თბილისის ღია სასწავლო უნივერსიტეტი

გალუმოვი კახა

კიბეროპერაციები

„წარმოდგენილია მაგისტრის აკადემიური ხარისხის მოსაპოვებლად“

თბილისი. 0156. საქართველო

ავტორი: კახა გალუმოვი / . . . . . /

ნაშრომის საიდენთიფიკაციო ნომერი: . . . . . .

თბილისის ღია სასწავლო უნივერსიტეტი

ჰუმანიტარულ და სოციალურ მეცნიერებათა სკოლა

„ეროვნული და საერთაშორისო უსაფრთხოების სამაგისტრო პროგრამა“

ჩვენ, ქვემეორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით გალუმოვი კახას მიერ შესრულებულ ნაშრომს დასახელებით: „კიბეროპერაციები“ და ვაძლევთ რეკომენდაციას განხილულ იქნას თბილისის ღია სასწავლო უნივერსიტეტის ჰუმანიტარულ და სოციალურ მეცნიერებათა სკოლის საგამოცდო კომისიის მიერ მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

თარიღი: ... სექტემბერი, 2021 წელი

ხელმძღვანელი: / . . . . . /

ხარისხის მართვისა და სტრატეგიული განვითარების
სამსახურის უფროსი: /...../

რეცენზენტი /...../

სარჩევი

1. რეზიუმე 04
2. შესავალი 08
3. დესტრუქციული სახელმწიფო კიბერაქტორების მოკლე დახასიათება 10
4. საფრთხეები საქართველოს კიბერსივრცისთვის 16
5. არჩევნების უსაფრთხოება 21
6. კიბერტერორიზმი 35
7. კიბერთავდასხმა, როგორც ფსიქოლოგიური ეფექტის მქონდე ოპერაცია.... 39
8. კიბერსივრცის გამოყენება თანამედროვე კონფლიქტებში 45
9. ნატო - კიბერუსაფრთხოება 52
10. დასკვნა 66
11. გამოყენებული ლიტერატურა 68

რეზიუმე

სამაგისტრო ნაშრომი - „კიბეროპერაციები“ - შედგება შესავლის, შვიდი თავის, დასკვნის და დანართის სიისგან.

პირველ თავში - „დესტრუქციული სახელმწიფო კიბერაქტორების მოკლე დახასიათება“ - განხილულია რამდენიმე ქვეყნის მაგალითი, თუ რა მიზნებისთვის იყენებენ კიბერ სივრცეს ისეთი ქვეყნები, როგორიცაა რუსეთი, ირანი, ჩრდილოეთ კორეა. თემაში გაეცნობით ასევე იმ კიბერ ოპერაციებს, რომელსაც აქტიურად იყენებს რუსეთი სხვადასხვა ქვეყნებთან მიმართებაში, მათ შორის საქართველოში. გაეცნობით ინფორმაციას თავდაცვის მმართვის ეროვნული ცენტრი (Национальный центр управления обороной РФ, NDMC) - ის შესახებ, რომელიც წარმოადგენს მთლიანი რუსეთის თავდაცვის სამინისტროს, შეიარაღებული ძალების და კონტროლის უმაღლესს ორგანოს.

მეორე თავში - „საფრთხეები საქართველოს კიბერსივრცისთვის“ - განხილულია საქართველოსთვის მიმდინარე საფრთხეები და გამოწვევები. ასევე, კიბერ სივრცის გამოყენებით, რუსეთის მხრიდან წამოსული შეტევები, სამიზნე აუდიტორია და მათზე გათვლილი კიბერ ღონისძიებები. დღეს მსოფლიოში აქტიურად განიხილავენ ინფორმაციის კონფიდენციალურობისა და მისი ხელმისაწვდომობის საფრთხეს. ამ მიმართულებით კი განხილულია საინფორმაციო - ტექნიკური და საინფორმაციო - ფსიქოლოგიური ზემოქმედებები.

მესამე თავში - „არჩევნების უსაფრთხოება“ - თავში აღწერილია არჩევნებში რუსეთის მხრიდან ჩარევის გზები. მათი კიბერ ოპერაციების სამიზნე ქვეყნების გამოცდილება. ასევე გავიხილავთ საარჩევნო პროცესებში ხშირად გამოყენებულ საინფორმაციო ოპერაციების ტექნიკებს, საფრთხეებს, მის აქტორებს და რისკების მმართვის პრაქტიკებს და რჩევებს.

მეოთხე თავში - „კიბერტერორიზმი“ - აღნიშნული თავიდან გაიგებთ რა არის კიბერტერორიზმი და რას მოიცავს იგი. განხილულია კიბერსივრცის ფლობა ტერორისტული დაჯგუფებებისთის, მათი სამოქმედო გეგმები და მოქმედებები სხვადასხვა, მათთვის სასურველი მიზნების მისაღწევად. განხილულია ისეთი ტერორისტული ორგანზაციები, როგორი არის მაგალითად.: ISIS, Hizballa, Hamas, Al Qaida, თალიბანი.

მეხუთე თავში - „კიბერფსიქოლოგია“ - განხილულია კიბერ სივრცის გამოყენება ფსიქოლოგიური ეფექტის მქონე ოპერაციებით. რუსეთის კიბერფსიქოლოგია პოლონეთის მიმართ. რუსული მედია და სხვა საინფორმაციო საშუალებების მოქმედების პრინციპები და მათ მიერ განხორციელებული შეტევები. ასევე რუსული კიბერფსიქოლოგიის მცდელობა და განხორციელებული შეტევები საქართველოში. აღნიშნულ თემაში წარმოდგენილია რუსეთის მიერ გამოყენებული გზები, ინფორმაციის მანიპულაციისთვის. გაეცნობით ინტერნეტ ტროლების და ინტერნეტ ბოტების საქმიანობას ფსიქოლოგიური განხრით.

მეექვსე თავში - „კიბერსივრცის გამოყენება თანამედროვე კონფლიქტებში“ - განხილულია, თუ რას წარმოადგენს კონცეფცია კიბერსივრცის გამოყენება სხვადასხვა კონფლიქტებში, განხილულია კონფლიქტების დროს გამოყენებული კიბერ შეტევები, მათი მოქმედების არეალი და პრევენციული ზომები. კიბერ ომი. კიბერ კონფლიქტების მიზანი, კიბერ ომი უკრაინაში, დესტრუქციული ინფორმაციის და კიბერ გავლენის განეიტრალების ღონისძიებები. გაეცნობით კიბერ სივრცეში სახელმწიფო უზენაესობის სამი ძირითადი სფეროს, ასევე სამხედრო კონფლიქტების გამოცდილებას.

მეშვიდე თავში - „ნატო - კიბერუსაფრთხოება“ - განხილულია სხვადასხვა მუხლები კიბერშეტევების შემთხვევაში, კიბერ ოპერაციების გამოწვევა და საფრთხეები „ნატო“-სთვის. ჩრდილოატლანტიკური ხელშეკრულების მე -5 მუხლი, მისი გამოყენება კიბერ შეტევის შემთხვევაში, თუ როგორ გაამართლებს სამხედრო პასუხი მე-5 მუხლის კიბერშეტევაზე. ნატო-ს კიბერ სივრცესთან დაკავშირებული საკითხების განვითარების ეტაპები. კიბერ სივრცე და სამხედრო კონფლიქტები: დოქტრინალური მიდგომები ტერმინოლოგიაზე. ნატო-ს ამჟამინდელი სტრატეგიის ძირითადი გამოწვევები.

თემის ძირითად მიზანს კი წარმოადგენს - მოსალოდნელი საფრთხეების და რისკების შესახებ წარმოდგენის შექმნა და რეკომენდაციების შემუშავება მათ სამართავად.

Resume

The master's thesis - "Cyber Operations" - consists of an introduction, seven chapters, a conclusion and an appendix.

The first chapter - "A Brief Description of Destructive State Cyberactors" - discusses the examples of several countries and for what purposes the cyberspace is used by countries such as Russia, Iran, North Korea. You will also learn about the cyber operations that Russia is actively using in relation to various countries, including Georgia. You will find information about the National Center for Defense Management (NDMC), which is the highest body of the Russian Ministry of Defense, Armed Forces and Control.

The second chapter - "Threats to Georgian Cyberspace" - discusses the current threats and challenges for Georgia. Also, using cyberspace, attacks from the Russian side, target audience and cyber measures targeted at them. Nowadays, the world is actively discussing the threat to privacy of information and its access. In this regard, information-technical and information-psychological impacts are discussed.

The third chapter - "Election Security" - describes the ways in which Russia interferes in the elections. Experience of countries targeting their cyber operations. We will also look at the information operations techniques, threats, actors, and risk management practices and advice that are frequently used in electoral processes.

In the fourth chapter - "Cyberterrorism" - you will learn what cyberterrorism is and what it entails. The possession of cyberspace for terrorist groups, their action plans and actions to achieve various, desired goals are discussed. Terrorist organizations such as ISIS, Hizballa, Hamas, Al Qaeda, Taliban are also discussed.

The fifth chapter - "Cyberpsychology" - discusses the use of cyberspace in operations with psychological effects. Additionally, Russian cyberpsychology towards Poland, Principles of operation of the Russian media and other media and the attacks carried out by them, attempts at Russian cyberpsychology and attacks in Georgia are also discussed. This topic presents ways used by Russia to manipulate information. You will learn about the activities of Internet trolls and Internet bots from a psychological point of view.

The sixth chapter - "The use of cyberspace in modern conflicts" - discusses what is the concept of the use of cyberspace in various conflicts, discusses the cyber attacks used during conflicts, their scope and preventive measures. Cyber War. The purpose of cyber conflicts, cyber war in Ukraine, measures to destroy destructive information and cyber influence. You will learn about the three main areas of state sovereignty in cyberspace, as well as the experience of military conflicts.

Chapter 7 - "NATO - Cyber Security" - discusses various articles in case of cyber attacks, the challenge of cyber operations and the threats to NATO. Article 5 of the North Atlantic Treaty, its use in the event of a cyber attack, how to justify a military response to an Article 5 cyber attack. Stages in the development of NATO cyberspace issues. Cyberspace and Military Conflicts: Doctrinal Approaches to Terminology. The main challenges of the current NATO strategy.

The main goal of the thesis is to create an idea of the expected threats and risks and to develop recommendations for their management.

შესავალი

კიბერ საფრთხეებთან ბრძოლა მსოფლიოს უმნიშვნელოვანესი გამოწვევაა. 21-ე საუკუნეში, კიბერ სივრცის საინფორმაციო ომი, ფაქტობრივად 3-ე მსოფლიო ომთან არის გაიგივებული. აქედან გამომდინარე, მნიშვნელოვანია ვიცოდეთ კიბერ რისკების, გამოწვევების და საფრთხეების შესახებ. უახლეს ისტორიაში კიბერ დანაშაულის მეტად გავრცელებულ ფორმებს წარმოადგენს ისეთო ფორმები, როგორიც არის, მაგალითად: ონლაინ თაღლითობა, როგორც კომპიუტერულ, ისე სხვა ტექნოლოგიურ სისტემებთან უნებართვო წვდომა, ამ წვდომის შედეგად მიღებული ინფორმაციის უნებართვო დამუშავება და გამოყენება და სხვა მრავალი.

კიბერ დანაშაულებებით განპირობებული მზარდი სტატისიკა მსოფლიოში, განპირობებულია არასაკმარისი ინფორმაციით კიბერის შესახებ, საზოგადოების დაბალი ცნობიერებით. კიბერ სივრცეში დამნაშავეები ძირითადად ისეთ სხვადასხვა პროგრამებს და საშუალებებს იყენებენ, როგორიც არის ფიშინგი, სპამი, ელექტრონული ფოსტა, ბოტნეტი, MALWARE და სხვა.

აღნიშნული თემა საყურადღებოა საქართველოშიც. იგი აქტუალური და საინტერესო გახდა 2008 წლის აგვისტოს შეტევების შემდეგ, რომელიც აგრესორი ქვეყნის, რუსეთის მხრიდან იყო გამოწვეული და დღემდე გრძელდება სხვადასხვა ფორმით. თემაში განხილულია ისეთი ძირითადი კიბერ თემები, როგორიც არის კიბერ ფსიქოლოგია, კიბერ ტერორიზმი. თემა ასევე მოიცავს მცირე ინფორმაციას სხვადასხვა დესტრუქციული სახელმწიფო კიბერ აქტორების შესახებ, არჩევნების კიბერ უსაფრთხოებას, კიბერ სივრცის გამოყენებას თანამედროვე კონფლიქტურ სიტუაციებში, საქართველოში მიმდინარე საფრთხეებს, მათი მოგვარების გზებს და სხვა.

კვლევის მიმართულება.: რუსეთის მიერ კონფლიქტებსა თუ მშვიდობიან პერიოდში კიბეროპერაციების გამოყენება.

კიბერ უსაფრთხოების შესახებ კვლევის მიზანია მკითხველმა მიიღოს ინფორმაცია კიბერ საფრთხეებსა და გამოწვევებზე, თუ რა საფრთხეს შეიცავს დღევანდელი ციფრული ომი ჩვენთვის და ჩვენი მოსახლეობისათის, ქვეყნისთვის და ზოგადად მსოფლიოსთვის. ასევე ნახოს პრევენციული ზომების შესახებ ინფორმაცია და გამოიყენოს ყოველდღიურობაში.

კვლევების შედეგად კი შეგვიძლია ვთქვათ შემდეგი.: რუსეთის კიბეროპერაციების ეფექტი ტექნიკურიდან გადადის ფსიქოლოგიური ეფექტისაკენ. საინფორმაციო ოპერაციებში ხშირად გამოიყენება კიბეროპერაციები. ძირითადი სამიზნე კრიტიკული ინფრასტრუქტურის გარდა, არის ასევე დემოკრატიული პროცესები, არჩევნები და დემოკრატიული წყობილება. რუსეთი იყენებს როგორც სახელმწიფო აქტორებს, ასევე კიბერკრიმინალს, რადგან მათ შორის ყველა ზღვარი წაშლილია.

დესტრუქციული სახელმწიფო კიბერაქტორების მოკლე დახასიათება

კიბერდომეინი სახმელეთო თუ საჰაერო, კოსმოსური თუ საზღვაო დაპირისპირების მეხუთე სივრცეთ, დაახლოვებით 21 საუკუნის პირველ ათწლეულში დამკვიდრდა. მისი ელემენტების გამოყენება კი პოლიტიკური თუ სხვა სამხედრო მიზნების მისაღწევადაა განკუთვნილი. ამავდროულად უნდა გვახსოვდეს, რომ ნებისმიერი კიბეროპერაცია ჰიბრიდული თუ სხვა სრულმასშტაბიანი ომის ნაწილია.

კიბერშეტევებიდან გამომდინარე, რუსეთის ფედერაცია ერთერთ ლიდერ პოზიციაზე იმყოფება მსოფლიოში. სტრატეგიული დაგეგმვის კორექტირებულ დოკუმენტებში[1], უსაფრთხოების დოქტრინას საერთაშორისო თვალსაზრისით დიდი ადგილი უჭირავს, და ეს გამოწვეულია კრემლის აღქმით ახალი ან/და მომავალი სამხედრო საფრთხეებისა და

[1] Доктрина информационной безопасности Российской Федерации. Указ президента РФ от 05.12.2016

მუქარის წარმოქმნით, ასევე მიმდინარე პროცესებში ამავე სამხედრო საფრთხეების საინფორმაციო სივრცეში წანაცვლებით[2].

კიბერ სივრცე რუსული მხრიდან განიხილება როგორც უბრალო საინფორმაციო სივრცე, რომელიც აერთიანებს როგორც კომპიუტერულ სისტემებს, ასევე ადამიანის მიერ შემნილ ან და გადამუშავებულ ინფორმაციებს. აგრესორი ქვეყნის აღქმით, CNO ორ მიმართულებად იყოფა, ერთერთი მიმართულება ეს არის საინფორმაციო-ტექნიკური და მეორე საინფორმაციო-ფსიქოლოგიური დომეინი. მათივე სახელმძღვანელოებში, განმარტებების სახით ვკითხულობთ, რომ მოქმედების სამიზნის მიხედვით ორი ტიპის საინფორმაციო ზემოქმედება ხორციელდება, რომელიც ძირითადად ომის და სამხედრო კონფლიქტების დროს წარმოიქმნება. ტექნიკურ სისტემებზე ზემოქმედება რომლებიც აგროვებენ, ინახავენ ან/და ამუშავებენ ინფორმაციას და მოწინააღმდეგის შეიარაღებულ ძალებსა თუ მოსახლეობაზე ფსიქოლოგიური ზემოქმედება.

აღსანიშნავია, რომ ზოგიერთი დესტრუქციული აქტივობა კიბერსივრცეში მუდმივად მიმდინარეობს და ის არ არის დამოკიდებული მოწინააღმდეგის იმდროინდელი დაპირისპირებებისა თუ პარტნიორობის ხარისხზე[3].

ამერიკელი მკვლევარები, რომელიც კიბერსივრცის წამყვანი სპეციალისტები არიან, აღნიშნავენ, რომ საქართველოსთან ომი, არაბული გაზაფხულის და 2011 წელს, რუსული ოპოზიციის მიერ, სოც.ქსელებით მიერ ორგანიზებული მასშტაბური გამოსვლების შედეგების ანალიზზე დაყრდნობით, რუსეთმა ორგანიზაციულ-დოქტრინალური ცვლილებები განახორციელა. 2014 წელს, რუსეთის თავდაცვის მაშინდელმა მინისტრმა, შოიგუმ, კიბერსარდლობის შექმნა დააანონსა, მოგვიანებით, 2017 წელს გაცხადდა საინფორმაციო

[2] Великая Победа в Великой Войне" Патрушев Н. https://tass.ru/politika/1950207

[3] NATO Defense College “NDC Fellowship Monograph Series”. Handbook of Russian Information Warfare. Fellowship Monograph 9 by Keir Giles. ISBN: 978-88-96898-16-1

ოპერაციების ჯარების შესახებ ინფორმაცია, რომლებიც პასუხისმგებელნი იქნებიან როგორც ტექნიკურ, ისე პროპაგანდისტულ და სხვა საინფორმაციო კონფრონტაციის ელემენტებზე. აქვე უნდა აღინიშნოს, რომ 2014 წელის ბოლოს, ჩამოყალიბდა თავდაცვის მმართვის ეროვნული ცენტრი (Национальный центр управления обороной РФ, NDMC), და ეს უკანასკნელი წარმოადგენს მთლიანი რუსეთის თავდაცვის სამინისტროს, შეიარაღებული ძალების და კონტროლის უმაღლესს ორგანოს. მაშინდელი თავდაცვის მინისტრის განცხადებით, მათი ძირითადი მიზანი და დანიშნულება, კიბერშეტევებისგან დაცვა გახლდათ[4]. ყოველივე ზემოთ აღნიშნული, რეალური საფრთხის შემცველია საქართველოსთვის. ოკუპანტი ქვეყნის, მაღალი რანგის სამხედრო პირებზე დაყრდნობით, მათმა საინფორმაციო ოპერაციების ჯარებმა 2016 წლის შემოდგომაზე, პირველად მიიღეს მონაწილეობა სამეთაურო საშტაბო სწავლებაში. „Кавказ-2016“- ეს კი აშკარად გულისხმობს, რომ რუსეთს აქვს განზრახვა, აკონტროლოს საინფორმაციო სივრცე და ეს უკანასკნელი სამხედრო გზით.

ამერიკის შეერთებული შტატების ეროვნული დაზვერვის ინფორმაციით, რუსეთი აქტიურადაა ჩართული კრიტიკული ინფრასტრუქტურის ICS-ზე (Industrial Control Systems - ICS) დინსტაციური წვდომის საშუალებების განვითარებაში. რუსმა აქტორებმა განახორციელეს რამოდენიმე ICS მწარმოებლის პროგრამ(ებ)ის კომპრომეტაცია, ლეგალური პროგრამული უზრუნველყოფის განახლებებში მავნე პროგრამული კოდის ჩანერგვა და ამ გზით მომხმარებლის სისტემასთან პირდაპირი წვდომის დამყარება[5].

საქართველოს წინააღმდეგ, 2008 წელს განხორციელებულ კიბერშეტევაში დიდი როლი ითამაშა ძლიერი ტექნიკური საშუალებების მქონე კრიმინალურმა ორგანიზაცია - RBN

[4] Khatuna Mshvidobadze. Russian Military Preps Cyber Warriors. 25.04.2017. ხელმისაწვდომია http://www.cyberlightglobal.com/insight-blog/

[5] Hearing: World Wide Cyber Threats (Open).Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015.

(Russian Business Network), რომელიც ინტენსიურ თავდასხმებს ახორციელებდა ქართულ ქსელებზე. გართულებული ატრიბუციის გამო, რუსული სადაზვერვო სამსახურები კონსპირაციის მაღალი დონის მქონე ჰაქტივისტურ[6] ჯგუფებს, ან უკვე მოქმედ ჯგუფებს არსებულ საფარქვეშ. ამგვარი კიბერშეტევები წარმოადგენდა ერთერთ უმნიშვნელოვანეს ელემენტს, რუსეთის მთავრობის მიერ მხარდაჭერილ კიბერ შეტევებში საქართველოს მიმართ 2008 წელს, მანამდე კი ესტონეთში 2007 წელს. აღნიშნული შეტევები რეგულარულად ხორციელდებოდა რუსეთ-უკრაინის კონფლიქტში მეიდანზე განხორციელებული პროცესების და ასევე ყირიმის ანექსიის პერიოდში. მრავალი ტექნიკური დასტური არსებობს იმისა, რომ რუსეთის სახელმწიფოს მიერ წარმოებულ თუ მხარდაჭერილ კიბერშეტევებს, False Flag ოპერაციებს წარმოადგენდა კიბერხალიფატის საფარქვეშ.

