A Conversation with Dominique de Villepin
Can the Two-State Solution Be Saved? 161

Andrew B. Friedman
States, Countries, and Peoples:
A Comparative Look at Bicameralism in African Federal States ... 165

Andrés Serbin
Contending Geopolitical Narratives and Global Tectonic Shifts ... 193

An Interview with Admiral Takei and
Rear Admiral Girrier
Perspectives on U.S.-Japan Naval Leadership 209

Dr. Khatuna Burkadze
A Shift in NATO's Article 5 in the Cyber Era? 215

An Interview with General Patrick de Rousiers
From the Front Line to the Front Door 227

An Interview with Richard Plepler
The Crooked Timber of Humanity:
How HBO Is Redefining Storytelling 233

The Fletcher Forum of World Affairs aims to provide a broad, interdisciplinary platform for analysis of legal, political, economic, environmental, and diplomatic issues in international affairs. The editorial board of *The Fletcher Forum of World Affairs* believes that the publication's audience values and expects the inclusion of conflicting viewpoints; the board does not expect readers to concur with all of the views expressed by *Forum* authors. This inherent diversity supports the very definition of a "forum," i.e., a public meeting place for open discussion.

The views and opinions expressed in the journal are solely those of individual authors and should not be regarded as reflecting any official opinion or position of *The Fletcher Forum of World Affairs*, The Fletcher School, or its faculty.

A Shift in NATO's Article 5 in the Cyber Era?

Dr. Khatuna Burkadze

ABSTRACT:

The North Atlantic Treaty (the founding treaty of NATO), which defines the principle of collective defense of the Alliance, was officially signed by the Allies on 4 April 1949. According to Article 5 of the North Atlantic Treaty, "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." In that time, the potential power of cyberspace could not even begin to be conceptualized. Information technologies may have a disruptive effect as computers can be instrumental in carrying out new forms of war. In view of the foregoing, the following questionable issues should be outlined: Do we need amendments in Article 5 of the North Atlantic Treaty to define whether a cyber-attack rises to the level of an armed attack? If not, how should the principle of collective defense of NATO be interpreted to give the Allies legal guidance on the concept of cyberattacks?

INTRODUCTION

Technological advances are key to societal development. However, they can be used as tools for carrying out destructive actions. In light of increasing cyber threats, it is important to understand how the current

Khatuna Burkadze *has been a Fulbright scholar at the MIT Center of International Studies as well as a visiting researcher at Columbia University, Bard College and the Fletcher School of Law and Diplomacy. Professor Burkadze has the ten years' experience of implementing projects with the focus on NATO-related issues and has experience lecturing on the subjects of Public International Law and Cyber Law. She is a graduate of the Fletcher School of Law & Diplomacy, Tufts University. Dr. Burkadze has successfully completed the Leaders Program in Advanced Security Studies at the George C. Marshall European Center for Security Studies and National Security Program organized by the RAND Corporation and Rondeli Foundation. She is an alumnus of the U.S. Department of State's Program on American Foreign Policy as well as the author of dozens of articles and book chapters.*

international legal framework can be applied in case of cyberattacks. As Professor Joel Trachtman argues in *The Future of International Law: Global Government*, "the development of cyberspace must be met with the development of cybersecurity. Because of the international nature of cyberspace, and assuming that states are unwilling to deny their people the benefits of cyberspace and unwilling to or incapable of walling off their cyberspace frontiers, cybersecurity is an international issue."[1]

International security affairs specialists began to consider the possibility of cyber warfare as a new form of armed attack in the mid-1990s, both as an element of classic armed conflict and as a stand-alone proposition. However, the subject faded from the security agenda following the 9/11 attacks; [2] but that changed in 2007 when NATO Member State Estonia became the victim of massive cyberattacks. The next year, cyber operations figured prominently in the international armed conflict between the Russian Federation and Georgia.[3] In the course of the Russian-Georgian war, the Russian Federation engaged in targeted and massive cyberattacks against Georgia alongside land, aerial, and naval assaults. According to internet technical experts, it was the first time a cyberattack had coincided with a shooting war.[4] These attacks showed that the protection of cyberspace is as now as important for national security as land, maritime, and air defenses.

