);

Identify structural, geopolitical, legal, and operational barriers—including border coordination challenges, regulatory fragmentation, security risks, and unresolved strategic infrastructure debates (e.g., Anaklia Port);

Assess opportunities for strengthened regional and international cooperation in support of corridor efficiency and resilience; and

Develop evidence-based policy recommendations for the Government of Georgia, private logistics actors, and international development partners aimed at improving transit functionality, investment attractiveness, and long-term sustainability.

Main Part

Middle Corridor Dynamics and Infrastructure Performance in Georgia

Recent data from the World Bank and national statistical agencies show a marked increase in freight volumes transiting the Middle Corridor.³ Freight flows rose from approximately 1.5 million tons in 2022 to about 2.8 million tons in 2023, reflecting growing demand for alternative Eurasian transport routes in the context of regional sanctions, geopolitical realignments, and global supply chain diversification. This growth has been particularly influenced by the expansion of China–Europe express rail services, enhancements in port terminal capacity, and the partial digitalization of customs and border management systems along the corridor. Infrastructure development has produced both immediate and long-term economic effects. During construction phases, projects generate employment in civil engineering, transport infrastructure, manufacturing supply chains, and local services. Over the longer term, the establishment of logistic terminals, processing zones, and customs brokerage services stimulates job creation in logistics, warehousing, value-added processing, hospitality, and trade facilitation. International development institutions, including the World Bank and Asian Development Bank,⁴ emphasize multiplier effects: each dollar invested in transport infrastructure yields broader gains across employment, freight efficiency, and regional economic integration—provided that governance, investor confidence, and regulatory stability are maintained.

The Middle Corridor itself represents a strategic multimodal route linking China and Central Asia to Europe via Kazakhstan, the Caspian Sea, Azerbaijan, Georgia, and Turkey. OECD and World Bank projections suggest that freight volumes could triple by 2030,⁵ contingent on targeted investments, harmonized customs procedures, and coordinated transport regulation among corridor states. Key operational challenges remain, including multiple border crossings, technical interoperability across rail systems, divergent safety and tariff standards, and port handling constraints. These issues underscore the necessity of a coordinated regional governance mechanism in logistics, customs, and infrastructure management.

The Baku–Tbilisi–Kars (BTK) railway, operational since 2017, serves as the backbone of the

3 National Statistics Office of Georgia (Geostat) — Major Indicators of Seaports and Terminals — 2023.

4 World Bank — The Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2030 (2023); related presentations (2024).

5 OECD — Realising the Potential of the Middle Corridor (2023).

South Caucasus segment of the corridor.⁶ While its original capacity was projected at 6.5 million tons annually—with upgrade plans to reach 15–17 million tons—actual volumes remain significantly lower due to logistical bottlenecks, tariff-setting disputes, fragmented scheduling, and insufficient interoperability.⁷ Accelerating capacity utilization requires synchronized planning among Azerbaijan, Georgia, and Turkey, supported by transparent regulatory frameworks and digital rail dispatch coordination.

Georgia's East–West Highway modernization has significantly improved freight transit efficiency, especially by reducing travel times and lowering heavy vehicle operating costs. Investments in road widening, tunnel construction, and route realignment have enhanced both safety and international haulage competitiveness. These improvements strengthen Georgia's role as the primary land bridge between the Caspian Basin and Black Sea maritime gateways. Georgia's maritime system is anchored by Poti and Batumi ports, where container flows are concentrated. APM Terminals Poti handled approximately 592,589 TEU in 2023, adjusting to 545,297 TEU in 2024 in response to broader global freight price fluctuations. Overall, Georgian ports increased total cargo volumes from ~13.9 million tons in 2023 to ~15.5 million tons in 2024. However, the absence of a deep-sea port remains a structural limitation for handling Panamax and post-Panamax vessels. The Anaklia Deep Sea Port project, though strategically transformative, has faced legal disputes, contract termination controversies, and ongoing ICSID arbitration, which have adversely affected investor confidence and signaled concerns regarding the predictability of the investment climate. This case exemplifies how geopolitical sensitivity, governance uncertainty, and great-power competition shape infrastructure outcomes in the South Caucasus. In addition to these structural challenges, territorial occupation, Russian military presence in the region, and unresolved conflicts elevate risk perception among private and institutional investors. Border inefficiencies—such as multiple inspections, inconsistent customs procedures, and incompatible digital systems—increase transit times and operational costs. OECD policy reviews have consistently emphasized the necessity of implementing a “One-Stop Border” model, harmonizing tariff policies,⁸ and expanding single-window digital customs platforms to improve predictability and transparency.

Financing remains a critical challenge. Large-scale corridor infrastructure requires high upfront capital expenditure, which is difficult for a small economy to sustain. Therefore, effective development depends on public-private partnerships (PPPs), strategic collaboration with multilateral development banks, and innovative financing instruments that distribute risk. Technical modernization—including rail automation, port mechanization, cold-chain expansion, and integrated tracking systems—is essential but capital-intensive.

Policy Implementation “Roadmap”

The effective development of Georgia's transit and logistics system requires a phased policy approach that balances immediate operational improvements with long-term strategic trans-

⁶ BTK Railway Consortium. (2023). Baku–Tbilisi–Kars Technical Specifications and Capacity Reports.

OC-Media, Ports Europe, & White & Case LLP. (2024). Anaklia Port Development and Legal Arbitration Overview.