კიბერ კრიმინალების და ჰაქტივისტური დაჯგუფებების გარდა, რუსეთი ასევე აქტიურად იყენებს ე.წ. False Person - ის შესაძლებლობებს. მათ მიერ მართული დაჯგუფება - „კიბერბერკუტი“ (Киберберкут) - ახორციელებს როგორც სამხედრო ოპერაციების მხარდაჭერას, ისე სტრატეგიული ამოცანების მხარდაჭერას. აღნიშნული დაჯგუფება ახორციელებს როგორც ფსიქოლოგიურ, ისე ტექნიკურ პროპაგანდისტულ კიბერშეტევებს. იგი 2014 წლიდან აქტიურად ჩაერთო როგორც კიბერშპიონაჟის აქტებში, ასევე DDOS შეტევებში ნატოს, უკრაინისა და გერმანიის სამთავრობო საიტების წინააღმდეგ[7]. აქ ფოკუსირება ხდება ჰაკერული გზით მოპოვებული ინფორმაციის გამოქვეყნებაზე. რომელიც ძირითადად ემსახურება სახელმწიფოების დისკრედიტაციას, ნდობის შემცირებას, შიშს და სხვა.

[6] Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. Report, 2017

[7] Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. www.dia.mil/military-power-publications

უკრაინის ენერგო სისტემაზე განხორციელებული კიბერშეტევა[8], რომელიც 2014-2015 წლებში განხორციელდა, გააჩინა განცდა, რომ რუსეთის ფედერაცია მხოლოდ DDOS და DEFACEMENT შეტევებით ან/და კიბერშპიონაჟის ოპერაციებით და აქვე, არ არსებობს იმის გარანტია, რომ იგი არ განახორციელებს კრიტიკულ ინფრასქტრუქტურაზე მიზანმიმართულ აქციებს, რასაც შეიძლება გარკვეული საფრთხე, მათ შორის მსხვერპლიც მოჰყვეს.

რაც შეეხება სხვადასხვა ქვეყნის მოქმედებებს კიბერის მხრივ. მაგალითად ჩინეთი. ჩინეთი კიბეროპერაციებს ძირითადად კომერციული მიზნებისთის იყენებს. აქედან გამომდინარე ნაკლებად სავარაუდოა რაიმე საფრთხის შემცველი იყოს საქართველოსთის. მაგრამ არ უნდა დავივიწყოთ ჩვენთან არსებული სამთავრობო თუ არასამთავრობო სტრუქტურის ქსელები და მათზე არსებული ინფორმაციები. მიუხედავად კიბერ სფეროში ურთიერთთანამშრომლობისა, ჩინეთის მთავარ სამიზნედ კიბერშპიონაჟის მხრივ, კვლავაც ამერიკა რჩება. ეს ის შემთხვევაა, როცა დაინტერესების სფერო საკმაოდ დიდია. აუცილებელია საქართველომ დიდი ყურადღება დაუთმოს მნიშვნელოვან კიბერ უსაფრთხოების პროექტებს, რომელიც ხორციელდება ამერიკის შეერთებული შტატების პატრონაჟით ქართულ სახელმწიფო თუ კერძო სტრუქტურებში.

ირანი - ქვეყანა, რომელმაც შეძლო და გახდა ერთერთი უძლიერესი კიბერაქტორი. მიუხედავად იმისა, რომ მისი პოტენციალი ვერ ედრება რუსეთის ან/და ჩინეთის პოტენციალს, იგი წარმოადგენს ჩრდილოეთ კორეის დონის აქტორს და განვითარებული ქვეყნების კრიტიკული ინფრასტრუქტურისთვის მნიშვნელოვან საფრთხეს წარმოადგენს[9]. ირანმა კიბერშესაძლებლობების განვითარება რუსეთისა და ჩინეთისგან მიღებული ტექნოლოგიური

[8] Dr Andrew Foxall. Putin's Cyberwar: Russia's Statecraft in the Fifth Domain. Russia Studies Centre Policy Paper No. 9 (2016). The Henry Jackson Society May 2016

[9] Worldwide Threat Assessment of the US Intelligence Community. Daniel R. Coats, Director of National Intelligence. 13 February, 2018.

დახმარების ხარჯზე მოახერხა. ასევე, ამ კიბერპოტენციალს ხელი შეუწყო ისრაელსა და საუდის არაბეთთან მიმდინარე დაპირისპირებებმა. დღეს, ირანის სამხედრო ძალებისათვის, კიბერ ოპერაციები და კიბერ შეტევები მნიშვნელოვან როლს ასრულებს. ისინი ძირითადად სარგებლობენ ძლიერი, მოდიფიცირებული მალვეარით, რომელიც რუსეთის დონეს ვერ უახლოვდება, თუმცა რეალური საფრთხის შემცველია ნებისმიერი სამიზნე ქვეყნის ინფრასტრუქტურისათვის[10].

მეტი კონკრეტიკისთის, შეგვიძლია აღვნიშნოთ, რომ ირანის დესტრუქციული კიბერშეტევები რელურ საფრთხეს წარმოადგენს მცირე ბანკებისთვის, ენერგეტიკული კომანიების ან ნავთობსადენის კონტროლის სისტემებისადმი, მაგრამ, გაცილებით დიდი და ფართომასშტაბიანი კიბერშესაძლებლობებისთის, რომელიც უფრო მაღალ ტექნოლოგიურ შეტევებს გულისხმობს, ირანი მზად არ არის[11.] მათთვის კიბერშეტევების რამდენიმე მიმართულება გახლავთ დამახასიათებელი, მაგალითად ისეთი, როგორიც არის მონაცემთა წაშლა, DDOS შეტევები, მაკომპრომეტირებელი მასალების გამოქვეყნებით საინფორმაციო ოპერაციები, კიბერშპიონაჟი, ტერორისტული აქტებისთის ხალხზე საჭირო ინფორმაციების მოპოვება და სხვა.

ოფიციალურმა თეირანმა, საუდის არაბეთის Aramco – ს და ყატარის RasGas - ზე, 2012 წელს კიბერშეტევა განახორციელა სადაც გამოყენებული იყო მაღალტექნოლოგიური მალვეარი, რომელმაც მწყობრიდან ათასობით კომპიუტერის გამოყვანა შეძლო. 2012-2013 წლებში, ირანელმა ჰაკერებმა ამერიკულ ბაკებსა და საფონდო ბირჟების წინააღმდეგ, DDOS შეტევები განახორციელეს. 2014 წელს, მათ მოახერხეს და ამერიკული კაზინო Las Vegas

[10] https://www.csis.org/analysis/iran-and-cyber-power?fbclid=IwAR3iyUKkYWcKV7HEGF96CMC-FyHDyEMgMNK0qXtNvJCL45B8f3BfQmVKYe4

[11] https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Iran_Military_Power_LR.pdf

Sands-იდან მონაცემები წაშალეს. ამავე წელს, ღაზას სექტორში მიმდინარე ესკალაციისას, ისრაელის თავდაცვის ძალების ინფრასტრუქტურა ირანული DDOS შეტევის მსხვერპლი გახდა. 2016-2017 წლებში კი საუდის არაბეთის წინაათმდეგ განხორციელებულმა შეტევებმა, ათეულობით სხვადასხვა ობიექტებიდან ინფორმაციების წაშლა გამოიწვია. სამიზნე ობიექტები იყვნენ სახელმწიფო უწყებების, სამოქალაქო ავიაციისა და ცენტრალური ბანკის ქსელები[12].

ჩრდილოეთ კორეა - კიდევ ერთი აქტორი, რომელიც პოლიტიკური მიზნებისათვის იყენებს კიბერ სივრცეს და მისს შესაძლებლობებს. მის სამიზნე ობიექტებში ძირითადად თავისუფალი მედია და ამერიკის შეერთებული შტატები მოისაზრება. ჩრდილოეთ კორეა პასუხისმგებელია 2014 წლის ბოლოს, Sony Pictures Entertainment-ის წინააღმდეგ განხორციელებულ შეტევაზე[13], რომლის დროსაც, ქსელში შეღწეული მავნე კოდის საშუალებით განადგურდა სენსიტიური ინფორმაცია. საინტერესოა ის ფაქტიც, რომ აღნიშნული თავდასხმა ზუსტად ემთხვევა იმ სავარაუდო თარიღს, როდესაც ჩრდილოეთ კორეის სახელმწიფო მეთაურის შესახებ, კრიტიკული ფილმი უნდა გამოსულიყო. ეს ფაქტი ამ ფილმის ჩვენების ხელმშემშლელ ფაქტორად ჩაითვალა.

საფრთხეები საქართველოს კიბერსივრცისთვის

ოპერაციები, რომელიც მიმდინარეობს კიბერ სივრცეში, მთლიანობის, ხელმისაწვდომობისა და ელ. სერვისების კონფიდენციალურობის როგორც ხელყოფის, ისე დარღვევის (Confidentiality, Integrity, Availability)[14] განზრახ მცდელობას წარმოადგენს.

[12] Statement for the record. worldwide threat assessment of the US intelligence community february 9, 2016

[13] Statement for the record. World Wide Cyber Threats (Open). House Permanent Select Committee on Intelligence. Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015.

[14] https://www.cmu.edu/iso/aware/presentation/security101-robotics.pdf

ამგვარი ქმედებები კი შესაძლოა როგორც სერვისის დაზიანებას ისახავდეს მიზნად ან/და მის შეფერხებას (Computer Network Attack)[15], ისე კომპიუტერული ქსელის გამოყენებას, თავდასხმების მიზნით (Computer Network Exploitation)[16]. აგრეთვე, ინფორმაციის მოპოვებასა და მონაცემთა ბაზებზე არასანქცირებულ წვდომას.

ბოლო წლების განმალობაში, კიბერ ღონისძიებები, წარმატებით გამოიყენება როგორც ღია, ისე ფარული არხების მეშვეობით, სამიზნე აუდიტორიისთვის ცნობიერების შესაცვლელად, მათთვის სასურველი მიმართულებით. უნდა აღინშნოს, რომ მნიშვნელოვანია ვიცოდეთ, კიბერ ოპერაციები არ გახლავთ მხოლოდ ინფორმაციულ-ტექნიკურ ეფექტებზე ორიენტირებული ქმედებები, ის, როგორც საინფორმაციო ზემოქმედებებისათის, ასევე საინფორმაციო - ფსიქოლოგიური ზემოქმედებების დამახასიათებელი ნაწილია.

რაც შეეხება საინფორმაციო - ტექნიკურს - ეს ყოველივე კი გულისხმობს ისეთ სისტემებზე ზემოქმედებას, რომლებიც ახდენენ ინფორმაციის მოძიებას, გადამუშავებას და შემდეგ გადაცემას. საინფორმაციო - ფსიქოლოგიური კი გულისხმობს ზემოქმედებას, შეიარაღებულ ძალებსა და მოსახლეობაზე.

აღსანიშნავია, რომ ზოგიერთი დესტრუქციული აქტივობები, კიბერ სივრცეში გამუდმებით მიმდინარეობს, რომელიც არ არის მოწინააღმდეგის იმ პერიოდის პარტნიორობისა თუ დაპირისპირებების ხარისხზე დამოკიდებული[17].

იმ დანაყოფების რიცხვი, რომელიც ჩართული არის სახელმწიფოთა კიბერ უსაფრთხოების სფეროში, იზრდება ყოველდღიურად, ხოლო მათი ბიუჯეტი უტოლდება მილიარდობით დოლარს. ამ მიმართულებით ქვეყნების მზარდ ინტერესებს ადასტურებს ისიც, რომ სხვადასხვა ეკონომიკური სირთულეებისა და კრიზისებისა, ჯერ ამ მიმართულებით

[15] https://ccdcoe.org/cyber-definitions.html
[16] https://ccdcoe.org/cyber-definitions.html
[17] NATO Defense College "NDC Fellowship Monograph Series". Handbook of Russian Information Warfare. Fellowship Monograph 9 by Keir Giles. ISBN: 978-88-96898-16-1

დაფინანსება არცერთ ქვეყანას არ შეუმცირებია. აღსანიშნავია, რომ ეს ყოველივე მხოლოდ თავდაცვას არ ემსახურება. 2014 წლის ნატო - უელსის სამიტის წინ არსებული მონაცემებით, საშუალოდ 30 ქვეყანას, უკვე გააჩნდა შემდევობის პოტენციალი.

დღეს მსოფლიოში აქტიურად განიხილავენ ინფორმაციის კონფიცენციალურობისა და მისი ხელმისაწვდომობის საფრთხეს. ბოლო პერიოდში შენიშნება შემდეგი ტენდეცია, რომ ამგვარი კიბერ თავდასხმები, იმის ნაცვლად, რომ ორიენტირებული იყოს ინფორმაციის განადგურებაზე ან წვდომის შეზღუდვაზე, იგი მიმართულია მის სრულ შეცვლაზე, მისი მთლიანობის, სანდოობისა თუ სიზუსტის კომპრომეტირების მიზნით. რა თქმა უნდა, აღნიშნული ფაქტები უდიდესი საფრთხის შემცველნი არიან, როგორც კერძო, ისე სახელმწიფო სექტორეისათვის, რომლის ხელშიც გადის კრიტიკული მნიშვნელობის მქონე სერვისების უდიდესი ნაწილი.

ზოგადად, სახელმწიფოსათვის ის საფრთხეც მნიშვნელოვანია, რომელიც მაგალითად სამხედრო მოსამსახურეების მიერ სოც. მედიაში იქმნება, ან ელ ტრანზაქციების ფორმებში, ან თუნდაც საძიებო მექანიზმებში სხვადასხვა პერსონალური ინფორმაციის გაჟონვით წარმოიქმნება. მაგალითად დღეს, თავდაცვისა და უსაფრთხოების სექტორში მიმდინარეობს ინფორმაციის ციფრულ ფორმატში გარდაქმნის პროცესი. რომლის შედეგადაც, ელ. ჩანაწერები უფრო მეტად გახდება ხელმისაწვდომი ნებისმიერი მსურველისათვის. ეს კი გულისხმობს შემდეგს, რომ ნებისმიერი სამხედრო მოხელე, ან მათი ოჯაის წევრები, თანამშრომლები, ანდაც სამეგობრო, სრულიად შესაძლებელია გახდეს უცხო ქვეყნის როგორც ტერორისტული. ისე სხვადასხვა სპეც სამსახურების თავდასხმის ობიექტები. დიაც, ამგვარი პროექტები, უფრო მეტად მოწყვლადი ხდება სხვადასხვა კიბერ თავდასმებისათვის.

ხაზი უნდა გაესვას იმას, რომ კერძო სექტორთან თანამშრომლობის გარეშე კიბერ თავდაცვის სისტემების შემქნა - ფუნქციონირება არის შეუძლებელი. კერძოდ, სამთავრობო თუ სამხედრო კომუნიკაციის ქსელების დაცვა, არ ნიშნავს მის ეფექტურ დაცვას, რადგან

თანამედროვე სახელმწიფოში, სწორედ რომ კერძო სექტორშია გაერთიანებული კრიტიკული სერვისების უმეტესობა. ასეთებია კვების, სადაზღვეო თუ საბანკო მომსახურებები. ასე რომ მათზე თავდასხმები, ისეთი როგორიც არის კომერციული ინტერესები[18], ნეგატიურად აისახება ქვეყნის თავდაცვის უნარიანობაზე.

ჩვენთან არსებული კიბერ საფრთხეების სიდიდე და მოცულობა არის მზარდი სხვადასხვა თვალსაზრისით, როგორც სირთულის, ისე მრავალფეროვნების მხრივ. ეროვნული მნიშვნელობის კრიტიკული ინფრასტრუქტურის გარდა, თავდასხმების სამიზნეს ასევე წარმოადგენს საქართველოში მდებარე სხვადასხვა ქვეყნის, საერთაშორისო ორგანიზაციების ან/და უცხო კომერციული სტრუქტურების საკუთრებაში მყოფი ინფრასტრუქტურა.

საქართელოსთვის, ყველაზე დიდი კიბერ საფრთხე ოკუპანტი ქვეყნისგან მომდინარეობს. კრემლი - საინფორმაციო ტექნიკური თუ ფსიქოლოგიური ეფექტებით. ჰიბრდული ომის ერთერთი ძირითადი სამიზნე. ეს ომი კი სხვადასხვა კიბერ ოპერაციებსა თუ შეტებევს აერთიანებს. აღნიშნულმა შეტევებმა, შესაძლოა ჩვენს ქვეყანაში უდიდესი ზარალიც გამოიწვიოს, მათ შორის შეიძლება იყოს მსხვერპლიც. ამიტომ, სუსტად დაცული ინფრასტრუქტურის პირობებში, უბრალო, დაბალტექნოლოგიური შეტევაც კი შესაძლოა წარმოუდგენლად დიდი მასშტაბების ზარალზე გადიოდეს.

სხვადასხვა კიბერ მოქმედებებით შექმნილი თუ გავრცელებული კონტენტები ძირითადად პროპაგანდისტულია, რომელიც ძირითადად საინფორმაციო - ფსიქოლოგიურ შეტევებს ახდენს. რუსეთის სასარგებლოდ ჩვენი ცნობიერების შეცვლის მცდელობა, ნატო-სა და ზოგადად პროდასავლური განწყობების უარყოფიტად შეცვლა. ეს ყველაფერი კი შესაძლოა გახდეს კონვენციური მოქმედებების წინაპირობაც კი.

[18] ხშირია შემთხვევები, როდესაც თავდასხმითი კიბეროპერაციები კერძო სექტორის წინააღმდეგ ზოგიერთი სახელმწიფოს მხრიდან საკუთარი ეკონომიკური თუ საგარეო პოლიტიკური მიზნების განსახორციელებლადაა გამოყენებული. მაგალითად, უკანასკნელი წლების განმავლობაში, ირანისა და ჩრდილოეთ კორეის მიერ აშშ-ის კომერციულ აქტორებზე განხორციელებული შეტევები.

ისეთი ქვეყნებისგან, როგორიც არის ჩინეთი და ირანი, რეალურად კიბერ საფრთხე მინიმალურია, ორმხრივი, მეგობრული ურთიერთობების გამო. თუმცა, ჩინური არასახემწიფო აქტორების შეტევებისგან წამოსული საფრთხე დღის წესრიგშია. რომელიც გულისმობს ეკონომიკური მონაცემებისა თუ სხვადასხვა სენსიტიური ინფორმაციის დაუფლებას. რაც შეეხება ირანს, მათ ექსტემისტულად განწყობილ კიბერ თავდასხმელების ინტერესებს სრულიად შესაძლებელია ჩვენთან განთავსებული, სტრატეგიული პარტნიორების მონაცემები წარმოადგენდეს, რომლებიც მათთვის იდეოლოგიურ მოწინააღმდეგებად ითვლება.

ისეთი ტერორისტული ორგანიზაციები, როგორებიც გახლავთ თალიბანი, ჰამასი, Hizballah, al Qa'ida, ISIS, ცდილობენ ტერორისტული აქტების განსახორციელებლად მოიპოვონ სხვადასხვა სენსიტიური ინფორმაციები. ანტი ტერორისტული ქვეყნების მოქალაქეებზე, განსაკუთრებით კი სამხედრო ან მსგავს პერსონალზე, რომლის მიზანია შიშით და ტერაქტით გამოწვეული მღელვარებით მიიღოს გადაწყვეტილება და დატოვოს მსგავსი კოალიციის რიგები ან/და შეწყვიტონ ტერორისტული ორგანიზაციის წინააღმდეგ სხვადასხვა სამხედრო ღონისძიებები.

უნდა აღინიშნოს, რომ ისინი ამ ეტაპზე დიდ ტექნიკურ საშუალებებს არ ფლოვებ და მათი კიბერ შეტევები მხოლოდ დროებითი პარალიზებით ან ლოკალური, უმნიშვნელო დაზიანებებით შემოიფარგლება. ნაკლებად სავარაუდოა ისინი მასშტაბური კიბერ შეტევების მიზეზები გახდნენ.

ზოგადად, მოგებაზე ორიენტირებული კიბერ დამნაშავეების საყრდენი გახლავთ ელექტრონული ბაზრები, რომელიც გამოიყენება ისეთი არალეგალური შესყიდვებისათვის, როგორიც არის ფინანსური მონაცემები, პერსონალური ინფორმაცია, რომელიც არის მოპარული და ა.შ. ისინი წარმატებით აღწევენ სხვადასხვა ბიზნესისა და ფინანსური ინსტიტუტების ქსელებში, რათა მოიპოვონ და ჰქონდეთ წვდომა ფინანსურ ოპერაციებზე,

პერსონალურ ინფორმაციებზე, სამედიცინო ჩანაწერებზე და სხვა. ეს ყველაფერი ერთად კი წარმოადგენს იმფორმაციას შემდეგი კრიმინალური ოპერაციების სადაგეგმად და განსახორციელებლად. საინტერესოა, რომ ბოლო პერიოდში, ამგვარმა ჰაკერულმა თავდასხმება გადაინაცვლა სადაზღვეო და ჯანდაცვის სფეროში. ისინი შავ ბაზარზე გასაყიდად ეძებენ ისეთ უმნიშვნელოვანეს ინფორმაციას, რომელიც არის სენსიტიური, ამავდროულად შეიცავს სახემწიფო მნიშვნელობის ინფორმაციებსაც კი. მათგან წამოსული საფრთხეები რთულად პროგნოზირებადია. განსაკუთრებით თუ ეს მართულია, ან წამოსულია რუსეთის მიერ. რადგან ეს არის ქვეყანა, სადაც ზღვარი, რომელიც გავლებულია სახელმწიფოსა და კრიმინალურ აქტორებს შორის, დიდი ხანია წაშლილია.