The rate at which attack technologies are proliferating is accelerating, not slowing down.[5] It should be apparent that rapid technological change can cause considerable disarray in military policy.[6] Military implications of new warfare technologies can be very difficult to assess correctly.[7]

The fact that international law is often dismissed as window-dressing on *Realpolitik* is misleading. Such an approach understates the importance of international agreements in maintaining peace and security. For liberal democracies that respect the rule of law, international law undoubtedly shapes and bounds governments' activities. At a time when the actions of unscrupulous states and violent extremist groups continue to threaten peace and security internationally, it is even more important that such actions are countered with a strong commitment to existing international law and the values that it represents.[8]

Therefore, because of the lack of norms on cyber behavior, new interpretation of the principle of collective defense in the case of cyberattacks remains a key issue in the digital era. In the case of Estonia, NATO did not define cyberattack as a clear military action. Yet, the next year in 2008, the Alliance adopted its first cyber defense policy. Since then, activities in the realm of cyber defense have significantly increased. However, there are

still many uncertainties with regards to the applicability of international law to cyberspace. Due to the gap between law and policy, it is necessary to explore both the current strategic documents of the Alliance on cyber issues and existing international legal framework, for clarifying NATO's possible reaction against a new form of armed attack by using Article 5 of the North Atlantic Treaty in the future.

NATO'S CHALLENGES IN CYBERSPACE

The Alliance formulated its mission in cyberspace — to protect its own networks, enhance the capabilities of the member states, and to cooperate with partner nations, the European Union (EU), and industry — after suffering its first major cyberattacks in 1999, during Operation Allied Force.[9] These incidents included denial-of-service attacks and defacements of the webpage for the Supreme Headquarters Allied Powers Europe, while the U.S. military saw a tripling of defacement attacks. These protest attacks were conducted by nationalist Russian, Serb, and Chinese hackers after the accidental bombing of the Chinese Embassy in Belgrade.[10]

In April and May of 2007, the relocation of a Soviet-era war memorial in Estonia unleashed a series of large and sustained distributed denial-of-service attacks flooding networks or websites with attack traffic, rendering them inaccessible.[11] The main targets were the websites of the Estonian presidency and parliament, almost all of the country's government ministries, political parties, three of Estonia's six biggest news organizations, two of the biggest banks, and communications firms.[12] "The cyber-attacks are from Russia. There is no question. It's political," said Merit Kopli, editor of Postimees, one of the two main newspapers in Estonia. Postimees' website was targeted and inaccessible to international visitors for a week.[13] Estonian officials echoed Kopli's opinion, declaring that their country was the first to fall victim to cyber warfare. They accused Russia of orchestrating the attacks, officially or unofficially. Prime Minister Andrus Ansip said that security officials traced the initial attacks to Russian servers, including domains registered to the government and to the administration of President Vladimir V. Putin.[14]

Prime Minister Ansip and other Estonian public officials alluded to Article 5 of the NATO Treaty, recognized by Article 51 of the Charter of the United Nations.[15] Estonian Defense Minister Jaak Aaviksoo, meanwhile, discussed the situation with NATO officials and later stated the following during an interview with British newspaper *The Guardian*: "At present, NATO does not define cyberattacks as a clear military action. This

means that the provisions of Article 5 of the North Atlantic Treaty, or, in other words collective self-defense, will not automatically be extended to the attacked country. Not a single NATO defense minister would define a cyberattack as a clear military action at present. However, this matter needs to be resolved in the future."[16]

There was reasonable doubt that the above-mentioned attacks were encouraged by the Kremlin. However, they served to show that the protection of cyberspace is as important for the national security of NATO member states as land, maritime, and air defenses. The Former Secretary of Defense of the United States, Ash Carter, said, "The 20th century NATO playbook was successful in working toward a Europe whole, free and at peace, but the same playbook would not be well-matched to the needs of the 21st century. Together with our NATO allies, we must write a new playbook, which will prepare NATO to counter new challenges like cyber warfare."[17] This playbook will need to provide a new smart strategic vision for the Alliance.

NATO'S CYBER DEFENSE AND INTERNATIONAL LAW

The U.N. Charter and the North Atlantic Treaty (the founding treaty of NATO) were adopted in 1945 and 1949 when the creation of cyberspace was a matter of the future rather than a consideration of the times. Currently, it is clear that information and communication technologies have transformed the nature of war and changed historical understanding of armed attacks.