⁷ Popkhadze, Guro. 2025. “Anaklia's Strategic Gamble: Will Washington's New Maritime Strategy Matter?” *Geopolitics*, June 8, 2025. <https://surl.lu/tnwogz>, Accessed 10.11.2025

⁸ OECD — Realising the Potential of the Middle Corridor (2023).

formation. In the short term (1–3 years), priority should be placed on enhancing administrative efficiency and improving the business environment. This includes the full implementation of a single-window customs system and the digitalization of border and cargo clearance procedures, which together will streamline transactions and reduce procedural delays. At the same time, the government should advance targeted public–private partnerships (PPPs) and expand cooperation with established global port and logistics operators. These measures are expected to increase investor confidence, accelerate infrastructure upgrades, and improve logistics performance across key corridors. In the medium term (3–7 years), the focus should shift toward network integration and regional coordination. This involves developing multimodal logistics hubs—particularly near Poti and key inland transport nodes—allowing for efficient transfer between rail, road, and maritime systems. Additionally, coordinated investment in the Baku–Tbilisi–Kars (BTK) railway will be essential to raise its operational capacity from the initial 6.5 million tons towards 15 million tons and beyond,⁹ in alignment with growing demand along the Middle Corridor. Establishing a formal regional coordination mechanism among Georgia, Azerbaijan, Turkey, and other corridor partners will further ensure standardized operational practices, reduce bottlenecks, and enhance trade competitiveness. Finally, the long-term horizon (7+ years) should focus on positioning Georgia as a core node in wider Eurasian connectivity and sustainable infrastructure ecosystems. This phase entails the integration of green and digital energy corridors, including electricity interconnectors, hydrogen transport networks, and data infrastructure, alongside the realization of a deep-sea port to accommodate larger vessel classes and higher cargo volumes. Complementing these physical investments, the state must progress toward full legal, regulatory, and institutional alignment with EU standards, ensuring transparency, predictability, and long-term investor trust. Collectively, these measures will allow Georgia to establish itself as a resilient, competitive, and strategically indispensable logistics and energy hub linking Europe and Asia.

Conclusion

Georgia's strategic position at the crossroads of the South Caucasus and the Black Sea continues to shape its role as a critical transit, logistics, and connectivity hub between Europe and Asia. The growing importance of the Middle Corridor reflects both structural transformations in global supply chains and the geopolitical reconfiguration of Eurasian trade routes. Rising freight volumes, expanding infrastructure capacity, and increasing interest from international transport operators underscore the corridor's economic potential. However, the realization of this potential is neither automatic nor guaranteed. It depends on the country's ability to address persistent structural, regulatory, and geopolitical challenges. The analysis demonstrates that Georgia has made significant progress in modernizing its transport infrastructure—particularly through the Baku–Tbilisi–Kars railway, the East–West Highway upgrades, and ongoing improvements at Poti and Batumi ports. Nonetheless, gaps remain in multimodal integration, border management efficiency, and long-term port capacity, particularly regarding the unresolved strategic development of a deep-sea port. Investor confidence and large-scale capital mobilization continue to be shaped

⁹ BTK Railway Consortium. (2023). Baku–Tbilisi–Kars Technical Specifications and Capacity Reports. OC-Media, Ports Europe, & White & Case LLP. (2024). Anaklia Port Development and Legal Arbitration Overview.

by political stability, legal predictability, and transparent governance practices. Regional instability, technical interoperability constraints, and uneven regulatory coordination along the corridor further complicate operational performance.¹⁰

Sustainable progress will require a phased and coordinated policy approach, combining short-term efficiency measures, medium-term network integration, and long-term strategic positioning. Strengthening digital customs platforms, expanding public–private partnerships, and formalizing regional logistics governance frameworks are immediate priorities. Over time, integrating green energy transmission lines, digital connectivity corridors, and deeper alignment with EU regulatory standards will enhance Georgia’s strategic value and resilience.

Ultimately, Georgia’s potential to function as a reliable and competitive Eurasian transit hub rests on the interplay of infrastructure modernization, institutional credibility, and regional cooperation. By pursuing reforms that enhance transparency, efficiency, and international coordination, Georgia can solidify its role not only as a transport corridor but also as a strategic platform for economic development, regional stability, and long-term economic resilience within the South Caucasus–Black Sea connectivity architecture.

Bibliography

- BTK Railway Consortium. (2023). *Baku–Tbilisi–Kars Technical Specifications and Capacity Reports*.
OC-Media, Ports Europe, & White & Case LLP. (2024). *Anaklia Port Development and Legal Arbitration Overview*.
- OECD — Realising the Potential of the Middle Corridor (2023).
- World Bank — The Middle Trade and Transport Corridor: Policies and Investments to Triple Freight Volumes and Halve Travel Time by 2030 (2023); related presentations (2024).
- National Statistics Office of Georgia (Geostat) — Major Indicators of Seaports and Terminals — 2023.
- Popkhadze, Guro. 2025. “Anaklia’s Strategic Gamble: Will Washington’s New Maritime Strategy Matter?” *Geopolitics*, June 8, 2025. <https://surl.li/fnalcc>, Accessed 10.11.2025
- Tekla Aslanishvili and Orit Halpern. 2020. “Scenes from a Reclamation.” *E-flux Architecture: New Silk Roads*, February 2020. <https://surl.li/sqjefe>, Accessed 10.11.2025

¹⁰ Tekla Aslanishvili and Orit Halpern. 2020. “Scenes from a Reclamation.” *E-flux Architecture: New Silk Roads*, February 2020. <https://www.e-flux.com/architecture/new-silk-roads/313102/scenes-from-a-reclamation/>.

DEFENSE INNOVATION AND INTERNATIONAL COOPERATION: SHAPING THE FUTURE OF GLOBAL SECURITY

Shahryar Huseinli

Cadet of Military Institute named after Heydar Aliyev

Abstract

In the rapidly evolving landscape of global defense and security, innovation and international cooperation have emerged as indispensable pillars for ensuring long-term stability, resilience, and the capacity to address emerging threats. As the complexity of modern warfare continues to escalate, defense innovation plays a crucial role in shaping the future of military strategy and security infrastructures. This innovation is not merely confined to the development of new technologies but also involves the integration of cutting-edge systems such as artificial intelligence (AI), unmanned systems, quantum computing, and robust cybersecurity measures. These technologies serve to enhance both national defense capabilities and the collective strength of international alliances. The growing prevalence of geopolitical tensions and the rise of unconventional threats—ranging from cyberattacks and terrorism to hybrid warfare—has underscored the necessity for technological superiority. In response, nations are increasingly turning to advanced technologies not only to strengthen their own defense systems but also to foster collaborative defense initiatives with global partners. Through strategic alliances and cooperative programs, countries are leveraging innovation to create more resilient defense architectures capable of deterring and mitigating a wide array of threats. As defense strategies become more reliant on technological advancements, the importance of international cooperation has never been greater. By pooling resources, sharing expertise, and coordinating responses, states can enhance their collective defense posture and adapt more swiftly to the evolving security landscape. This collaborative approach, driven by technological innovation, represents a transformative shift in how nations address defense and security challenges on the global stage.