არჩევნების კიბერუსაფრთხოება

არჩევნები არის დემოკრატიული წყობის ძირითადი ატრიბუტი, სწორედ ამიტომ ის არის რუსული ჰიბრიდული ომის მთავარი სამიზნე ყველგან და ყოველთვის, არ აქვს მნიშვნელობა ეს ხდება ამერიკის შეერთებულ შტატებსა თუ დანარჩენი კონტინენტის რომელიმე ქვეყანაში, რეფერენდუმი თუ სხვა მსგავსი სახის ღონისძიება, ხშირად გამხდარა რუსული კიბერ ოპერაციების სამიზნე. აღსანიშნავია, რომ არჩევნების შედეგებით მანიპულირებას რუსეთი ცდილობს როგორც ტექნიკური, ისე ფსიქოლოგიური ეფექტების მქონე კიბერ ოპერაციებით. კონკრეტულად.: ტექნიკურ ეფექტს იძლევიან სტანდარტული კიბერ შეტევები, ხოლო ფსიქოლოგიურ ზეწოლაში იგულისხმება ამომრჩევლის დამოკიდებულების შეცვლა, მანიპულაცია, მისთის სასურველი კანდიდატის მიმართ ნდობის დაკარგვა. ამ და სხვა მრავალ გზებს რუსეთი რათქმაუნდა ახორციელებს სხვადასხვა საინფორმაციო ოპერაციების საშუალებებით. ჩვენ ვიცით, რომ კიბერ შეტევა ხშირად წარმოადგენს საინფორმაციო ოპერაციის ჩასატარებელ ინსტრუმენტს და მიზნად ისახავს ინფორმაციული უპირატესობის მოპოვებას. ხანდახან, კიბერ შეტევები მიმდინარეობს საინფორმაციო ომის პარალელურად. მაგალითად.: კიბერ შეტევის შედეგად ხდება სოციალური ქსელიდან, ელექტრონული ფოსტიდან ან სხვა გზებიდან ინფორმაციის არასანქცირებული მოპოვება, ამის შემდენ მოპოვებული მასალის ორიგინალის ან ხშირ შემთხვევაში ფაბრიკაციის სახით ვრცელდება ინტერნეტში.

მიმდინარე თავში ჩვენ გავიხილავთ საარჩევნო პროცესებში ხშირად გამოყენებულ საინფორმაციო ოპერაციების ტექნიკებს, საფრთხეებს, მის აქტორებს და რისკების მმართვის პრაქტიკებს და რჩევებს.

როგორც უკვე აღვნიშნე, არჩევნები არის ხალხის მიერ საკუთარი ნების გამოხატვით, დემოკრატიის ფუძედემბლური პრინციპი. ხალხის ნდობას კი მხოლოდ და მხოლოდ არჩევნების გზით მოსახლეობის მიერ მხარდაჭერილი მთავრობა იმსახურებს, აქედან გამომდინარე ის, როგორც დემოკრატიული წყობილების ძირითადი და მნიშვნელოვანი ატრიბუტი, რუსული ჰიბრიდული ომის ერთ-ერთ ძირითად სამიზნეს წარმოადგენს. ეს უკანასკნელი, ტექნიკურთან ერთად, აღნიშნულ კიბეროპერაციებში ფსიქოლოგიურ ზემოქმედებებსაც ამატებს.

უმეტესად, როდესაც არჩევნების კიბერ უსაფრთხოებაზე ვიწყებთ საუბარს, ხმის მიცემის ელექტრონულ პროცესურებთან დაკავშირებით, საუბარი გადადის მის გამართულობასა და დაცულობაზე. ზოგადად კიბერუსაფრთხოების პერსპექტივებიდან გამომდინარე, საარჩევნო პროცესის ნებისმიერი ეტაპი, რომელსაც შეხება აქვს, ან შეიძლება ჰქონდეს ელექტრონულ მოწყობილობასთან, რისკის შემცველია. მითუმეტეს დღეს, ციფრულ ეპოქაში, კომპიუტერული სისტემები და მათი პროგრამული უზრუნველყოფა, საარჩევნო პროცესების თითქმის ყველა ეტაპზე გვხვდება. ეს კი თავისთავად მათ სისუსტეებსაც გულისხმობს.

კიბერშეტევების პოტენციური მიმართულება შეიძლება განისაზღვროს როგორ ტექნიკური, ისე ადამიანური ფაქტორებით. ის შეიძლება მოიცავდეს როგორც საინფორმაციო სივრცეს, ასევე თვითონ მათ, ვინც მართავს მათ. სახელმწიფო სექტორსა, ბიზნესზე თუ ინდუსრტიაზე განხორციელებულ თავდასხმებში, კივერ ინციდენტების უმეტესობა ადამიანური ფაქტორის გამოყენებით, მავნე აქტორებითაა განპირობებული. ამავდროულად, ყველაზე მოწყვლად სამიზნეებს წარმოადგენენ კომპიუტერული სისტემებისა და პროგრამული უზრუნველყოფის ვენდორები და ამ მხრივ არც საარჩევნო სისტემების კიბერ უსაფრთხოება წარმოადგენს გამონაკლისს.

ზოგადად, კიბერ შეტევა ეს არის ქსელზე თავდასხმის ერთ-ერთი ფორმა. რომლის მიზანს წარმოადგენს კომპიუტერის, ან ქსელის მყწობრიდან გამოყვანა, შეფერხება - მათ შორის განადგურება, არასანქცირებული კონტრულის მოპოვება და არსებული ინფორმაციის მთლიანობის დარღვევა ან/და უკანონო დაუფლება. მისი გავრცელების ძირითად სახეებში შედის ფიშინგი, DDOS, MITM, DEFECEMENT შეტევები და სხვა. ხშირად ამგვარი ოპერაციის მიზანი ინფორმაციული უპირატესობის მოპოვებაა, რაც რუსული სამხედრო და პოლიტიკური წრეებისთის ნაცნობი ტერმინია, რომელიც გულისხმობს[19] ინფორმაციის მიღების, დამუშავების, შესაძლებლობას, რომელიც ხელს უშლის მოწინააღმდეგეს იგივე ფუნქციის განხორციელებაში.

რაც შეეხება საინფორმაციო ოპერაციების კიბერ ელემენტებს. იგი მოიცავს დაინტერესების ობიექტების ქსელების კომპრომეტაციას ისეთი ინფორმაციის მოპოვების მიზნით, რომელიც მომავალში შეიძლება გამოყენებული იქნას შანტაჟისათვის, დაშინების ან/და დისკრედიტაციისთვის. ასევე მასმედიის საშუალებებში კონტროლირებადი გავრცელებისათვის. თვითონ საინფორმაციო ოპერაცია - ის საინფორმაციო კონტენტის გავრცელებას წარმოადგენს, საზოგადოებრივი აზრის მანიპულაციისთვის ან/და მათ ქცევაზე გავლენის მოხდენის მიზნით. სამიზნე აუდიტორია კი ზოგჯერ საკუთარი მოსახლეობა და ქვეყნის შიგნით არსებული პოლიტიკის ელიტაა. ამათ გარდა სრულიად შესაძლებელია სამიზნეს წარმოადგენდეს სხვა, უცხო ქვეყნის გარკვეული ჯგუფები, მათ შორის პოლიტიკოსები, რელიგიური უმცირესობების წარმომადგენლები და სხვა. სწორედ მათთის არის შექმნილი კონტენტი - რომელიც გულისხმობს ცრუ და ნამდვილი ამბავის ნაზავებს, მათი დაბნევის, დემორალიზაციისა და გავლენის მოპოვებისათვის.

[19] Манойло А.В., Петренко А.И., Фролов Д.Б.. Государственная информационная политика в условиях информационнопсихологических конфликтов высокой интенсивности и социальной опасности: Учебное пособие. М.: МИФИ. - 392 с. 2004

აღსანიშნავია, რომ ახალ, ციფრულ ეპოქაში, ტექნოლოგიების მძლავრმა წინსვლამ, ასევე, კიბერ შესაძლებლობების განვითარებამ, მსოფლიო ქვეყნებს საშუალება მისცა უპრეცედენტო მასშტაბების საინფორმაციო ოპერაციების განხორციელებისა. რადგან ვიცით, რომ მსგავსი ოპერაციებისათვის საჭირო კიბერინსტრუმენტები ძალიან იაფი და შესაბამისად ხელმისაწდომია. როგორც ვიცით, საინფორმაციო ოპერაციების ტაქტიკა, როგორც მცდარ და შეცდომაში შემყვან ინფორმაციის გავრცელებას გულისხმობს, ისე მოპარული ინფორმაციის კონტროლირებად გაჟონვას ინტერნეტში. ასევე, სოც. ქსელების გამოყენებას სხვადასხვა სახის კონფლიქტების გასაღვივებლად, მათ შორის იგულისხმება პოლიტიკური მიზნებიც.

რაც შეეხება, არჩევნებზე ზეგავლენის მოხდენას, საინფორმაციო ომის, მათ შორის სხვადასხვა კიბერშეტევების საშუალებით, მრავალს შეუძლია. ეს შეიძლება მოხდეს როგორც ქვეყნის შიგნიდან, ისე მის ფარგლებს გარეთ. მათ შორის შეიძლება იყვნენ ცალკეული სახელმწიფოები, ჰაკერები, რომლებიც შეიძლება მოქმედებდნენ როგორ ინდივიდუალურად, ისე ჯგუფურად, სვადასხვა ტერორისტული ორგანიზაციები, ჰაქტივისტები და პოლიტიკურად ომტივირებული ჯგუფები. აღსანიშნავია ისიც, რომ აღჩევნებში ჩარევის მოტივაციას შესაძლოა წარმოადგენდეს ასევე სახელმწიფოს ეროვნული, ან/და გეოპოლიტიკური ინტერესები, მათ შორის ფინანსური ინტერესებიც, ქვეყნის დემოკრატიისა და მისი წყობისადმი ნდობს შესუსტება და სხვა მრავალი.

აღჩევნებისადმი ზეგავლენის თვალსაზრისით თუ ვიმსჯელებთ, ყველაზე დიდ ფართხეს, მაინც სხვა ქვეყნები და მასთან დაკავშირებული ჰაკერთა დაჯგუფებები ახდენენ. რა თქმა უნდა, ამ საკითხშიც მოწინავე პოზიციას იკავებს რუსეთი. ეს არის მსოფლიოში ერთადერთი ქვეყანა, რომელიც საქართელოსადმი მტრული და აგრესიული განწყობით გამოირჩევა საუკუნეების მანძილზე. აქედან გამომდინარე, იგი საქართველოს მისივე გავლენის სფეროდ აღიქვამს და სწორედ ამიტომ, ჩვენი ქვეყანაც მისი პირდაპირი სამიზნეა საინფორმაციო თუ

სხვა სახის კიბერ ომში. ხაზგასმით უნდა აღინიშნოს ისიც, რომ მსგავსი საქმიანობა სხვა, მოწინააღმდეგე ქვეყნისთვის ან და მათი მთავრობისათვის დემოკრატიული პროცესებისადმი ნეგატიური და მომაკვდინებელი საქმიანობაა.

რუსეთი იმდენად სწრაფად იწაფება მსგავს საქმიანობებში, რომ არჩევნების შედეგებით მანიპულირება, როგორც ტექნიკური ასევე ფსიქოლოგიური ეფექტების გამოყენებით, მისთვის დიდ და რთულ პრობლემას აღარ წარმოადგენს. იგი ფსიქოლოგიური ზემოქმედებით ცდილობს ამომრჩეველს შეუცვალოს განწყობა, მისთვის აქამდე დადებითად განწყობილი ფიგურა შეცვალოს უარყოფითად. განსაკუთრებით ბოლო ათეული წლებია რუსეთი ევროპასა და მათ შორის ამერიკაშიც ბევრჯერ გამხდარა აღნიშნული ზემოქმედების მთავარი მოქმედი ფიგურა. ასე რომ, რუსეთი მსგავსი კიბერ ოპერაციებით აყენებს როგორც მნიშვნელოვან ზარალს, ასევე მისდამი ცნობიერების დადებითად შეცვლას ცდილობს, რომლის მთავარი მიზანიც მისი მთავრობის, ასევე პრორუსული ელიტის გაძლიერებაა.

ამგვარი პროცესებისადმი ჩარევები კრემლმა ჯერ კიდევ 2014 წელს, უკრაინაში კონფლიქტისას, მასირებული შეტევებით დაიწყო. რა თქმა უნდა, სამიზნე ობიექტი უკრაინის საარჩევნო ინფრასტრუქტურა გახლდათ. პრეზიდენტ იანუკოვიჩის გადადგომის შემდეგ, ცხადია არჩევნები დაინიშნა. არჩვნებამდე კი რამდენიმე დღით ადრე, პრორუსულმა ძალებმა, დაჯგუფება „კიბერბერკუტმა“, უკრაინის ცენტრალური საარჩევნო კომისიის პროგრამიდან, მოახერხეს და მოახდინეს სისტემური ფაილების წაშლა, ამან კი გამოიწვია არჩევნების შედეგების გამოცხადების დაგვიანება. რეალურად საარჩევნო კომისიამ შეძლო და სარეზერვო ფაილები აღადგინა, მაგრამ თითქმის 20 საათი დასჭირდათ ამ შეფერხების მოსაგვარებლად. ასედან გამომდინარე, „კიბერბერკუტს“ არჩევნებამდე სულ რამდენიმე თვით ადრე ქჰონდა უკვე წვდომა საარჩევნო კომისიის ადმინისტრაციულ მონაცემებსა და შიდა ელექტრონულ ფოსტაზე. აღნიშნული ხარვეზის პერიოდში, საარჩევნო კომისიის პერსონალური საიტი ფაბრიკაციულ ინფორმაციას ავრცელებდა, რომ არჩევნებში ვითომ

ულტრამემარჯვენე კანდიდატმა გაიმარჯვა. უკრაინის მხარის ამ ინფორმაციის მკაცრად უარყოფის მიუხედავად, რუსული მედია აქტიურად აშუქებდა აღნიშნული კანდიდატის გამარჯვების შესახებ ინფორმაციას. უკრაინაში, ამგვარ ინციდენტებზე რეაგირების ჯგუფის ინფორმაციით, ამგვარი ხარვეზის გამომწვევ მალვეარს, რუსულ სამხედრო დაზვერვასთან მივყავართ, იგი პირდაპირ კავშირში იყო ამ ფაქტთან, და მას იყენებდა დაჯგუფება APT28.

საინტერესოა ასევე ამერიკის, გერმანიისა და საფრანგეთის მაგალითები, სადაც რუსული ხელწერა ფიგურირებს. 2016 წელს, ამერიკის შეერთებული შტატების საარჩევნო პროცესებისა და აქტივობის დროს, მრავალმხრივი კამპანია მიმდინარეობდა რუსეთის მხრიდან დემოკრატიული პროცესებისადმი. მიზანი კი ხალხის რწმენის შერყევა გახლდათ, ასევე მიზნებში უნდა განვიხილოთ საპრეზიდენტო კანდიდატის რეპუტაციის შელახვის მცდელობა, მისივე საქმიანობის კარგად წარმართვის პოტენციალის შესამცირებლად. ამ კამპანიის დროს გამოყენებული იყო როგორც მრავალმხრივი საინფორმაციო ომი, რომელიც გულისხმობს სოც. მედიის ყალბი ანგარიშების მეშვეობით მცდარი ინფორმაციის მასობრივი გავრცელებას, ასევე პოლიტიკური პროცესის დელეგიტიმიზაციას, ისე სხვადასხვა სახის კიბერ თავდასხმებს, რომლის საშუალებითაც, რუსულმა აქტორებმა, APT28 და APT29-მ მოიპოვეს არაავტორიზებული წვდომა დემოკრატიული პარტიის როგორც ელექტრონულ ფოსტაზე, ისე მათ მიერ გამოყენებულ სერვერებზე. მათ მიერ მოპოვებული ინფორმაციის გამოქვეყნება ხდებოდა DCLeaks.com და WikiLeaks პლატფორმებზე, "Guccifer 2.0"-ის სახელით და IRA-ს[20] მეშვეობით კი ხდებოდა ამერიკის მოქალაქეების სახელით ათასობით ყალბი ანგარიშების შექმნა, რომელთაც შემდგომ დისკუსიებმაც მოახდინეს გარემოს პოლარიზება, ამავე დროს, აღნიშნულმა ორგანიზაციამ დაიწყო ყალბი კონტენტის

[20] **Internet Research Agency** იგივე **Trolls from Olgino**. სანკტ-პეტერბურგში ბაზირებული რუსული კომპანია, რომელიც ჩართულია გავლენის ოპერაციებში რუსული ბიზნესისა და პოლიტიკური ინტერესების სასარგებლოდ. მისი რამდენიმე წევრი ოფიციალურად მხილებულია აშშ-ის 2016 წლის საპრეზიდენტო არჩევნებში ცარევის მცდელობებში.

გავრცელება, თითქოსდა მრჩეველი, პრეზიდენტობის კანდიდატ კლინტონს ბენღაზის ინციდენტისას პასუხისმგებლობას ამერიკელების მსხვერპლზე აკისრებდა. აღსანიშნავია ისიც, რომ არ არსებობდა პირდაპირი მტკიცებულებები ტრამპის სასარგებლოდ ხმების მანიპულირებისა, მაგრამ, უდავოა, რომ კრემლის ჩარევამ გააღრმავა მაშინდელი პოლიტიკური უთანხმოება, ასევე ახდენდა საარჩევნო გარემოებების პოლარიზაციასა და ამ უკანასკნელმა უკვე გამოიწვია ამერიკელი ამომრჩევლის რწმენის შერყევა არჩევნების შედეგებზე. ხაზი უნდა გაესვას იმას, რომ DNC hack განიხილება, როგორც კრემლის უმაღლეს დონეზე სანქცირებული ჩარევა ამერიკის შეერთებული შტატების არჩევნებში, მისდამი დემოკრატიული პროცესების რწმენის შესუსტებისა და არჩევნებში მონაწილე კონკრეტული კანდიდატის კომპომეტაციის მიზნით.

2017 წლის 5 მაისი. საფრანგეთი. პრეზიდენტის არჩევნებამდე რამდენიმე დღით ადრე, მიზანმიმართული ფიშინგის გზით, მოპოვებული გახდა მაკრონის საარჩევნო გუნდის ინფორმაცია, რომელიც რამდენიმე გიგაბაიტის ინფორმაციას მოიცავდა. რეალურად მათი ავთენტურობა ან/და ცალსახა სიყალბე ნამდვილად რთული დასადგენია. აღნიშნული მასალა კი უშუალოდ არჩევნების წინა დღეს გამოქვეყნდა სპეციალურად შექმნილ პლატფორმაზე, რომელმაც შეაფერხა მაკრონის გუნდის მხრიდან მყისიერი რეაგირება. ამის პარალელურად დიდი ძალისმებით მუშაობდნენ ბოტები, ინტერნეტში დიდი რაოდენობით ნეგატიური ინფორმაციის გასავრცელებლად. აქაც აღსანიშნავია, რომ ყველაფერი ერთ მიზანს ემსახურებოდა და ეს გახლავთ რუსეთისადმი პოზიტიურად განწყობილი კანდიდატის მხარდაჭერა, რომელიც ამ შემთხვევაში უშედეგოდ დასრულდა.

2015 წელს, გერმანიის ბუნდესტაგის არჩევნების წინ, მათივე სერვერებიდან განხორციელდა ელექტრონული ფოსტის კონტენტის მოპარვა, ასევე პარალელურად მსგავსი ფაქტი დაფიქსირდა ანგელა მერკელის პარტიის საინფორმაციო სისტემიდანაც. თუმცა აღნიშნული მოპოვებული ინფორმაციების გამოქვეყნება არ მომხდარა. ამ შეტევების

პარალელურად გერმანიაში, ნეგატიური ინფორმაციის გავრცელების, გაღვივების მიზნით სოციალურ ქსელებში რუსულმა ბოტებმა და ტროლებმა აქტიურობა დაიწყეს. აქაც ყველაფერი მიზნად ისახავდა პოლიტიკურ პოლარიზაციას, ასევე საარჩევნო პროცესებისადმი ამომრჩევლების ნდობის შესუსტებას, რაც პირდაპირ მიანიშნებს არჩევნების შედეგების დელეგიტიმიზაციას. ხდებოდა ახალი კონტენტების შექმნა, მათი გავრცელება. მაგალითად ერთერთი ეხებოდა გერმანელი გოგონას გაუპატიურებას, არაბი მიგრანტის მიერ. გერმანულმა სპეცსამსახურებმა გამოთქვეს ვარაუდი, რომ რუსეთის საარჩევნო ჩართულობა არ იყო რომელიმე კანდიდატის ან პარტიის მხარდასაჭერად მიმართული აქცია, არამედ ეს უბრალოდ მიზნად ისახავდა გერმანიის დემოკრატიული პროცესების და მათი საარჩევნო ინსტიტუტის დისკრედიტაციას. ეს ყველაფერი კრემლის გეოპოლიტიკური ინტერესების რეალიზაციაა, ან მისი ხელშეწყობა, რომელიც გულისხმობს ქვეყანაში ნებისმიერი მომავალი ხელისუფლების ნდობისა და მხარდაჭერის შესუსტებას. ამ ინფორმაციის დასადასტურებლად შეგვიძლია მოვიყვანოთ შემდეგი ფაქტი, რომ მერკელმა არჩევნებში გაიმარჯვა, თუმცა აღსანიშნავია, ულტრამემარკვენე პარტიამ დაიკავა მესამე ადგილი ბუნდესთაგში, რაც 1940 წლის შემდეგ ყველაზე ნაკლებ ხმას მიუთითებს. მმართველი კოალიციის ჩამოყალიბებას კი რამდენიმე თვე დასჭირდა[21].

