ივანე ჯავახიშვილის სახელობის
თბილისის სახელმწიფო უნივერსიტეტი

მარიამ გიგაური

კიბერუსაფრთხოების როლი საერთაშორისო ურთიერთობებში: კიბერუსაფრთხოების გავლენა ნატოს დღის წესრიგის ტრანსფორმაციაზე

დიპლომატია და საერთაშორისო პოლიტიკა

სამაგისტრო ნაშრომი შესრულებულია დიპლომატიისა და საერთაშორისო პოლიტიკის მაგისტრის აკადემიური ხარისხის მოსაპოვებლად

თემის ხელმძღვანელი: ეკა აკობია
ასოცირებული პროფესორი
საერთაშორისო ურთიერთობების დოქტორი

თბილისი, 2018

ანოტაცია

კიბერსივრცე გახდა ერთ-ერთი განმსაზღვრელი მახასიათებელი თანამედროვე ცხოვრების. ინტერნეტქსელის გაჩენამ და ციფრული ინფრასტრუქტურის განვითარებამ მსოფლიოში თამაშის ახალი წესები დაამკვიდრა. კიბერუსაფრთხოება კი წარმოადგენს ბოლო ათწლეულის ერთ-ერთ ყველაზე მნიშვნელოვან გამოწვევას. რაც ყველაზე მნიშვნელოვანია, კიბერუსაფრთხოების უმთავრესი საკითხები პირდაპირ დაკავშირებულია ტექნოლოგიებთან. კვლევის მთავარ მიზანს წარმოადგენს შეისწავლოს კიბერ-უსაფრთხოების როლი საერთაშორისო ურთიერთობებში. კონკრეტულად, რა განაპირობებს დღევანდელ გლობალურ არენაზე კიბერუსაფრთხოების საკითხის დღის წესრიგის ერთ-ერთ მთავარ გამოწვევად დაყენებას და რა გავლენის მოხდენა შეუძლია კიბერ-უსაფრთხოების სფეროში მიმდინარე მოვლენებს მთლიან საერთაშორისო სისტემაზე?

ნაშრომში არსებული საკვლევი კითხვის შესაწავლა წარმოებს ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის მაგალითზე, კერძოდ, რამდენად მნიშვნელოვანი ადგილი უკავია კიბერუსაფრთხოებას ნატოს ძირითად დღის წესრიგში და რა გავლენას ახდენს კიბერ სივრციდან წარმოშობილი გამოწვევები ნატოს მისიასა და ძირითად ამოცანებზე? დასმულია საკვლევი კითხვა: როგორ შეცვალა კიბერუსაფრთხოების გამოწვევებმა ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის დღის წესრიგი 2002-2017 წლებში? წარმოდგენილია კვლევის მთავარი ჰიპოთეზა: საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებამ ნატოს სამხედრო-პოლიტიკური სტაბილურობა მოწყვლადი გახადა თანამედროვე გამოწვევების წინაშე და ალიანსის ძირითადი ამოცანების ტრანსფორმაცია განაპირობა. რაც შეეხება კვლევის მეთოდოლოგიას, მონოგრაფიულ გამოკვლევასთან ერთად გამოყენებულია კონტენტ და დისკურს ანალიზის მეთოდები. ნაშრომში თეორიულ ჩარჩოდ გამოყენებულია ლიბერული ინსტიტუციონალიზმი და ურთიერთდამოკიდებულების ლიბერალური თეორია.

ვფიქრობ, ნაშრომი სასარგებლო იქნება საერთაშორისო ურთიერთობებში კიბერ-სივრცისა და კიბერუსაფრთხოების საკითხებით დაინტერესებულ პირთათვის, და მათთვის, ვინც იკვლევს ნატოს განვითარების საკითხებს.

Abstract

Cyberspace has become an intrinsic feature of the modern world. The creation of the Internet and the rapid development of information and communication technologies resulted in dramatic changes in terms of new rules, practices and patterns of behaviour that were adopted in International Relations. It is worth mentioning that Cyber Security is one of the most serious global challenges of the past decade. In fact, the issue gains more significance due to further technological developments. The research intends to assess the impact and influence of Cyber Security on the International Relations; more precisely, it delves into factors that make Cyber issues top priority of states' agenda. Moreover, the paper examines how changes in the field of Cyber Security may affect whole International system.

The research is based and conducted on the example of the North Atlantic Treaty Organization; in particular, how important is the Cyber Security on NATO's main agenda and how does the challenges generated by the cyber space affect NATO mission and key tasks? The main research question is how Cyber Security challenges determined and changed the agenda of the North Atlantic Treaty Organization for 2002 – 2017 years. The paper testifies following hypothesis: The development of information and communication technologies has made NATO's military-political stability vulnerable to modern security challenges and has transformed the main tasks of the alliance.

As for methodology, the research work uses qualitative methods, based on analysis of relevant sources, research papers, academic journals, official government documents and etc. In order to make profound assessment the methods of content and discourse analysis will be used as well.

Regarding the theoretical framework the research relies on Liberal Institutionalism and Liberal Theory of Interdependence.

The given research can be particularly useful for scholars who are interested in cyberspace and Cyber Security issues and for those who deal with NATO development issues.

სარჩევი

1. შესავალი 6
   1.1. საკვლევი კითხვა და ჰიპოთეზა 8
   1.2. კვლევის მეთოდოლოგია 12
2. ოპერაციონალიზაცია: როგორ განვსაზღვოთ „კიბერუსაფრთხოება“ 13
3. ნატო, კიბერუსაფრთხოება და საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარება 18
   3.1. კიბერუსაფრთხოების სფეროში ნატოს ევოლუცია 2002-2017 წლებში და ალიანსის დღის წესრიგის ტრანსფორმაცია 23
   3.2. რა გავლენა მოახდინა მოახდინა 2007 წელს განხორციელებულმა კიბერ-თავდასხმამ ესტონეთის ტრანსფორმაციაზე? 27
   3.3. კიბერ-ომი საქართველოს წინააღმდეგ 32
   3.4. 2017 წლის მნიშვნელოვანი კიბერ-თავდასხმები 34
4. კიბერუსაფრთხოება და ალიანსის სწრაფად ცვლალებადი სამხედრო-პოლიტიკური გარემო 36
   4.1. ნატოს მიდგომა კიბერ-თავდაცვის მიმართულებით 37
   4.2. ნატოს კიბერუსაფრთხოებისა და თავდაცვის შესაძლებლობები 38
   4.3. თანამშრომლობა პარტნიორებთან 40
5. ლიტერატურის მიმოხილვა 42
6. თეორიული ჩარჩო 46
7. კიბერუსაფრთხოების გამოწვევები და ნატოს ტრანსფორმაციის უნარი - არის თუ არა ნატოს დღევანდელი როლი და აქტივობები საკმარისი? 51
8. დასკვნა 55
9. ბიბლიოგრაფია 60
10. დანართი 63

1. შესავალი

წინამდებარე ნაშრომის კვლევის სფეროს წარმოადგენს კიბერსივრცე, კონკრეტულად, ბოლო ორი ათწლეულის ერთ-ერთი ყველაზე მნიშვნელოვანი გამოწვევა - კიბერუსაფრთხოება. კიბერუსაფრთხოების როლსა და მნიშვნელობაზე საერთაშორისო ურთიერთობებში დიდი დებატები მიმდინარეობს. მიუხედავად იმისა, რომ ბოლო პერიოდში აღნიშნული საკითხის მიმართ ინტერესი და კვლევები საგრძნობლად გაიზარდა, პრობლემა სხვა საკითხებთან შედარებით ახალია და ნაკლებად არის შესწავლილი.

კიბერსივრცე გახდა ერთ-ერთი განმსაზღვრელი მახასიათებელი თანამედროვე ცხოვრების. ინტერნეტქსელის გაჩენამ და ციფრული ინფრასტრუქტურის განვითარებამ მსოფლიოში თამაშის ახალი წესები დაამკვიდრა. რაც ყველაზე მნიშვნელოვანია, კიბერუსაფრთხოების უმთავრესი საკითხები პირდაპირ კავშირშია ტექნოლოგიების განვითარებასთან. კიბერ-საფრთხეები და თავდასხმები უფრო და უფრო გავრცელებულ, დახვეწილ და საზაიანო ხასიათს იძენენ.

როგორც უკვე აღვნიშნე, კიბერსივრციდან მომდინარე გამოწვევებმა შეცვალა არამარტო ჩვეულებრივი ადამიანების ყოველდღიური ცხოვრება, არამედ სახელმწიფოებისა თუ ორგანიზაციების დღის წესრიგში მნიშვნელოვანი ადგილი დაიკავა. კიბერ-გამოწვევების აქტუალურობა პირდაპირ დაკავშირებულია ტექნოლოგიურ განვითარებასთან. საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებამ ჩვენს ყოველდღიურ ცხოვრებაზე მნიშვნელოვანი გავლენა მოახდინა და ჩვენი ცხოვრების განუყოფელ ნაწილად იქცა. ინტერნეტის ქსელის გაჩენამ და ტექნოლოგიების განვითარებამ კომპლექსურად ურთიერთდამოკიდებული მსოფლიო ერთმანეთზე კიდევ უფრო გადააჯაჭვა. ცალსახაა, რომ ტექნოლოგიურმა მიღწევებმა ჩვენი ცხოვრება უფრო გაამარტივა, გააადვილა საკომუნიკაციო ტრანზაქციები, მანძილისა და დროის ფაქტორი შეამცირა და, ერთი შეხედვით, ყველას

კეთილდღეობაში მნიშვნელოვანი წვლილი შეიტანა. თუმცა, მეორე მხრივ, აშკარად უფრო დიდი პრობლემებიც ჩანს. ციფრულ ტექნოლოგიებზე დამოკიდებულებამ როგორც ინდივიდები, ასევე ორგანიზაციები და რაც მთავარია, სახელმწიფოები უფრო მოწყვლადები გახადა ელექტრონული სივრციდან მომდინარე გამოწვევების წინაშე. უამრავ დადებით ფაქტორთან შედარებით, ციფრული ტექნოლოგიების განვითარებამ მრავალი პრობლემა და საშიშროება შესძინა კაცობრიობას (ამის დასამტიკცებლად, წინამდებარე ნაშრომში რამდენიმე მაგალითს განვიხილავთ და გავაანალიზებთ).

დღეს სახელმწიფოები კიბერ-ტექნოლოგიებს ისეთივე ლეგიტიმურ და საჭირო ნაწილად განიხილავენ თავიანთი სტრატეგიული ინსტრუმენტების ყუთში, როგორც დიპლომატიას, ეკონომიკურ სიძლიერესა და სამხედრო შესაძლებლობებს. ინტერნეტმა და კომპიუტერულმა ტექნოლოგიებმა ძალის ცენტრების უპრეცენდენტო ცვლილება გამოიწვია და ხელი შეუწყო ახალი საომარი სივრცის წარმოქმნას. შესაბამისად, შეიძლება თამამად ითქვას, რომ დღეს კიბერუსაფრთხოება წარმოადგენს საერთაშორისო გამოწვევას.

განსაკუთრებით ბოლო ათწეულია, რაც მსოფლიო ახალი საშიშროებებისა და გამოწვევების წინაშე აღმოჩნდა. კიბერუსაფრთხოება კი ერთ-ერთი ასეთი გამოწვევაა და აღნიშნულ სფეროში თანამშრომლობის აუცილებლობა დღის წესრიგში დადგა. მრავალი პოლიტიკური საკითხი ჩართულია კიბერუსაფრთხოებაში, განსაკუთრებით აღსანიშნავია მისი გავლენა საერთაშორისო ურთიერთობებზე, სადაც უკვე ძალიან შეამჩნევად არის გაზრდილი და კიდევ უფრო გაიზრდება მისი მნიშვნელობა. სწორედ საკითხის ასეთი აქტუალურობიდან გამომდინარე, გადავწყვიტე, რომ კვლევა მეწარმოებინა კიბერუსაფრთხოების ირგვლივ.

1.1. საკვლევი კითხვა და ჰიპოთეზა

წინამდებარე კვლევის მთავარ მიზანს წარმოადგენს შეისწავლოს კიბერუსაფრთხოების როლი საერთაშორისო ურთიერთობებში. კონკრეტულად, რამ განაპირობა კიბერუსაფრთხოების საერთაშორისო ურთიერთობების დღის წესრიგში ერთ-ერთ მთავარ გამოწვევად დაყენება და რა გავლენის მოხდენა შეუძლია კიბერ-საფრთხეებს ეროვნულ და საერთაშორისო უსაფრთხოებაზე? ნაშრომში არსებული საკვლევი კითხვის შესაწავლა წარმოებს ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის მაგალითზე, კერძოდ, რამდენად მნიშვნელოვანი ადგილი უკავია კიბერუსაფრთხოებას ნატოს ძირითად დღის წესრიგში და რა გავლენას ახდენს კიბერსივრციდან წარმოშობილი გამოწვევები ნატოს მისიასა და ძირითად ამოცანებზე? წინამდებარე ნაშრომი, ასევე, იკვლევს იმ გზას, რომელიც დროთა განმავლობაში ცვლიდა ნატოს გაგებას და დამოკიდებულებას „კიბერ“-ის მიმართ.