Keywords: Defense innovation, international cooperation, artificial intelligence (AI), unmanned systems, quantum computing, cybersecurity, geopolitical tensions, hybrid warfare, technological superiority, strategic alliances, military strategy, global security, defense architecture, technological advancements.

Introduction

International cooperation plays a pivotal role in enhancing transparency, interoperability, and the alignment of strategic objectives among nations. Through alliances such as NATO and regional defense partnerships, states can collaboratively develop, test, and deploy innovative defense technologies while effectively managing global risks. These cooperative efforts not only strengthen collective deterrence but also facilitate the transfer of knowledge and the development of capacities between nations at various stages of technological maturity. Thus, the convergence of innovation and cooperation represents a transformative shift in the design and implementation of security architectures.¹

The future of global security hinges on balancing national interests with collective defense innovation. Ethical considerations, regulatory frameworks, and responsible governance of emerging technologies will shape how effectively new defense technologies are deployed, both in military and humanitarian contexts. Furthermore, investment in education, research, and dual-use technologies will be critical in ensuring sustainable progress and the ethical application of military innovations. As nations navigate the complexities of modern warfare, cross-border collaboration will remain essential to addressing global threats such as cyberattacks, terrorism, and hybrid warfare.

Ultimately, defense innovation and international collaboration will define the future trajectory of global security. By prioritizing strategic partnerships, technological research, and transparent governance, nations can foster a safer and more stable world order. The integration of scientific advancement with diplomatic cooperation will not only enhance military readiness but also promote peace through shared innovation and mutual understanding.

Today, while weapons remain powerful, ideas are far stronger than armaments. Modern warfare extends beyond tanks and guns to encompass information, computers, and cyberspace. Security, in the contemporary context, entails not only robust military forces but also the strength of intellect, science, technology, and cooperation.

In the 21st century, the global landscape is confronted with new and evolving threats. Whereas in the 20th century, the power of a nation was often measured by the size of its military—its soldiers, tanks, and weapons—today, the true measure of a nation's power lies in its scientific, technological, and intellectual capabilities.

According to the World Bank, global military expenditure reached a historic high of 2.44 trillion dollars in 2023. However, a significant portion of this investment is no longer directed towards conventional weaponry but toward cutting-edge technologies such as artificial intelligence (AI), cyber defense, drones, and space exploration.

This shift underscores a clear reality: in the future, it will be ideas, technology, and international cooperation—rather than military forces—that will safeguard our global security.

Imagine the following scenario:

In one country, a student develops a drone powered by Artificial Intelligence (AI).

In another country, a young programmer designs a sophisticated cyber defense system.

Meanwhile, in yet another location, a student creates a project focused on energy security.

¹ NATO. "Innovation, resilience, and emerging technologies in defense". NATO Publications. Retrieved from, (2023). <https://www.nato.int>

If these ideas stand alone, they are like isolated stars scattered across the sky. However, when connected through international cooperation, they form a constellation that has the potential to protect the world.

Let us explore these concepts in more detail:

1. Defense Innovation: The Engine of Modern Security

1.1 Artificial Intelligence (AI)

Artificial Intelligence is now at the core of defense modernization. AI systems are capable of processing vast amounts of complex data at speeds far beyond human decision-making capabilities, enabling predictive analytics, threat detection, and autonomous responses. According to the RAND Corporation (2023), AI can make military decisions up to five times faster than traditional command structures.²

The U.S. Replicator Initiative (2023) seeks to deploy thousands of low-cost autonomous drones capable of coordinating independently on the battlefield. Similarly, Israel's Iron Dome system utilizes AI to intercept incoming rockets with an accuracy rate exceeding 95%.

Countries like China, Russia, and India are making significant investments in military AI, with China aiming to establish global leadership in this domain by 2030. However, the rapid acceleration of AI-driven warfare also presents profound ethical challenges—most notably, the question of how much decision-making should be delegated to machines. Striking a balance between operational efficiency and moral considerations will ultimately determine the legitimacy of future defense systems.³

1.2 Unmanned Aerial Vehicles (UAVs) and Autonomous Systems

Once used solely for reconnaissance, drones have now become multi-role assets in combat, logistics, and humanitarian operations. The 2020 Nagorno-Karabakh conflict marked a turning point when Azerbaijan's innovative use of UAVs demonstrated how technology could change the course of war. NATO described this as “a new era of modern warfare.”

In the Russia-Ukraine conflict, drones are used daily—not only for strikes but also for evacuations, communications, and reconnaissance. By 2030, the global drone market is expected to exceed 90 billion USD (PwC).

Drones symbolize a broader truth: innovation is not only about destruction but also preservation. Medical delivery drones now provide emergency aid in disaster zones, proving that defense technology can save lives as well as protect them.

1.3 Cybersecurity: The Invisible Battlefield

The digital realm is now the most active front in global defense. The 2007 cyberattack on Estonia, which paralyzed government systems, revealed the devastating potential of cyber warfare. In response, NATO established the Cooperative Cyber Defence Centre

² European Defence Agency. “Defence innovation through collaboration and technological excellence”. Brussels: EDA Publications. (2023).

³ U.S. Department of Defense. “National Defense Strategy of the United States of America”. Washington, DC: Office of the Secretary of Defense. (2022).

of Excellence in Tallinn. More recently, the 2021 Colonial Pipeline attack in the United States exposed the vulnerability of critical infrastructure.⁴

Cybersecurity Ventures (2024) predicts that global cybercrime costs will reach 10.5 trillion USD per year by 2030, surpassing the global trade in illegal drugs. Cybersecurity has thus become as essential as air defense or missile systems. Every soldier with a computer is now part of a new, invisible army.

1.4 Robotics and Human–Machine Collaboration

Modern robotics allows militaries to perform high-risk operations without endangering human lives. The U.S. military is testing robotic systems such as Boston Dynamics’ “Spot” for reconnaissance and mine detection. In 2022, China unveiled its first autonomous combat tank, symbolizing the global competition for robotic dominance.