ზემოთ ჩამოთვლილი, საარჩევნო ინციდენტების მაგალითების ანალიზიდან ცხადია, მოქმედებს სქემა, კიბერთავდასხმების შემდეგ ხდება საინფორმაციო სისტემების პენეტრაცია, წვდომის მოპოვება სენსიტიურ ინფორმაციაზე და ამის შემდეგ პოლიტიკურ პარტებსა და თუ ზოგადად პოლიტიკური ფიგურებისადმი კონტროლირებადი გავრცელება მათი დისკრედიტაციის მიზნით. რაც შეეხება ბოტებს და ტროლებს, მათ მიერ შექმნილი ყალბი პროფილებისა და ბლოგების გამოყენებით ხდება გავრცელებული ინფორმაციების

[21] Laura Galante, Shaun Eee. Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Atlantic Councis Issue Brief. September, 2018

კომენტირება, სადაც მიმდინარეობს რუსული ნარატივების დამკვიდრება, ასვე ცრუ ინფორმაციის გავრცელება და საზოგადოებისადმი კრემლის სასურველი აზრის ჩამოყალიბება. და ეს ყველაფერი ნეგატიური განწყობის გაღრმავების მიზნით.

თუ ჩვენ გავითვალისწინებთ რუსეთის მხრიდან საქართელოში სხვადასხვა პროცესების, მათ შორის შიდაპოლიტიკური ამბებით დაინტერესების ხარისხს, ასევე გავითვალისწინებთ სახელმწიფო თუ კერძო სექტორის ქსელების მოწყვლადობას, მათ შორის რუსულ კიბერაქტორების მიერ პენეტრაციის მასშტაბებს, ცხადია, ყურადსაღებია ქართულ საარჩევნო კამპანიებშიც ოკუპანტი ქვეყნის ჩარევის ალბათობებიც.

ჩვენ ვიცით, რომ რუსეთთან დაკავშირებულ აქტორებს, მაგალითად როგორიც არის APT28, ქართულ სახელმწიფო, ბიზნეს თუ საკომუნიკაციო ქსელებთან, დიდი ხნის განმალობაში ჰქონდა არასანქცირებული წვდომა. რის შედეგადაც, წლების განმალობაში დიდი რაოდენობით სენსიტიური ინფორმაციის გადინება ხდებოდა რუსული სპეცსამსახურების ხელში[22]. საქართველოში მიმდინარე არჩევნებიბსას, გარდა იმ არალეგალურად მოპოვებული მასალებისა, მათ მიერ გასავრცელებელ კომპონენტების კიდევ ერთ წყარო სოც. ქსელებსა და სხვადასხვა ღია წყაროებში, პოლიტიკოსებისა და პოლიტიკურად მოაზროვნე ძალების გამონათქვამები და აზრები სენსიტიურ თემები მოიაზრება. აქედან გამომდინარე, ძალიან მნიშვნელოვანია არჩევნებში და ზოგადად საარჩევნო პერიოდში მოხდეს კრემლისებული ჩარევების, მათი მაგალითების განხილვებისა და ანალიზის შედეგად, შეტევების ტაქტიკების, კიბერსაფრთხეების, მეთოდებისა და სხვა დანარჩენი რისკების შესამცირებლად სხვადასხვა რეკომენდაციების გათვალისწინება და დამუშავება.

[22] Fire eye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. ხელმისაწვდომია https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf

ამ დრომდე ჩვენს ხელთ არსებული ინფორმაციის წყაროზე დაყრდნობით, რუსეთი არჩევნებში ჩარევისათვი შემდეგ ხერხებს[23] მიმართავს.:

1 - ფიშინგი

2 - სოციალური ინჟინერია

3 – DDOS

4 - პორტების სკანირება

5 - MITM – (Man In The Middle)

6 – SQL-Injection

7 - ინსაიდერული შეტევა

8 - ინფორმაციის კონტროლირებადი გაჟონვა

9 - ცრუ ან შეცდომაში შემყვანი ინფორმაციის გავრცელება

10 - საინფორმაციო ოპერაციები

11 - ანტაგონისტური განწყობების გაღვივება

არჩევნების ტეპების, სხვადასხვა სისტემების თუ კანონმდებლობისა, საუკეთესო პრაქტიკა არსებობს, რაც უზრუნველყოფ ამ პროცესის კიბერ უსაფრთხოებებს, მიმდინარე არჩევნების მშვიდ, სამართლიან და სანდო დაცულობას. ეს გულისხმობს როგორც შინაარსობრივ, ისე ტექნიკურ თვალსაზრისს.

პრაქტიკაში დასამკვიდრებლად შეგვიძლია შემდეგი მაგალითები განვიხილოთ.:

1 - კიბერ უსაფრთხოების პროაქტიული კულტურის დანერგვა - წარმატებულად ჩატარებული კიბერ შეტევების თითქმის აბსოლუტური უმრავლესობა დაკავშირებულია ადამიანურ ფაქტორთან, ანუ მომხმარებლის შეცდომასთან. ამიტომ, ისეთი

[23] Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center. Cyber Threats to Elections – a Lexicon. 2018

კიბერუსაფრთხოების დანერგვა, როგორიც არის „ზემოდან - ქვემოთ“ პოლიტიკა, რისკების შემცირების ძალიან მნიშვნელოვანი ინსტრუმენტი გახლავთ. კიბერ უსაფრთხოების კულტურა, მომხმარებლის კიბერ ჰიგიენის გათვითცნობიერებული ჩვევები, ასევე განაპირობებს თავდასხმის ობიექტის მხრიდან სამიზნედ შერჩევის ხარისხს და იმის შესაძლებლობას, რაც ქმნის თავდასხმის წამატებული შედეგების მინიმალიზაციასა და ფსიქოლოგიური ზემოქმედების განეიტრალებას.

ა - კიბერ უსაფრთხოების საკითხებში ტოპ-მენეჯერების ჩართულობა;
ბ - დეტალური გეგმის შემუშავება ან/და იმპლემენტაცია ინციდენტების მართვის საკითხებში;
გ - საარჩევნო ადმინისტრირებებში კადრების სანდოობის შემოწმება;
დ - უწყებათაშორისი, საჯარო და კერძო თანამშრომლობის ფარგლებში, გარე რესუსრსების გამოყენება.

2 - სისტემების კიბერ უსაფრთხოებისადმი კომპლექსური მიდგომა - კომპრომეტაციამ, რომელიც შესაძლოა იყოსსაარჩევნო სისტემის ნებისმიერ სეგმენტში, არის შანსი გამოიწვიოს მთლიანად არსებული სისტემის პენეტრაცია. აღსანიშნავია, რომ თავდასხმელები იმ სუსტ წერტილს ეძებენ, რომლის მეშვეობითაც შემდეგ სისტემებში ხდება შეღწევა. სისტემებს, რომელსაც ინტერნეტთან კავშირი არ აქვთ, შესაძლოა მეხსიერების ბარათებით ან სხვა გარე მოწყობილობების საშუალებით მათი კომპრომეტაცია.

ა - იმ ყველა კომპიუტერისა და მოწყობილობების დაცვა, მიუხედავად მათი კუთვნილებისა, რომელიც პირდაპირ შემხებლობაში არის პროცესებთან;
ბ - იმ მენეჯმეტების ცენტრალიზება და ოპტიმიზაცია, რომლებიც არიან კიბერ უსაფრთხოების სფეროში.

3 - ძლიერი პაროლის და ორმაგი ავტორიზაციის პოლიტიკის დანერგვა - მომხმარებლის სააბტორიზაციო მონაცემების გამოყენება უდიდეს შემთხვევებში ხდება

თავდასხმელების სისტემების კომპრომეტაციის საგანი. აუცილებელია პაროლში გამოყენებულ იქნას რვა (8) ან მეტი სიმბოლო, მათ შორის ასოებისა და სხვადასხვა სიმბოლოების ჩართულობა. ასევე 2 დონიანი ავტორიზაციის დაცვის პოლიტიკის დანერგვა.

4 - მენეჯმენტი და წვდომის კონტროლი - თავდასხმელთა სამიზნეს, ნებისმიერი ავტორიზებული მომხმარებელი წარმოადგენს. ამის გამო, ხშირად, სულ რაღაც ერთი მომხმარებლის კომპრომეტაციაც კი საკმარისია ქსელის სრულად ათვისებისა და კონტროლისათვის. აქედან გამომდინარე, რაც უფრო მეტ ადამიანს აქვს წვდომა ქსელთან და რაც უფრო დიდია მათი წვდომის არეალი, მით უფრო ადვილია და მეტია საფრთხე კომპრომეტაციისა.

ა - მოხდეს იმ პირთა რაოდენობის შეზღუდვა, რომელსაც სისტემაზე ავტორიზებული წვდომა გააჩნია;
ბ - მხოლოდ მინიმალური უფლებების პრინციპით, მხოლოდ აუცილებელ ინფორმაციაზე წვდომა ავტორიზებულ პირთათვის;
გ - იმ მომხმარებლის წვდომის ავტომატური გაუქმება, რომელიც დათხოვნილ იქნა სამსახურიდან, ან შეიცვალა პოზიცია ან სამუშაო სფერო.

5 - სისტემებისა და მგრძნობიარე მონაცემების გამიჯვნა - მნიშვნელოვანია სისტემის ნებისმიერი სეგმენტი, ამიტომ აუცილებელი არის მათი პრიორიტეტების განსაზღვრა მონაცემთა სენსიტიურობის თვალსაზრისით, რადგან დაცვის ყოველი დამატებითი ღონისძიება ზედმეტ პროცედურებსა და ხარჯებს მოიცავს.

ა - სისტემური აკრძალვე ყველა მობილური მოწყობილობის გამოყენებისა;
ბ - იმ მოწყობილობების კონფიგურირება, რომელიც შეიცავს სენსიტიურ ინფორმაციას, მხოლოდ კონკრეტული ქმედების განხორციელების შესაძლებლობებით.

6 - ლოგირების, მონიტორინგისა და სარეზერვო ასლების სისტემის შექმნა - მათი ასლების სისტემა, შესაძლებლობას იძლევა, რომ მოხდეს შეტევის დეტექცია და ინციდენტის შემდგომ, ადვილად მოხდეს სისტემის აღდგენა.

ა - მიმდინარე სარეზერვო ასლების შექმნის იმპლემენტაციის ავტომატური პროცესი. ასლის შექმნის შემდგომ, ფაილს უნდა ჰქონდეს მხოლოდ წაკითხვის ფუნქცია, ასევე რეგულარულად უნდა ხდებოდეს ფაილების აღდგენის შესაძლებლობების ტესტირება. ბ - შექმნილი მონაცემების ბაზების ნებისმიერი ცვლილების ლოგირება, ასევე მონიტორინგი როგორც ადამიანური რესურსებით, ისე ანომალიების აღმომჩენი კომპიუტერული უზრუნველყოფით.

7 - ვენდორის/კონტრაქტორის ხარისხის გათვალისწინება კიბერუსაფრთხოების თვალსაზრისით - საარჩევნო პროცესების პროგრამულად უზრუნველყოფისა და საოპერაციო სისტემების, აგრეთვე სხვადასხვა სერვისის მომწოდებლის ან/და ავტორიზებული ქვდომის მქონდე კონტრაქტორის, არასათანადო დაცულობა სისტემისთვის გახლავთ რეალური ინსაიდერული საფრთხე, რადგან ის წარმოადგენს მონაცემთა გაჟონვის, ან განადგურების, ან შეცვლის ერთ-ერთ საყურადღებო მიმართულებას[24].

თემის დასასრულს, რამოდენიმე პრაქტიკული რჩევა, თუ რა უნდა ვიცოდეთ საარჩევნო პროცესების ადმინისტრირებასთან შემხებმა პირებმა. მიუხედავად იმისა, რომ კიბერ ოპერაციების უმრავლესობა, მტრული სახელმწიფოს სტრატეგიული ამოცანების - არჩევნებზე ზეგავლებასა და მსგავსი პროცესების განხორციელებას ემსახურება, განპირობებულია ადამიანური და მომხმარებლის შეცდომების ფაქტორებით. ისეთი შეტევების თავიდან ასაცილებლად, როგორებიცაა ფიშინგი, სოციალური ინჟინერია და სხვა, შესაძლებელია მომხმარებლის კიბერ ჰიგიენის წესების დაცვით. ეს არის საუკეთესო

[24] Defending Digital Democracy Project. Belfer Center for Science and International Affairs. Harvard Kennedy School. The State and Local Election Cybersecurity Playbook. 2018.

აქტივობა, ასევე პრაქტიკა, კიბერ უსაფრთხოების ასამაღლებლად, რომელიც მომხმარებლების გათვითცნობიერებულ ჩვევებს ემყარება.

1 - დაუშვებელი არის კომპიუტერული მოწყობილობების პაროლის გარეშე დატოვება, მისი პაროლის ან/და ინფორმაციის სხვა პირზე გადაცემა, მიუხედავათ მათი ერთმანეთთან დამოკიდებულებისა.

2 - რთული პაროლის გამოყენების პოლიტიკის დანერგვა - ზოგადად, პაროლი უნდა მოიცავდეს მინიმუმ 8 სიმბოლოს, ასოებს და ციფრებს, სასურველია გამოყენებულ იქნას როგორც დიდი, ისე პატარა ასოები პაროლის კომბინაციაში. ასევე, არა არის რეკომენდირებული პაროლში გამოყენებული იყოს საკუთარი სახელები, გვარები, დაბადების თარიღი და სხვა.

3 - სავალდებულოა სისტემების, პროგრამების, აპლიკაციების, ანტივირუსის რეგულარული და ავტორიზებული (ლიცენზირებული) განახლებები.

4 - ყველგან, მიზანშეწონილია ორმაგი ავტორიზაციის დაყენება იქნება ეს სამსახურის განგარიშები თუ პირადი მოხმარების სხვადასხვა აპლიაციებზე, როგორიც არის ელ. ფოსტა, სოც. ქსელი, მობაილბანკი და სხვა. სასურველია მეორე ავტორიზაციისთვის, სმს კოდების ნაცვლად გამოყენებული იყოს სხვა ფიზიკური მოწყობილებები ან/და მობილური აპლიკაციები, ისეთი როგორიც არის Google, Duo, Authenticator, Authy და სხვა.

5 - ძალიან დიდ რისკებს შეიცავს მტრულად განწყობილი სახელმწიფოების აპლიკაციებისა და პროგრამების გამოყენება. საჭიროა ყურადღება მივაქციოთ აპლიაკციების გააქტიურებისას რა მონაცემებზე ითხოვს წვდომას (მაგ.: მიკროფონი, კამერა, და ა.შ)

6 - საარჩევნო ადმინისტრაციის მიერ კიბერ უსაფრთხოების პოლიტიკაისადმი სერიოზული აღქმა - სავალდებულოა მენეჯმენტის თითოეული დონის წარმომადგენელი

იაზრებდეს მსგავს საფრთხეებსა და გამოწვევებს. მენეჯმენტი რეგულარულად უნდა ახდენდეს მისდამი დაქვემდებარებული თანამშრომელბის ამ საკითხებზე ცნობიერების ამაღლებას. მათ შორის კიბერ ჰიგიენის თვალსაზრისითაც.

კიბერტერორიზმი

კიბერტერორიზმი - ეს არის კომპიუტერის, ქსელის და საინფორმაციო ტექნოლოგიების საშუალებით განხორციელებული ქმედება, რომელიც მიზნად ისახავს ხელი შეუშალოს ჯგუფის, ორგანიზაციის ან სახელმწიფოს პოლიტიკურ, სოციალურ თუ ეკონომიკურ საქმიანობას ან ახდენს ფიზიკური ძალადობის და შიშის პროვოცირებას და მოტივირებულია ტრადიციული ტერორისტული იდეოლოგიებით, კვალიფიცირდება, როგორც კიბერტერორისტული ქმედება.[25]

[25] Defining cyber terrorism. Ruben Tuitel. Per concordiam - journal of european security and defense issues, vol. 7, issue 2, 2016. ISSN 2166-322x (print) ISSN 2166-3238 (online)

მაგალითად, ისეთი ტერორისტული ორგანზაციები, როგორი არის ISIS,Hizballa, Hamas, Al Qaida, თალიბანი თუ სხვა, სადაზვერვო ინფორმაციის მოსაპოვებლად რეგულარყლად იყენებენ ინტერნეტს. ისინი ინტერნეტს იყენებენ ინფორმაციის მოპოვების, პროპაგანდის გავრცელების, რეკრუტირებისა თუ სხვა მიზნებისთვის. კერძოდ, ჰეზბოლა და ჰამასი საკუთარ კიბერ აქტივობებს ახლო აღმოსავლეთის რეგიონზე ავრცელებენ, აისისის წევრები კი ცდილობენ შემდეგი განსახორციელებელი ტერაქტებისათვის მოიძიონ სენსიტიური ინფორმაციები, არატერორისტული ქვეყნების მოქალაქეებზე.[26]

ასევე, კიბერ სივრცეს წარმატებით იყენებს ნიგერიაში არსებული ტერორისტული დაჯგუფება Boko Haram-ი. იგი ინტერნეტს როგორც სხვა დანარჩენი, ფინანსების მოსაძიებლად, დეზინფორმაციის და პროპაგანდის გასავრცელებლად იყენებს. ამ ორგანიზაციას ისეთი პასუხისმგებლობა ეკისრება, როგორებიცაა ქალაქ აბუჯაში გაეროს შტაბბინის დანგრევა, ნიგერიაში მოსწავლე გოგონების გატაცება და სხვა მრავალი ათასი უდანაშაულო ადამიანის მკვლელობა. ამ ორგანიზაციის ქმედებები ასევე ვრცელდება კამერუნის და ჩადის ტერიტორიებზე.[27]

დღეს ყველაზე ძლიერი კიბერ ტერორისტული დაჯგუფება ასოცირდება აისისთან, Cyber Chaliphate, რომლის ძირითად სამიზნეს ამერიკის შეერთებული შტატებისა და სხვა არატერორისტული ქვეყნების სახელმწიფო თუ კერძო სექტორების რეგულარული კიბერშეტევები. ასეთ კიბერ თავდასხმებს მიეკუთვნება აშშ-ს ცენტრალური სარდლობის YouTube და Twitter – ანგარიშების გატეხვა. თუმცა ეს თავდასხმები ეკონომიკურ ხასიათს არ ატარებდა. მათი მიზანი დაშინება, პროპაგანდა და მუქარის შემცველი მასალების

---

[26] Joint statement for the record to the Senate Armed Forces Comitee. Foreign cyber threat to the United States of America. January 5, 2017

[27] Defining cyber terrorism. Ruben Tuitel. Per concordiam - journal of european security and defense issues, vol. 7, issue 2, 2016. ISSN 2166-322x (print) ISSN 2166-3238 (online)

გამოქვეყნებაა. აისის-ს ტვიტერზე ათიათასობით გამომწერი ყავს, ის ამ პლატფორმაც პოტენციური ახალწვეულების მოსაზიდადაც იყენებს.

ISIS-ის ყველაზე წარმატებული და ამავდროულად გახმაურებული კიბერშეტევა გახლავთ ფრანგული ტელევიზიის, TV 5 Monde – ზე მრავალფაზიანი შეტევა. არც მანამდე და არც მის შემდეგ, დაჯგუფებას მსგავსი სიძლიერის კიბერთავდასხმა არ განუხორციელებია. თუმცა, ბოლო პერიოდში, სხვადასხვა წყაროებსა თუ მათ შორის ჩვენთვის პარტნიორი ქვეყნების სპეცსამსახურების მონაცემებში, წინ წამოიწია მოსაზრებამ[4], რომ ეს ოპერაცია წარმოადგენდა რუსული სპეცსამსახურების False Flag ოპერაციას.

ტერორისტული ორგანიზაციები საბედნიეროდ (ჯერჯერობით) არ ფლობენ ისეთ ძლიერ კიბერსაშუალებებს, რომ სერიზოული ზიანი მიაყენონ სამიზნე ობიექტს. დღეს, ყველაზე ცნობილ კიბერშეტევებს წარმოადგენს საიტებსა და სოციალურ ქსელებზე თავდასხმები, რაც იწვევს ხარვეზებს, თუმცა მცირე ხნით.

დღევანდელი მონაცემებით, ყველაზე რეალურ კიბერსივრცის გამოყენება გულისხმობს ფინანსურ თაღლითობებს, ტერორისტული ორგანიზაციების მიერ სადაზვერვო ინფორმაციის შეგროვებას, გარკვეული სახის პროპაგანდას და ა.შ. მაგალითად, რამდენიმე წლის წინ, რადიკალური ისლამის მიმდევარების მიერ დაწყებულ იქნა მასშტაბური ჯიჰადისტური კამპანია სოციალურ ქსელში, სადაც ათიათასობით მიმდევარი გამოუჩნდა, მათ შორის საქართველოშიც. ეს უკანასკნელი ითვალისწინებდა ჯიჰადისტური მოწოდებების გავრცელებასა და რეკრუტირებისათვის საჭირო პლატფორმების შექმნას. ჩვენ ვიცით, რომ სოციალური ქსელი კარგად იძლევა საშუალებას პროპაგანდა განვაცორციელოთ ფართო მასებში. სწორედ ახალი ძალების მოზიდვას ემსახურებოდა ეს კამოანიაც ამგვარი ფორმით წარმართვის დროს.