Traditional applications of the use of force prohibition fail to adequately safeguard shared community values threatened by Computer Network Attacks (CNA).[18] The use of force is strictly limited in international law according to the U.N. Charter. Consequently, the central questions are the following: Could a cyberattack be equated to an armed attack according to international law? If a cyberattack equates to an armed attack, how should the principle of collective defense of NATO be interpreted to give member states legal guidance on the concept of a cyberattack? Do we need amendments in Article 5 of the North Atlantic Treaty to clearly define what constitutes a cyberattack? Answers to these questions can provide insights for defining rules of cyber operations in case of cyberattacks.

The definitions of the use of force and armed attack are not provided in the U.N. Charter. In this regard, in its argument on a case concerning Nicaragua, the International Court of Justice rejected a narrow interpretation of "use of force" that limits the term to the employment of either

kinetic force or non-kinetic operations generating comparable effects. The Court held that a state's arming and training of guerrilla forces engaged in hostilities against another state qualified as a use of force, a position that has since become widely accepted.[19] The logic of the holding leads to the conclusion that non-destructive cyber operations may amount to a use of force. For example, providing malware to a rebel group and training its members to employ that malware in a destructive manner would seemingly qualify.[20]

However, every unfriendly act does not cross the use of force threshold. The International Court of Justice held that financing guerrillas, albeit an unlawful "intervention," did not fall into the same category. Therefore, cyber operations intended to economically coerce another state to engage in, or desist from, a particular course of action would not amount to a use of force; nor would financing a rebel group's cyber operations. Beyond these directly parallel examples, uncertainty remains as to where the threshold lies.[21]

The NATO Cooperative Cyber Defense Center of Excellence launched a major research project in late 2009 to examine the public international law governing cyber warfare[22] and cyber operations, resulting in the Tallinn Manual 1.0 and Tallinn Manual 2.0. These two documents provide international experts' analysis on how existing international law applies to cyber warfare and cyber operations. Through Tallinn Manual 1.0, the International Group of Experts developed a nonexclusive list of factors that would likely influence the characterization of cyber operations by a state as a use of force: severity, immediacy, directness, invasiveness, measurability, military character, state involvement, and presumptive legality. Additional factors found meaningful by the Experts included, inter alia, the prevailing political environment, the nexus of an operation to prospective military force, the attacker's identity, the attacker's track record with respect to cyber operations, and the nature of the target. These and other factors operate in concert as states make case-by-case determinations. Of them, severity alone can qualify a cyber operation as a use of force.[23] In this regard, the Group unanimously agreed that any cyber operation causing greater than *de minimis* damage or injury suffices. For instance, they concurred that the damage to Iranian nuclear facilities in 2010 resulting from the Stuxnet virus crossed the threshold.[24]

As for the concept of cyberattacks and cyberwarfare, there are no widely accepted definitions. The U.S. Department of Defense defines "computer network attacks" as "actions taken by using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[25] Yale

Law Professor Oona Hathaway and her colleagues have devised a broader definition of a "cyberattack." In a 2012 article, they wrote: "A cyberattack consists of any action taken to undermine the functions of a computer network for a political or national security purpose." The article goes on to say that "any action" includes "hacking, bombing, cutting, inflecting, and so forth," as long as the action has the objective of undermining or disrupting a computer network. The word "purpose" seems to apply to the intent of the attacking party.[26]

According to the Tallinn Manual's Rule 30. "A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[27] In this regard, Professor Antonia Chayes, in an article titled, "Rethinking Warfare: The Ambiguity of Cyber Attacks," highlights that a cyber operation can constitute an attack even before the damaging consequences of such an operation become evident, citing the example of implanting malware that will be activated at a later time, but for which the intended consequences meet the requisite threshold of harm as an event that could be defined as an attack "irrespective of whether the malware is activated" this is a direct parallel to implanting. In a similar vein, a cyberattack that has been launched but defeated still amounts to an attack. The Manual does warn that great care should be exercised when identifying the perpetrator of the attack.[28]

Professor Chayes emphasizes that these definitional iterations help to refine the issues, although they cannot be expected to answer all questions. They do serve to narrow differences in approach somewhat and to begin to assure that officials are addressing common issues. However, the lack of internationally accepted distinctions among "cybercrime," "cyberattack," and "cyber war" make concerted international action more difficult to achieve. The definitions alone do not delineate civilian and military roles, nor do they designate a legal framework under which to operate, since the issue of whether an attack warrants a military response-even in the military domain-remains ambiguous. Economic attacks may be handled through a variety of international means, judicial and diplomatic. But crippling economic attacks without serious casualties might not be sufficient to warrant acts in self-defense under Article 51 of the U.N. Charter nor, as in the case of Estonia, a collective response under Article 5 of the North Atlantic Treaty.[29]