According to Oxford Insights (2024), autonomous robotics could reduce battlefield casualties by up to 60% by 2040. These machines can operate in nuclear, chemical, and urban environments where human soldiers would face deadly risks. Yet, their deployment also demands strong ethical and legal frameworks to prevent misuse.

1.5 Space Technology: The Fifth Domain of Warfare

Space has become the ultimate strategic high ground. As of 2024, more than 7,000 active satellites orbit Earth (Space Foundation, 2024). These systems enable global communication, GPS navigation, and surveillance.

During the Ukraine conflict, Starlink satellites ensured uninterrupted military and civilian communication. The United States, China, and Russia are in a technological race to dominate this domain, making space the fifth battlefield—after land, sea, air, and cyberspace.⁵

However, the militarization of space raises profound questions about the future of peace. Should space remain a realm of scientific cooperation, or will it become the next arena of conflict?

2. The Ethical Dimension of Defense Technology

History demonstrates that technology is neutral—it can protect or destroy.

- Atomic energy devastated Hiroshima and Nagasaki but today powers 10% of global electricity (IEA, 2023).
- The internet connected humanity but also enabled disinformation campaigns that cost the world economy 78 billion USD (OECD, 2022).

The same tools that ensure defense can also endanger humanity if used without ethical boundaries. Therefore, responsible innovation, international law, and moral governance must guide technological development.

As I wrote:

“We must remember: security is not only for one nation, it is for all humanity. A cyber-attack in one country can hurt others. Climate crisis has no borders. Terrorism has no passport.”

3. International Cooperation: The Foundation of Global Security

⁴ P. Scharre, “Army of None: Autonomous Weapons and the Future of War.” New York: W. W. Norton & Company. . (2018).

⁵ P. W. Singer, “Wired for War: The Robotics Revolution and Conflict in the 21st Century.” New York: Penguin Press. (2009).

3.1 NATO and Collective Defense

NATO's strategy of Smart Defence emphasizes resource sharing, interoperability, and joint innovation. Member states invest at least 2% of GDP in defense; in 2023, the U.S. contributed 877 billion USD, more than half of NATO's total spending. NATO's Defence Innovation Accelerator for the North Atlantic (DIANA) fosters partnerships with tech startups, ensuring that cutting-edge technologies reach allied forces faster.

3.2 United Nations Peacekeeping and Technological Integration

The United Nations Peacekeeping Forces operate across 12 missions with over 87,000 personnel (UN, 2024). Drones, satellite monitoring, and AI-based predictive tools are now integrated into peacekeeping operations to prevent conflict escalation and protect civilians. These innovations show that technology can serve peace, not only war.⁶

3.3 Regional Cooperation

Regional partnerships strengthen collective resilience. The European Union's PESCO initiative fosters cross-border defense research and capability development. In Asia, ASEAN adopted a joint cybersecurity strategy in 2022. The Azerbaijan–Turkey strategic alliance remains a prime example of regional military cooperation based on trust, shared training, and technology transfer. This partnership demonstrates how smaller nations can achieve regional stability through mutual innovation.⁷

As I emphasized:

“Defense is not only about protecting borders. Defense is also to build bridges—bridges between nations, students, and scientists. If we do not build these bridges, the world will be divided. If we build them, security will be in the light of ideas, not in the shadow of weapons.”

4. Looking Toward 2050: The Future Landscape of Security

By 2050, AI could manage 80% of battlefield decisions (RAND, 2024) and increase global GDP by 15.7 trillion USD (PwC). Space will emerge as the primary domain for strategic competition, while cyber warfare and biotechnology will become the greatest security threats.⁸

The fundamental question remains:

Will weapons or ideas shape the future of global security?

The answer depends on whether humanity can balance innovation with cooperation. True power will belong not to those who build the strongest weapons, but to those who build the strongest partnerships.

The students, scientists, and innovators of today will design the defense architecture of tomorrow. They will determine whether artificial intelligence and automation will secure peace—or magnify chaos. Every idea shared in this conference is a building stone for the bridge to the future.

“This conference is one of those bridges. Every idea here is a stone for the future of security.

6 H., Binnendijk, & Gompert, D. C. “The new era of deterrence and the future of NATO”. RAND Corporation. (2021).

7 L. Kello, “The Virtual Weapon and International Order.” Yale University Press. (2017).

8 Brimley, S., FitzGerald, B., & Sayler, K. “Game changers: Disruptive technology and U.S. defense strategy.” Center for a New American Security (CNAS). (2013).

We must build not only walls, but also bridges between nations—because the future of security will not be in the shadow of weapons, but in the light of ideas.”⁹

Conclusion

The continuous advancement of defense innovation and the strengthening of international cooperation represent the foundation of global security in the twenty-first century. Technological breakthroughs such as artificial intelligence, unmanned systems, and cyber capabilities are reshaping the defense landscape, allowing nations to respond to complex and rapidly changing threats more effectively. However, innovation alone cannot guarantee security without collaboration, transparency, and ethical governance.

International partnerships serve as a bridge between technology and strategy, ensuring that innovation contributes not only to military strength but also to peace and stability. Shared research programs, joint military exercises, and knowledge exchange between allies are vital in addressing global challenges that no single nation can overcome alone. Moreover, balancing national security priorities with collective defense responsibilities will remain an essential task for policymakers and military leaders alike.

In conclusion, the integration of defense innovation and international cooperation defines the path toward a safer and more stable world. Nations that invest in responsible technological development and mutual trust will not only secure their borders but also contribute to global peace. The future of security depends on the ability of states to innovate together, act responsibly, and sustain a shared vision for lasting stability.