როგორც აღინიშნა, ამ ეტაპზე კიბერ ტერორიზმი ვებ გვერდებისა და სხვადასხვა სერვერების დაზიანებით შემოიფარგლება და ასეთი შეტევები ხორციელდება

ანტიტერორისტული კოალიციის წევრი ქვეყნებისადმი. მაგალითად ისეთის, როგორიც არის საქართველო. ამ მოსაზრების დადასტურება ჰიპერმარკეტ „კარფურზე“ განხორციელებული შეტევით შეგვიძლია. ეს იყო “Charlie Hebdo”- ს მოვლენების გამოძახილი საქართველოში. მიუხედავად იმისა, რომ ეს შეტევა გარკვეული ზიანის გარეშე დასრულდა, მსგავსი შეტევები სრულიად შესაძლებელია იყოს არაპროპორციული ზიანს მომტანი სახელმწიფოსთვის[28].

უნდა გავითვალისწინოთ, რომ კიბერ შეტევების განხორციელების ალბათობები დღითიდღე იზრდება და ეს რამდენიმე ფაქტორით არის გათალისწინებული[29].:

1 – უკვე განხორციელებული შეტევები, მიუხედავად იმისა, თუ ვინ იდგა რეალურად ამ შეტევების უკან, აღქმულ იქნა წარმატებულად, რაც ამგვარი თავდასხმების ეფექტურობის განცდას ქმნის.

2 - ასპარეზზე გამოვიდა კომპიუტერულ სისტემებში უკეთესად გარკვეული ექსტრემისტების თაობა და ორგანიზაციები ეცდებიან მათი ცოდნის გამოყენებას ტერორისტული მიზნების მისაღწევად.

3 - ავღანეთსა და სირია-ერაყის ტერიტორიაზე ტერორისტული ორგანიზაციების კონვენციური ძალების მიერ განცდილი მარცხი, ასევე გაზრდილი უსაფრთხოების ზომები ტერორისტული აქტების წინააღმდეგ, ამ ორგანიზაციებს დიდი ალბათობით კიბერთავდასხმების განხორციელებისაკენ უბიძგებს.

---

[28] Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. Report, 2017. ხელმისაწვდომია www.dia.mil/Military-Power-Publications
ვ. სვანიძე. პარიზის ტერაქტი და ახალი გამოწვევები საქართველოში. ვ.სვანიძე, ა. გოცირიძე. „კიბერ თავდაცვა; კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები“. საქართველოს თავდაცვის სამინისტრო, თბილისი, 2015წ. გვ. 210-214

[29] A,Gotsiridze. Terrorist’s Cyber Activities – a growing Threat. Scientific & practical cyber security journal, 2018. https://journal.scsa.ge/issues/2018/03/975

კიბერთავდასხმა, როგორც ფსიქოლოგიური ეფექტის მქონდე ოპერაცია

ბოლო ათეული წლებია სხვადასხვა სახის კიბეროპერაციებით ცდილობენ წარმატების მიღწევას, შეცვალონ მათთვის სასურველი აუდიტორიის ცნობიერება. აქედან გამომდინარე უნდა ვთქვათ, რომ კიბერთავდასხმების ნაწილი გამოიყენება ფსიქოლოგიური ზემოქმედების მოხდენის მიზნებისთის. ასეთ შედეგებზე ორიენტირებული ოპერაციები კიბერ სივრცეში, მიმართულია პირველ რიგში შეიარაღებულ ძალებზე და მშვიდობიან მოსახლეობაზე. დღეს

ასეთი კიბეროპერაციები მუდმივად მიმდინარეობს სხვადასხვა სამიზნე აუდიტორიების წინააღმდეგ.

მაგალითად, რუსეთი - პოლიტიკურად ნებისმიერ ინფორმაციას, განიხილავს როგორც ძალაუფლების ერთერთ მნიშვნელოვან წყაროს, რომელიც ქმნის სხვადასხვა სამიზნე აუდიტორიაში ახალი ნიადაგის მომზადებას, მისთვის სასურველი შედეგების მისაღებად.

რუსეთისთვის ეს სფერო გახლავთ მნიშვნელოვანი დომეინი, რომელიც შეიძლება გამოყენებულ იქნას როგორც მისი, ადგილობრივი მოსახლეობის ადვილად სამართავად, ისე სხვა ქვეყანაში გავლენების მოსაპოვებლად. მოკლედ, რომ ვთქვათ, ამ ხერხს ის ახალი ტიპის სტრატეგიულ ომს უწოდებს. რუსეთი გამუდმებით ცდილობს სამიზნე აუდიტორიის ქსელების კომპრომეტაციას, რაც მათი ისეთი ინფორმაციების მოპოვებას გულისხმობს, რომელსაც შემდეგ გამოიყენებენ მათ დასაშინებლად, ან ფალსიფიკაციის მიზნებისთის, ან შანტაჟისთის და სხვა.

ზემოთ აღნიშნულ აგრესორ ქვეყანაში საკმაოდ მრავლად არის საინფორმაციო სააგენტოები, ტელე და რადიო მაუწყებლები, რომელიც საინფორმაციო კონფროტაციის სანდო და წარმატებულ საშუალებებს წარმოადგენენ. მაგალითისთის შეგვიძლია მოვიყვანოთ.: „Russia Today", სხვადასხვა ტორილები, ისეთი როგორიც არის „sputnik news" და ა.შ.

ინფორმაციის მანიპულაციისთის, რუსეთი საკმაოდ აქტიურად იყენებს დაქირავბულ მუშახელს, ე.წ. „ტროლების ქარხანას". ეს არის ღია არხებით ნებისმიერი თემისადმი რუსული განწყობების ასამაღლებელი მექანიზმი. მათი მცირე ნაწილის გამოაშკარავება 2012 წელს, ვიკილიქსმა მოახერხა. ესენი იყვნენ ახალგაზრდული ორგანიზაციები „Наши" და „Молодая гвардия Единой Росии". მაგალითად.: The Internet Research Agency (IRA) იგივე Trolls from Olgino - გახლავთ ანაზღაურებადი ტროლების ერთერთი უმსხვილესი დაჯგუფება, რომელიც

რუსეთის მთავრობის მიერ ფინანსდება. ისინი ძირითადად პროსამთავრობო დანიშნულებით მუშაობენ, ერთვებიან სხვადასხვა დისკუსიაში სახელმწოფოს სასარგებლოდ. ხოლო ძირითად მიზანს წარმოადგენს რუსეთის მიმართ ნეგატიურად განწყობილი აუდიტორიის წინააღმდეგ ბრძოლა.

რუსული ტროლინგის მიზანი ყოველთვის არ გახლავთ სამიზნე აუდიტორიის დარწმუნება რაიმე სახის კონკრეტული ქმედების სისწორეში, არამედ მათი მიზანი ყალბი ინფორმაციის ულევი ნაკადის წარმოქმნა წარმოადგენს სოციალურ მედიაში. რომელიც მიზნად ისახავს სხვადასხვა სახის ეჭვის გაჩენას, შიშს, არასტაბილურობის გაცდის შექმნას და ა.შ. კიდევ ერთი ინსტრუმენტი - ინტერნეტ ბოტები - ეს გახლავთ აპლიკაცია, რომელიც ინტერნეტში კონტენტის ავტომატურად გავრცელებისთის არის შექმნილი. აპლიკაციის საშუალებით ბოტი მისთვის სასურველი ინფორმაციის დამალვის შესაძლებლობას იძლევა და საერთოდ, რეალური წყაროს მოძიება, შეუძლებელი გახადოს.

კონტენტი, რომლის გავრცელებასაც ემსახურება ზემოაღნიშნული საშუალებები, წარმოადგენს ცრუ და ნამდვილი ინფორმაციის ნაზავს, რომელიც მიმართულია სამიზნე აუდიტორიის დაბნევის, დემორალიზაციისა და მასზე გავლენის მოპოვებისაკენ. სამიზნე აუდიტორიას წარმოადგენს საკუთარი მოსახლეობა, სხვა ქვეყნის მოსახლეობის გარკვეული ჯგუფები, ქვეყნის შიდა და სამიზნე ქვეყნების პოლიტიკური ელიტა. პროპაგანდის გავრცელების არხები მრავალფეროვანია და მოიცავს სატელევიზო და რადიო არხებს, ბოტებს და ტროლებს სოციალურ მედიაში, ოპტიმიზირებულ საძიებელ სისტემებს, მოსყიდულ ჟურნალისტებს საზღვარგარეთის მედიაში და სხვა.

სასურველი ინფორმაციის გავრცელება, მათ შორის უკვე არსებულზე კონტროლის განხორციელება, მინიმუმ სამი მიმართულებით ხორციელდება. ესენია[30].:

1. დაინტერესების ქვეყანაში მართადი საკომუნიკაციო სივრცის, სამაუწყებლო არხების შექმნა და სოციალურ ქსელებში დომინირება პოლიტიკური თუ ეკონომიკური არასტაბილურობის განცდის დათესვის მიზნით;

2. პრორუსული პოლიტიკური პარტიების თუ ჯგუფების საინფორმაციო მხარდაჭერის კობერარხების შექმნა პრორუსული ელიტის ჩამოყალიბებების მიზნით; განწყობის დანერგვა, რომ პრორუსული ძალები შესაძლოა მოხვდნენ პარლამენტში ან მთავრობის ფორმირებაში მიიღონ მონაწილეობა;

3. სოცილური ქსელებისა თუ კიბერსივრცის სხვ სეგმენტის გამოყენება ძირგამოთხრილი საქმიანობისთვის, განსაკუთრებით მეზობლებთან ურთიერთობის კონტექსტში, რამაც შესაძლოა დააზიანოს სტრატეგიულ პარტნიორებთან ან მეზობელ სახელმწიფოებთან ურთიერთობები და აგრესიის შემთხვევაში გაართულოს პოლიტიკური თუ სხვა სახის მხარდაჭერის მიღება.

მეტი თვალსაჩინოებისთვის, რუსეთის სახელმწიფო თუ სხვა მასთან ასოცირებული აქტორების მხრიდან, საინფორმაციო-ფსიქოლოგიურ მაგალითს წარმოადგენს რუსეთი პოლონეთის წინააღმდეგ, 2014-2015 წლებში წარმოებული საინფორმაციო კონფრონტაცია, რომლის უმეტესი ნაწილი კიბერ არხებით მიმდინარეობდა[31] .

დავიწყოთ თავიდან. 2014 წელი. უკრაინის მოვლებენის პარალელურად, პოლონეთის სახელმწიფო საიტებზე, მათ შორის პრეზიდენტის და ვარშავის საფონდო ბირჟის გვერდებზე დაიწყო მასშტაბური ჰაკერული და DDOS[32] შეტევები. სადაც პასუხისმგებლობა აიღო „კიბერ-

[30] ანდრო გოცირიძე - რუსეთის კიბერაქტივობები - მზარდი საფრთხე საქართველოსთის.
[31] Russia's hybrid war against Poland - https://jamestown.org/program/russias-hybrid-war-against-poland/
[32] https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

ბერკუტმა“ და მიზეზად პოლონეთის უკრაინისადმი მხარდაჭერა დაასახელა. პოლონეთი მოწინავე ქვეყანა გახრდათ ევროპაში, რომელმაც მხარი დაუჭირა უკრაინას რუსეთთან წინააღმდეგობის მიმართებაში. ასევე, პოლონეთი გახლავთ ის ერთერთი ქვეყანა ხუთიდან, რომელმაც საქართველოს მხარდაჭრა გამოუცხადა რუსეთთან ომის დროს. სწორედ ეს გახლავთ ძირითადი მიზეზები რუსული ჰიბრიდული ომისა პოლონეთის მიმართ.

როგორც აღვნიშნე, რუსული „საინფორმაციო კონფრონტაციის[33]“ ერთერთ მიმართულებას, ძირგამომთხრელი საქმიანობის მიზნით, სოც. ქსელებისა და ზოგადად კიბერ სივრცის გამოყენება წარმოადგენს, განსაკუთრებით კი პარტნიორ ქვეყნებთან ან/და მეზობელ ქვეყნებთან მიმართებაში. რამაც შესაძლო არის გამოიწვიოს ურთიერთობების შესუსტება და სხვა.

2013 წლის ინვისში. სოციალურ ქსელ, YouTube-ში გავრცელდა რამდენიმე ვიდეო, რომელიც გახრდათ მუქარის შემცელი[34]. ოფიციალურად, ქართული მხარის მონაცემებით, ატვირთული იყო აფხაზეთიდან, მალაიზიაში წინასწარ მომზადებული დაშიფრული სერვერის მეშვეობით. ვიდეოები ატვირთა სამარ ჩოკუტაევმა, რომელიც ყირგიზეთს მოქალაქე გახლავთ. ვიდეოში ნახსენები მუქარა მიმართული გახლდათ როგორც ქართველი ჯარისკაცების მიმართ, ასევე საქართველოს ხელისუფლების და მისი მოქალაქეების მისამართით. მსგავსი ფაქტი მოხდა 2015 წელს, ამერიკაში „კიბერხალიფატის“ სახელით, სოციალურ ქსელებში გამოჩნდა ამერიკელი ჯარისკაცების მონაცემები. ამავე პერიოდში მათი ოჯახის წევრებმა მიიღეს მუქარის შემცველი წერილები. აღნიშნული ფაქტის გარკვევის შემდეგ დადგინდა, რომ ეს ფაქტი მოხდა ჯიჰადისტების საფარქვეშ, რუსული სამთავრობო სტრუქტურებიდან. ეს გახლავთ დაჯგუფება - APT28/Fancy

[33] Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.

[34] ჯიჰადის ვიდეოს საქმე - https://www.radiotavisupleba.ge/a/jihadis-videos-sakme-gakhsnilia/25125703.html

Bear[35], რომელიც ასევე პასუხისმგებელია ამერიკის შეერთებული შტატების საპრეზიდენტო არჩევნების დროს კიბერშეტევებზე. ასევე, იგივე ტექნოლოგიით, მსგავსი ფაქტი ამავე წელს, საფრანგეთში განხორციელდა.

ხშირ შემთხვევაში ხდება შეფარების უწყებების გამოყენება, false flag ოპერაციები და სხვა ფარული ღონისძიებები. კრემლთან დაახლოვებული ან/და დაფინასებული ორგანიზაციები, სახელმწიფო ინტერესებთან არის სრულ თანხედრაში, და გართულებული ატრიბუციის[36] პირობებში, აწარმოებენ კიბერ ოპერაციებს DDOS შეტევებიდან, კიბერ შპიონაჟის რთული ფორმებითა თუ დეზინფორმაციის კამპანიებთ.

რუსულ კიბერ ოპერაციებში, მნიშვნელოვან როლს ასრულებენ ეს დაჯგუფებები.: APT 28 (Fancy Bear) და APT 29 (Cozy Bear)[37]. ეს დაჯგუფებები ასოცირდებიან რუსეთის გენშტაბის სამხედრო დაზვერვასთან. ეს უკანასკნელნი პასუხისმგებელნი არიან ამერიკის შეერთებული შტატების საპერზიდენტო არჩევნებში ჩარევაში. ისინი ინფორმაციებს ეუფლებოდნენ დემოკრატიული პარტიის სერვერებიდან (ე.წ. DNC Hack). არსებული მონაცემებით ირკვევა, რომ APT 29-ს სერვერებზე წვდომა დაახლოვებით 1 წლის განმალობაში ჰქონდა. (იგულისხმება ჩატები, ელ ფოსტა და ა.შ). სარწმუნოა, რომ რუსეთის ამგვარი ჩარევა შესაძლოა მიზნად ისახავდეს დემოკრატიული პროცესებისა თუ ზოგადად არჩევნების ინსტიტუტის დისკრედიტაციას.

და ბოლოს, როდესაც კიბერის ფსიქოლოგიურ ასპექტებზე ვსაუბრობთ, უნდა აღვნიშნოთ საქართველოს მაგალითიც. 2019 წლის ოქტომბერში, საქართველოში განხორციელდა

[35] - APT 28 (იგივე FANCY BEAR, Sofacy, Pawn Storm) - რუსული წარმოშობის კიბერაქტორი, რომელიც აქტიურია 2000-იანი წლების შუა პერიოდიდან და პასუხისმგებელია საჰაერო სივრცეზე, თავდაცვის და ენერგეტიკის სფეროებსა თუ სახელმწიფო და მედიასექტორზე განხორციელებულ კიბერთავდასხმებზე.

[36] - ატრიუცია - მიკუთვნება; კიბერშეტევის ანონიმურ ავტორთა დადგენა.

[37] APT 29 (Cozy Bear) - APT 29 (იგივე CozyDuke ან COZY BEAR) - რუსული ჰაკერული დაჯგუფება, რომელმაც ახლო წარსულში განახორციელა წარმატებული კიბერშეტევები თეთრ სახლზე, სახელმწიფო დეპარტამენტზე და აშშ-ის გაერთიანებულ შტაბებზე.

კიბერშეტევა. აღნიშნული შეტევა მალევე მოექცა მსოფლიოს ყურადღების ქვეშ, აქედან გამომდინარე, აშშ-მ, ბრიტანეთმა, ნატოს წევრმა ქვეყნებმა ერთხმად დაადანაშაულეს რუსეთი საქართველოზე კიბერთავდასხმაში. კიბერ თვდასხმამ როგორც სამთავრობო, ისე არასამთავრობო ორგანიზაციების საიტების დეფეისმენტი გამოიწვია. აქვე, არსებობს რამდენიმე ტელევიზიის სამაუწყებლო პერიოდის შეფერხების ფაქტებიც.

საიტებზე მთავარ გარეკანზე, საქართელოს ექს პრეზიდენტის, მიხეილ სააკაშვილის ფოტო წარწერით.: I'll back იყო გამოსახული. ამ გარემოებამ გარკვეულწილად საზოგადოებაში შიშის და მათ შორის, სახელმწიფო სტრუქტურების მიმართ, ნდობის მოშლა გამოიწვია. ბრიტანეთის საგარეო სამინისტროს განცხადებაში ეს თავდასხმა, კვალიფიცირებულია როგორც საქართველოს სუვერენიტეტის წინააღმდეგ მიმართული აქცია.

აღნიშნული ჯგუფი, რომელსაც უწოდებენ სანდვორმს (Sandworm), პარტნიორები რუსულ სამხედრო დაზვერვასთან გადიან კვალზე. ის ასევე დაკავშირებულია უკრაინის, ბრიტანეთის და ამერიკის შეერთებული შტატების სამთავრობო თუ კერძო სექტორებზე თავდასხმებში[38]. მიუხედავად აღნიშნული პრობლემის უმოკლეს დროში მოგვარებისა, ეს ფაქტი ერთის მხრივ ხაზს უსვამს, რომ ჩვენი კრიტიკული ინფრასტრუქტურა ძალიან მოწყვლადია, მეორე მხრივ კი ადასტურებს მოსაზრებას, რომ გარკვეულ პირობებში, დაბალტექნოლოგიურმა შეტევებმაც კი შესაძლოა გამოიწვიოს არაპროპორციული ზარალი. შეგრძნება და ასევე შესაძლოა მოხდეს სახელმწიფო დემოკრატიის რწმენის უნდობლობა.

[38] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

კიბერსივრცის გამოყენება თანამედროვე კონფლიქტებში

გეოპოლიტიკური და გეოსტრატეგიული გარემოს ანალიზი აჩვენებს, რომ ამჟამად ხდება როგორც ფილოსოფიის, ისე ომის ხელოვნების რეფორმირება, პროცესები, რომლებიც გამოწვეულია ახალი ტექნოლოგიების გამოყენებით, რაც კონფლიქტების დროს სხვადასხვა ინტენსივობისა და სხვადასხვა სტრატეგიის გამოყენების საშუალებას იძლევა. ეს ახალი მეთოდები, კონფლიქტისა და უსაფრთხოების ტრადიციულ გაგებასთან ერთად, ხშირად მოიხსენიება, როგორც "კიბერ ომი".

კონცეფცია არ არის სრულიად ახალი, რომელიც წარმოადგენს ომის ჩვეულებრივი და არატრადიციული / არარეგულარული მეთოდების ერთობლიობას, რომელიც სცილდება ბრძოლის ველს და მოიცავს დაპირისპირების ეკონომიკურ, დიპლომატიურ, ინფორმაციულ და პოლიტიკურ მეთოდებს[39]. ეს კონცეფცია, პირველ რიგში, დაფუძნებულია არატრადიციული სამხედრო საშუალებებით დისტანციურ ობიექტებზე და პროცესებზე მიზნობრივი ზემოქმედების უნარზე, განსაკუთრებით იმ პროცესებსა და ობიექტებზე, რომლებიც კრიტიკულია სახელმწიფოს და შეიარაღებული ძალების ფუნქციებისთვის. როგორც ასიმეტრიული მიდგომა, კიბერსივრცის გამოყენება მიზნად ისახავს ფართომასშტაბიანი შედეგების მიღწევას მოკრძალებული საშუალებების გამოყენებით, როგორიცაა მტრის სამხედრო ოპერაციების შეფერხება ან მოსახლეობის მხრიდან პოლიტიკური მხარდაჭერის აღკვეთა[40]. ზოგადად კონფლიქტებში ეგრეთ წოდებული რბილი მოქმედებები კოორდინირებულია უფრო ჰოლისტიკური სტრატეგიის გამოყენებით, რომელიც სხვადასხვა ეტაპზე (დაწყება, მწვავე ფაზა, გადაწყვეტა) განსხვავდება ინტენსივობის მიხედვით და რომელიც მიზნად ისახავს შიდა და გარე პროცესების დესტაბილიზაციას. საბოლოო მიზანია მოცემული სახელმწიფოს დასუსტება ეკონომიკური

[39] Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly* 52 2009: 34-39.