As for NATO's official position on interconnection between the existing international legal regulations and cyberspace, the Wales Summit Declaration (issued by the Allies in Wales on 4–5 September 2014) emphasizes: "Our policy recognizes that international law, including international humanitarian law and the U.N. Charter, applies in cyberspace. Cyberattacks

can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defense is part of NATO's core task of collective defense. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis."[30] This means that, on the one hand, member states of the Alliance agreed that international law applies to cyberspace but, on the other hand, in the case of a cyberattack, a decision about invoking Article 5 will be made by the members of NATO based on the particular criteria. Therefore, the principle of collective defense is not an automatic mechanism.

The exact criteria by which cyber incidents may trigger an Article 5 invocation of collective defense have not been determined. However, the North Atlantic Council is very likely to consider the following elements in its deliberations.

- **Scope:** Is the incident widespread across a geographic area or industrial sectors? The wider the attack is, the more likely NATO action will be;
- **Duration:** Is the incident a single event or does it last over time as part of a longer campaign? NATO is more likely to act for extended incidents;
- **Intensity/Scale:** Has the incident caused death or substantial property destruction? If not, NATO is unlikely to declare collective defense;
- **External Actor:** Is the incident directed from a foreign or domestic adversary? NATO is unlikely to act against a purely domestic foe.[31]

NATO'S CYBER VIEW

Nowadays, one of the key challenges of the North Atlantic Alliance is cyber threats because cyberattacks are becoming more common, sophisticated, and damaging. State and non-state actors can use cyberattacks in the context of military operations. In recent events, cyberattacks have even been part of hybrid warfare.[32]

NATO's Secretary General Jens Stoltenberg says: "We are implementing our cyber defense pledge which is ensuring that we are strengthening the cyber defenses of both NATO networks but also helping NATO allies to strengthen their cyber defenses. We exercise more, we share best practices and technology and we also work more and more closely with all allies considering how we can integrate their capabilities, strengthening

NATO's capability to defend our networks. We have also decided that a cyberattack can trigger Article 5 and we are in the process of establishing cyber as a military domain meaning that we will have land, air, sea and cyber as military domains."[33] Therefore, NATO's Secretary General highlights that cyber defense is one of the important components of collective defense of the Alliance.

As for the key decisions of NATO on cyber issues, the 2002 Prague Summit first placed cyber defense on the Alliance's political agenda. According to the Declaration of Prague Summit, the North Atlantic Alliance decided to strengthen capabilities to defend against cyberattacks.[34] Since 2002, cyber defense topics have been included in the deliberations of the North Atlantic Council and Defense Ministers.[35]

At the Warsaw Summit in July 2016, the Allies: "recognize cyberspace as a domain of operations, in which, NATO must defend itself as effectively as it does in the air, on land, and at sea."[36] A key concern in implementing cyberspace as an operational domain is to establish an accurate understanding of the actual "territory" that comprises cyberspace upon which a military operation depends. In NATO operations, the area in which a designated Joint Force Commander plans and executes a specific mission at the operational level is referred to as the Joint Operations Area (JOA).[37] It is difficult to draw clear boundaries that distinguish the area within which a NATO operational commander would have authority to take military decisions. As Scott Applegate put it, "One difficulty in defining borders in cyberspace is that the physical geography of cyberspace does not even remotely match the logical geography."[38] A second challenge in implementing cyberspace in the domain of military operations is the nature of cyberspace threats — in particular, the asymmetries in the relationships between attackers and defenders.[39]

However, the best way to improve NATO mission assurance in cyberspace is to recognize the opportunities presented by the cyber incidents that cyber incident response centers and the networked organizations they support that deal with them on a daily basis. And this means to recognize the legitimate role for the NATO Command Structure to act as an enabler for collective defense in cyberspace through partnership and information-sharing.[40]

At the same time, it is important to analyze how the current Strategic Concept of the Alliance provides adequate guidance for the North Atlantic Council's (NAC) latest decision about recognizing cyberspace as a domain of operations. The current Strategic Concept for the Defense and Security of the Members of NATO, which was adopted by the Allies in Lisbon in