Bibliography

- NATO. “Innovation, resilience, and emerging technologies in defense”. NATO Publications. Retrieved from, (2023). <https://www.nato.int>
- U.S. Department of Defense. “National Defense Strategy of the United States of America”. Washington, DC: Office of the Secretary of Defense. (2022).
- European Defence Agency. “Defence innovation through collaboration and technological excellence”. Brussels: EDA Publications. (2023).
- Scharre, P “Army of None: Autonomous Weapons and the Future of War.” New York: W. W. Norton & Company. . (2018).
- Singer, P. W. “Wired for War: The Robotics Revolution and Conflict in the 21st Century.” New York: Penguin Press. (2009).
- Binnendijk, H., & Gompert, D. C. “The new era of deterrence and the future of NATO”. RAND Corporation. (2021).
- Kello, L. “The Virtual Weapon and International Order.” Yale University Press. (2017).
- Brimley, S., FitzGerald, B., & Saylor, K. “Game changers: Disruptive technology and U.S. defense strategy.” Center for a New American Security (CNAS). (2013).
- United Nations Institute for Disarmament Research (UNIDIR). “Responsible innovation in defense: Global governance and ethics.” Geneva: UNIDIR. (2022).
- O’Hanlon, M. E. “The future of warfare: The rise of artificial intelligence and autonomous systems.” Brookings Institution Press. (2020).

⁹ United Nations Institute for Disarmament Research (UNIDIR). “Responsible innovation in defense: Global governance and ethics.” Geneva: UNIDIR. (2022).

FROM REGIONAL POWER TO GLOBAL ACTOR: CHINA'S MILITARY MODERNIZATION AND INTERNATIONAL STRATEGY

Lieutenant Giorgi Phkhakadze

The Learner of a Master's Degree Program (International Relations and Diplomacy) of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Supervisor: Ketevan Chakhava

Assistant Professor of Master's Program in Security Studies of
LEPL-David Aghmashenebeli National Defence Academy of Georgia

Abstract

The paper examines changes in the place of the People's Republic of China on the current global security scene through both defense innovation and transnational partnerships. From a regional force to a global strategic power, China has evolved in three decades, motivated by the lofty dream of "national rejuvenation" that covers technology, economic transformation and military might. Central to this transformation is the Military-Civil Fusion (MCF) strategy which integrates civilian scientific innovation and industrial capacity with military modernization. Through indigenous development in artificial intelligence (AI), cyber warfare, hypersonic weaponry, quantum computing, and space technologies, China has rapidly advanced toward attaining self-reliance and technological superiority. At the same time, China's expanding international partnerships reinforce its strategic ambitions. Institutions such as the Shanghai Cooperation Organization (SCO) and initiatives like the Belt and Road Initiative (BRI) are a quintessential exemplar of China's multidimensional approach to security cooperation, regional stability, and influence projection. Bilateral relations with Russia, Pakistan, and Iran further illustrate how Beijing combines economic, defense, and ideological cooperation in an effort to challenge traditional Western security frameworks. These are both pragmatic and ideological ties; at the same time they increase China's power on geopolitical grounds as well as promoting an alternative, multipolar vision of global security based on sovereignty, mutual benefit, and non-interference. By analysing the correlation between defense innovation and strategic partnership, this paper reveals that the Chinese model is a new paradigm in international relations – one in which technological modernization and global cooperation would redefine the paradigms of power and stability. Finally, China's course is evidence that innovation and collaboration represent not just mechanisms of national development but major drivers of the architecture of 21st-century global security.

Keywords: China; Defense Innovation; Military-Civil Fusion; Global Security; Belt and Road Initiative (BRI); Shanghai Cooperation Organization (SCO); Artificial Intelligence; Cyber Warfare; Strategic Partnerships; Multipolarity; Global Governance; International Relations.

Introduction

In the last 30 years the People's Republic of China faced one of the most extraordinary transformations in world history, transforming from a predominantly regional power into an important player in the global security edifice. Not random but deliberate, through this evolution the nation's strategy, including defense innovation, economic modernization and strategic partnership, has moved in line with the vision of national revival. The Chinese leadership has repeatedly stressed that technology capabilities and broad-based military modernization are vital to reinstating China's historical dominance in a highly competitive international community. At the core of this transformation is the country's thrust toward defense innovation, particularly within Military-Civil Fusion (MCF), which overcomes the divide between civilian scientific advancement and military modernization. Such a policy allows China to use the advancements of artificial intelligence (AI), cyber warfare, quantum computing, space technology, and hypersonic weapons it has begun to advance to strengthen its defense capabilities and reshape the course of global technological competition. In addition, China's global partnerships—multilateral institutions such as the Shanghai Cooperation Organization (SCO), world projects like the Belt and Road Initiative (BRI), and strategic bilateral relationships with countries including Russia, Pakistan, and Iran—broaden its geopolitical influence and offer an alternative set of global security norms rooted in both multipolarity and sovereignty.¹ This twofold strategy—technological development in China and strategic cooperation internationally—is evident in these strategies to determine the international model to come. Where the western powers focus on alliance politics and deterrence strategies and Beijing instead advocates for a different type of security cooperation — one of development, interdependence and respecting state autonomy. This understanding is central to assessing how China's rise will transform the guiding principles and practices of 21st-century global security. This paper tries to answer these research questions accordingly:

1. How has the Chinese military innovation, especially through the Military-Civil Fusion (MCF) strategy, shaped its national defense capability and global technological position?
2. How do China's international partnerships, (The SCO, BRI, and the others) play a role in achieving its broader security and geopolitical objectives?
3. How does defense innovation and international cooperation reflect China's bid for a new multipolar global order and compete with current Western-centric security architectures?

Through the framing of this analysis, it is possible to argue that China's simultaneous technological self-reliance and strategic engagement at the global level presents a unique paradigm in international relations—where innovation and cooperation are not merely implements of power but rather the essential conditions reshaping global security governance in the wake of the twenty-first century.