კიბერუსაფრთხოებამ ნატოს დღის წესრიგში ბოლო ორი ათწლეულია უმნიშვნელოდან მაღალი პრიორიტეტის მქონე გამოწვევებში გადაინაცვლა, და განსაკუთრებით, ბოლო წლებში, უკვე მის ერთ-ერთ უმთავრეს გამოწვევად იქცა. ნატო, რომელიც თითქმის 70 წელია სამხედრო-პოლიტიკური ხასიათის ორგანზიაციაა და მთავარი აქცენტი სწორედ მის სამხედრო შეიარაღებასა და სიძლიერეზე კეთდება, გვერდს ვერ აუვლიდა ტექნოლოგიურ განვითარებას. ახალი ტექნოლოგიური აღჭურვილობები დაინერგა ორგზანიზაციის სტრუქტურაშიც და მის მიერ წარმოებულ მისიებსა თუ სხვადასხვა ოპერაციებშიც გამოიყენება. ახალი ტექნოლოგიების განვითარებამ ხელი შეუწყო ალიანსს, მოეხდინა თავდაცვითი შესაძლებლობების მოდერნიზება და თანამედროვე გამოწვევებთან ადაპტირება. თუმცა, ერთი მხრივ თუ შევხედავთ, დავინახავთ, რომ ტექნოლოგიურმა რევოლუციამ და დიგიტალიზაციის პროცესმა ნატოს შესაძლებლობა მისცა ახალი გამოწვევების წინაშე უფრო მდგრადი, სწრაფი, მოდერნიზებული და წარმატებული გამხდარიყო. გამარტივდა როგორც ცალკეული წევრების, ასევე, მთლიანად ალიანსის სამხედრო თუ არასამხედრო სტრუქტურების მუშაობა. თუმცა,

მეორე მხრივ, ცხადია, რომ ტექნოლოგიური მიღწევებით არამხოლოდ ნატო სარგებლობს, არამედ მისი ხილული თუ უხილავი მტრებიც. შესაბამისად, მიმდინარეობს ბრძოლა არა სამხედრო შეიარაღების, არამედ ტექნოლოგიური შეიარაღების ზრდასა და სრულყოფაში. ვისაც სრულყოფილად განვითარებული ტექნოლოგიები ექნება, ის უფრო დაცულიც იქნება და მეტი წარმატების შანსსაც მოიპოვებს.

მაშასადამე, ზემოთ განხილული მსჯელობის შედეგად, ნათელია, რომ ტექნოლოგიური პროგრესი, ერთი მხრივ, ხელს უწყობს ნატოს თანამედროვე გამოწვევებთან ბრძოლასა და მათთან გამკლავებაში, აძლიერებს მას და შესაძლებლობას აძლევს მისი ყველა მიმართულება მოდერნიზებული და ადაპტირებული იყოს, მაგრამ, მეორე მხრივ, ვხედავთ, რომ ტექნოლოგიური რევოლუცია, ინფორმაციული და საკომუნიკაციო ტექნოლოგიების ზრდა პარალელურად აფერხებს და საფრთხეს უქმნის ნატოს, წარმატებით გაართვას თავი მის წინაშე არსებულ გამოწვევებს, რომლის მაგალითებსაც წინამდებარე ნაშრომში უფრო დეტალურად განვიხილავთ. აქედან გამომდინარე, საკვლევით თემის მიზანია, შეისწავლოს, თუ როგორ გავლენას ახდენს ტექნოლოგიური განვითარება ნატოს მიზნებისა და ამოცანების სრულყოფილად განხორციელებაზე. ნაშრომის მთავარი **საკვლევი კითხვა** კი შემდეგში მდგომარეობს: როგორ შეცვალა კიბერუსაფრთხოების გამოწვევებმა ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის დღის წესრიგი 2002-2017 წლებში?

ნაშრომში წარმოდგენილია **ჰიპოთეზა:** საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებამ ნატოს სამხედრო-პოლიტიკური სტაბილურობა მოწყვლადი გახადა თანამედროვე გამოწვევების წინაშე და ალიანსის ძირითადი ამოცანების ტრანსფორმაცია განაპირობა.

საკვლევ თემაში, **დამოუკიდებელ ცვლადად** წარმოდგენელია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარება და მათი სიძლიერე. ნაშრომში აღნიშნული ცვლადი შეიძლება სხვადასხვაგავარად იყოს გამოყენებული, ამიტომ,

მსურს რომ ზუსტად განვმარტო თუ რას ვგულისხმობ კიბერ-სივრცის საინფორმაციო და კომპიუტერულ ტექნოლოგიებში. ეს არის იგივე ციფრული (დიგიტალური) ტექნოლოგიები, ასევე მას ხშირად უწოდებენ ციფრულ ინფრასტრუქტურას. ზოგადად, ინტენეტ-ქსელი და მასთან დაკავშირებული კომპიუტერული სისტემების დანერგვა, განვითარება და კიბერ-რეალობაში მიღწეული პროგრესი არის ნაშრომის მთავარი დამოუკიდებელი ცვლადი, რომელიც გავლენას ახდენს როგორც მთლიანად ალიანსის, ასევე მისი ცალკეული წევრი ქვეყნების ქმედებებზე, ძირითად ამოცანებსა და სხვა აქტორებთან ურთიერთობებზე. ტექნოლოგიების განვითარებასა და მის სიძლიერეში იგულისხმება კომპიუტერული მექანიზმებისა და სისტემების დახვეწა, ინოვაციების დანერგვა.

ნაშრომში **დამოკიდებულ ცვლადებად** წარმოდგენილია ნატოს სამხედრო-პოლიტიკური სტაბილურობა და ალიანსის არსებული ძირითადი ამოცანები.

თანამედროვე პერიოდში, ამა თუ იმ სახელმწიფოს თუ ორგანიზაციის სიძლიერე, სტაბილურობა თუ უსაფრთხოება არაა დამოკიდებული ერთ კონკრეტულ გამოწვევაზე. დღეს, ერთი რომელიმე სახელმწიფო ან სახელმწიფოთა გაერთიანება სამხედრო შეიარაღებით თუ ძლიერია, ან ეკონომიკურ გიგანტს წარმოადგენს, არ ნიშნავს იმას, რომ მას საერთაშორისო არენაზე დამოუკიდებლად თამაში თამამად შეუძლია, ხელშეუხებელია და მას საფრთხე არ ემუქრება. ეს ასე არაა. მის სიძლიერეს და სტაბილურობას ნებისმიერ დროს და ნებისმიერ ადგილას შეიძლება საფრთხე დაემუქროს. დღეს სტაბილურობა, ეკონომიკური, პოლიტიკური თუ სამხედრო ძლიერება რეგიონალურ თუ გლობალურ დონეზე განვითარებულ ინტეგრაციულ და ურთიერთდამოკიდებულ პროცესებზეა გადაჯაჭვული.

თავის მხრივ, ნახევარ საუკუნეზე მეტია, თითქმის 70 წელია, რაც ევროატლანტიკურ სივრცეში სტაბილური და უსაფრთხო გარემოს უმთავრესი არქიტექტორი სწორედ ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციაა. მან თავისი მიზნებისა და ამოცანების სწორად დასახვითა და სწორი ნაბიჯების გადადგმით, დაამტკიცა, რომ 21-ე

საუკუნეში წარმოადგენს ჯერჯერობით ყველაზე ეფექტურ და წარმატებულ ორგანიზაციას უსაფრთხოების სფეროში. დღეს ნატო წარმოადგენს წარმატებულ ალიანსს, რომელმაც დაარსების დღიდან დღემდე შეძლო და რეალურად უზრუნველყო საკუთარი წევრი ქვეყნების დამოუკიდებლობისა და ტერიტორიული მთლიანობის უზრუნველყოფა და შექმნა მათთვის უსაფრთხო გარემო. ისიც ფაქტია, რომ ნატო, რომელიც დაარსების დროს 12 სახელმწიფოსგან შედგებოდა, რამდენიმე გაფართოების ეტაპის გავლის შემდეგ დღეს უკვე 29 წევრს აერთიანებს. გაფართოებასთან ერთად კი ფართოვდება საფრთხეები და გამოწვევებთან ბრძოლაც შედარებით რთული ხდება, რადგან იზრდება როგორც დასაცავი ტერიტორია, ასევე, სახელმწიფოთა და მოქალაქეების რაოდენობა. ზოგადად, ისტორიაც მრავალ მაგალითს გვაძლევს იმისა, რომ კოალიციები თუ ალიანსები ყოველთვის რაღაც კონკრეტული მიზნის მისაღწევად ერთიანდებოდნენ, ხოლო როდესაც დასახული ამოცანა შესრულდებოდა, ეს ალიანსიც იშლებოდა. ნატოს შემთხვევაში კი თუ ვიმსჯელებთ, ფაქტია, რომ დღემდე ისე მოვიდა, მოუწია ახალ და ახალ საფრთხეებთან გამკლავებისთვის ტრანსფორმაციის განცდა. მაგრამ, დღეს კიდევ უფრო ფართო, მრავალგანზომილებიანი გამოწვევების წინაშეა და კიდევ ერთი დიდი გამოცდის ჩაბარება მოუწევს: რამდენად შეძლებს თანამედროვე ტექნოლოგიებით გაჟღენთილი თუ ტრადიციული საფრთხეებით გამოწვეული პრობლემები წარმატებით გადალახოს? შესაბამისად, საკვლევი თემის პროცესში სწორედ იმ გარემოებას გამოვიკვლევ, რამდენად შესაძლებელია, რომ ნატოს დღეისათვის არსებული სტაბილურობა კითხვის ნიშნის ქვეშ მოექცეს. ასევე, შევეცდები შევისწავლო ბოლო ორი ათწლულის განმავლობაში ალიანსის წინაშე მდგარი გამოწვევების შედეგად, ტრანსფორმირდა თუ არა ნატოს ძირითადი მიზნებისა და ამოცანების მთავარი მიმართულებები.

ზემოთ აღნიშნული დამოკიდებული ცვლადების ოპერაციონალიზაციას კი მოვახდენ ბოლო ორ ათწლულში ალიანსის დღის წესრიგში შეტანილი ცვლილებების ანალიზით, ნატოს ძირითადი ამოცანებისა და ამ ამოცანების მიღწევის მიზნით გადადგმული

ნაბიჯებით, და თანამედროვე გამოწვევების წინაშე მიღებული ზომებისა და გატარებული ღონისძიებების შეფასებით ოფიციალური დოკუმენტების შესწავლის გზით.

1.2 კვლევის მეთოდოლოგია

კვლევის მეთოდად გამოყენებულ იქნება მონოგრაფიული გამოკვლევა, რომელიც "ცალკეული შემთხვევის, თემის ან სოციალური ჯგუფის სიღრმისეული შესწავლაა მკვლევართა ხელთ არსებული ყველა საშუალების მეშვეობით," (ზურაბიშვილი 2006, 61). მონოგრაფიული კვლევის ფარგლებში გამოიყენება მრავალმეთოდური მიდგომა (ზურაბიშვილი 2006, 63), რომელიც მოიცავს მრავალ თვისებრივ მეთოდს, მაგრამ, ამავდროულად რაოდენობრივსაც, "მონოგრაფიულ გამოკვლევაში გამოყენებული მეთოდები სავსებით არ შემოიფარგლებოდა თვისებრივი მეთოდებით - პირიქით, ისინი ხშირად მდიდრდებოდა სტატისტიკური და რაოდენობრივი მონაცემებით" (ზურაბიშვილი 2006, 64). ნაშრომში სიღრმისეულად იქნება განხილული ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის და მისი ცალკეული წევრი სახელმწიფოების მოქმედებები კიბერ-სივრცეში, რომლის მაგალითზეც ვიკვლევთ კიბერ-უსაფრთხოების გავლენას.

საკითხის თავისებურებიდან გამომდინარე, მოვახდენთ საკვლევი თემის გარშემო არსებული ლიტერატურის, ისტორიული მასალების და პირველადი დოკუმენტების ანალიზს. ჰიპოთეზის დასამტკიცებლად დაგვჭირდება გამოვიყენოთ საკითხის ირგვლივ არსებული ლიტერატურა, ოფიციალური დოკუმენტები და განცხადებები, ექსპერტების შეხედულებები, ახალი ამბები(ნიუსები), სტატიები და იმ მკვლევარების ნააზრევი, რომლებიც პირდაპირ თუ ირიბად ეხებიან საკვლევ საკითხს. ანუ ყველა ჩამოთვლილის გაანალიზება, რაც გულისხმობს კონტენტ-ანალიზის მეთოდს (Qualitative Methods, Spring 2004).

ასევე, მიზანშეწონილია, გავაანალიზოთ ნატოს და წევრი ქვეყნების ლიდერებისა და სახელმწიფო მოხელეთა განცხადებები, რაც საშუალებას მოგვცემს ალიანსის და მისი წევრი ქვეყნების შემდგომი ქმედებები ავხსნათ; ეს კი გულისხმობს დისკურს-ანალიზის მეთოდის გამოყენებას (Qualitative Methods, Spring 2004).