[40] Keir Giles, The Next Phase of Russian Information Warfare (Riga: NATO Strategic Communications Centre of Excellence, 2016, http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.

დესტაბილიზაციის სტიმულირებით, მოსახლეობის იმედგაცრუებისა და უკმაყოფილების გამოწვევით, კონტროლირებადი და უკონტროლო მიგრაციის პირობების შექმნა, სამოქალაქო წინააღმდეგობის წარმოშობა და კრიტიკული ინფრასტრუქტურის შელახვა. თანამედროვე მაგალითებია უკრაინა[41], საქართველო[42] და ევროკავშირის ზოგიერთ ქვეყანა, ბოლოდროინდელი და მიმდინარე საომარი მოქმედებებით[43].

ამჟამად, არ არსებობს უნივერსალური ნორმა-განმარტება, რომელიც ასახავს "კიბერსივრცის" კონცეფციას. საერთაშორისო ხელშეკრულებები იყენებენ "საინფორმაციო სივრცის" კონცეფციას, როგორც საქმიანობის სფეროს, რომელიც დაკავშირებულია ინფორმაციის ფორმირებასთან, შექმნასთან, ტრანსფორმაციასთან, გადაცემასთან, გამოყენებასთან, შენახვასთან და აქვს გავლენა, მათ შორის ინდივიდუალურ და საზოგადოებრივ ცნობიერებაზე, საინფორმაციო ინფრასტრუქტურაზე და თავად ინფორმაციაზე. ამრიგად, "საინფორმაციო სივრცე" განმარტებულია, როგორც "საინფორმაციო რესურსების, საინფორმაციო სისტემებისა და ტექნოლოგიების ერთობლიობა, საინფორმაციო და საკომუნიკაციო ინფრასტრუქტურა, რომელიც უზრუნველყოფს ორგანიზაციებსა და მოქალაქეებს შორის ინფორმაციის ურთიერთქმედებას, ასევე მათი ინფორმაციის საჭიროებების დაკმაყოფილებას".

ყოველივე ზემოაღნიშნულის გათვალისწინებით, დასახული ამოცანის შესასრულებლად, სასარგებლო ჩანს ამერიკელი სპეციალისტების ჯგუფის მოსაზრების დათანხმება

---

[41] Volodymyr P. Gorbulin, Oleksandr S. Vlasiuk, Ella M. Libanova, Oleksandra M. Liashenko, *Donbas and The Crimea: The Value of Return* (Kyiv: National Institute of Strategic Studies, 2015); Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts

[42] David J. Smith, "Russian Cyber Capabilities, Policy and Practice," *inFocus Quarterly* (Winter 2014), www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities/

[43] See, for example, Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773-816, https://doi.org/10.1080/01402390.2016.1273830.

კიბერუსაფრთხოების სფეროში კრიტიკული ტერმინოლოგიის საფუძვლების შესწავლით[44]. ამ ექსპერტების აზრით, "კიბერსივრცე" არის ინფორმაციის სივრცის ნაწილი და არის "ელექტრონული (მათ შორის ფოტოელექტრონული და ა.შ.) გარემო (რომლის მეშვეობითაც ხდება ინფორმაციის შექმნა, მიღება, შენახვა, დამუშავება და განადგურება").

ზემოაღნიშნულიდან გამომდინარე, კიბერ სივრცეში სახელმწიფო უზენაესობის სამი ძირითადი სფეროა:

ინფორმაციის შეგროვების, გადაცემის, შენახვისა და დამუშავების ელექტრონული გარემო, რომელიც ჩამოყალიბებულია კომპიუტერული ტექნოლოგიის ქსელებით, საკომუნიკაციო და საკომუნიკაციო საშუალებების ქსელებითა და ინფორმაციის შესანახი საშუალებების ქსელებით, რომლებიც მდებარეობს ეროვნულ ტერიტორიაზე;

ICT, რომელიც განსაზღვრავს ელექტრონული გარემოს გამოყენების მეთოდებსა და გზებს კიბერსივრცის კონკრეტული სუბიექტის (მოქალაქე, ორგანიზაცია, საჯარო ხელისუფლება, ასევე შეიარაღებული კონფლიქტის სუბიექტები, ასევე კრიმინალური, მათ შორის ტერორისტული) ორგანიზაციების საჭიროებების დასაკმაყოფილებლად. ინფორმაციის შეგროვებით, გადაცემით, შენახვით, მიღებით ან გავრცელებით;

ადგილობრივი ან განაწილებული საინფორმაციო სისტემები, სისტემები წარმოების ავტომატური მართვისა და ადამიანური საქმიანობისათვის.

კონფლიქტების მიზანია მონაწილე აქტორებმა გავლენა მოახდინოს ოპონენტებზე ინტეგრირებული ადაპტირებული და ასიმეტრიულად სინქრონიზებული დესტრუქციული საშუალებებით, რაც მათზე გავლენას მოახდენს მრავალგანზომილებიან სივრცეში და ცხოვრების სხვადასხვა სფეროში. მთავარი მიზნებია საზოგადოებაზე კონტროლის აღება,

[44] Russia – US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013. http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russiau_s_bilateral_on_terminology_rus.pdf

ადამიანების მენტალიტეტზე გავლენის მოხდენა, ადამიანების მანიპულირება, რომლებიც პასუხისმგებელნი არიან სახელმწიფოში მნიშვნელოვანი გადაწყვეტილებების მიღებაზე.

ტექნოლოგია არ არსებობს თავისთავად, არამედ როგორც ცენტრალური ინსტიტუტებისადმი ნდობის შესამცირებლად უფრო ფართო და სტრატეგიულად შემუშავებული კამპანიის ნაწილი. თავდაპირველი მიზანი იყო უკრაინის მთავრობისადმი სამოქალაქო ნდობის დაკარგვის პირობების შექმნა საინფორმაციო კამპანიის განხორციელებით, რომელიც მიზნად ისახავდა სახელმწიფო ძალაუფლების, უკრაინის შეიარაღებული ძალების ხელმძღვანელობის დისკრედიტაციას და კრიმინალური და სეპარატისტული საქმიანობის გაფართოებას. ამ საინფორმაციო კამპანიამ გამოიწვია ქვეყანაში სოციალურ-პოლიტიკური დესტაბილიზაცია და კვლავაც უარყოფით გავლენას ახდენს ახლაც[45].

ამ სტრატეგიამ წარმატებით მოახდინა ინოვაციური კიბერ ტექნოლოგიების ინტეგრირება ადგილზე ფრთხილად დაგეგმილ არატრადიციულ და არარეგულარულ ძალებთან, რამაც 2014 წელს გამოიწვია ყირიმის ანექსია და სამხედრო კონფლიქტი სამხრეთ -აღმოსავლეთ უკრაინაში.

საომარი მოქმედებების კვლევისა და ანალიზის კომბინაცია აჩვენებს, რომ კიბერთან დაკავშირებული საქმიანობა და ინფორმაციული ომი ფართოვდება როგორც სპექტრის თვალსაზრისით, ასევე მეომარებისთვის ღირებულების თვალსაზრისით. უკრაინის ილოვაისკში და დებალცევოში ბრძოლას წინ უძღოდა საინფორმაციო სივრცეში აქტივობის მნიშვნელოვანი ზრდა. ფართოდ გავრცელდა ნეგატიური ინფორმაცია უკრაინის შეიარაღებული ძალების ძირითადი ჩინოვნიკების და მთავრობის წარმომადგენლების შესახებ (როგორც წესი, ნეგატიური ინფორმაციის გავრცელება წინ უძღოდა ახალი

[45] Jānis Bērziņš, “Russia’s new generation warfare in Ukraine: Implications for Latvian Defense Policy,” Policy Paper no. 02 (Riga: Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014).

სამხედრო კამპანიის დაწყებას)[46]. მასიური პრაქტიკა, რომელსაც დუგანი კიბერ აგრესიას უწოდებს, ავსებს დეზინფორმაციით და ყალბი ფრონტით ინტერნეტში[47].

2015 წლის თებერვალში დებალცევში ყველაზე ინტენსიური მოქმედებების დროს ონლაინ საინფორმაციო ნაკადების შინაარსობრივი ანალიზი და მოდელირება InfoStream სიახლეების მონიტორინგის ტექნოლოგიის გამოყენებით[48] აჩვენებს ამპლიტუდის რყევებს იმ ხარისხზე, რაც კრიტიკულია შეტყობინებების გავრცელებისთვის.

მედიის ანალიზმა აჩვენა - კიბერ აგრესია მთავრობის მთავარ ფიგურებზე, სავარაუდოდ, ხელს უწყობს ნეგატიური ინფორმაციის ნაკადების გაფართოებას, რაც მიზნად ისახავს არსებული სამოქალაქო უნდობლობისა და ანტისახელმწიფოებრივი ქცევის გაღრმავებას. როდესაც ასეთი ინფორმაცია აღწევს სოციალურ მედიას, ყალბი და მავნე ინფორმაციის გავრცელება ხელს უწყობს რწმენებს და ქცევებს, რომლებიც ჩვეულებრივ შეზღუდული იქნება არსებული სოციალური ზნეობებითა და სოციალური მოლოდინებით. მაშინაც კი, თუ ინფორმაცია არ იწვევს რწმენის ცნობიერ ცვლილებას, მას შეუძლია გავლენა მოახდინოს მომავალი ინფორმაციის ინტერპრეტაციაზე, შექმნას ეფექტური ფონი და დასაყრდენი ინტერპრეტაციისთვის.[49] ამან შეიძლება შემატოს ადგილობრივი აგრესორის სურათი, რომელსაც სურს გავლენა მოახდინოს კონფლიქტის მიმდინარეობაზე, რათა შეასუსტოს თავდასხმის ქვეშ მყოფი მთავრობის მხარდაჭერა. ზოგიერთ შემთხვევაში, ასეთი საინფორმაციო ომს შეუძლია შეცვალოს კინეტიკური ოპერაციები, შეარყევს თავდაცვითი კამპანიები მათ დაწყებამდე.

---

[46] http://colonelcassad.livejournal.com/2474409.html

[47] Duggan, "Strategic Development of Special Warfare in Cyberspace." NEWS | Oct. 1, 2015. https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyber/

[48] InfoStream – ახალი ამბების მონიტორინგის ტექნოლოგია, http://infostream.ua

[49]Elizabeth Stoycheff and Erik C. Nisbet, "Priming the Costs of Conflict? Russian Public Opinion About the 2014 Crimean Conflict," International Journal of Public Opinion Research (2016): edw020. https://doi.org/10.1093/ijpor/edw020

კიბერ აგრესია ხშირად მალავს თავის ავტორს და მოტივებს ტექნოლოგიური მეთოდების მოსასხამის ქვეშ, რომელსაც შეუძლია შენიღბოს მათი მანიპულაციური მიზნები. დამალვის მეთოდები მოიცავს ხელისუფლებისადმი ანონიმურ პრეტენზიებს, სიახლეებით ნახევრად სიმართლეებით მანიპულირებულ ამბებს, შეტყობინებების გამეორებას, ინფორმაციის გადატვირთვას, ფსევდო კიბერ ოპერაციებს (მთავრობა მოქმედებს როგორც მეამბოხე), "მაჯის თოჯინების" გამოყენებას (მთავრობის აგენტები, რომლებიც მოქმედებენ როგორც ონლაინ კომენტატორები) და ასტროტურფინგი (შექმნა ყალბი მოძრაობა).[50]

უკრაინაში, 2014 წლის შემდეგ ამგვარი ქმედებების შედეგებმა გამოიწვია შეიარაღებული ძალების დისკრედიტაცია, უკმაყოფილება და უნდობლობა, მიმართული ძირითადად სახელმწიფოს მთავარი სამხედრო და პოლიტიკური ხელისუფლების წინააღმდეგ, ეჭვები სამხედრო მოქმედებების აუცილებლობაში, სამოქალაქო მორალის დაზიანებაში და სამხედრო მოსამსახურეთა შორის დეზერტირების წახალისებაში. მედიის დამოკიდებულება არასაიმედო ან ყალბ წყაროებზე,ნეგატიურმა ამბებმა და შეიარაღებული ძალების ხელმძღვანელობის ქმედებების კრიტიკამ ხელი შეუწყო მტრის საინფორმაციო კამპანიას.[51] რუსულმა ძალებმა შეძლეს უკვე არსებული დაუცველობის გამოყენება სოციალურ, პოლიტიკურ და ეკონომიკურ სისტემაში, რათა გამოიწვიოს ღია კონფლიქტი და ამგვარი ოპერაციების კულმინაცია დაემთხვა დონბასში კინეტიკური ოპერაციების დაწყებას 2014 წელს. კიბერ აქტივების გამოყენება გახდა ძალაუფლების პროექციის ფორმა, რომელმაც ხელი შეუწყო კრიზისების გაჩენას შორს და წინა ხაზზე, შექმნა უფრო რთული კრიზისების ფორმები, რომლებიც შეეხო ინფრასტრუქტურას, საბანკო სისტემას, პოლიტიკურ ხელმძღვანელობას და არა მხოლოდ ფრონტზე მებრძოლ შეიარაღებულ ძალებს. ხაზები. ისევ და ისევ, ტრადიციული სამხედრო კონფლიქტის გაფართოება არ არის ახალი

[50] Duggan, “Strategic Development of Special Warfare in Cyberspace.”

[51]Sazonov, Müür and Mölder, eds., Russian Information Campaign Against the Ukrainian State and Defence Forces https://www.researchgate.net/publication/313259170_Russian_Information_Operations_Against_the_Ukrainian_State_and_Defence_Forces_April-December_2014_in_Online_News

სტრატეგია, მაგრამ ახალი ტექნოლოგიები იძლევა როგორც საშუალებებს, ასევე დაუცველობას, რაც საშუალებას მისცემს ასეთი ოპერაციების განხორციელებას მასშტაბით, რომელიც აქამდე არ იყო და აგრესორის მხრიდან რესურსების დაბალი ხარჯებით.

დესტრუქციული ინფორმაციის და კიბერ გავლენის განეიტრალების ღონისძიებებია:

· ინტერნეტ რესურსების მფლობელების გაფრთხილება (თუ ცნობილია) ყალბი, არაზუსტი ინფორმაციის გავრცელებასთან დაკავშირებული შეზღუდვების შესახებ, მისი წაშლის რეკომენდაციით, თუ ინფორმაცია საზიანოა ეროვნული უსაფრთხოების სუბიექტებისა და ობიექტებისთვის (პიროვნება, საზოგადოება და სახელმწიფო)

· არასანდო / საეჭვო რესურსების საჯარო რეესტრების შექმნა.

თანამედროვე ტექნოლოგიებმა შეცვალა მტრის ძალებზე ზემოქმედების უნარი, რამაც გამოიწვია მენეჯმენტისა და დაცვის გავლენის რბილი და სამხედრო მეთოდების რეორგანიზაციის აუცილებლობა, მათ შორის პერსონალის მომზადება საბრძოლო მზადყოფნის განუწყვეტლივ შესანარჩუნებლად. სხვადასხვა ქვეყნების გამოცდილება ადასტურებს, რომ ეროვნული უსაფრთხოების და თავდაცვის მაღალი დონე უნდა შენარჩუნდეს გლობალური ეკონომიკური კრიზისის პირობებშიც კი და მნიშვნელოვნად შემცირდეს სამხედრო

ბოლო ათწლეულის სამხედრო კონფლიქტების გამოცდილება გვიჩვენებს, რომ სტრატეგიული უპირატესობა აქვს ერთ – ერთ აქტორს, რომელმაც პირველმა გაიგო და დაიწყო ახალი ტექნოლოგიების გამოყენება, რომელსაც შეუძლია გამოიყენოს ისინი თავიანთი შესაძლებლობების გასაძლიერებლად და შესაბამისად, შეუძლია უპირატესობას მიაღწიოს უმაღლეს ტრადიციულ ძალებზე - და ხშირად სტაბილური რეაქციების პროვოცირების გარეშეც კი. მოწინავე ტექნოლოგიური სისტემების გამოყენება შესაძლებელს გახდის სახელმწიფოს უკვე არსებული სამხედრო პოტენციალის ეფექტურობის გაზრდას. ეროვნული უსაფრთხოების კონცეფციებისა და ეროვნული სამხედრო სტრატეგიების

გათვალისწინებით, ტექნოლოგიურად განვითარებული სახელმწიფოები პრიორიტეტს ანიჭებენ განათლებას და მეცნიერებას, როგორც იარაღს ტექნოლოგიურად ინტენსიური საომარი საშუალებების შესაქმნელად, ინოვაციური კონტროლის ტექნოლოგიების გამოყენებაში და ხელს შეუწყობს სწრაფ და დამაჯერებელ გამარჯვებას მიმდინარე და მომავალ სამხედრო კონფლიქტებში.

გამოწვევები ნატოსთვის

ნატო აღიარებს, რომ ჰიბრიდული ომი არის სტრატეგია, რომლის გაგებაც და სწავლა უნდა დაიწყოს. ნატომ განსაკუთრებული ყურადღება უნდა მიაქციოს იმ როლს, რასაც კიბერ ოპერაციები ასრულებენ ჰიბრიდულ სტრატეგიებში.

ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლში ნათქვამია, რომ "შეიარაღებული თავდასხმა ნატოს ერთ -ერთ, ან რამდენიმე წევრზე, ევროპაში ან ჩრდილოეთ ამერიკაში, განიხილება როგორც თავდასხმა ყველა წევრზე". ამიტომ, ალიანსი მიიღებს "ისეთ ქმედებებს, რასაც საჭიროდ ჩათვლის, მათ შორის შეიარაღებული ძალის გამოყენებას, ჩრდილო ატლანტიკური რეგიონის უსაფრთხოების აღდგენისა და უსაფრთხოების უზრუნველსაყოფად". კიბერშეტევებთან დაკავშირებით მე-5 მუხლთან დაკავშირებით პირველი საკითხი არის დავა იმაზე, თუ რამდენად არის კიბერშეტევები „შეიარაღებული თავდასხმები“[52]. თუ კიბერშეტევები არ შეიძლება ჩაითვალოს ძალადობრივად[53] მაშინ მათი

[52] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 3.

[53] იხილეთ: Rid, *Cyber War Will Not Take Place.*

"შეიარაღებული თავდასხმის" სტატუსი საკამათოა. თუ კიბერშეტევა არ განიხილება შეიარაღებულ თავდასხმად, მაშინ ასეთი მოვლენა ავტომატურად არ იწვევს იმ რეაქციულ პროცესს, რომელსაც საფუძვლად დაედო ევროპის უსაფრთხოება მეორე მსოფლიო ომის შემდეგ. თუმცა, ეს თვალსაზრისი საკამათო გახდა 2007 წელს ესტონეთის წინააღმდეგ კიბერშეტევების შემდეგ. ნატოს გენერალურმა მდივანმა იენს სტოლტენბერგმა კიდევ ერთხელ დაადასტურა, რომ ნატო კიბერშეტევებს განიხილავს მე-5 მუხლის მოვალეობის შემსრულებელი ქმედების განხორციელების სულისკვეთებით.[54] ეს ასახავს შეერთებული შტატების ცალმხრივ პოზიციას[55].

როგორ უნდა გამართლდეს სამხედრო პასუხი მე-5 მუხლის კიბერშეტევაზე, იმის გათვალისწინებით, რომ ატრიბუციის პროცესი (როგორც აღწერილია რიდისა და ბუკენანის მიერ) მოითხოვს დროს, ინვესტიციას და მრავალმხრივ მიდგომას პასუხის გასაცემად. კიბერ შეტევაზე შეიარაღებული რეაგირების ლეგიტიმურობის შესახებ შეთანხმების შემთხვევაშიც კი, ნატოს მეთაურების ნდობა მათ ქმედებებში მაინც დაეფუძნება შეცდომებისადმი მიკუთვნებულ მეცნიერებას. უფრო მეტიც, ნატოს გაუჭირდება გადამწყვეტი რეაგირება, თუ კიბერშეტევის განხორციელებაში ეჭვმიტანილ მოწინააღმდეგეს აქვს ჩამონტაჟებული უნარი უარყოს თავისი მონაწილეობა, როგორც ეს მოხდა რუსეთის და ასადის რეჟიმის შემთხვევაში სირიაში. თუ კიბერ ოპერაციები განხორციელდებოდა ჩვეულებრივი სამხედრო ოპერაციების პარალელურად (როგორც საქართველოში 2008 წელს), მე -5 მუხლზე დაფუძნებული ქმედებები სრულად იქნება გამართლებული.

---

[54] Paul McLeary, "NATO Chief: Cyber Can Trigger Article 5," *Defense News*, 25 March 2015, доступно на www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930 (по состоянию на 23 января 2016).

[55] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, 31 May 2011, доступно на http://www.wsj.com/articles/SB10001424052702304563104576355623135782718

ნატო-ს წევრები, განსაკუთრებით შეერთებული შტატები და გაერთიანებული სამეფო, განახორციელებენ ყველაზე დიდ ინვესტიციებს კიბერ ოპერაციებში. თუმცა, ეს არის სახელმწიფოები, რომლებიც მკაცრად შეზღუდულია არატრადიციული ტაქტიკის ღია გამოყენება. ლიბერალური დემოკრატიული პრინციპები, მათ შორის კანონის უზენაესობა, მთავრობის ანგარიშვალდებულება და გამჭვირვალობა, ზღუდავს ამ სახელმწიფოებს მშვიდობიან დროს არატრადიციული ოპერაციების გამოყენებისგან.