Main Part

Defense Innovations

China's rapid military innovation has been a major tenet of its national strategy and China's rapid progress in defense technology has been central to its national strategy and its ambition to

¹ The State Council Information Office of the People's Republic of China. China's National Defense in the New Era. Beijing: State Council, July 2019. <https://surl.li/megnde>, Accessed 10.11.2025

redefine global power dynamics in the twenty-first century. In the last 30 years, the national defense and technology have drastically improved from heavily foreign dependent on imports and reverse-engineering into one of the most advanced and self-reliant military innovation systems in the world. The transformation has been orchestrated by a long-term vision to attain “national rejuvenation”—a belief promoted by Chinese rulers that connects economic modernization, technological advancement, and military power as synergistic elements to the strength of the state.²

Central to this modernization is the “Military-Civil Fusion” (MCF) strategy, which aims to obliterate the traditional split between civilian and military sectors. The policy is intended to encourage private technology companies, universities, and state-owned enterprises to work side by side with the People’s Liberation Army (PLA) and defense research institutions. Innovations created for commercial operations, such as artificial intelligence (AI), robotic systems, autonomous devices, quantum computing, and satellite technology become systematically built into defense production and military operations. The MCF framework guarantees that civilian scientific breakthroughs serve the greater good of China’s defense capabilities and, thus, the rapid advance of next-generation technologies in the PLA.³

Modernization efforts by the PLA have focused on indigenous innovation, cutting reliance on foreign suppliers – particularly on core technologies (such as microelectronics, aerospace parts, cybersecurity systems). This pursuit of self-sufficiency has only grown since Western export restrictions and sanctions against Chinese defense and technology firms. In retaliation for this, China has invested heavily in the development of its own defense industrial structure and research environment to create a domestic supply chain that can endure sustained technological competition with global powers such as the U.S.⁴

One major area in which China has made considerable progress has been the development of hypersonic weapons and the anti-access/area denial (A2/AD) systems. Hypersonic glide vehicles with speeds over Mach 5 and unpredictable maneuvers are a new category of strategic weapon developed to bypass traditional missile defense systems. Combined with the development of long-range anti-ship ballistic missiles such as the DF-21D and DF-26, these developments have greatly altered the military balance in East Asia. In strengthening this capability, China seeks to discourage foreign military operations—namely by the U.S.—in the South China Sea and the Taiwan Strait, in addition to maintaining control of its maritime periphery.⁵

A key part of China’s defense innovation is cyber and information warfare. The PLA understands the need for domination of information in modern conflicts, as controlling data, communi-

2 Official white paper outlining China’s defense modernization goals and strategic principles. (Accessed 10/20/2025) 2. Ministry of National Defense of the PRC. China’s Military Strategy (2015). <http://eng.mod.gov.cn/Database/WhitePapers/>, Accessed 10.11.2025

3 Details the PLA’s modernization priorities and “active defense” doctrine. (Accessed 10/20/2025) 3. Xi Jinping. The Governance of China, Volume IV. Beijing: Foreign Languages Press, 2022. – Compilation of Xi’s speeches and policy visions, including his statements on the “Military-Civil Fusion” strategy. (Accessed 10/15/2025) 4. U.S. Department of Defense. Military and Security Developments Involving the People’s Republic of China 2024. Washington, D.C.: Office of the Secretary of Defense, 2024. <https://media.defense.gov/>, Accessed 10.11.2025

4 Comprehensive annual report assessing China’s defense innovations, PLA reforms, and strategic capabilities. (Accessed 10/10/2025) 5. Shanghai Cooperation Organization (SCO). About SCO. <https://eng.sectsco.org/>, Accessed 10.11.2025

5 Official information on the SCO’s structure, member states, and regional security initiatives. (Accessed 10/12/2025) 6. Belt and Road Forum for International Cooperation. The Belt and Road Initiative: Progress, Contributions, and Prospects. Beijing: National Development and Reform Commission, 2023. <https://www.beltandroadforum.org/>, Accessed 10.11.2025

cations, and perception can be as important as physical force.⁶ The establishment of the Strategic Support Force (SSF) in 2015 unified China's space, cyber, and electronic warfare capabilities within a cohesive command, emphasizing the need for integrated cross-domain operations. The SSF, along with its task force members, is also responsible not just for protecting China's information infrastructure, but also for carrying out offensive cyber operations and psychological warfare. This acknowledges Beijing's recognition that potential future conflicts will likely begin in the digital realm—in information systems, public opinion, and the global flow of data. Equally significant is China's swift advances in space technology, which are now a critical requirement for both civilian and national defense purposes. China's BeiDou Navigation Satellite System (BDS), which was finalized in 2020, offers global positioning and timing services independent of the U.S. GPS system. It improves the accuracy of PLA tasks, from missile guidance to naval navigation, while also solidifying China's position as a provider of space infrastructure to developing countries. Furthermore, the creation of the China National Space Administration (CNSA) and the achievements of Chang'e lunar missions and Tiangong space station illustrate the dual-use nature of Chinese space innovation—advancing both scientific prestige and military capability.⁷

China's investment in artificial intelligence and autonomous systems is another frontier for defense innovation. The government's "Next Generation Artificial Intelligence Development Plan," released in 2017, explicitly recognizes AI as a national security strategic technology. Research institutions for the PLA and state-owned defense conglomerates like the China Electronics Technology Group Corporation (CETC) are also working on AI-powered surveillance, target recognition, and decision-support systems. These technologies increase operational efficiency and allow the deployment of autonomous drones and robotic combat units, enabling real-time data analysis on battlefields. Through these developments, China seeks to create a type of "intelligentized warfare"—a doctrine that uses data, machine learning, and automation to outpace rivals in both speed and adaptability.⁸

More than a military strategy specifically related to individual technologies, China's defense innovation strategy mirrors a wider strategic vision. Progress in technologies is interpreted not as protection for the nation but as a means of transforming the international order. China—as one of the leaders of emerging technology—will dictate global standards, mold international institutions, and expand its soft power to the maximum. China's companies, for example, in 5G and satellite communication networks, and those in cybersecurity infrastructure, have evolved as geopolitical levers of influence, giving Beijing leverage in the world of diplomacy and security negotiations. Moreover, China's defense innovations are closely linked to the idea of "active defense," which involves deterring threats through technological superiority and rapid response capabilities rather

6 Overview of the BRI's development and its security and strategic dimensions. (Accessed 10/14/2025) 7. China Global Television Network (CGTN). Global Security Initiative Explained. April 2023. <https://news.cgtn.com/>, Accessed 10.11.2025

7 Analysis of how the BRI influences regional and global defense partnerships. (Accessed 10/19/2025) 10. Center for Strategic and International Studies (CSIS). China Power Project: Understanding Chinese Military-Civil Fusion. Washington, D.C., 2024. <https://chinapower.csis.org>, Accessed 10.11.2025/