გარდა ზემოთ აღნიშნულისა, კვლევის პროცესში გავაანალიზებ იმ ძირითად კიბერ-მოვლენებს, რასაც მნიშვნელოვანი გავლენის მოხდენა შეუძლია საკველევი თემის ირგვლივ. ასევე, მოვახდენ ოფიციალური დოკუმენტების, განცხადებებისა და გადადგმული ნაბიჯების ანალიზს დაწყებული 2002 წლის ნატოს პრაღის სამიტიდან 2016 წლის ვარშავის სამიტის ჩათვლით, და ასევე, გავაანალიზებ 2017 წლის განმავლობაში კიბერსივრცეში მომხდარ მნიშვნელოვან კიბერ-ინციდენტებს და ნატოს წარმომადგენლების ოფიციალურ განცხადებებს კიბერუსაფრთხოების საკითხთან დაკავშირებით. ასევე, ნაშრომში განხილული იქნება ნატოს ამჟამინდელი გენერალური მდივნის მოსაზრებები და განცხადებები კიბერ-საფრთხეებთან დაკავშირებით.

ასევე, უნდა აღინიშნოს, რომ კვლევის პროცესში შეხვედრები, დისკუსიები და აზრთა გაზიარების შესაძლებლობა მქონდა საკითხით დაინტერესებულ პირებთან და საქართველოში კიბერუსაფრთხოების საკითხებზე მომუშავე საჯარო მოხელეებთან. რის შედეგადაც, დამატებით, გარკვეული მიმართულებების და დასკვნების გამოტანის შესაძლებლობაც მომეცა.

2. ოპერაციონალიზაცია: როგორ განვსაზღვროთ „კიბერუსაფრთხოება“

აღნიშნულ თავში განვსაზღვრავთ, თუ რას წარმოადგენს კიბერუსაფრთხოება და რატომ არის ის ასეთი მნიშვნელოვანი. გარდა ამისა, აღნიშნულ ნაწილში აუცილებლად უნდა განიმარტოს ის ძირითადი ცნებები და ტერმინოლოგია, რომელიც შეგვხვდება

ნაშრომში და კიბერუსაფრთხოების ფენომენის კვლევისას მათი ზუსტად გაგება აუცილებელია.

დანართის სახით კი, უფრო ფართოდ იქნება მოცემული იმ მნიშვნელოვანი ტერმინების განმარტება, რომლებიც კიბერუსაფრთხოებისა და საინფორმაციო ტექნოლოგიებთან დაკავშირებით გამოყენებული იქნება ნაშრომში.

თავდაპირველად უნდა განისაზღვროს თუ რას გულისხმობს კიბერუსაფრთხოება.

კიბერუსაფრთხოება (**Cybersecurity),** რომელსაც ასევე მოიხსენიებენ საინფორმაციო ტექნოლოგიების უსაფრთხოების სახელით, აქცენტს აკეთებს კომპიუტერული სისტემების, ქსელების, პროგრამებისა და მონაცემების დაცვაზე გაუთვალისწინებელი, არალეგალური და არასანქცირებული წვდომის, შეღწევის, შეცვლისა და განადგურებისაგან. (University of Maryland University College)

კიბერუსაფრთხოება არის საქმიანობა ან პროცესი, შესაძლებლობა ან უნარი, ან მდგომარეობა, რომლის საშუალებით საინფორმაციო და საკომუნიკაციო სისტემები და მასში არსებული ინფორმაცია არის დაცული ან მიმართულია მათი განადგურების, უნებართვოდ გამოყენების, შეცვლის ან ექსპლუატაციის წინააღმდეგ. (National Initiative for Cybersecurity Careers and Studies)

ფართო გაგებით, კიბერუსაფრთხოება არის ერთგვარი სტრატეგია, პოლიტიკა და სტანდარტები, რომელიც ეხება უსაფრთხოებას და ოპერირებას კიბერ სივრცეში, და მოიცავს მთლიანი საფრთხისა და მოწყვლადობის შემცირებას, შეკავებას, საერთაშორისო ჩართულობას, ინციდენტებზე რეაგირებას, სიმტკიცეს; ასევე, პოლიტიკების შემუშავებას და აქტივობების დანერგვას ისეთი კუთხით, როგორებიცაა კომპიუტერული ქსელების ოპერაციები, ინფორმაციის უზრუნველყოფა, კანონმდებლობის გატარება, დიპლომატია, თავდაცვა და სადაზვერვო მისიები, რადგანაც ისინი დაკავშირებულნი არიან გლობალური საინფორმაციო და

საკომუნიკაციო ინფრასტრუქტურის უსაფრთხოებისა და სტაბილურობის უზრუნველსაყოფად. (National Initiative for Cybersecurity Careers and Studies)

რატომ არის კიბერუსაფრთხოება ასეთი მნიშვნელოვანი? - მთავრობები, სამხედრო და თავდაცვის დაწესებულებები, კორპორაციები, ფინანსური ინსტიტუტები, საავადმყოფოები და სხვა ბიზნესები აგროვებენ, გადასცემენ და ინახავენ დიდი რაოდენობით კონფიდენციალურ ინფორმაციას კომპიუტერებში და უგზავნიან მონაცემებს ქსელების საშუალებით სხვა კომპიუტერებს. კიბერ-შეტევების მზარდი რაოდენობისა და სიზუსტის გათვალისწინებით, დიდ ყურადღებას და სიფრთხილეს მოითხოვს სენსიტიური კერძო და ბიზნეს ინფორმაციების, ასევე ეროვნული უსაფრთხოების დაცვის უზრუნველყოფა.(University of Maryland University College)

კიბერ-შეტევები და კიბერ-შპიონაჟი უკვე აღიქმება როგორც ყველაზე დიდი საფრთხე ეროვნული უსაფრთხოებისთვის, რომელიც თითქმის ტერორიზმსაც ჩრდილავს. (University of Maryland University College)

კიბერუსაფრთხოების გავლენა საკმაოდ მნიშვნელოვანია დღევანდელ საინფორმაციო სამყაროში. როგორც შეერთებული შტატების ყოფილმა პრეზიდენტმა ბარაკ ობამამ განაცხადა, „ამერიკის ეკონომიკური კეთილდღეობა 21-ე საუკუნეში დამოკიდებულია კიბერუსაფრთხოებაზე“. (The White House Office of the Press Secretary. 2009)

აშშ-ს 2010 წლის ეროვნული უსაფრთხოების სტარტეგიაში ნათქვამია: „კიბერ-უსაფრთხოების საფრთხეები წარმოადგენს ეროვნული უსაფრთხოების, საზოგადოებრივი დაცულობისა და ეკონომიკის ერთ-ერთ ყველაზე სერიოზულ გამოწვევას, რომელსაც ვუპირისპირდებით როგორც ერი“. (Department of Defense Strategy for Operating in Cyberspace. 2011). 2017 წლის 18 დეკემბერს გამოქვეყნდა აშშ-ის პრეზიდენტის, დონალდ ტრამპის პირველი „ეროვნული უსაფრთხოების სტრატეგია“, რომლის მიხედვითაც, კიბერუსაფრთხოებას და მასთან დაკავშირებულ საკითხებს მნიშვნელოვანი ადგილი უკავია. სტრატეგიაში აღნიშულია, რომ კიბერშეტევები

თანამედროვე კონფლიქტების მთავარი მახასიათებელი გახდა. შეერთებული შტატები კი შეაჩერებს, დაიცავს და საჭიროების შემთხვევაში დაამარცხებს ვირუსულ აქტორებს, რომლებიც კიბერსივრცის შესაძლებლობებს აშშ-ს წინააღმდეგ გამოიყენებენ. (National Security Strategy of the United States of America, December 2017).

კიბერუსაფრთხოების გარდა, უნდა განისაზღვროს თავად ის სივრცე, რომელშიც ხდება კიბერ საფრთხების წარმოშობა, და საიდანც ემუქრება საშიშროება მთლიან საერთაშორისო სისტემას. კიბერ-სივრცე წარმოადგენს ერთგვარ ვირტუალურ კიბერ-საერთაშორისო სისტემას. იგი წარმოადგენს მეხუთე გლობალურ საერთო სივრცეს, ხმელეთის, ზღვის, ჰაერისა და კოსმოსის შემდეგ, რომელიც დიდად საჭიროებს კოორდინაციას, თანამშრომლობას და სამართლებრივ ზომებს ყველა ერისთვის. აუცილებელია, რომ საერთაშორისო საზოგადოებამ გაითვალისწინოს კიბერ საფრთხეების ზრდა და საშიშროება და გაერთიანდეს ამ გლობალური გამოწვევის საპასუხოდ.(Schjolberg Stein. 2012)

თავად ტერმინი **კიბერ-სივრცე** განისაზღვრება, როგორც საინფორმაციო ტექნოლოგიების ინფრასტრუქტურის ურთიერთდამოკიდებული ქსელი, რომელიც მოიცავს ინტერნეტს, სატელეკომუნიკაციო ქსელებს, კომპიუტერულ სისტემებს, ჩაშენებულ პროცესორებსა და კონტროლერებს. (National Initiative for Cybersecurity Careers and Studies). თუმცა, განსხვავებით სხვა კომპიუტერული ტერმინებისგან, კიბერ-სივრცეს არ გააჩნია ერთი კონკრეტული განსაზღვრება. ზოგადად, იგი გამოიყენება კომპიუტერების ვირტუალური სამყაროს აღსაწერად. იგი აღნიშნავს ვირტუალურ სივრცეს, რომელიც კომპიუტერის, მოდემისა და საკომუნიკაციო სისტემების მეშვეობით იქმნება. პირველად ტერმინი კიბერ-სივრცე შემოიტანა ამერიკელმა მწერალმა უილიამ გიბსონმა 1984 წელს დაწერილ წიგნში ”ნეირომანტი” (Neuromancers (1984)). (The Tech Terms Computer Dictionary)

კიბერ-სივრცე წარმოადგენს ერთგვარ პირობით გარემოს, რომელშიც მიმდინარეობს კომუნიკაცია კომპიუტერული ქსელების საშუალებით.

კიბერ-სივრცე გაეროს დეფინიციით განიმარტება, როგორც ელექტრონული, ვირტუალური სივრცე, რომელშიც ხდება ინფორმაციისა და მონაცემების გადაცემა და ნებისმიერი სხვა სახის კომუნიკაცია ელექტრონული საშუალებით და არა მხოლოდ კომპიუტერით. მოიაზრება როგორც ინტერნეტთან დაკავშირებული კომპიუტერი, კომპიუტერული ქსელი, მობილური თუ სხვა ტექნიკური საშუალება, რომელიც ტექნოლოგიურად უზრუნველყოფს აღნიშნული მოქმედებების შესრულებას რამდენიმე ობიექტს შორის. ხშირად კიბერ-სივრცის აიგივებენ და მოიხსენიებენ ინტერნეტის სახელწოდებით. ტერმინი ასევე აღნიშნავს კორპორაციების, სამხედრო, სამთავრობო და სხვა ორგანიზაციების ელექტრონულ საინფორმაციო გარემოს. (United Nations Multilingual Terminology Database)

ასევე, აუცილებელია განიმარტოს კიდევ ერთი მნიშვნელოვანი და ბოლო პერიოდში მეტად აქტუალური ცნება - კიბერ-ომი.

Cyber-war - კიბერ-ომი - სახელმწიფოს მხრიდან ინფორმაციული ომის განზრახ გამოყენება, ისეთი იარაღების საშუალებით, როგორებიცაა ელექტრო-მაგნიტური პულსის ტალღა, ვირუსი, ჭია, ტროას ცხენები და სხვა, რომელიც მიზანმიმართულია მოწინააღმდეგე სახელმწიფოს ელექტრონული მოწყობილობებისა და ქსელების წინააღდეგ. (Cyberlaw - კიბერსივრცის სამართალი)

კიბერ-ომს ასევე განმარტავენ, როგორ საომარ მოქმედებას ვირტუალურ სივრცეში და მის ირგვლივ, რომელიც უმთავრესად ხორციელდება ინფორმაციული ტექნოლოგიების გამოყენებით. უფრო ფართო გაგებით, ეს გულისხმობს, ასევე, სამხედრო კამპანიების მხარდაჭერას ტრადიციული ოპერირების სივრცეებში (როგორებიცა: ხმელეთი, ზღვა, ჰაერი და კოსმოსი) ვირტუალური სივრცის იარაღების საშუალებით. ზოგადად, ტერმინი ასევე აღნიშნავს მაღალტექნოლგიურ ომებს საინფრომაციო საუკუნეში, რომელიც ეფუძნება ყველა სამხედრო სექტორისა თუ საკითხის კომპიუტერიზაციას, ელექტორინიზციასა და დაქსელვას. (ავსტრიის კიბერუსაფრთხოების სტრატეგია, 2013)

ქვემოთ, დანართის სახით, ასევე განმარტებულია რამდენიმე მნიშვნელოვანი ტერმინი, რომელთა დეფინიცია საჭიროა ნაშრომის უკეთესად გასააზრებლად, და იმ გარემოების გათავალისწინებითაც, რომ კიბერ-ტერმინოლოგიის ქართული შესატყვისები არც თუ ისე მრავალფეროვანია, უმჯობესია ცხადი გახდეს, თუ რა იგულისხმება კონკრეტულ ცნებაში.