რუსეთი დიდი ხანია ადანაშაულებს დასავლეთს უაღრესად საკამათო სტრატეგიების გამოყენებაში, რომელსაც დასავლელი მეცნიერები ახლა რუსეთს მიაწერენ. ტიმოტი ლ. თომასის აზრით, რუსი თეორეტიკოსები დიდი ხანია განიხილავენ საბჭოთა კავშირის დამარცხებას, როგორც საიდუმლო საინფორმაციო ომის შედეგს.[56]

მუხლი 5 ნატო და მისი გამოყენება კიბერშეტევის შემთხვევაში "

კიბერ საფრთხეები და თავდასხმები უფრო გავრცელებული, დახვეწილი და დამანგრეველი ხდება. ალიანსი მუდმივად ცვალებადი კომპლექსური საფრთხის ლანდშაფტის წინაშე დგას. კიბერშეტევები ბოლო დროს ჰიბრიდული ომის ნაწილი იყო. ნატო და მისი მოკავშირეები ეყრდნობიან ძლიერ და გამძლე კიბერ თავდაცვას, რათა შეასრულონ ალიანსის ძირითადი მისიები კოლექტიური თავდაცვის, კრიზისების მართვისა და საერთო უსაფრთხოებისათვის. ნატო მზად უნდა იყოს დაიცვას თავისი ქსელები და ოპერაციები მზარდი კიბერ საფრთხეებისა და თავდასხმებისგან. სანამ ნატო მუშაობს კიბერუსაფრთხოების უფრო ყოვლისმომცველ პოლიტიკაზე, მისი ამჟამინდელი სტრატეგია ორი ძირითადი გამოწვევის წინაშე დგას:

[56] Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in Cyberpower and National Security, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles: Potomac Books, 2009), 477

1. არსებული გეგმა კიბერშეტევებს ათავსებს ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლისა და კოლექტიური დაცვის კონცეფციის

2. ნატოს კიბერუსაფრთხოების სტრატეგია ამჟამად მკაცრად თავდაცვითი ხასიათისაა. თავდაცვითმა ზომებმა შეიძლება შეაფერხოს ინდივიდუალური კიბერშეტევა, მაგრამ ისინი არ აღმოფხვრიან პირველადი საფრთხეს, რადგან კიბერშეტევებისგან მდგრადი და გრძელვადიანი დაცვის ყველაზე ეფექტური გზა არის შეურაცხმყოფელი (და, შესაბამისად, პრევენციული) შესაძლებლობები.

მოკლედ გადავხედოთ როგორ განვითარდა ნატოს კიბერ სივრცესთან დაკავშირებული საკითხები 2007 წლიდან:

2007 - ნატომ შეიმუშავა ნატოს კიბერ თავდაცვის პოლიტიკა;
2008 - ალიანსმა შეიმუშავა ნატოს კიბერ თავდაცვის კონცეფცია;
2008 წელი - ბუქარესტში ნატოს სამიტის დეკლარაციაში სახელმწიფოთა და მთავრობათა მეთაურებმა მიიღეს კიბერ თავდაცვის პოლიტიკა. ამ სამიტზე შეიქმნა ნატოს ორი ახალი კიბერშეტევის ერთეული:

• ოპერატიულ დონეზე, ბრიუსელში კიბერ თავდაცვის მენეჯმენტის ოფისის შექმნა (CDMA), რომელსაც აქვს ერთადერთი პასუხისმგებლობა ნატოს შტაბბინაში კიბერ თავდაცვის კოორდინაციაზე და მასთან დაკავშირებულ სარდლებსა და სააგენტოებზე;

• თანამშრომლობის კიბერ თავდაცვის ბრწყინვალების ცენტრი ტალინში, ესტონეთი; 2013 წელი - ნატოს ხუთი ქვეყანა (კანადა, დანია, ნიდერლანდები, ნორვეგია და რუმინეთი) შეთანხმდნენ ითანამშრომლონ კიბერ თავდაცვის შესაძლებლობების განვითარების მრავალეროვნულ პროექტზე. ქვეყნები „გააუმჯობესებენ ტექნიკური ინფორმაციის გაცვლას;

ზოგადი საფრთხის გაცნობიერება; და შეიმუშავეთ მოწინავე კიბერ თავდაცვის სენსორები ”. 2013 წელი - გამოქვეყნდა ტალინის გზამკვლევი საერთაშორისო სამართლისათვის კიბერ ომისათვის. ეს 300 გვერდიანი სახელმძღვანელო დაიწერა მკვლევართა ჯგუფის მიერ ნატო-ს ერთობლივი კიბერ თავდაცვის ცენტრის მოწვევით ტალინში, ესტონეში.

”პროექტი სახელწოდებით ტალინის სახელმძღვანელო 2.0; 2015 წელი - განხორციელდა შემდეგი ძირითადი აქტივობები:

• "დახურული ფარები 2015"

• "კიბერ კოალიცია 2015"

• CyCon 2015 - კიბერ კონფლიქტის მე -7 კონფერენცია;

2016 წელი - ევროპარლამენტის პლენარულმა სხდომამ მიიღო დირექტივა ქსელებისა და ინფორმაციული სისტემების უსაფრთხოების შესახებ („NIS დირექტივა“), რომელიც არის კიბერუსაფრთხოების პირველი პანევროპული წესი;

2016 წელი - ვარშავის სამიტზე მოკავშირეებმა აღიარეს კიბერ თავდაცვა, როგორც ახალი საოპერაციო ტერიტორია, ქსელების, მისიებისა და ოპერაციების უკეთ დაცვის მიზნით.

2017 - გამოქვეყნდა ტალინის გზამკვლევი 2.0 საერთაშორისო სამართლის შესახებ კიბერ ოპერაციებისთვის, ეს არის ყველაზე სრულყოფილი ანალიზი იმის შესახებ, თუ როგორ გამოიყენება არსებული საერთაშორისო სამართალი კიბერსივრცეში; 2017 წელი - ნატო და ფინეთი აძლიერებენ კიბერ თავდაცვის თანამშრომლობას;

2018 - იაპონიამ გადაწყვიტა შეუერთდეს ნატო -ს კიბერ თავდაცვის ბრწყინვალების ცენტრს ტალინში;

2018 - ავსტრალია და პორტუგალია შეუერთდნენ კოალიციურ კიბერ თავდაცვის ბრწყინვალების ცენტრს (CCDCOE) ტალინში. (ნატოს LibGuide, 2018)

როგორც აღვნიშნე, სანამ ალიანსი მუშაობს კიბერუსაფრთხოების უფრო სრულყოფილ პოლიტიკაზე, მისი ამჟამინდელი სტრატეგიით არის რამდენიმე ძირითადი გამოწვევა:

1. ახლანდელი გეგმა კიბერშეტევებს ათავსებს ჩრდილოატლანტიკური ხელშეკრულების მე -5 მუხლისა და კოლექტიური თავდაცვის კონცეფციის ფარგლებში, რითაც ქმნის მაღალი ზღურბლებს ჩართულობისათვის. (Roggeveen, 2017). შესაძლოა მე–5 მუხლთან დაკავშირებული ყველა საკითხი ნათელია კლასიკურ საოპერაციო რაიონებში (ხმელეთი, ჰაერი, ზღვა), მაგრამ როდესაც საქმე ეხება ახალ ოპერატიულ ზონას - კიბერნეტიკას, ბევრი პრობლემა ბუნდოვანი და ბუნდოვანი ხდება და საჭიროებს გადახედვას. მოდით განვსაზღვროთ ისეთი კითხვები, რომლებიც მოითხოვს უფრო ნათელ და ზუსტ გაგებას:

მე-5 მუხლის თანახმად, მხოლოდ "შეიარაღებულ თავდასხმას" შეუძლია კოლექტიური დაცვის განხორციელება. რა შეიძლება გამოიწვიოს კიბერშეტევამ, რომელიც გამოიყენებს მე-5 მუხლს? არავინ იცის, რადგან ეს არის სიტუაციურად დამოკიდებული.

ერთ-ერთი უახლესი და გასაოცარი მაგალითი იმისა, თუ როგორ გადავიდა კიბერშეტევები ტრადიციულ ომს სუსტი გავლენისა და იძულებითი პოლიტიკური ზეწოლის მიზნით - ახლახანს აშშ -ს კონგრესმა მხარი დაუჭირა რუსეთის წინააღმდეგ ახალ სანქციებს 2016 წლის აშშ -ის საპრეზიდენტო არჩევნებში ჩარევის გამო. მაშინდელი საპრეზიდენტო კანდიდატის დონალდ ტრამპის სასარგებლოდ.

კიბერშეტევების სისწრაფე და სიმდაბლე ართულებს მათი მასშტაბისა და ზემოქმედების სწრაფად განსაზღვრას; გარდა ამისა, უნდა მოხდეს თუ არა დაღვრის ან მესამეული ზემოქმედების ზემოქმედების შეფასება? ვინაიდან კიბერ შესაძლებლობები კვლავაც იქნება ეროვნული, შესაძლებელია, რომ ზოგიერთ წევრ სახელმწიფოს შეეძლოს სიმეტრიულად რეაგირება, ზოგი კი საჭიროებს ასიმეტრიულ პასუხებს. პროპორციულობის განაჩენი არის პოლიტიკური განაჩენი, რადგან ის მოითხოვს უფრო მოქნილ და ისტორიულად

დამოკიდებულ განსჯას, ვიდრე IF-THEN გამოთქმა კოდში. ასევე არსებობს შესაძლებლობა, რომ წევრ სახელმწიფოს შეეძლოს მკვეთრი რეაგირება კიბერშეტევისას.

2. გარდა ამისა, ის საშუალებას იძლევა გამოყენებულ იქნას ძირითადად თავდაცვითი და რეაქტიული ზომები, რაც ნაკლებ ადგილს ტოვებს პრევენციული ან შეტევითი ოპერაციებისთვის. ალიანსის კიბერუსაფრთხოების სტრატეგია ამჟამად მკაცრად თავდაცვითი ხასიათისაა. ნატოს კომპიუტერული ინციდენტების რეაგირების სისტემა (NCIRC) იცავს ალიანსის საკუთარ ქსელებს და მხარს უჭერს მოკავშირეებს მათ ინდივიდუალურ კიბერ თავდაცვაში დაზვერვის შეგროვებითა და გაზიარებით, მაღალი მზაობის კიბერ თავდაცვის გუნდების გამოყენებით და მოკავშირე ქვეყნებისთვის სამიზნეების შემუშავებით, რათა ხელი შეუწყოს ეროვნულ კიბერ თავდაცვას. დაცვის შესაძლებლობები და ინვესტიცია განათლებაში, სწავლებაში და განხორციელებაში.

მიუხედავად იმისა, რომ ნატოს წევრთა ეროვნული ქსელების დაცვა პრიორიტეტული უნდა იყოს, კიბერშეტევებისგან მდგრადი და გრძელვადიანი დაცვის უზრუნველსაყოფად ყველაზე ეფექტური გზა არის შეტევითი შესაძლებლობების გამოყენება და მოწინააღმდეგეთა ქსელებისა და სისტემების დარღვევა.

ნატოს კიბერუსაფრთხოების პოლიტიკამ უნდა უზრუნველყოს მკაფიო საფუძველი გადაწყვეტილებისათვის შეტევითი კიბერ ოპერაციების დაუდგენელ ტერიტორიასთან დაკავშირებით. (Roggeven, 2017) და რა არის გამოსავალი?

1. ნატომ უნდა შექმნას ახალი თანამედროვე საზოგადოებრივი დოქტრინა (კოლექტიური თავდაცვის კონცეფციის გარდა), რომელიც მოიცავს შემდეგ საკითხებს: • "შეიარაღებული თავდასხმის" კონცეფცია მკაფიოდ უნდა იყოს განსაზღვრული კიბერ სფეროსთვის. სხვა სიტყვებით რომ ვთქვათ, მან უნდა აღწეროს რას წარმოადგენს

თავდასხმა, რომელიც აკმაყოფილებს მე -5 მუხლის მოთხოვნებს და რა საპასუხო ქმედებები განხორციელდება;

ალიანსმა უნდა იპოვოს მკაფიო გზა "კიბერ მუხლის მე-5" ღონისძიებასთან გასამკლავებლად. აუცილებელია გადახედოს რა არის მე-5 მუხლი და შეიარაღებული თავდასხმა თანამედროვე მსოფლიოში. ყველაზე დიდი გამოწვევა არის შეზღუდვების (ფიზიკური და კიბერნეტიკური) საერთო გაგების მიღწევა, რამაც შეიძლება აიძულოს წევრი სახელმწიფო გამოიყენოს მე -5 მუხლი და განსაზღვროს რას ნიშნავს პროპორციულობა საპასუხოდ. გადაწყვეტილებები პოლიტიკური ხასიათისაა და მოითხოვს სტრატეგიული კიბერსივრცის მყარ გაგებას და მის განვითარებას ჩართული პოლიტიკური აქტორების მხრიდან. საბოლოო ჯამში, წარმატება იქნება დამოკიდებული იმაზე, თუ როგორ არის შერწყმული კიბერნეტიკა ტრადიციულ პოლიტიკურ და სამხედრო ძალაუფლებასთან. (ლიმნელი, 2016) გარდა ამისა, კიბერშეტევების შეფასების „ინდივიდუალური“ მიდგომა უნდა გადაფასდეს და უნდა შეიქმნას ერთიანი ბარიერი კიბერშეტევის „შეიარაღებული თავდასხმის“ კვალიფიკაციისათვის. შედეგად, ის ალიანსს საშუალებას მისცემს მიიღოს უფრო გადამწყვეტი, „რაოდენობრივი“ და ამდენად უფრო ყოვლისმომცველი გადაწყვეტილებები, როდესაც მოკავშირეს კიბერშეტევა მოჰყვება.

ალიანსმა უნდა ჩამოაყალიბოს ჩარჩო, რომელიც საშუალებას მისცემს მოკავშირეებს იმოქმედონ არა მხოლოდ თავდაცვითი, არამედ შეტევითი მიმართულებით: კიბერუსაფრთხოების მიმდინარე განვითარება მოითხოვს უფრო პროაქტიულ მიდგომას. კიბერ საფრთხეების დასაძლევად, ნატომ უნდა გამოიყენოს უფრო ფართო და დინამიური ოპერატიული ჩარჩო, ვიდრე კოლექტიური თავდაცვა. როდესაც ნატოს მოწინააღმდეგეების კიბერ შესაძლებლობები უფრო დახვეწილი ხდება, ალიანსმა უნდა მიიღოს კიბერუსაფრთხოების პოლიტიკა, რომელსაც შეუძლია ეფექტურად გაუმკლავდეს ამ საფრთხეებს. (Roggeveen, 2017)

ნატომ უნდა უზრუნველყოს, რომ მას აქვს თანამედროვე კიბერ შესაძლებლობები და, რაც მთავარია, შეინარჩუნოს ნდობა: რომ დარჩეს საიმედო თავდაცვის ალიანსად, ნატოს უნდა ჰქონდეს საიმედო კიბერპოლიტიკა, მათ შორის კიბერ შეკავება, თუმცა, ამის გაკეთება კიბერ სივრცეში ახლა უფრო რთულია. ეს საკითხები უნდა იქნას განხილული მკაფიო, თანმიმდევრული (შესაძლოა საჯარო) პოლიტიკით, რომელიც მოიცავს მკაფიოდ მითითებას ალიანსის მიერ განხორციელებული ყველა კიბერ აქტივობისა.

დასასრულს, ეს არის ძალიან მოკლე პოლიტიკა, რომელიც უფრო დეტალურად უნდა იქნას განხილული ზოგადი კონტექსტისა და სხვა საკითხების გათვალისწინებით. მიუხედავად ამისა, ჩვენ შეგვიძლია დარწმუნებით ვთქვათ, რომ ამ პრობლემების გადალახვა მოკავშირე ქვეყნების საზოგადოებას საშუალებას მისცემს შეიმუშაოს საჭირო ჩარჩო კიბერუსაფრთხოების მიმდინარე საფრთხეების ამომწურავი წინააღმდეგობის გაწევისთვის.

სახელმწიფოს უსაფრთხოება დიდწილად დამოკიდებულია ვირტუალურ სივრცეში პოლიტიკური, ეკონომიკური და სოციალური ფუნქციების განხორციელების უნარზე.

1. კიბერსივრცეში (მათ შორის სამხედრო მიზნებისთვის) საქმიანობის სფეროში ტერმინოლოგია შემუშავებასა და დამტკიცებას საჭიროებს.

2. კიბერსივრცეში მოქმედებები სხვადასხვაგვარად აღიქმება სხვადასხვა სამთავრობო უწყებებისა და სამსახურების წარმომადგენლების მიერ.

3. ჟურნალისტიკაში ზოგადად მიღებული ტერმინი "კიბერ -ომი" შეუსაბამოა ოფიციალურ დოკუმენტებსა და სამეცნიერო ლიტერატურაში გამოსაყენებლად.

კიბერსივრცე და სამხედრო კონფლიქტები: დოქტრინალური მიდგომები ტერმინოლოგიაზე

კიბერუსაფრთხოების პრობლემების გააზრების ნებისმიერი მცდელობა ხელს უშლის საერთო ტერმინოლოგიური ბაზის არარსებობას. ამ მხრივ, აუცილებელია მკაფიოდ გამოვყოთ კიბერსივრცე და საინფორმაციო სივრცის ცნებები; კიბერუსაფრთხოება და, მეორე

მხრივ, ინფორმაცია და ინფორმაციულ-ფსიქოლოგიური უსაფრთხოება (ისევე როგორც ნებისმიერი სხვა სახის საქმიანობა, რომლის საბოლოო მიზანია გავლენა მოახდინოს ადამიანზე, ადამიანთა ჯგუფებზე ან მთლიანად საზოგადოებაზე საინფორმაციო და საკომუნიკაციო ტექნოლოგიების საშუალებით).

საინფორმაციო სივრცის გამოყენება გონებაზე ზემოქმედებისათვის არ არის ექვივალენტი და არც კი არის პირდაპირ კავშირში ICT– ის გავლენით პროგრამულ უზრუნველყოფასა და აპარატურაზე, საინფორმაციო და საკომუნიკაციო ქსელებზე, ასევე ამ ქსელებში გადაცემულ ინფორმაციაზე. ამ მიზეზით, შემოთავაზებულია განხორციელდეს ფუნდამენტური განსხვავება კიბერ სივრცეში მოქმედებებსა და ინფორმაციულ სივრცეში მოქმედებებს შორის ობიექტ-სამიზნე კრიტერიუმის მიხედვით. დამხმარე განმსაზღვრელი არის კიბერსივრცის ტერმინების და კიბერსივრცეში სპეციალური ქმედებების სავალდებულო დაკავშირება ICT– სთან, ან უფრო ზუსტად, ელექტრონულ გარემოსთან, რომელშიც ნებისმიერი ქმედება ინფორმაციის და ურთიერთქმედების ხორციელდება ციფრული სიგნალების გამოყენებით.

გარდა ამისა, როგორც ჩანს, ლოგიკურად გამართლებულია „კიბერსივრცის“ კონცეფციის ამოსავალი წერტილი. ამ დროისთვის არ არსებობს კონსენსუსული განმარტება, მიუხედავად ამისა არსებული მოვლენების გამოყენებით სესაძლებელია მივიღო განმარტება, რომელიც აკმაყოფილებს სამ შეზღუდულ კრიტერიუმს:

1) განსახილველი კონცეფციის შევიწროვება ელექტრონულ გარემოზე, საინფორმაციო სივრცისგან განსხვავებით, რომელშიც შესაძლებელია ურთიერთქმედება როგორც ელექტრონულ, ისე ნებისმიერ სხვა გარემოში;

2) ელექტრონული გარემოსა და რადიო სპექტრში ინფორმაციის ურთიერთქმედების "კიბერსივრცის" განსაზღვრებიდან გამოყოფა, რომელიც ხორციელდება ანალოგური სიგნალების საშუალებით;

3) ინტერნეტთან დაკავშირებულ ქსელებთან და აღჭურვილობასთან მისი სავალდებულოობის უარყოფა, რაც შეუსაბამოდ ავიწროებს „კიბერსივრცის“ განმარტებას. კიბერსივრცის კონცეფციის ინტერნეტთან დაკავშირების მიდგომა გამოიყენება ბევრ საერთაშორისო დოკუმენტში, კერძოდ, საერთაშორისო სტანდარტში ISO / IEC 27032: 2012. თუმცა, ასეთი განმარტებები შეუმჩნეველია ინტერნეტიდან იზოლირებული კიბერსივრცის სეგმენტები, როგორიცაა სამრეწველო კონტროლის სისტემები, დახურული სამხედრო ქსელები და ა.შ.

დასავლეთ-აღმოსავლეთის ინსტიტუტისა და მოსკოვის სახელმწიფო უნივერსიტეტის ინფორმაციული უსაფრთხოების პრობლემების ინსტიტუტის (IPIB) ექსპერტთა ჯგუფმა კიბერსივრცე განსაზღვრა როგორც „ელექტრონული (მათ შორის ფოტოელექტრონული და ა.შ.) გარემო, რომლის მეშვეობითაც ხდება ინფორმაციის შექმნა, გადაცემა, მიღება, შენახვა, დამუშავება და განადგურება“.

ამ მიდგომის საფუძვლად შეიძლება გამოყენებულ იქნას კიბერსივრცის შემდეგი განმარტება: კიბერსივრცე არის ელექტრონული გარემო, რომელშიც ინფორმაციის შექმნა, შენახვა, მოდიფიკაცია, გადაცემა და მოცილება ხორციელდება ციფრული სიგნალების გამოყენებით.