8 Research on how China integrates civilian technology with military applications. (Accessed 10/18/2025) 11. Carnegie Endowment for International Peace. China-Russia Cooperation: The New Strategic Axis. 2024. <https://carnegieendowment.org/>, Accessed 10.11.2025

than through aggressive forward deployments.⁹ This doctrine combines defensive posture with offensive capability to enable China to exercise power in contested regions while ensuring that a narrative of strategic restraint is reinforced. It also allows China to project power through dual-use technologies—tools designed for civilian use (such as satellites or undersea cables) that can serve military functions when necessary. Overall, China’s defense innovation constitutes an all-round and systemic transformation. It combines economic progress with science and technology and military modernization in an integrated national project. From hypersonic missiles to cyber warfare, from AI-enabled operations to space systems, these developments are revolutionizing the regional and global security environment over time. They are more than technological development—not just a sign of technological advancement, they represent a clear commitment from China to guard its interests, shield its sovereignty, and reshape the rules of the international system. With technological change being the overarching principle of our increasingly competitive dynamic, China’s defense innovations will continue to play a central role in securing the global order and shaping the future of security and strategic stability.¹⁰

International Partnerships

Although emphasizing national sovereignty, China has also established strategic partnerships to bolster its defense, security, and global aspirations. China’s approach to international engagement in the 21st century is much more than just diplomacy or trade, and has become a complex strategy that spans economic influence, defense cooperation, and ideological alignment. Those partnerships represent means by which China advocates a different kind of global security: multipolar, non-Western, and rooted in the doctrines of sovereignty, reciprocity, and common prosperity. A leading mechanism through which China promotes its security cooperation is the Shanghai Cooperation Organization (SCO). Formed in 2001, the SCO had its roots in the early efforts toward trust and demilitarization in the border regions of its founding member countries (China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan). Over time it has developed into a major regional institution that deals with counterterrorism, separatism, extremism, and transnational crime. Under the SCO’s Regional Anti-Terrorist Structure (RATS), China undergoes joint military exercises, intelligence sharing and border cooperation. Together, they add to China’s stature in Central Asia and its larger effort to provide stability on its western frontier. The SCO also serves as an important diplomatic counterweight to Western-led alliances like NATO. By emphasizing non-interference, mutual support and a focus on all parties, China and its allies in SCO offer another international framework of security governance for the future—one that prioritizes regional solutions over foreign intervention. Its widening membership, with India, Pakistan, and Iran now in full force, only demonstrates how China has succeeded in marshaling a large and varied coalition together determined to reshape the nature of global peace. Another pillar of China’s international engagement is the Belt and Road Initiative (BRI), which started in 2013. In its

9 In-depth analysis of the expanding China-Russia defense and geopolitical partnership. (Accessed 10/21/2025) 12. United Nations Office for Disarmament Affairs (UNODA). Developments in Emerging Military Technologies: AI, Cyber, and Space. 2023. <https://disarmament.un.org/>, Accessed 10.11.2025

10 Discussion of China’s role in international norms related to defense innovation. (Accessed 10/19/2025)

framing as a chiefly economic and infrastructure project, the BRI has considerable strategic and security implications. China is extending in part through investments in ports, railways, digital infrastructure and energy corridors through Asia, Africa, the Middle East and Europe and extending in part through geopolitical accession. These infrastructure projects are also often couched in terms of security cooperation—joint maritime patrols, the protection of Chinese forces abroad and the formation of logistical hubs to support future defense operations. One striking instance of the dual-use of the BRI is the China–Pakistan Economic Corridor (CPEC). The corridor links western China with the Arabian Sea via Pakistan’s Gwadar Port. China and Pakistan still have deep military collaboration with Pakistan, like arms transfers, joint exercises and intelligence cooperation in addition to more economic investment. In the development of these kinds of projects China can both advance its energy security and expand its global penetration; in addition they enhance strategic leverage over regions that previously had Western-style domination. China’s defense diplomacy is reflected in the Middle East and Africa, where often BRI-related projects are followed by security accords. The establishment of China’s first overseas military base in Djibouti in 2017 marks this new phase of international cooperation. With official designation and operation since then as a “logistics facility,” it also supports anti-piracy operations, humanitarian missions and the protection of Chinese citizens overseas. In practice, however, it gives the PLA Navy power projection in the Indian Ocean and allows it to protect vital maritime trade routes. China has emerged as a key supplier of military equipment and training programs in Africa, offering an alternative to Western models, often with political caveats attached. These multilateral efforts are reinforced by bilateral relations. China’s strategic relationships with Russia, Pakistan and Iran demonstrate its potential to create alliances designed to achieve both concrete and ideological goals. Particularly important is the China–Russia partnership. Not a formal military alliance, it represents one of the strongest strategic alignments in modern world politics. The two countries take part in joint military exercises as laid out by the Vostok and Joint Sea exercises, coordinate positions in the United Nations Security Council and have advanced technologies for defense. Both governments have a vision for countering Western domination and advancing a “multipolar” world order. In recent years, such collaborations have grown stronger on missile defense, Arctic navigation and space exploration—all of which have significant defense concerns. China’s ties to Pakistan—often dubbed an “all-weather partnership”—are a part of its South Asian strategy, and they form a crucial part of it. The two countries are deeply involved in military cooperation, co-producing aircraft such as the JF-17 Thunder and working on nuclear technology. Pakistan also serves as an important partner to counter India’s regional influence and to maintain China’s strategic depth in the region. At the same time, China’s expanding relationships with Iran show that it is prepared to engage with nations that challenge Western-led sanctions and security regimes. The 25-year cooperation deal signed between Beijing and Tehran in 2021 also provisions for energy trade, infrastructure development and defense cooperation. This partnership not only provides China access to energy sources but also offers Iran political and economic alternatives to isolation—showing how China’s alliances can strategically dilute Western power in vital geographic areas. The relationship of both of these partnerships are not only personal; they also represent a widening ideological cohesion.