3. ნატო, კიბერუსაფრთხოება და საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარება

ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცია (ნატო) წარმოადგენს სამხედრო-პოლიტიკურ ალიანსს, რომელიც 1949 წლის 4 აპრილს შეიქმნა. ეს არის ჩრდილოეთ ამერიკის 2 და ევროპის 27 სახელმწიფოსაგან შემდგარი კავშირი, რომლის მიზანია ჩრდილოატლანტიკურ სივრცეში მშვიდობის, მისი წევრი ქვეყნების თავისუფლებისა და უსაფრთხოების უზრუნველყოფა, როგორც პოლიტიკური ისე სამხედრო საშუალებებით. ალიანსი მკაცრად იცავს და პატივს სცემს ისეთ ღირებულებებს, როგორიცაა წევრი ქვეყნების სუვერენიტეტი, ტერიტორიული მთლიანობა, დემოკრატია, ინდივიდუალური თავისუფლება, ადამიანის უფლებები და კანონის უზენაესობა. (რა არის NATO? საინფორმაციო ცენტრი ნატოსა და ევროკავშირის შესახებ, 2017)

ვაშინგტონის ხელშეკრულების (ჩრდილოატლანტიკური ხელშეკრულება) ხელმოწერით შეიქმნა უსაფრთხოების ერთიანი სისტემა, რომელიც ალიანსში შემავალი წევრი ქვეყნების მჭიდრო თანამშრომლობასა და საერთო ფასეულობებს ეფუძნებოდა. ნატოს თავდაცვის ქოლგის ქვეშ დასავლეთ ევროპამ და ჩრდილოეთ ამერიკამ მალე მიაღწიეს სტაბილურობის უპრეცედენტოდ მაღალ დონეს და ევროპის ეკონომიკური თანამშრომლობისა და განვითარებისათვის მყარი საფუძველი შექმნეს. ჩრდილოატლანტიკური ხელშეკრულება 14 პუნქტისაგან შედგება. თუმცა, მისი მეხუთე

პუნქტი ხელშეკრულების ქვაკუთხედს წარმოადგენს. ჩრდილოატლანტიკური ალიანსის ერთ-ერთი უმთავრესი პრინციპია კოლექტიური თავდაცვა, რომლის თანახმად, ერთ ან ერთზე მეტ სახელმწიფოზე განხორციელებული შეიარაღებული თავდასხმა განიხილება როგორც თავდასხმა ნატოს ყველა წევრ სახელმწიფოზე. არსებულ შემთხვევაში, ალიანსი დახმარებას გაუწევს საფრთხის ქვეშ მყოფ წევრ ქვეყანას ან ქვეყნებს და განახორციელებს ყველა საჭირო ქმედებას, მათ შორის სამხედრო ძალის გამოყენებას, ჩრდილოატლანტიკური რეგიონის უსაფრთხოების აღდგენისა და შენარჩუნების მიზნით. (რა არის NATO? საინფორმაციო ცენტრი ნატოსა და ევროკავშირის შესახებ, 2017)

დამფუძნებელი ხელშეკრულების თანახმად, ალიანსის წევრები იღებენ ვალდებულებას და პასუხისმგებლობას ერთობლივად გაიზიარონ კოლექტიური უსაფრთხოების წინაშე მდგარი საფრთხეები.

ნატო შეიქმნა ნახევარ საუკუნეზე მეტი ხნის წინ და იმ დროიდან მოყოლებული ალიანსის მთავარი ამოცანაა წევრი სახელმწიფოების თავდაცვისა და უსაფრთხოების უზრუნველყოფა. ნატოს დაარსებიდან დღემდე ორგანიზაციამ განიცადა არაერთი ცვლილება ახალ გამოწვევებსა და საფრთხეებზე ადეკვატური რეაგირების მიზნით. (რა არის NATO? საინფორმაციო ცენტრი ნატოსა და ევროკავშირის შესახებ, 2017)

რა წარმოადგენს დღეს ნატოს უმთავრეს უსაფრთხოების გამოწვევებს? ნატოს ოფიციალური განცხადებების მიხედვით, ალიანსი დღეს უფრო ფართო სპექტრის საფრთხეების წინაშეა, ვიდრე წარსულში იყო. აღმოსავლეთით, რუსეთი უფრო გამყარდა ყირიმის უკანონო ანექსიითა და აღმოსავლეთ უკრაინის დესტაბილიზაციით, ისევე როგორც სამხედრო შეიარაღების მობილიზებით ნატოს საზღვრებთან ახლოს. სამხრეთით, ახლო აღმოსავლეთსა და აფრიკაში უსაფრთხოების გარემოს გაუარესების გამო გაიზარდა სიკვდილიანობა, მომრავალდა ფართომასშტაბიანი მიგრაციის ნაკადები და მოხშირდა ტერორისტული შეტევები. ნატო შეკავებას ახდენს თავისი შეკავებისა და თავდაცვის პოტენციალის ამაღლებით, ასევე, მხარს უჭერს საერთაშორისო ძალისხმევას

სტაბილურობისა და უსაფრთხოების გაძლიერებისათვის ალიანსის ფარგლებს გარეთ. ნატო თავის უმნიშვნელოვანეს გამოწვევებად, ასევე, ხაზგასმით აღნიშნავს კიბერ შეტევებს, მასობრივი განადგურების იარაღის გავრცელებას, ენერგოუსაფრთხოების საკითხებს, ასევე, გარემოსდაცვით საკითხებთან დაკავშირებულ გამოწვევებსა და ზოგადად უსაფრთხოების საკითხებს. (NATO, What are today's security challenges?, 2017) როგორც ნატოს ოფიციალურ განცხადებაშია აღნიშნული, ეს გამოწვევები ძალიან ბევრია ერთი კონკრეტული ქვეყნისთვის თუ ორგანიზაციისთვის გასამკლავებლად, შესაბამისად, ნატო მჭიდროდ თანამშრომლობს თავის პარტნიორთა ქსელთან, რათა წვლილი შეიტანოს აღნიშნულ გამოწვევებთან საბრძლოველად. (North Atlantic Treaty Organization)

თავის მხრივ, კიბერუსაფრთხოების უმთავრესი პრობლემური საკითხები და გამოწვევები პირდაპირ დაკავშირებულია ტექნოლოგიებთან.(Institute on Science for Global Policy) ტექნოლოგიების ზრდა და განვითარება ისეთი ტემპით მიმდინარეობს, რომ შეიძლება სწრაფადვე გახდეს ვადაგასული. დიგიტალური საინფორმაციო ტექნოლოგიები არის სწრაფად ცვალებადი - რაც გულისხმობს, რომ დომეინები, ინტერნეტ და კომპიუტერული მექანიზმები, პროგრამული უზრუნველყოფა და ასევე მათი განადგურების მექანიზმები დიდი სიჩქარით ვითარდება და ყოველდღიურად მისი განახლება ხდება. აღნიშნული გარემოება დიდ საფრთხეს და გამოწვევებს ქმნის უსაფრთხოების უზრუნველყოფისთვის.

თავისუფლად შეიძლება ითქვას, რომ თანამედროვე ციფრული ტექნოლოგიები/ინფრასტრუქტურა წარმოადგენს ერთგვარ შეირაღებას, რომელმაც გარკვეულწილად ჩაანაცვლა სამხედრო შეიარაღება კლასიკური გაგებით. დიგიტალური ინფრასტურუქტურის განვითარებამ იმდენად მაღალ დონეს მიაღწია, რომ სახელმწიფოებისთვის თუ ორგანიზაციებისთვის ერთგვარ იარაღად იქცა, რომელიც არამარტო კიბერ-სივრცეშია ეფექტური, არამედ ჩვეულებრივ, არა-ვირტუალურ სივრცეშიც. თავისუფლად შეგვიძლია წარმოვიდგინოთ და გადავიტანოთ

კლასიკური გაგებით სამხედრო შეიარაღება და ჯარისკაცები ელექტორუნულ საბრძოლო ველზე. ანუ, კიბერსივრცე წარმოდგენილია როგორც ბრძოლის ველი, ხოლო ერთი მხრივ ციფრული და საკომუნიკაციო ტექნოლოგიებით განსწავლული პირები და, მეორე მხრივ - ჰაკერები, წარმოგვიდგებიან როგორც კიბერ ან ელექტორუნულ ჯარისკაცებად. ასეთ ბრძოლის ველზე კი ბრძოლა არის ყოველმხრივ ასიმეტრიული, რომლის წინასწარ განსაზღვრა თუნდაც მეტოქის სამხედრო არსენალისა და/თუ შეიარაღების ხარჯზე უკვე შეუძლებელია. ვერ განვსაზღვრავთ, თუ რომელი მხარე უფრო ძლიერია იმ მომენტში, რომელს აქვს გამარჯვების უფრო მეტი შანსი; ან თუ მოიგებს, რამდენად და რის ფასად დაუჯდება მას ეს გამარჯვება. შესაბამისად, მაშინ, როცა ტექნოლოგიების განვითარება იმ შესაძლებლობას იძლევა რომ მინიმალური დანახარჯებით მეტოქეს მაქსიმალური ზარალი აჩვენო და მის არსებობას, სოციალურ, პოლიტიკურ თუ ეკონომიკურ კეთილდღეობას სერიოზული საფრთხე შეუქმნა და მოწყვლადი გახადო მისი ეროვნული უსაფრთხოება აღნიშნული გამოწვევების წინაშე, იმის ნათელ სურათს გვაძლევს, რომ კლასიკური გაგებით, სამხედრო შეიარაღება ნელ-ნელა მის უპირველეს და შეუცვლელის მნიშვნელობას კარგავს, და დიდი ყურადღება სწორედ ტექნოლოგიურ შეიარაღებაზე გადადის.

კიბერ სინამდვილე არის როგორც გლობალური, ასევე დემოკრატიული. სახელმწიფოებს, ქვეყნებს, ორგანიზაციებს, კორპორაციებს და ასევე, ცალკეულ ინდივიდებს შესწევთ იმის ძალა, რომ მოახდინონ გლობალური ზეგავლენა კიბერ სივრცეში. ამის მაგალითად შეიძლება მოვიყვანოთ ინდივიდ ჟულიან ასანჟის „ვიკილიქსის“ გავლენიდან და შედეგებიდან დაწყებული, პატარა ესტონეთის შემთხვევით დამთავრებული, რომელმაც კიბერუსაფრთხოების პოლიტიკის დისკუსიები დღის წესრიგში დააყენა. (Lieberthal and Singer 2012. 4) კიბერუსაფრთხოების მნიშვნელობის საკითხი ერთ-ერთ მთავარ საკითხად აქცია სტაქსნეტის (Stuxnet) ვირუსული პროგრამის გავრცელებამ, რომელიც შეიჭრა ირანის ბუშერის ბირთვული ელექტროსადგურის საკომპიუტერო სისტემაში და საფრთხე

შეუქმნა ბირთვულ და ინდუსტრიულ ობიექტებს. ეს იყო ნათელი დასტური და ყურადსაღები პრეცედენტი იმისა, თუ როგორ შეიძლება კომპიუტერულ ღილაკზე თუნდაც ერთი თითის დაჭერით მსოფლიოს უსაფრთხოებასა და სტაბილურობას საფრთხე შეუქმნა.

მართალია ინტერნეტს არ გააჩნია ფორმალური საზღვრები, მაგრამ ის წარმოადგენს მზარდ ადგილს (სივრცეს), რომელშიც სახელმწიფოები როგორც მოქმედებენ, ასევე ღელავენ აღნიშნულის გამო. (Sanger and Markoff. 2011) ინტერნეტი, რომელიც 50-60-იან წლებში გამოიგონეს ამერიკის მთავრობის დაკვეთით, იმ მიზანს ემსახურებოდა, რომ შექმნილიყო ისეთი სანდო საკომუნიკაციო ქსელი, რომელიც საბჭოთა კავშირიდან მომავალ ბირთვულ საფრთხეს შეაკავებდა. თუმცა, როგორც აღმოჩნდა მისი შექმნის მსურველებს და შემქმნელებს ბოლომდე გათვლილი არ ჰქონდათ, რომ ასეთი გამოგონება მომავალში უამრავ სიკეთესთან ერთად უფრო მეტ პრობლემას და საშიშროებასაც წარმოშობდა.