რაც შეეხება ტერმინს "კიბერ ომი"- ეს ტერმინი არის შეცდომაში შემყვანი და არასწორი ოფიციალური ტერმინოლოგიის მიზნებისათვის, მთავარი მიზეზი იმაში ჩანს, რომ ის მიმართავს „ომის“ კონცეფციას, რომელიც არ შეიძლება გამოყენებულ იქნას თვითნებურად და უნდა ემყარებოდეს მკაფიო სამართლებრივ განსაზღვრებას. იმავდროულად, ომისა და სამხედრო კონფლიქტის არც ერთი განმარტება, რომელიც მოყვანილია სამხედრო დოქტრინაში, მათი ამჟამინდელი ფორმით, არ შეიძლება გამოყენებულ იქნას კიბერსივრცეში მოქმედებებზე.

ამასთან დაკავშირებით, ნათქვამია, რომ "კიბერ ომის" კონცეფცია შეიძლება გამოყენებულ იქნას არაოფიციალურ კომუნიკაციაში - მასმედიაში, ჟურნალისტიკაში და ზეპირ გამოსვლებში, მაგრამ არ არის შეიარაღებული ძალების და რუსეთის ფედერაციის სახელმწიფო ორგანოების ოფიციალური ტერმინოლოგიის ნაწილი.

თუ ჩვენ შევეცდებით ჩამოვაყალიბოთ კიბერსივრცეში დაპირისპირების უმაღლესი ეტაპის განმარტება, აუცილებელია გავითვალისწინოთ შესაძლო კრიტერიუმები ასეთი კონცეფციის არსებითი მახასიათებლების იდენტიფიცირებისათვის. პრინციპში, ჩვენ შეგვიძლია ვისაუბროთ მინიმუმ სამ კრიტერიუმზე:

1. მიზნის დასახვის კრიტერიუმი: თუ ჩვენ ვაშენებთ დაპირისპირების გრადაციას მასში მონაწილე მხარეების მიზნების შესაბამისად, მაშინ მისი უმაღლესი ფორმის თვისება - ომი - არის ომის სპეციალური, პოლიტიკური მიზნებისკენ სწრაფვა. თუმცა, საეჭვო ჩანს, რომ ასეთი მიდგომა შეიძლება გამოყენებულ იქნას კიბერსივრცეში დაპირისპირებაზე. უპირველეს ყოვლისა, სახელმწიფოს მოტივაცია შეიძლება მნიშვნელოვნად განსხვავდებოდეს მედიატორის მოტივაციისგან, რომელიც მოქმედებს როგორც დაპირისპირების უშუალო მონაწილე.

კიბერ სივრცეში კონფრონტაციებში შუამავალი მსახიობების მონაწილეობა ასევე არ ჯდება ომის ამ გაგებაში და ანონიმურობის პრობლემის ხარჯზე. სანამ სახელმწიფო ვერ შეძლებს მტრის იდენტიფიცირებას, მას არ შეუძლია დასახოს და მიაღწიოს პოლიტიკურ მიზნებს მასთან მიმართებაში - მათ შორის ომის მიზნებს. ეს საკითხი ჯერ არ არის გადაწყვეტილი.

ამ მიდგომის კიდევ ერთი შეზღუდვაა კიბერ სივრცეში დაპირისპირების ასიმეტრიული ხასიათი მისი მონაწილეების ICT ინფრასტრუქტურაზე დამოკიდებულების ხარისხის მიხედვით. მაგალითად, შეერთებულ შტატებსა და ჩრდილოეთ კორეას შორის კიბერ სივრცეში დაპირისპირების შემთხვევაში, ამ უკანასკნელის მოტივაცია შეიძლება

შეესაბამებოდეს ომის პოლიტიკურ მიზნებს. ამავდროულად, აშშ -ის ომის მიზნები მისი მოწინააღმდეგის წინააღმდეგ აშკარად ვერ ხერხდება კიბერსივრცეში, ვინაიდან ჩრდილოეთ კორეა საკმარისად არ არის დამოკიდებული ICT- ზე თავისი ეკონომიკისა და სამხედრო პოტენციალის თვალსაზრისით. შედეგად, ომის კონცეფციას არ შეუძლია ადეკვატურად აღწეროს ასეთი დაპირისპირება, რადგან ის შეუსაბამო ხდება მისი ერთ -ერთი მხარისთვის.

2. საერთაშორისო სამართლებრივი კრიტერიუმი: კიბერსივრცეში კონფრონტაციის უმაღლესი ფორმის განსაზღვრის კონსტრუირება საერთაშორისო კრიტიკაში "აგრესიის" კონცეფციის განსაზღვრის კრიტერიუმების საფუძველზე, პირველ რიგში გაეროს დოკუმენტებში, მათ შორის გაეროს გენერალური რეზოლუციის 3314 1974 წლის 14 დეკემბრის ასამბლეა "აგრესიის განსაზღვრა". დოკუმენტი განსაზღვრავს აგრესიას, როგორც "სახელმწიფოს მიერ შეიარაღებული ძალის გამოყენებას სხვა სახელმწიფოს სუვერენიტეტის, ტერიტორიული ხელშეუხებლობის ან პოლიტიკური დამოუკიდებლობის წინააღმდეგ ან სხვაგვარად შეუთავსებელია გაეროს ქარტიასთან".

ამ მიდგომის პრობლემა იმაში მდგომარეობს, რომ კიბერ სივრცეში შეიარაღებული ძალის გამოყენების კონცეფცია არ არის გადაწყვეტილი, ისევე როგორც შუამავალი აქტორების გამორიცხვა მისგან. ხსენებული რეზოლუციის მე -3 მუხლი უზრუნველყოფს ქმედებების კონკრეტულ ჩამონათვალს, რომლებიც კვალიფიცირდება როგორც აგრესია - რომელიც, თუმცა, არ მოიცავს კიბერსივრცეში მოქმედებებს.

3. "ბარიერის კრიტერიუმი": ზიანის ბარიერის განსაზღვრა, რომლის გადაჭარბება ნიშნავს კონფრონტაციის გადასვლას სამხედრო კონფლიქტის სტატუსზე. ეს მიდგომა უფრო ხშირად გამოიყენება კონფლიქტების არაფორმალური კლასიფიკაციისთვის. მაგალითად, მსოფლიოში ერთ -ერთი ყველაზე პატივცემული უსაფრთხოების კვლევითი ინსტიტუტი, SIPRI, იყენებს ტერმინს "ომი" იმ კონფლიქტებზე, რომლებშიც საბრძოლო მსხვერპლი აღემატება 1000 -ს წელიწადში; უფსალას უნივერსიტეტის (ფინეთი) ექსპერტები მიიჩნევენ,

რომ 25 – ზე მეტი ადამიანის საბრძოლო დანაკარგებით დაპირისპირება ყოველწლიურად არის „შეიარაღებული კონფლიქტი“.

ამრიგად, „კიბერ სივრცეში სამხედრო კონფლიქტი არის დაპირისპირება ორს ან მეტი მხარეს შორის, რომელიც შეიძლება იყოს როგორც სახელმწიფო, ასევე მოქმედი სახელმწიფოს მითითებით, შუამავალი აქტორები, რომლებიც ახორციელებენ სპეციალურ ქმედებებს და სპეცოპერაციებს კიბერსივრცეში, რომელთა შედეგები, პირდაპირ თუ შეგნებულად შესაძლებელია, მოიცავს ადამიანთა სიკვდილს რამაც სერიოზული ზიანი მიაყენა საშიში ძალების შემცველ საგნებს, ან სხვა სამოქალაქო და სამხედრო ინფრასტრუქტურის მასიური ფიზიკური განადგურება. ”

ასე რომ, ორ სახელმწიფოს შორის სამხედრო კონფლიქტის ფარგლებში სამხედრო ოპერაციების ჩატარების კონტექსტში (სახელმწიფოთა კოალიცია), კიბერნეტიკური გავლენა არის მიზანმიმართული და ორგანიზებული მტრის მოქმედება, რომელიც ხორციელდება აპარატურისა და პროგრამული უზრუნველყოფის გამოყენებით. კიბერ სივრცე არის აპარატურისა და პროგრამული უზრუნველყოფის ინსტრუმენტების ერთობლიობა, რომელიც გამოიყენება ავტომატიზირებულ სისტემებში სამოქალაქო და სამხედრო მიზნებისათვის. კიბერ ქმედებები, ჩემი აზრით, პირობითად შეიძლება იყოს დაკავშირებული რამოდენიმე დონის კიბერსივრცესთან, რომელშიც ისინი შემოდიან და სადაც ისინი ასრულებენ თავიანთ "ბინძურ საქმეს".

კიბერსივრცის პირველ დონეზე არის აპარატურა ინფორმაციის დამუშავებისა და გადაცემისათვის - კომპიუტერები და მათი პერიფერიული მოწყობილობები, აპარატურა მონაცემთა გადაცემისათვის და სხვა.

კიბერსივრცის მეორე ფენა არის პროგრამული უზრუნველყოფის კომპონენტები.

მესამე დონე არის შინაარსი, რომელზე წვდომაც და ცვლილებებიც, მტრის მიერ ტექნიკისა და პროგრამული უზრუნველყოფის გამოყენებით, კლასიფიცირდება როგორც კიბერ ზემოქმედების მესამე დონე.

ტექნოლოგიისა და სოციალური სისტემების ფუნდამენტურმა ცვლილებებმა, რომლებიც დაკავშირებულია კომპიუტერისა და საკომუნიკაციო ტექნოლოგიების ფართო გამოყენებასთან, არ შეიძლება გავლენა იქონიოს სამხედრო ოპერაციების მომზადებისა და ჩატარების თეორიასა და პრაქტიკაზე. ეს არის ცნობილი ნიმუში. ჩვენ ვხედავთ მის გამოვლინებას თითქმის ყოველდღე, ნებისმიერ თანამედროვე სამხედრო კონფლიქტში.

ასევე მნიშვნელოვანია სახელმწიფოს თავდაცვის მომზადების ასპექტი კიბერსივრცეში მისი ინტერესების დასაცავად. ტრადიციულად, სამხედრო ამოცანების გადაწყვეტის ტვირთი შეიარაღებულ ძალებს ეკისრებათ. თუმცა, მათი თანამედროვე შემადგენლობით, ნაკლებად სავარაუდოა, რომ მათ შეეძლოთ დამოუკიდებლად გაეწიათ აგრესორის წინააღმდეგ ბრძოლა ომში, როგორც ნაცნობ სფეროებში, ასევე კიბერსივრცეში. ამრიგად, დღეს მთავარი ამოცანაა ნათლად გვესმოდეს შესაძლო ომის ზოგადი ხასიათი.

კიბერსივრცე არ არის სტატიკური. ახალი ლოკალური ქსელები მუდმივად ჩნდება და კიდევ უფრო ხშირად იცვლება არსებული ქსელების კონფიგურაცია: ემატება ახალი სეგმენტები, პროგრამული უზრუნველყოფა იხვეწება ან იცვლება, ტერმინალური მოწყობილობების რაოდენობა იცვლება ამა თუ იმ მიმართულებით.

დასკვნა

კიბერ უსაფრთხოების ცოდნა და მისი გამოყენება ყოველდღიურ ცხოვებაში წარმოადგენს მსოფლიო წესრიგისა და სამოქალაქო საზოგადოების ჩამოყალიბების მნიშვნელოვან პროცესს. ბოლო პერიოდში, რაც უფრო მეტი კომპანია ან/და ორგანიზაცია გადადის ციფრულ მომსახურებებზე, მით უფრო იზრდება კიბერ უსაფრთხოების დარღვევის შანსები. კიბერ უსაფრთხოება გახლავთ ერთერთი ყველაზე სენსიტიური დაცვის პროცესი სხვადასხვა აქტორებისგან.: ჰაკერებისგან, კიბერ თაღლითებისგან და სხვა. დღევანდელ ეპოქაში ყოველდღიურად ხდება ახალი ტექნოლოგიების შექმნა ან უკვე არსებულის განახლება, რომელთა წყალობითაც ხდება მნიშვნელოვნად დიდი ინოფრმაციების გადინება, გაგზავნა, მიღება და ა.შ. ეს ყოველივე რათქმაუნდა დიდი რისკის ქვეშ დგას. ამიტომ, კიბერუსაფრთხოება მსოფლიოში ყველაზე მნიშვნელოვანი საკითხი გახდა. ნებისმიერი კიბეროპერაცია ჰიბრიდული თუ სხვა სრულმასშტაბიანი ომის ნაწილია.

კიბეროპერაციების ერთერთი მთავარი მიზანი სასურველი სამიზნე აუდიტორიისთვის ცნობიერების შეცვლას ემსახურება. მათი უმრავლესობა კი ფსიქოლოგიური ზემოქმედების მოხდენით ხორციელდება. ამის თვალსაჩინო მაგალითი კი მსოფლიოში ყველაზე აგრესორი ქყვეყანა - რუსეთი გახლავთ. ის პოლიტიკურად ნებისმიერ ინფორმაციას, განიხილავს როგორც ძალაუფლების ერთერთ მნიშვნელოვან წყაროს. გამუდმებით ცდილობს დაინტერესების ქვეყნის ქსელების კომპრომეტაციას, რაც მათი ისეთი ინფორმაციების მოპოვებას გულისხმობს, რომელსაც შემდეგ გამოიყენებენ სამიზნე აუდიტორიის დასაშინებლად, ან ფალსიფიკაციის მიზნებისთის, ან შანტაჟისთის და სხვა.

ბოლო პერიოდში, ჰაკერულმა თავდასხმება გადაინაცვლა სადაზღვეო და ჯანდაცვის სფეროში. ისინი შავ ბაზარზე გასაყიდად ეძებენ სენსიტიურ ინფორმაციას, რომელიც

ზოგიერთ შემთხვევაში შესაძლოა სახელმწიფო მნიშვნელობისაც კი იყოს. განსაკუთრებით რთულად სამართავია იმგვარი საფრთხეები, რომლებსაც ზურგს დესტრუქციული სახელმწიფო - რუსეთი უმაგრებს. სადაც ზღვარი, სახელმწიფოსა და კრიმინალურ აქტორებს შორის, დიდი ხანია წაშლილია.

დღევანდელი მონაცემებით, ყველაზე რეალურ კიბერსივრცის გამოყენება გულისხმობს ფინანსურ თაღლითობებს, ტერორისტული ორგანიზაციების მიერ სადაზვერვო ინფორმაციის შეგროვებას, გარკვეული სახის პროპაგანდას და ა.შ. ტერორისტული ორგანიზაციები საბედნიეროდ (ჯერჯერობით) არ ფლობენ ისეთ ძლიერ კიბერსაშუალებებს, რომ სერიზოული ზიანი მიაყენონ სამიზნე ობიექტს. თუმცა საჭიროა მათი კონტროლი და მუდმივი მზადება ასეთი ორგანიზაციებისგან თავდასაცავად.
უნდა აღინიშნოს, რომ კიბერ სივრცის დაცვა, მისი განვითარება და უსაფრთხოებისადმი სწრაფვა, მათ შორის ხელს უწყობს სახელმწოფოთა შორის მეგობრული და მშვიდობიანი ურთიერთობების ჩამოყალიბებასა და განვითარებას, ტექნოლოგიურ განვითარებასა და ახალი თავდაცვითი სისტემების დანერგვას.

გამოყენებული ლიტერატურა

1. ანდრო გოცირიძე - რუსეთის კიბერაქტივობები - მზარდი საფრთხე საქართველოსთის. https://www.gfsis.org/files/library/opinion-papers/95-expert-opinion-geo.pdf
2. ახალი ამბების მონიტორინგის ტექნოლოგია, http://infostream.ua
3. ვ. სვანიძე. პარიზის ტერაქტი და ახალი გამოწვევები საქართველოში. ვ.სვანიძე, ა. გოცირიძე. „კიბერ თავდაცვა; კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები“. საქართველოს თავდაცვის სამინისტრო, თბილისი, 2015წ. გვ. 210-214
4. ჯიჰადის ვიდეოს საქმე - https://www.radiotavisupleba.ge/a/jihadis-videos-sakme-gakhsnilia/25125703.html
5. A,Gotsiridze. Terrorist's Cyber Activities – a growing Threat. Scientific & practical cyber security journal, 2018. https://journal.scsa.ge/issues/2018/03/975
6. David J. Smith, "Russian Cyber Capabilities, Policy and Practice," *inFocus Quarterly* (Winter 2014), www.jewishpolicycenter.org/2013/12/31/russian-cyber-capabilities/
7. Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. Report, 2017
8. Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. www.dia.mil/military-power-publications
9. Defence Intelligence Agency. Russia Military Power - building a military to support great power aspirations. dia-11-1704-161. Report, 2017. ხელმისაწვდომია www.dia.mil/Military-Power-Publications
10. Defending Digital Democracy Project. Belfer Center for Science and International Affairs. Harvard Kennedy School. The State and Local Election Cybersecurity Playbook. 2018.
11. Defining cyber terrorism. Ruben Tuitel. Per concordiam - journal of european security and defense issues, vol. 7, issue 2, 2016. ISSN 2166-322x (print) ISSN 2166-3238 (online)
12. Defining cyber terrorism. Ruben Tuitel. Per concordiam - journal of european security and defense issues, vol. 7, issue 2, 2016. ISSN 2166-322x (print) ISSN 2166-3238 (online)

13. Dr Andrew Foxall. Putin's Cyberwar: Russia's Statecraft in the Fifth Domain. Russia Studies Centre Policy Paper No. 9 (2016). The Henry Jackson Society May 2016
14. Duggan, "Strategic Development of Special Warfare in Cyberspace." NEWS | Oct. 1, 2015. https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyber/
15. Duggan, "Strategic Development of Special Warfare in Cyberspace
16. the 2014 Crimean Conflict," International Journal of Public Opinion Research (2016): edw020. https://doi.org/10.1093/ijpor/edw020
17. Fire eye special report, 2014. APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. ხელმისაწვდომია https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf
18. Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Forces Quarterly* 52 2009: 34-39.
19. Hearing: World Wide Cyber Threats (Open).Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015.
20. https://www.csis.org/analysis/iran-and-cyber-power?fbclid=IwAR3iyUKkYWcKV7HEGF96CMC-FyHDyEMgMNK0qXtNvJCL45B8f3BfQmVKYe4
21. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Iran_Military_Power_LR.pdf
22. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and
23. https://www.cmu.edu/iso/aware/presentation/security101-robotics.pdf
24. https://ccdcoe.org/cyber-definitions.html
25. https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html
26. Keir Giles, The Next Phase of Russian Information Warfare (Riga: NATO Strategic Communications Centre of Excellence, 2016, http://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles.
27. Jānis Bērziņš, "Russia's new generation warfare in Ukraine: Implications for Latvian Defense Policy," Policy Paper no. 02 (Riga: Center for Security and Strategic Research, National Defence Academy of Latvia, April 2014).
28. Joint statement for the record to the Senate Armed Forces Comitee. Foreign cyber threat to the United States of America. January 5, 2017
29. Khatuna Mshvidobadze. Russian Military Preps Cyber Warriors. 25.04.2017. ხელმისაწვდომია http://www.cyberlightglobal.com/insight-blog/

30. Laura Galante, Shaun Eee. Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Atlantic Councis Issue Brief. September, 2018
31. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 3.
32. NATO Defense College "NDC Fellowship Monograph Series". Handbook of Russian Information Warfare. Fellowship Monograph 9 by Keir Giles. ISBN: 978-88-96898-16-1
33. Office of the Director of National Intelligence, Cyber Threat Intelligence Integration Center. Cyber Threats to Elections – a Lexicon. 2018
34. Paul McLeary, "NATO Chief: Cyber Can Trigger Article 5," *Defense News*, 25 March 2015, доступно на www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930 (по состоянию на 23 января 2016).
35. Rid, Cyber War Will Not Take Place.
36. Russia's hybrid war against Poland - https://jamestown.org/program/russias-hybrid-war-against-poland/
37. Russia – US Bilateral on Cybersecurity. Critical Terminology foundations. EastWest Institute Worldwise Cybersecurity Initiative, Moscow state university information security institute. November 2013. http://wiki.informationsecurity.club/lib/exe/fetch.php?media=documents_all:russiau_s_bilateral_on_terminology_rus.pdf Sazonov, Müür and Mölder, eds., Russian Information Campaign Against the Ukrainian State and Defence Forces https://www.researchgate.net/publication/313259170_Russian_Information_Operations_Against_the_Ukrainian_State_and_Defence_Forces_April-December_2014_in_Online_News
38. See, for example, Martin Kragh and Sebastian Åsberg, "Russia's Strategy for Influence through Public Diplomacy and Active Measures: the Swedish Case," *Journal of Strategic Studies* 40, no. 6 (2017): 773-816, https://doi.org/10.1080/01402390.2016.1273830.
39. Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, 31 May 2011, доступно на http://www.wsj.com/articles/SB10001424052702304563104576355623135782718
40. Statement for the record. worldwide threat assessment of the US intelligence community february 9, 2016
41. Statement for the record. World Wide Cyber Threats (Open). House Permanent Select Committee on Intelligence. Testimony of The Honorable James Clapper, Director of National Intelligence. September 10, 2015.
42. Timothy L. Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in Cyberpower and National Security, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles: Potomac Books, 2009), 477

43. Volodymyr P. Gorbulin, Oleksandr S. Vlasiuk, Ella M. Libanova, Oleksandra M. Liashenko, *Donbas and The Crimea: The Value of Return* (Kyiv: National Institute of Strategic Studies, 2015); Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts
44. Worldwide Threat Assessment of the US Intelligence Community. Daniel R. Coats, Director of National Intelligence. 13 February, 2018.
45. Великая Победа в Великой Войне" Патрушев Н. https://tass.ru/politika/1950207
46. Доктрина информационной безопасности Российской Федерации. Указ президента РФ от 05.12.2016
47. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.