2010, defines the following cyber objectives of the North Atlantic Alliance: developing further ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defense capabilities; bringing all NATO bodies under centralized cyber protection; and better integrating NATO cyber awareness, warning and response with member nations.[41]

Despite these clarifications, the current Strategic Concept needs to be modified for the following reasons: (1) NATO's historical understanding on the core elements of collective defense has changed. Historically, NATO focused on land, air, and naval defense capabilities. Because of the cyber threats, the Alliance should defend itself as effectively as it does in the air, on land, and at sea. (2) Through recognizing cyberspace as an operational domain, the NAC officially supported NATO's broader defense. According to this decision, cyber defense will continue to be integrated into the Alliance's operations and missions. The Alliance should enhance not only land, air, and naval defense capabilities, but also cyber defense capabilities. Therefore, to implement the NAC's latest decision on cyber space, it is necessary to provide new guidance. This guidance would clarify a strategic vision for managing international cyber conflicts in the future.

CONCLUSION

The decision to recognize cyberspace as a domain of operations made by the Allies at the Warsaw Summit represents an evolutionary rather than revolutionary change in NATO's approach to tackling current and emerging cyber threats. This decision is a crucial step in enabling NATO to treat cyber defense not only as a static protective discipline, but as a means for mission assurance.[42] Thus, the Allies need to update the current Strategic Concept of 2010 to implement the Warsaw Summit Declaration of 2016. The new guidance should allow the North Atlantic Alliance to be a more effective player in cyberspace and provide cyber security of NATO's 29-member states at the regional and global levels in the future.

As for Article 5 of the North Atlantic Treaty, despite the changing security environment, the original treaty has never had to be modified.[43] Practically, it is impossible to make an amendment in Article 5 to clearly define what constitutes a cyberattack. Nevertheless, the Tallinn Manuals emphasize that the language of the North Atlantic Treaty allows for the possibility of using collective defense in cases of cyberattacks. These manuals analyze existing binding regulations applicable to cyberspace. We can say that the Tallinn Manuals are non-binding documents with

the interpretations of binding international norms. Professor Schmitt mentioned that these Manuals are intended to be secondary sources of law: they explain the law, but they do not create it.[44]

In an article titled "The Dark Future of International Cybersecurity Regulation," Professor Michael Glennon highlights that states are not likely to consent to new international rules that restrict the use of cyber weapons. For better or worse, these and other conditions necessary to promote the emergence and development of legal constraints are not present in sufficient degree to support further international rules governing cyber conflict any more than those conditions have been present in the past to support the emergence of rules governing clandestine or covert intelligence operations of which cyber activity normally is a part.[45] Despite the dark future of international cybersecurity regulation, law is a form of cooperation. The cost of non-cooperation is high.[46]

States need to interact to foster a better understanding of how international law regulates their cyber conduct.[47] Within the global context, NATO, as the strongest political-military alliance in the history, can play an important role in the process of intensifying dialogues among different players of cyberspace for several reasons. Based on the assessment of the Alliance's cyber activities, it is clear NATO has a good understanding on international legal aspects of cyber space; the Tallinn Manuals are the result of the Allies' efforts. NATO has also achieved consensus among the Allies on key aspects of cyber space. Lastly, the Alliance has the best practice on how to develop cyber security capacity through multinational exercises, training, projects and other activities. ***f***

ENDNOTES

1 Joel P. Trachtman, *The Future of International Law: Global Government*, Cambridge University Press, 2013: 95.
2 Michael N. Schmitt, "The Law of Cyber Warfare: Quo Vadis?," 25 *Stanford Law & Policy Review*, Spring, 2014: 269.
3 Ibid.
4 John Markoff, "Before the Gunfire, Cyber Attacks," *The New York Times*, August 12, 2008, <http://www.nytimes.com/2008/08/13/technology/13cyber.html> (Accessed February 7, 2018).
5 Benjamin Wittes and Gabriella Blum, *The Future of Violence: Robots and Germs, Hackers and Drones — Confronting a New Age of Threat,* (2015), <https://www.lawfareblog.com/future-violence-robots-and-germs-hackers-and-drones-confronting-new-age-threat> (Accessed February 15, 2017).
6 Steven E. Miller, "Technology and War," *Bulletin of the Atomic Scientists*, 48, December 1985, <http://www.belfercenter.org/sites/default/files/files/publication/TechnologyandWar.pdf> (Accessed February 7, 2017).
7 Ibid., 47.