ბოლო ათი წლის განმავლობაში ნატო სულ უფრო და უფრო შირად ხდება კიბერ-შეტევების სამიზნე. ნატოს ქსელების წინააღმდეგ წარმოებული კიბერ-თავდასხმების უმრავლესობა სახელმწიფო აქტორებიდან არის წარმოებული. საეჭვო ქმედებები და მოვლენები ყოველდღიურად ვლინდება. უმეტესობის განეიტრალება და ადექვატური რეაგირება ავტომატურად ხდება, თუმცა ზოგიერთი მათგანი მოითხოვს ნატოს კიბერ-თავდაცვის ექსპერტებისგან ანალიზსა და პასუხს. (North Atlantic Treaty Organization, Factsheet,2017)

2016 წელს ნატოს ყოველთვიურად საშუალოდ 500 კიბერ-ინციდენტი ემუქრებოდა, რაც დაახლოებით 60%-იანი ზრდაა 2015 წელთან შედარებით. 2017 წლის განმავლობაში, ნატოს კიბერ ექსპერტების შეფასებით, კვლავ აღინიშნებოდა ევოლუცია კიბერ-შეტევებში პროგრამული სისტემების გავლით, რომლის სამიზნესაც ნატოსთან დაკავშირებული პერსონალური მოწყობილობები და ქსელები წარმოადგენდნენ. (North Atlantic Treaty Organization, Factsheet,2017)

როგორც უკვე აღვნიშნეთ, ტექნოლოგიური განვითარება ისეთი სწრაფი ტემპებით მიმდინარეობს, რომ მასთან არჩამორჩენა უკვე სერიოზულ გამოწვევას წარმოადგენს. ტექნოლოგიური რევოლუციის სწრაფი ტემპი კი ბოლო ათწლეულის განმავლობაში განსაკუთრებით შეიმჩნევა. თავის მხრივ, ნატო, რომელიც 70 წლის წინ სრულიად სხვა საფრთხეებთან გასამკლავებლად დაარსდა, ცივი ომის დასრულებისა და საბჭოთა ექსპანსიის დაშლის შემდეგ სრულიად ახალი გამოწვევების წინაშე დადგა. მას ან უნდა ტრანსფორმაცია განეცადა და თანამედროვე გამოწვევებს მორგებოდა, ან არადა მისი არსებობის საკითხი ეჭვქვეშ დადგებოდა. ორგანიზაცია, რომლის მიზანს და უმთავრეს ამოცანას ევროატლანტიკური უსაფრთხოების უზრუნველყოფა წარმოადგენს, იძლუებული გახდა თავის დღის წესრიგში გარკვეული ცვლილებები შეეტანა და თანამედროვე პრობლემების წინაშე კვლავ მომზადებული, ადაპტირებული და სრულფასოვანი წარმდგარიყო. ფაქტი სახეზეა, დღეს ნატო ისევ ქმედითი, ანგარიშაგასაწევი და ძლიერი სამხედრო-პოლიტიკური ალიანსია, რომლის არსებობის აუცილებლობა კვლავაც საციცოცხლოდ მნიშვნელოვანია. თუმცა, დღეს, ნატო კიდევ უფრო მრავალფეროვანი და მრავალგანზომილებიანი საფრთხეებისა და გამოწვევების წინაშე დგას. მისი ტრანსფორმაციის აუცილებლობა კი განსაკუთრებით ბოლო ათი წლის განმავლობაში ეჭვგარეშეა. გამომდინარე იქიდან, რომ წინამდებარე ნაშრომის ერთ-ერთ უმთავრეს მიზანს წარმოადგენს, შეისწვლოს თუ რამდენად განაპირობა კიბერუსაფრთხოების საკითხებმა ნატოს დღის წესრიგში ცვლილებების შეტანა, ამის გასაგებად განვიხილავ რამდენიმე მნიშვნელოვან მაგალითს, რომლებმაც საერთაშორისო დღის წესრიგზე თემის აქტუალურობა და პრობლემურობა შეუქცევადი გახადა; ასევე, ნატოს ოფიციალურ დოკუმენტებსა და ფაქტებზე დაყრდნობით იმ ბოლო წლების მნიშვნელოვან მოვლენებს გავაანალიზებ, რომლის საშუალებითაც ნატოს დღის წესრიგში კიბერუსაფრთხოების საკითხი წინა რიგებში გადმოწევა მტკიცდება

3.1 კიბერუსაფრთხოების სფეროში ნატოს ევოლუცია 2002-2017 წლებში და ალიანსის დღის წესრიგის ტრანსფორმაცია

მიუხედავად იმისა, რომ ნატო ყოველთვის იცავდა თავის საკომუნიკაციო და საინფორმაციო სისტემებს, 2002 წლის პრაღის სამიტზე პირველად აღინიშნა კიბერუსაფრთხოების საკითხი ალიანსის პოლიტიკურ დღის წესრიგში. მოკავშირეთა ლიდერებმა კი 2006 წლის რიგის სამიტზე კიდევ ერთხელ დაადასტურეს საინფორმაციო სისტემების დამატებითი დაცვის უზრუნველყოფის აუცილებლობა. (North Atlantic Treaty Organization)

2007 წლის აპრილსა და მაისში ესტონეთის საჯარო და კერძო ინსტიტუტების წინააღმდეგ კიბერშეტევების შემდეგ, 2007 წლის ივნისში მოკავშირე თავდაცვის მინისტრები შეთანხმდნენ, რომ ამ სფეროში აუცილებელი იყო გადაუდებელი სამუშაო რეფორმების გატარება. შედეგად, 2008 წლის იანვარში ნატომ დაამტკიცა კიბერთავდაცვის შესახებ პირველი პოლიტიკა. (North Atlantic Treaty Organization)

2008 წლის ზაფხულში, რუსეთსა და საქართველოს შორის არსებულმა კონფლიქტმა საერთაშორისო საზოგადოებას ნათლად აჩვენა, რომ კიბერშეტევებს აქვთ პოტენციალი, გახდეს ჩვეულებრივი ომის ძირითადი კომპონენტი. (North Atlantic Treaty Organization)

ერთ-ერთი ყველაზე მნიშვნელოვანი წინგადადგმული ნაბიჯი ნატოს დღის წესრიგში, კიბერუსაფრთხოების როგორც ერთ-ერთ პრიორიტეტულ საკითხად დაყენების, ნათელ მაგალითს წარმოადგენდა 2010 წლის ლისაბონის სამიტზე ახალი სტრატეგიული კონცეფციის დამტკიცება, რომლის დროსაც ჩრდილოატლანტიკურ საბჭოს (NAC) დაევალა ნატოს კიბერ თავდაცვის პოლიტიკის სიღრმისეული შემუშავება და მისი განხორციელებისათვის სამუშაო გეგმის მომზადება. (North Atlantic Treaty Organization)

2011 წლის ივნისში, ნატოს თავდაცვის მინისტრებმა დაამტკიცეს ნატოს რიგით მეორე პოლიტიკა კიბერუსაფრთხოების შესახებ, რომელიც ასახავს ალიანსის მასშტაბით

კიბერთავდაცვის სფეროში კოორდნირებული ძალისხმევის ხედვას სწრაფად მზარდი საფრთხეების კონტექსტში და ტექნოლოგიურ გარემოში, და მის განხორციელებასთან დაკავშირებული სამქომედო გეგმა. (North Atlantic Treaty Organization)

2012 წლიდან დღემდე აქტიურად მიმდინარეობს ნატოს კოლექტიური თავდაცვის სისტემაში კიბერუსაფრთხოების ინტეგრაციის პროცესი. ხოლო, 2012 წლის აპრილში კიბერთავდაცვა ნატოს თავდაცვის დაგეგმვის პროცესში შევიდა. თავდაცვის დაგეგმვის პროცესის შედეგად გამოვლენილი და პრიორიტეტულია შესაბამისი კიბერუსაფრთხოების მოთხოვნები. (North Atlantic Treaty Organization)

2012 წლის მაისში, ჩიკაგოს სამიტზე მოკავშირე ლიდერებმა დაადასტურეს თავიანთი ვალდებულება ალიანსის კიბერუსაფრთხოების გაუმჯობესების მიზნით ნატოს ყველა ქსელის ცენტრალიზებული დაცვის ქვეშ მოყვანა და კომპიუტერული ინციდენტების გამოხმაურების შესაძლებლობის (NCIRC) განახლება. (North Atlantic Treaty Organization)

2012 წლის ივლისში, ნატოს სააგენტოების რეფორმის ფარგლებში, ნატოს კომუნიკაციებისა და ინფორმაციების სააგენტო ჩამოყალიბდა. ხოლო, 2014 წლის აპრილში, ჩრდილოატლანტიკური საბჭო შეთანხმდა რომ თავდაცვისა და დაგეგმვის კომეტეტს/კიბერ-თავდაცვა სახელი გარდაქმეოდა და ეწოდა კიბერ-თავდაცვის კომიტეტი. (North Atlantic Treaty Organization)

2014 წლის მაისში NCIRC-ის სრული ოპერატიული შესაძლებლობები მიღწეულ იქნა, რაც უზრუნველყოფს ნატოს ქსელებისა და მომხმარებლების გაძლიერებულ დაცვას. (North Atlantic Treaty Organization)

აღსანიშნავია, რომ 2014 წლის უელსის სამიტზე ალიანსმა დაამტკიცა ახალი კიბერუსაფრთხოების პოლიტიკა და სამოქმედო გეგმა. მნიშვნელოვანი ყურადღება გამახვილდა კიბერსივრციდან მოსალოდნელ საფრთხეებზე, რომლებიც დღითიდღე უფრო ხშირი, დახვეწილი და უაღრესად საშიში ხდებოდა. აღნიშნულ გამოწვევასთან საბრძოლველად ალიანსმა გაძლიერებული კიბერპოლიტიკა მიიღო. ამ პოლიტიკამ

კიდევ ერთხელ დაადასტურა მოკავშირეების უსაფრთხოებისა და პრევენციის, გამოვლენის, მდგრადობის, აღდგენისა და დაცვის განუხორციელებლობის პრინციპები. (North Atlantic Treaty Organization) უელსის სამიტის კომუნიკეში, ასევე, განისაზღვრა, რომ ზემოთ აღნიშნული პოლიტიკა აღიარებს რომ საერთაშორისო სამართალი, მათ შორის, საერთაშორისო ჰუმანიტარული სამართალი და გაეროს ქარტია და მისი მანდატი უნდა მიესადაგებოდეს და ვრცელდებოდეს კიბერსივრცეშიც. კიბერშეტევებს შეუძლია მიაღწიოს იმ ზომას, რომ სერიოზული საფრთხე შეუქმნას ეროვნულ და ევროატლანტიკურ უსაფრთხოებას, კეთილდღეობასა და სტაბილურობას. სწორედ ამიტომ, ალიანსის წევრები კიბერუსაფრთხოების გამოწვევებს სერიოზულად უდგებიან. შესაბამისად, აღიარებენ, რომ კიბერუსაფრთხოება წარმოადგენს ნატოს ძირითადი ამოცანის კოლექტიური თავდაცვის ნაწილს; შესაბამისად, მასობრივი და გამანადგურებელი კიბერ შეტევის შემთხვევაში, განხილული და ამოქმედებული იქნება ორგანიზაციის მე-5 მუხლი. (North Atlantic Treaty Organization). ეს კი პირდაპირ იმის მტკიცების საშუალებას გვაძლევს, რომ კიბერ უსაფრთხოება იქცა ნატოს ერთ-ერთ უმთავრეს საკითხად და ტრადიციული ამოცანებისა და პრინციპების ერთგვარი ცვლილება/ტრანსფორმირება განაპირობა, რადგან მისი ქვაკუთხედის, კოლექტიური თავდაცვის ნაწილი გახდა; ამ ფაქტმა შესაძლებლობა და პრეცენდენტი დაუშავა იმისა, რომ ნატოს რომელიმე წევრ ქვეყნაზე განხორციელებულ მასობრივ კიბერ-თავდასხმის შემთხვევაში მოხდეს უპრეცედენტო რამ - ამოქმედდეს მეხუთე მუხლი. აღსანიშნავია ის ფაქტიც, რომ ნატომ, რომელიც წარმოადგენს სამხედრო-პოლიტიკურ ალიანსს და მისი სიძლიერე სწორედ მის სამხედრო შეირაღებაში გამოიხატება, თავისი 70 წლიანი არსებობის მანძლიზე მეხუთე მუხლი მხოლოდ ერთხელ, 9/11-ის მოვლენების შედეგად აამოქმედა. ახლა კი, როდესაც საუბარია, რომ აღნიშნული მუხლი გავრცელდეს კიბერ სივრცეში, ნათლად აჩვენებს თუ რამდენად მნიშვნელოვანია კიბერ უსაფრთხოება ალიანსისა და მისი თითოეული წვერისთვის, და რამდენად ტრანსფორმირდა ალიანსი თანამედროვე უმნიშვნელოვანესი გამოწვევის წინაშე.

2016 წლის ვარშავის სამიტი ერთ-ერთი მნიშვნელოვანი და წინ გადადგმული ნაბიჯი იყო კიბერუსაფრთხოების სფეროში. ალიანსმა გადადგა მნიშვნელოვანი ნაბიჯები კიბერუსაფრთხოების უზრუნველყოფისა და ჰიბრიდული საფრთხეების განეიტრალების მექანიზმების გასაძლიერებლად. ხაზი გაესვა ჰიბრიდული საფრთხეების საპასუხოდ ნატო-ს როლის შესახებ დამტკიცებული სტრატეგიის და შესაბამისი სამოქმედო გეგმის მნიშვნელობას.