China's discussion of international security revolves around sovereignty, non-interference, and mutual development—attributes which strike very close to the heart in countries who sometimes feel underserved by Western interventions. Through forums like the Forum on China–Africa Cooperation (FOCAC), the China–Arab States Cooperation Forum (CASCF) and the Global Security Initiative (GSI) declared by Xi Jinping in 2022, China advocates a vision of global governance based on inclusion and dialogue, instead of confrontation. This way, China's international partnerships are practical and ideological at once. Pragmatically they protect Chinese trade routes, investments, and citizens abroad whilst also developing a greater global military footprint. Ideologically, they believe in Beijing's goal of changing the world as usual—to construct a multipolar world in which security will be based on cooperation instead of competing. Such collaboration, however, positions China as a leader among emerging economies, providing a paradigm on development and security that undercuts the hegemony of Western institutions such as NATO or the US-centred Indo-Pacific system. At bottom, China's international partnerships show how defense innovation and diplomacy combine to shape foreign policy and the direction of the future of security. Blending economic policies, national defence cooperation, and normative norms of leadership, China is forging a global network in which it has expanded international power far beyond the four corners of its own land. This network not only assists China in its defence modernization, but also redefines the rules of international security—making China one important architect for this emerging multipolar order.

Conclusion

The 21st century trajectory of China suggests that defense innovation meets international partnership as a force shaping the global security landscape. China's emphasis on technological modernization, rooted in self-reliance, strategic foresight and comprehensive national power, has seen the country evolve from a regional player to a global security stakeholder. Pursuant to initiatives like Military-Civil Fusion, the People's Liberation Army has transformed into an advanced, intelligentized force that can function across several domains: land, sea, air, cyber, and space. This evolution will not only accelerate China's defense capabilities but also cements its aspirations to establish the technological and strategic terms of international order. But invention cannot account for China's rise. Its growing web of international partnerships plays a similarly vital role in molding the future of security. By constructing ties with entities such as the Shanghai Cooperation Organization (SCO) and the Belt and Road Initiative (BRI) and by participating in bilateral co-operation with countries such as Russia, Pakistan and Iran, China projects influence that goes deeper than its muscles of arms. These alliances combine economic development with new world-wide investment along with infrastructure and defense diplomacy, building a framework in a networked global context. They enable China to showcase an alternative model of security — one that stresses sovereignty, stability and multipolarity instead of the usual alliance politics. Defence innovation and international partnership together make up the two complementary pillars of China's grand strategy. Innovation enables China to fight against established powers technologically, and partnerships extend its footprint globally while legitimizing its leadership in a rapidly changing world.

Both dimensions serve, for as yet, an abstract vision: a conception of a new international order where security is neither contingent on Western hegemony nor a monopoly; security through co-operation among varying power centers under the principles they share. In short, China's case embodies the main content of this conference. It offers a glimpse into the extent to which innovation and cooperation can serve as instruments for shaping a future of global security — one in which technology, strategic partnership, and diplomatic engagement have the potential both to control and shape the landscapes of peace and power in the contemporary world.

Bibliography

- The State Council Information Office of the People's Republic of China. China's National Defense in the New Era. Beijing: State Council, July 2019. <https://surl.li/megnede>, Accessed 10.11.2025
- Official white paper outlining China's defense modernization goals and strategic principles. (Accessed 10/20/2025) 2. Ministry of National Defense of the PRC. China's Military Strategy (2015). <http://eng.mod.gov.cn/Database/WhitePapers/>, Accessed 10.11.2025
- Details the PLA's modernization priorities and "active defense" doctrine. (Accessed 10/20/2025) 3. Xi Jinping. The Governance of China, Volume IV. Beijing: Foreign Languages Press, 2022. – Compilation of Xi's speeches and policy visions, including his statements on the "Military-Civil Fusion" strategy. (Accessed 10/15/2025) 4. U.S. Department of Defense. Military and Security Developments Involving the People's Republic of China 2024. Washington, D.C.: Office of the Secretary of Defense, 2024. <https://media.defense.gov/>, Accessed 10.11.2025
- Comprehensive annual report assessing China's defense innovations, PLA reforms, and strategic capabilities. (Accessed 10/10/2025) 5. Shanghai Cooperation Organization (SCO). About SCO. <https://eng.sectesco.org/>, Accessed 10.11.2025
- Official information on the SCO's structure, member states, and regional security initiatives. (Accessed 10/12/2025) 6. Belt and Road Forum for International Cooperation. The Belt and Road Initiative: Progress, Contributions, and Prospects. Beijing: National Development and Reform Commission, 2023. <https://www.beltandroadforum.org/>, Accessed 10.11.2025
- Overview of the BRI's development and its security and strategic dimensions. (Accessed 10/14/2025) 7. China Global Television Network (CGTN). Global Security Initiative Explained. April 2023. <https://news.cgtn.com/>, Accessed 10.11.2025
- Summary of Xi Jinping's Global Security Initiative and its relation to China's partnerships and security framework. (Accessed 10/18/2025) 8. International Institute for Strategic Studies (IISS). The Military Balance 2024. London: Routledge/IISS, 2024. – Annual assessment of global military capabilities, including China's defense spending, innovations, and international partnerships. (Accessed 10/20/2025) 9. European Union Institute for Security Studies (EUISS). China's Belt and Road Initiative and Global Security: Strategic Implications. Brussels: EUISS, 2023. <https://www.iss.europa.eu/>, Accessed 10.11.2025
- Analysis of how the BRI influences regional and global defense partnerships. (Accessed 10/19/2025) 10. Center for Strategic and International Studies (CSIS). China Power Project: Understanding Chinese Military-Civil Fusion. Washington, D.C., 2024. <https://chinapower.csis.org>, Accessed 10.11.2025/
- Research on how China integrates civilian technology with military applications. (Accessed 10/18/2025) 11. Carnegie Endowment for International Peace. China-Russia Cooperation: The New Strategic Axis. 2024. <https://carnegie-icendowment.org/>, Accessed 10.11.2025
- In-depth analysis of the expanding China-Russia defense and geopolitical partnership. (Accessed 10/21/2025) 12. United Nations Office for Disarmament Affairs (UNODA). Developments in Emerging Military Technologies: AI, Cyber, and Space. 2023. <https://disarmament.un.org/>, Accessed 10.11.2025
- Discussion of China's role in international norms related to defense innovation. (Accessed 10/19/2025)