8 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* (Michael N. Schmitt ed.), (Cambridge University Press, 2017): 23, 24.
9 Jason Healey and Klara Tothova Jordan, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow," *Atlantic Council,* 2014, 1.
10 Ibid., 2.
11 Ibid.
12 Jeff Harley, "Information Operations," U.S. Army Strategic Command G3 Plans, Information Operations Branch, Newsletter, 2007, 16.
13 Ibid.
14 Steven Lee Myers, "Estonia Accuses Russia of Computer Attacks," *The New York Times,* May 18, 2007, <http://www.nytimes.com/2007/05/18/world/europe/18cnd-russia.html?h> (Accessed November 15, 2017).
15 "Internet Law — Should We Go to War Over a Massive Cyber-Attack?" Maricelle Ruiz, ed., Internet Law Forum, <http://www.ibls.com/internet_law_news_portal_view.aspx?id=1762&s=latestnews> (Accessed November 15, 2017).
16 Ibid.
17 Secretary of Defense Ash Carter Submitted Statement to the Senate Armed Services Committee on the FY 2017 Budget Request for the Department of Defense, March 17, 2016, 10, 11.
18 Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law,* 886 (1998–1999) 37.
19 See supra note 2. at 279–280.
20 Ibid., 280.
21 Ibid.
22 Ibid., 270.
23 Ibid., 280–281.
24 Ibid., 281.
25 Major Arie J. Schaap, "Cyber Warfare Operations: Development and Use Under International Law," 64 *Air Force Law Review,* 2009, 126.
26 Antonia Chayes, "Rethinking Warfare: The Ambiguity of Cyber Attacks," *Harvard National Security Journal,* 2015, 481.
27 Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare, (Michael N. Schmitt, ed.), Cambridge University Press, 2013, 106.
28 See supra note 26. at 482.
29 Ibid.
30 The Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, September 4–5, 2014 <https://www.nato.int/cps/ic/natohq/official_texts_112964.htm> (Accessed November 14, 2017).
31 See supra note 9. at 7.
32 NATO and Cyber Defense, <https://www.nato.int/cps/en/natohq/topics_78170.htm> (Accessed November 10, 2017).
33 Press conference by NATO's Secretary General Jens Stoltenberg ahead of the meeting of NATO Defense Ministers, June 28, 2017, <https://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en> (Accessed November 10, 2017).
34 The Prague Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, November 21, 2002, <https://www.nato.int/cps/ic/natohq/official_texts_19552.htm?> (Accessed November 10, 2017).

35 Brad Bigelow, "Mission Assurance: Shifting the Focus of Cyber Defense," the 9th International Conference on Cyber Conflict, Belgium, 2017.
36 The Warsaw Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, July 8–9, 2016, <https://www.nato.int/cps/en/natohq/official_texts_133169.htm#cybe> (Accessed November 16, 2017).
37 See supra note 35, 3–4.
38 Ibid., 4.
39 Ibid., 5.
40 Ibid., 10–11.
41 Strategic Concept for the Defense and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon, November 19–20, 2010, <https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf> (Accessed November 10, 2017).
42 Interview with Ambassador Sorin Ducaru (NATO's Assistant Secretary General for Emerging Security Challenges), "NATO's Efforts to Improve Its Cyber Defenses Against Emerging Threats," *Columbia Journal of International Affairs*, Winter 2016, <https://jia.sipa.columbia.edu/cyber-defense-possible> (Accessed November 21, 2017).
43 Founding Treaty — the North Atlantic Treaty, April 4, 1949, <https://www.nato.int/cps/en/natohq/topics_67656.htm> (Accessed November 21, 2017).
44 Michel Moutot, "Tallinn Manual 2.0 — the Rulebook for Cyberwar," June 3, 2017, <https://phys.org/news/2017-06-tallinn-manual-20the-rulebook-cyberwar.html> (Accessed November 23, 2017).
45 Michael J. Glennon, "The Dark Future of International Cybersecurity Regulation," *Journal of National Security Law and Policy*, 2013, 563.
46 Ibid.
47 See supra note 8. at 24.