ერთ-ერთი მნიშვნელოვანი ფაქტი კი, რაც კიდევ ერთხელ ხაზს უსვამს ნატოს დღის წესრიგში კიბერუსაფრთხოების საკითხის წინა პლანზე წამოწევას არის ის, რომ ალიანსის წევრებმა ინფორმაციული და საკომუნიკაციო ქსელის უსაფრთხოება ერთ-ერთ ძირითად თავდაცვით სფეროდ აღიარეს და შეთანხმდნენ, რომ კიბერსივრცეში ნატომ ისევე ეფექტიანად უნდა დაიცვას თავი, როგორც ხმელეთზე, ზღვასა და ჰაერში. (North Atlantic Treaty Organization)

ნატომ ასევე დაამტიცა მოკავშირეთა შეთანხმების ამსახველი დოკუმენტი (Cyber Defence Pledge), რომელიც ითვალისწინებს ალიანსის წევრ სახელმწიფოთა ვალდებულებას, გადადგან მნიშვნელოვანი ნაბიჯები აღნიშნულ სფეროში პროგრესის მისაღწევად, მათ შორის უზრუნველყონ ეროვნული ქსელებისა და ინფრასტრუქტურის კიბერუსაფრთხოების გაძლიერება, ამ მიზნით გამოყონ შესაბამისი ფინანსური რესურსები, ასევე, ხელი შეუწყონ კიბერუსაფრთხოების სფეროში ცნობიერების ამაღლებას და უნარების განვითარებას. (ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა, საქართველოს უსაფრთხოებისა და განვითარების ცენტრი (GCSD))

2017 წლის 16 თებერვალს თავდაცვის მინისტრებმა მხარი დაუჭირეს განახლებული კიბერ-თავდაცვის სამოქმედო გეგმას, ისევე როგორც საგზაო რუკას რომ კიბერსივრცე ჩაერთოს ოპერაციების განზომილებაშიც. ეს კი გაზრდის მოკავშირეების ერთად მუშაობის შესაძლებლობას, მათი შესაძლებლობების განვითარებასა და ინფორმაციების გაზიარებას. (North Atlantic Treaty Organization)

3.2 რა გავლენა მოახდინა 2007 წელს განხორციელებულმა კიბერ-თავდასხმამ ესტონეთის ტრანსფორმაციაზე?

იმისათვის, რომ უკეთესად შევისწავლოთ თუ რა და როგორი გავლენა აქვს კიბერუსაფრთხოების გამოწვევებს ალაინსზე, ამისათვის, წინამდებარე ნაშრომში რამოდენიმე კონკრეტულ მაგალითზე დაყრდნობით, შევეცდები ზოგადი სურათის წარმოჩენას. ამ ქვეთავში განხილული იქნება 2007 წელს ესტონეთზე განხორციელებული კიბერ-შეტევა, რომელიც არამარტო ესტონეთისთვის ან ნატოსთვის, არამედ მთლიანი საერთაშორისო საზოგადოებისთვის გარდამტეხი მოვლენა აღმოჩნდა. რამდენიმე კვირის განმავლობაში ესტონეთის სამთავრობო საიტებსა თუ სერვერებზე, მედია საშუალებებზე, ონლაინ ახალი ამბების სააგენტოებსა თუ საბანკო სტრუქტურებზე განხორციელებულმა კიბერ-შეტევამ მთლიანი საერთაშორისო საზოგადოება აალაპარაკა და ახალი გამოწვევის წინაშე მოწყვლადობა ნათლად წარმოაჩინა. შესაბამისად, შევეცდები მოკლედ განვიხილო აღნიშნული შემთხვევა და გავაანალიზო მისი გავლენა როგორც ესტონეთის, ისე ჩრიდლოატლანტიკური ალიანსის ქმედებებზე.

კიბერ-თავდასხმები, ინფორმაციული ომი, ყალბი სიახლეების გავრცელება –10 წლის წინ ესტონეთი იყო პირველი ქვეყანა, რომელიც გახდა ჰიბრიდული ომის მსხვერპლი. შედეგად, ამ ფაქტმა გავლენა მოახდინა ქვეყნის სრულ ტრანსფორმაციაზე. ეს გავლენა დღესაც მნიშვნელოვნად იგრძნობა ქვეყნის განვითარებაზე. (Damien McGuinness, 2017). თავად კიბერთავდასხმა, რომელიც ესტონეთში, 2007 წლის 27 აპრილს განხორციელდა, კიბერუსაფრთხოების სპეციალისტებისთვის დღესაც განხილვის საგანს წარმოადგენს. ესტონეთზე განხორციელებულმა კიბერშეტევამ სერიოზული კითხვის ქვეშ დააყენა ნატოს წევრი სახელმწიფოების ელექტრონული უსაფრთხოების საკითხი.

ცნობილი კიბერ-თავდასხმის მიზეზად ეთნიკურად რუსი და ეთნიკურად ესტონელი მოქალაქეების დაპირისპირება იქცა, რომელიც გამოწვეული იყო ტალინის ცენტრში

მდგარი ბრინჯაოს ჯარისკაცის მონუმენტის ადგილმდებარეობის შეცვლის გადაწყვეტილებით, რომელიც ადგილობრივმა მთავრობამ მიიღო.

ბრინჯაოს მონუმენტი აღმართული იქნა 1947 წელს საბჭოთა ხელისუფლების მიერ და მას თავდაპირველად ეწოდებოდა „ტალინის განმათავისუფლებელთა მონუმენტი“. ესტონეთში მცხოვრები ეთნიკურად რუსი საზოგადოებისთვის ეს მონუმენტი წარმოადგენდა საბჭოთა კავშირის გამარჯვებას ნაციზმზე. თუმცა, ეთნიკური ესტონელებისთვის წითელი არმიის ჯარისკაცები არ იყვნენ განმათავისუფლებები, პირიქით, მათ მოახდინეს ესტონეთის ანექსია, ამიტომაც, ესტონელებისთვის ეს მონუმენტი ჩაგვრის სიმბოლოს უფრო წარმოადგენდა საბჭოთა კავშირის მხრიდან. (Damien McGuinness, 2017).

2007 წელს, როდესაც, ესტონეთის მთავრობამ გადაწყვიტა ბრინჯაოს ქანდაკების გადატანა ტალინის ცენტრიდან სამხედრო სასაფლაოზე, ამ ფაქტმა გამოიწვია ეთნიკურად რუსი მოსახლეობის აღშფოთება, რომლებიც პროტესტის ნიშნად გამოვიდნენ ქუჩებში. პროტესტი გამწვავდა რუსეთის მხრიდან გავრცელებული ყალბი ახალი ამბების გავრცელებით, რომლის მიხედვითაც, მონუმენტი და საბჭოთა კავშირის ომის დროინდელი სასაფლაოები იყო განადგურებული ადგილობრივი ხელისუფლების გადაწყვეტილებით. 2007 წლის 26 აპრილს ტალინში დაიწყო აჯანყება, რომლის დროსაც დაშავდა 156 ადამიანი, 1000-მდე იქნა დაკავებული, ხოლო ერთი გარდაცვლილი. (Damien McGuinness, 2017). 27 აპრილიდან კი, ესტონეთზე დაიწყო კიბერ-თავდასხმები. კიბერ-თავდასხმების შედეგად, ესტონეთის საბანკო სისტემა და მისი ონლაინ სერვისები, მედიასაშუალებები და სამთავრობო ორგანოების ფუნქციები მოიშლა და მიუწვდომელი გახდა. სპამის მასიურმა დაგზავნამ გამოიწვია ესტონური სერვერების მწყობრიდან გამოყვანა. კიბერ თავდასხმის შედეგად ესტონელ მოსახლეობას აღარ შეეძლო საბანკო ტრანსაქციების გამოყენება, მთავრობის წარმომადგენლები ვეღარ იყენებდნენ ელექტრონული ფოსტას, ხოლო მედია საშუალებების და მაუწყებლობების ფუნქციონირება შეფერხდა. (Damien McGuinness, 2017)

კიბერ-აგრესია რადიკალურად განსხვავდება ჩვეულებრივი კონვენციური ომისგან. კიბერ-თავდასხმის დროს წარმოიშობა გაურკვევლობა და დაბნეულობა, რასაც წარმატებით იყენებს მტერი. ასეთი შეტევებისა და აგრესიის მსხვერპლი შეიძლება გახდეს თანამედროვე საერთაშორისო საზოგადოების ნებისმიერი წარმომადგენელი. ეს კი ნიშნავს იმას, რომ აგრესორს შეუძლია კიბერ შეტევით გამოიწვიოს არეულობა ნატოს წევრ ქვეყანაში, ალიანსის შურისძიების შიშის გარეშე. ნატოს მეხუთე მუხლის მიხედვით, წევრი ქვეყნებს შეუძლიათ დაიცვან ერთმანეთი თუ შეტევა ხდება კიბერსივრცეში, მაგრამ მეხუთე მუხლი შეიძლება გააქტიურებული იქნას მხოლოდ იმ შემთხვევაში, თუ თუ კიბერ-თავდასხმის შედეგად არის გამოწვეული ძალიან დიდი ზარალი და ამ ფაქტით გამოწვეული დანაკარგი თითქმის უტოლდება ტრადიციულ სამხედრო დაპირისპირებას. (Damien McGuinness, 2017)

გარდა ზემოთ განხილულისა, კიდევ ერთი გარემოება მდგომარეობს იმაში, რომ იდენტიფიცირება თუ ვინ დგას კიბერ-თავდასხმის უკან ასევე წარმოადგენს დიდ პრობლემას. ცნობილი ფაქტია, რომ 2007 წლის კიბერ-შეტევა ესტონურ სერვერებზე განხორციელებული იყო რუსული IP მისამართებიდან, ასევე, ონლაინ ინსტრუქციებიც კი რუსულ ენაზე იყო განთავსებული. მაგრამ, კონკრეტული დამამტკიცებელი საბუთი იმისა, რომ შეტევები განხორციელებული იყო რუსეთის მხრიდან დღემდე არ არსებობს. (Damien McGuinness, 2017)

ერთის მხრივ, 2007 წელს ესტონეთზე განხორციელებული კიბერ-თავდასხმა ესტონეთისთვის გახდა კარგი გაკვეთილი, რაც მათ დაეხმარა გამხდარიყვნენ ექსპერტები კიბერ თავდაცვის სფეროში. თავის მხრივ, ბრინჯაოს ქანდაკების გადატანის მიერ გამოწვეული დაძაბულობა შეიძლება წარმოადგენდეს პირველ, სახელმწიფოს მიერ მხარდაჭერილ კიბერ თავდასხმას სხვა ქვეყანაზე (როგორც უკვე აღვნიშნთ, მიუხედავად მრავალი ფაქტორისა, რუსეთის ბრალეულობა ოფიციალურად მაინც არ დასტურდება). (Damien McGuinness, 2017)

2007 წლის შეტევამდე ესტონეთში დაწყებული იყო ქვეყნის ინტერნეტიზაციის პროცესი, მაგრამ უპრეცენდენტო მოვლენამ უფრო მეტი გამოცდილება შესძინა მათ კიბერ თავდაცვის კუთხით და აქცია მსოფლიოში ყველაზე უფრო ინტერნეტზე დამოკიდებულ ქვეყანად. უფრო მეტიც, 2005 წელს ესტონეთი გახდა პირველი ქვეყანა რომელმაც შემოიღო არჩევნების ონლაინ ხმის მიცემის ფუნქცია. ამჟამად, ესტონეთში ფიქსირდება მსოფლიოში ყველაზე სწრაფი ინტერნეტი, რომლის გადმოწერის სიჩქარეც უტოლდება 46.35 მეგაბაიტს წამში, მეორე ადგილზეა ლიტვა 31.97 მბ წამში, მესამე ადგილს კი იკავებს სამხრეთ კორეა – 31.03 მბ წამში (Damien McGuinness, 2017).

დღეს, ესტონეთი წარმოადგენს ჩრდილო ანტლანტიკური ალიანსის კიბერ უსაფრთხოების ერთ-ერთი მთავარ და გამოცდილ აქტორს. 2014 წლის ივნისში ნატომ კიბერ თავდაცვის გაძლიერების პოლიტიკის მიღებით უდიდესი ნაბიჯი გადადგა კიბერუსაფრთხოების სფეროში.

ესტონეთი ნატოს წევრი გახდა 2004 წელს. ესტონეთი როგორც რუსეთის მოსაზღვრე ქვეყანა განიხილებოდა ნატოსთვის პოტენციურ საფრთხედ, რადგან რუსეთის მხრიდან განხორციელებულ ნებისმიერ პროვოკაციას შეიძლება გამოეწვია ნატოს მეხუთე მუხლის გააქტიურება, რაც ნიშნავდა, ნატოს ყველა წევრი ქვეყნის საბრძოლო მოქმედებაში ჩართვას და სწრაფ რეაგირებას თავმდასხმელზე. მაგრამ ესტონეთი გახდა ალიანსის კიბერ უსაფრთხოების გარანტი. 2008 წელს ესტონეთის დედაქალაქ ტალინში გაიხსნა ნატოს კოოპერატიული კიბერ თავდაცვის ცენტრი, სადაც ყურადღება მახვილდება კვლევებზე, კიბერ თავდაცვის სწავლებასა და განათლებაზე როგორც ტექნიკურ ასევე არატექნიკურ ასპექტებზე. (Damien McGuinness, 2017).

უფრო მეტიც, ნატოს კოოპერატიული კიბერ თავდაცვის ცენტრი, ცენტრალურ როლს თამაშობს კიბერ მომზადებებში. “Locket Shields” – დახურული ფარები, ეს არის სახელწოდება იმ ტრეინინგ-მომზადებისა რომელსაც ცენტრი ყოველწლიურად ატარებს და მასში მონაწილეობას იღებენ ექსპერტები ნატოს წევრი და არა-წევრი ქვეყნებიდან. ეს

არის ყველაზე დიდი მრავალეროვანი მომზადება, სადაც ინდივიდუალური ქვეყნები სწავლობენ თანამშრომლობას, პრობლემის ერთად აღმოფხვრას, ინფორმაციის გაზიარებას და კიბერ-კრიზისების უკეთ თავის გართმევას. ამგვარი წვრთნები კრიტიკულად მნიშვნელოვანია სხვადასხვა ქვეყნების სპეციალისტებს შორის ურთიერთობების შესაქმნელად, ინფორმირებულობების ასამაღლებლად, ინფორმაციის გასაზიარებლად. ეს კი საბოლოოდ კიბერ-გამოწვევების მყისიერ მოგვარებას და მასთან ბრძოლას ისახავს მიზნად. ყველაფერი ეს მიზნად ისახავს ხელი შეუწყოს ნდობის ჩამოყალიბებას ცალკეულ სახელმწიფოებს შორის და კიბერ ასპექტების გაძლიერებას. (Damien McGuinness, 2017).

ესტონეთი აგრძელებს ნატოს კოოპერატიული კიბერ თავდაცვის ცენტრის მხარდაჭერას, ხელს უწყობს ინფორმაციის გაზიარებას, ნდობის ჩამოყალიბებას ნატოს წევრ და არაწევრ სახელმწიფოებს შორის, ერთობლივი ღონისძიებების ჩატარებას რაც აძლიერებს ნატოს თავდაცვისუნარიანობას კიბერუსაფრთხოების ასპექტებში.

ესტონეთის ქალაქ ტარტუში განთავსებულია ნატოს კიბერ-კოალიციის სასწავლო ბაზა, სადაც ხორციელდება ნატოს კიბერ-თავდაცვის სწავლება. სწავლებების დროს ხდება იმიტირებული თავდასხმა კომპიუტერულ სისტემებზე და მათთან ბრძოლის და პრევენციის სწავლება.

მოკლედ რომ შევაჯამოთ აღნიშნული ქეისი და ვუპასუხოთ ანიშნული თავის კითხვას, თუ რა გავლენა მოახდინა კიბერ-თავდასხმამამ ესტონეთის ტრანსფორმაციაზე, აქ გაანალიზებულმა ქეისმა ნათლად აჩვენა, თუ რაოდენ კარგად შეიძლება გამოიყენოს მოწინააღმდეგემ როგორც პოტენციური დაძაბულობა საზოგადოებებში, ასევე საინფორმაციო და საკომუნიკაციო ტექნოლოგიები; ამათ ერთობლივ კომბინაციას კი კიდევ უფრო დიდი საფრთხის მოტანა შეუძლია. ესტონეთის შემთხვევაში, ეს შეტევა გახდა გაკვეთილი, რომელიც კარგად იქნა შესწავლილი და გამოყენებული.

დღესდღეობით ესტონეთი არის ნატოსა და ევროკავშირის ერთ-ერთი წამყვანი ქვეყანა კიბერუსაფრთხოების სფეროში. (Damien McGuinness, 2017).

3.3 კიბერ-ომი საქართველოს წინააღმდეგ

აღნიშნულ ქვეთავში განხილულია ქეისი, რომელიც ეხება საქართველოს - ნატოს არაწევრ ქვეყანას, თუმცა ქვემოთ განხილულმა შემთხვევამ, როგორც ალიანსი და მისი წევრები, ასევე მთლიანად საერთაშორისო საზოგადოება დააყენა მნიშვნელოვანი საფრთხის - კიბერ-ომის - საფრთხისა და მისი შედეგების წინაშე. მეორე მხრივ, ეს საკითხი ჩემთვის, როგორც საქართველოს მოქალაქისთვის, მნიშვნელოვანია პარალელების გასავლებად და კავშირის დასამყარებლად ისეთ თემასთან, როგორიცაა ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის სტაბილურობა. საქართველო, რომელიც წლებია გამოთქვამს სურვილს რომ გახდეს ალიანსის წევრი და ამ მიზნის მისაღწევად მრავალი ნაბიჯი გადადგა და დიდ პროგრესს მიაღწია, მისი მაგალითი და საქართველოს ქეისის კიბერუსაფრთხოების ჭრილში განხილვა სავსებით რელევანტურია წინამდებარე კვლევის პროცესში საკითხის არსის უკეთესად გაგებისა და გაანალიზების მიზნით.

2008 წლის აგვისტოში, საქართველო - რუსეთის ომის დროს, რუსეთის მხრიდან განხორციელდა მასიური კიბერშეტევა საქართველოს ინტერნეტ სივრცეზე, რის შედეგადაც გარკვეული პერიოდი პარალიზებული იყო ქვეყნის სამთავრობო და კერძო სექტორის ვებ - გვერდები.

საქართველოს კიბერუსაფრთხოების სტრატეგიის შესავალ ნაწილში წერია, რომ „2008 წლის აგვისტოში რუსეთის ფედერაციის მიერ საქართველოს წინააღმდეგ განხორციელებულმა ფართომასშტაბიანმა კიბერშეტევებმა ნათლად აჩვენა, რომ საქართველოს ეროვნული უსაფრთხოება ვერ შედგება კიბერსივრცის უსაფრთხოების

უზრუნველყოფის გარეშე. რუსეთ - საქართველოს ომის დროს, რუსეთის ფედერაციამ საქართველოს წინააღმდეგ სახმელეთო, საჰაერო და საზღვაო შეტევების პარალელურად, განახორციელა მიზანმიმართული და მასირებული კიბერშეტევები. აღნიშნულმა კიბერშეტევებმა აჩვენა, რომ კიბერსივრცის დაცვა ეროვნული უსაფრთხოებისთვის ისევე მნიშვნელოვანია, როგორც სახმელეთო, საზღვაო და საჰაერო სივრცეების დაცვა“. ეს კიბერშეტევა ბევრი საერთაშორისო ექსპერტის მიერ შეფასდა როგორც „ინფორმაციული/კიბერ ომი“ საქართველოს წინააღმდეგ, რასაც ქვეყანა მოუმზადებელი შეხვდა, არ არსებობდა საჭირო რესურსები, გამოცდილება და შესაბამისად საქართველომ კიბერშეტევის მოგერიება ვერ შეძლო. შედეგად ქვეყანა აღმოჩნდა სერიოზული საერთაშორისო ინფორმაციული ვაკუუმის წინაშე. პრობლემა გადაიჭრა ქვეყნის უცხოელი სტრატეგიული პარტნიორების, კერძოდ ესტონელების ჩარევის შემდეგ, რის შედეგადაც შეჩერებული და თავიდან აცილებული იქნა მთლიანი ინფრასტრუქტურის განადგურება. (კიბერ უსაფრთხოების ბიურო, „კიბერ თავდაცვა კიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოების პოლიტიკა, სტრატეგია და გამოწვევები“, 2015).

ზემოთ განხილული კიბეშეტევის გამოცდილებამ, საქართველო ახალი გამოწვევის წინაშე დააყენა და იძულებული გახადა, ახალი გამოწვევების წინააღმდეგ ადაპტირება დაეწყო. 2008 წლის აგვისტოს ომისა და მისი შედეგების გათვალისწინებით, რაც უკავშირდებოდა ქვეყნის დაუცველ კიბერსივრცეს, საქართველოს ხელისუფლებამ დაიწყო სამართლებრივ - ნორმატიულ ბაზაზე მუშაობა მოცემული მიმართულებით. გარდა ამისა, ბოლო წლებია აქტიურად მიმდინარეობს სხვადასხვა პოლიტიკების შემუშავება, დაფუძნდა კიბერ უსაფრთხოების ბიურო, შემუშავდა კიბერ უსაფრთხოების სტრატეგია და კიბერ-შეტევებთან გამკლავება ერთ-ერთ მნიშვნელოვან მიმართულებად იქცა. 2008 წელთან შედარებით, დღეს საქართველო უფრო მომზადებული და ტრანსფორმირებულია აღნიშნულ გამოწვევებთან საბრძოლველად,

ასევე საერთაშორისო პარტნიორებთან თანამშრომლობისა და გამოცდილების გაზიარების მიმართულებითაც მნიშვნელოვანი პროგრესია მიღწეული.

3.4. 2017 წლის მნიშვნელოვანი კიბერ-თავდასხმები

2017 წელს საერთაშორისო საზოგადოების განსაკუთრებული ყურადღება ორმა მასშტაბურმა და საშიშმა ვირუსულმა კიბერ-შეტევამ მიიპყრო. მაისში WannaCry-ის სახელით კიბერსივრცეში ერთ-ერთი სერიოზული და სახიფათო კიბერ-შეტევა განხორციელდა რომლის ზარალმაც 1 მილიარდს გადააჭარბა, 300 000-ზე მეტი კომპიუტერული სისტემა დააზიანა და 150-ზე მეტი ქვეყანა მოიცვა (იხილეთ დანართი #2). როგორც საკითხის მკვლევარები განმარტავენ, WannaCry წარმოადგენს ტროას ვირუსის ერთ-ერთი საშიში სახეობას, რომელსაც სისტემაში შეღწევისა და დაინფიცირების შემდეგ კომპიუტერი გამოჰყავს მწყობრიდან და მის მფლობელს ფაილებზე კონტროლის აღდგენის მიზნით, სთხოვს თანხის გადახდას ბიტკოინების (მსოფლიო მასშტაბის კრიპტოვალუტა და ელექტრონული გადახდის საშუალება) სახით.

2017 წლის ზაფხულში, WannaCry-ის მსგავსი და, ასევე, მეტად სახიფათო და მასშტაბური შეტევა განხორციელდა, რომელიც ვირუსული პროგრამის Petya-ს სახელით არის ცნობილი. ვირუსი Petya კომპიუტერულ სისტემაში მოხვედრის შემდეგ შიფრავდა მონაცემებს და მომხმარებელს კომპიუტერებთან წვდომის სანავცლოდ 300 დოლარის გადარიცხვას თხოვდა. ვირუსი უკრაინიდან გავრცელდა და შემდეგ 60 ქვეყანაზე მეტში გავრცელდა. მან დააზიანა უკრაინის მთავრობის, რკინიგზის, ბანკების, მობილური კომპანიების, მედიასაშუალებების რედაქციები, ასევე, ჩერნობილის ატომურ-ენერგეტიკული სადგურის კომპიუტერული ქსელი. კიევმა კიბერ-შეტევაში რუსეთი დაადანაშაულა. თავად რუსეთში ვირუსმა დააზიანა მსხვილი კომპანიები, მათ შორის, "როსნეფტი", ბანკები და სხვა დაწესებულებები. ამის შემდეგ, ვირუსმა

ევროპულ ორგანიზაციებს შეუტია, მათ შორის, დიდი ბრიტანეთის სარეკლამო კომუნიკაციების ჰოლდინგს WPP Group-ს, დანიაში - ლოგისტიკურ კომპანია Maersk-ს; ასევე ინდოეთში ჯავახარლალ ნერუს სახელობის უმსხვილეს პორტს. არსებული მონაცემებით, 28 ივნისის საღამოსთვის, 64 ქვეყნის 12,5 ათასი კომპიუტერი დავირუსდა. (imedinews.ge)

ზემოთ აღწერილმა შემთხვევებმაც ნათელი გახადა, თუ რამდენადაა საერთაშორისო საზოგადოება, ცალკეული სახელმწიფოები და სხვა კრიტიკული ინფრასტრუქტურის და მნიშვნელობის მქონე ინსტიტუტები მოწყვლადი მსგავსი ტიპის ასიმეტრიული საფრთხეების წინაშე.

4. კიბერუსაფრთხოება და ალიანსის სწრაფად ცვლალებადი სამხედრო-პოლიტიკური გარემო

კიბერ-საფრთხეები და თავდასხმები უფრო და უფრო გავრცელებულ, დახვეწილ და საზაიანო ხასიათს იძენენ. ალიანსს კი კომპლექსურად მზარდი საფრთხისშემცველი გარემო ემუქრება. სახელმწიფო და არასახელმწიფო აქტორებს შესაძლებლობა აქვთ კიბერ თავდასხმები გამოიყენონ სამხედრო ოპერაციების კონტექსტში. ბოლოდროინდელი მოვლენების მიხედვით, კიბერ-თავდასხმები გახდა ჰიბრიდული ომის შემადგენელი ნაწილი. (NATO, Cyber defence, 2016) რაც შეეხება თავად ჰიბრიდულ ომს, როგორც ფრენკ ჰოფმანი განსაზღვრავს, ჰიბრიდული საფრთხეებია, როდესაც ნებისმიერი მოწინააღმდეგე ერთდროულად იყენებს კონვენციური იარაღის, არარეგულარული ტაქტიკის, ტერორიზმის და კრიმინალური ქცევის შესაბამის კომბინაციას და საომარი მოქმედებების სივრცეს საკუთარი პოლიტიკური მიზნების მისაღწევად. როგორც ექსპერტები და თემაზე მომუშავე მკლევარები ამბობენ, ევრო-

ატლანტიკური უსაფრთხოების არქიტექტურას მსგავსი პროცესები საფუძველს უთხრის. (ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება, 2016)

მეორე მხრივ, ნატო და მისი მოკავშირეები ქმნიან ძლიერ და სტაბილურ კიბერ-თავდაცვის სისტემას, რათა შეასრულონ ალიანსის კოლექტიური თავდაცვის, კრიზისების მართვისა და ერთობლივი უსაფრთხოების ძირითადი პრინციპები. ნატო მზად უნდა იყოს რომ დაიცვას თავისი ქსელები და ოპერაციები მზარდი და დახვეწილი კიბერ-საფრთხეებისა და თავდასხმებისგან, რომელიც მის წინააღმდეგაა მიმართული.

- კიბერ-თავდაცვა ნატოს ძირითად ამოცანას წარმოადგენს კოლექტიური თავდაცვის სფეროში.
- ნატომ დაადასტურა რომ საერთაშორისო სამართალი უნდა ვრცელდებოდეს კიბერსივრცეში.
- კიბერთავდაცვის მიმართულებით, ნატოს ძირითადი აქცენტი ხორციელდება საკუთარი ქსელების (ოპერაციებისა და მისიების ჩათვლით) დასაცავად და ალიანსში მდგრადობის გასაძლიერებლად. (NATO, Cyber defence, 2016)

კიბერ-საფრთხეები განაგრძობს სწრაფ განვითარებას. ნატოს წევრი ქვეყნების წინააღმდეგ ბოლო დროს განხორციელებული მაღალი დონის კიბერ-თავდასხმები ცხადყოფს, რომ კიბერ-თავდაცვა და მდგრადობა უნდა იყოს ერთ-ერთი ძირითადი პრიორიტეტი. (North Atlantic Treaty Organization)

4.1 ნატოს მიდგომა კიბერ-თავდაცვის მიმართულებით

2014 წლის უელსის სამიტზე მოკავშირეებმა აღიარეს, რომ საერთაშორისო სამართალი უნდა ვრცელდებოდეს კიბერსივრცეშიც, და რომ კიბერ-შეტევებს შეუძლია ისეთივე ზიანის მიყენება საზოგადოებაზე, როგორიც ჩვეულებრივ სამხედრო შეიარაღებულ

თავდასხმას. შედეგად, კიბერ-თავდაცვა აღიარებულ იქნა ნატოს კოლექტიური თავდაცვის ძირითად ამოცანად. (North Atlantic Treaty Organization)

როგორც უკვე აღვნიშნეთ, 2016 წელს ვარშავის სამიტზე მოკავშირეებმა კიბერსივრცე აღიარეს ოპერაციების განზომილებად, ისევე როგორც ჰაერი, ხმელეთი და ზღვა. ეს საშუალებას აძლევს ნატოს სამხედრო მეთაურებს უკეთესად დაიცვან მისიები და ოპერაციები კიბერ-საფრთხეებიდან.

თუმცა, როგორც ნატოელი გადაწყვეტილების მიმღებები და ექსპერტები აცხადებენ, კიბერსივრცის დომინირების აღიარება ნატოს მანდატს არ ცვლის. როგორც ყველა ოპერაციულ განზომილებაში, ნატოს ქმედებები არის თავდაცვითი, პროპორციული და საერთაშორისო სამართლის შესაბამისი. (North Atlantic Treaty Organization)

ასევე, როგორც ზემოთ აღვნიშნეთ, ვარშავის სამიტზე მოკავშირეებმა მიიღეს Cyber Defence Pledge ეროვნული ქსელებისა და ინფრასტრუქტურის კიბერუსაფრთხოების გაძლიერების მიზნით. აქედან გამომდინარე, თითოეული მოკავშირე პასუხისმგებელია საკუთარ კიბერ-თავდაცვაზე, მაგრამ ნატო ეხმარება თავის წევრებს სხვადასხვა გზითა და საშუალებით. (North Atlantic Treaty Organization)

4.2 ნატოს კიბერუსაფრთხოებისა და თავდაცვის შესაძლებლობები

აღნიშნულ ქვეთავში ყურადღებას გავამახვილებ იმ მნიშვნელოვან მიმართულებებსა და შესაძლებლობებზე, რაც ნატომ განავითარა ბოლო დეკადის განმავლობაში კიბერსაფრთხეებთან გამკლავების მიზნით. პირველ რიგში, უნდა აღინიშნოს ნატოს კომპიუტერული ინციდენტების რეაგირების შესაძლებლობები (NCIRC) რომელიც დაფუძნებულია ევროპაში მოკავშირეთა ძალების უმაღლესი შტაბში, მონსში, ბელგიაში. ის იცავს ნატოს საკუთარ ქსელებს მრგვალი საათის კიბერ თავდაცვის მხარდაჭერის

საშუალებით. NCIRC-ის გუნდი შედგება 200-მდე ექსპერტთა ჯგუფისგან რომლებიც უმკლავდებიან ინციდენტებს და უზრუნველყოფენ ნატოს და მის მოკავშირეებს განახლებული ანალიზით იმ კიბერ გამოწვევებისა და საფრთხეების შესახებ, რასაც დღეს საერთაშორისო საზოგადოება უპირისპირდება. NCIRC-ის ფუნქციებში ასევე შედის ნატოს საინფორმაციო სისტემის მუდმივი მონიტორინგი და ალიანსის წინააღმდეგ მიმართული კიბერინციდენტების აღრიცხვა, ასევე, განსაკუთრებით საშიში კიბერთავდასხმების შესახებ ინფორმაციის სწრაფი გავრცელება და დროული რეაგირების უზრუნველყოფა. (North Atlantic Treaty Organization, Factsheet,2017)

ნატო, ასევე, ეხმარება მოკავშირეებს გაზარდონ საკუთარი კიბერთავდაცვა შემდეგი გზების საშუალებით:

- საფრთხეების შესახებ ინფორმაციის გაზიარება რეალურ დროში მავნე ინფორმაციული გაზიარების პლატფორმის საშუალებით, როგორც კიბერ-საფრთხეებთან გამკლავების საუკეთესო პრაქტიკა;
- სწრაფი რეაგირების კიბერსაწინააღდეგო ჯგუფების მხარდაჭერა, რომლებიც შეიძლება გაიგზავნოს მოკავშირეთა დასახმარებლად კიბერ-შეტევებთან გასამკლავებლად.
- სამიზნე ჯგუფების დადგენა-განვითარება, რათა ხელი შეუწყონ საერთო მიდგომის შემუშავებას კიბერუსაფრთხოების შესაძლებლობებისთვის;

ინვესტირება განათლებაში, ტრეინინგებსა და წვრთნებში, როგორიცაა მაგალითად, „კიბერ კოალიცია“ - ერთ-ერთი უმსხვილესი კიბერთავდაცვის სწავლება მსოფლიოში. (North Atlantic Treaty Organization, Factsheet,2017)

რამდენიმე ორგანო ასევე ხელს უწყობს ალიანსს და ცალკეულ წევრ სახელმწიფოებს კიბერუსაფრთხოების გასაუმჯობესებლად.

ნატოს კომუნიკაციებისა და საინფორმაციო სააგენტო, რომლის შტაბ-ბინებიც მდებარეობს ბრიუსელში, მონსსა და ჰააგაში, მხარს უჭრს ნატოს ოპერაციებს,

აკავშირებს ნატოს საინფორმაციო და საკომუნიკაციო სისტემებს და იცავს ნატოს ქსელებს. (North Atlantic Treaty Organization, Factsheet,2017)

ნატოს Cyber Range ტარტუში, ესტონეთში გამოიყენება კიბერ ექსპერტების მიერ, რათა განავითარონ თავიანთი შესაძლებლობები რეალისტური წვრთნების საშუალებით. Cyber Range ხელს უწყობს ნატოს წამყვან ყოველწლიურ კიბერუსაფრთხოების წვრთნებს „კიბერ კოალიციას“. (North Atlantic Treaty Organization, Factsheet,2017)

ნატოს კოოპერაციული კიბერთავდაცვის ცენტრი (CCDCOE) ტალინში, ესტონეთში წარმოადგენს ნატოს აკრედიტებულ კვლევით და სასწავლო დაწესებულებას, რომელიც მიმართულია კიბერ თავდაცვის შესახებ განათლების მიღების, კვლევის წარმოებისა და განვითარებისკენ. ცენტრი კიბერუსაფრთხოების საკითხებზე ექსპერტიზულ გამოცდილებას გვთავაზობს. (North Atlantic Treaty Organization, Factsheet,2017)

ნატოს საკომუნიკაციო და ინფორმაციული სისტემების სკოლა ლათინაში (NCISS), იტალიაში, უზრუნველყოფს როგორც ალიანსის წევრი ქვეყნების, ასევე არაწევრი პარტნიორი სახელმწიფოების პერსონალისთვის სწავლებებს ნატოს საკომუნიკაციო და საინფორმაციო სისტემების ოპერაციების შესახებ. სკოლა უახლოეს პერიოდში გადავა ოეირასში, პორტუგალიაში, სადაც ის უფრო მეტ ყურადღებას გაამახვილებს სასწავლო და საგანმანათლებლო საკითხებზე კიბერთავდაცვის მიმართულებით. (North Atlantic Treaty Organization, Factsheet,2017)

ნატოს სკოლა ქალაქ ობერმერგაუში, გერმანიაში, ასევე, მართავს კიბერ საკითხებთან დაკავშირებულ ტრეინიგებსა და საგანმანათლებლო სწავლებებს, რათა მხარი დაუჭიროს ალიანსის ოპერაციებს, სტრატეგიას, პოლიტიკას, დოქტრინასა და პროცედურებს. (North Atlantic Treaty Organization, Factsheet,2017)

ნატოს თავდაცვის კოლეჯი რომში, იტალიაში კი ხელს უწყობს სტრატეგიულ აზროვნებას სამხედრო-პოლიტიკურ საკითხებზე, მათ შორის კიბერუსაფრთხოების სფეროში. (North Atlantic Treaty Organization, Factsheet,2017)

4.3 თანამშრომლობა პარტნიორებთან

პარტნიორობა მნიშვნელოვან როლს ასრულებს კიბერგამოწვევებზე ეფექტურად გასამკლავებლად. ნატო პარტნიორობის ფართო ქსელს მოიცავს, მათ შორის საერთაშორისო ორგანიზაციებს, ინდუსტრიულ სფეროსა და აკადემიურ წრეს.

კიბერუსაფრთხოება ასევე ნატოსა და ევროკავშირს შორის გაძლიერებული თანამშრომლობის ერთ-ერთ უმნიშვნელოვანეს სფეროს წარმოადგენს, როგორც ორი ორგანიზაციის გაძლიერებული და კოორდინირებული ძალისხმევა ჰიბრიდული საფრთხეების წინააღმდეგ. ნატო და ევროკავშირი იზიარებენ ინფორმაციას კიბერ-კრიზისის რეაგირების ჯგუფებს შორის და ცვლიან საუკეთესო პრქტიკებს. (North Atlantic Treaty Organization, Factsheet,2017)

ევროკავშირი, ასევე, შეიმუშავოს ჩარჩო დოკუმენტი, სადაც განისაზღვრება კიბერშეტევებზე საპასუხო დიპლომატიური რეაქციის ნორმებიმ მათ შორის სანქციები. ეს გახდება ევროკავშირის ქვეყნების ერთობლივი კიბერდიპლომატიის შემადგენელი ნაწილი. დოკუმენტის მიზანია ხელი შეუწყოს კიბერუსაფრთხოების სფეროში კონფლიქტების პრევენციას, კიბერსაფრთხეების შემცირებას და საერთაშორისო ურთიერთობაში სტაბილურობას. (The Council of the European Union)

ნატო ასევე ეხმარება პარტნიორ ქვეყნებს კიბერ-გამოწვევებთან საბრძოლველად.

გარდა ამისა, კიბერუსაფრთხოების გამოწვევებთან საბრძოლველად მნიშვნელოვანია კერძო სექტორთან თანამშრომლობა, რადგან ისინი მნიშვნელოვანი მოთამაშეები არიან კიბერსივრცეში და მათი ცოდნა და ექსპერტიზა გასათვალისწინებელია ზემოთ აღნიშნულ გამოწვევებთან გასამკლავებლად. შესაბამისად, ნატო აძლიერებს კავშირებსა და თანამშრომლობას ინდუსტრიის წარმოამდგენლებთან ნატოს ინდუსტრიული კიბერ პარტნიორობის პლატფორმის საშუალებით, რომელიც მხარ უჭერს ნატოს შესაძლებლობებს, დაიცვას ჩვენი ქსელები, გაზარდოს მოქნილობა და დაეხმაროს

მოკავშირეებს კიბერ-შესაძლებლობების განვითარებაში. (NATO Cyber Defence factsheet, December 2017)

ინფორმაციის გაცვლა, წვრთნები, ტრეინინგები და განათლების მიღება წარმოადგენს იმ მცირე მაგალითებს, სადაც ნატო თავის პარტნიორებთან ერთად მუშაობს აღნიშნულ გლობალურ გამოწვევებთან დასაპირისპირებლად. (NATO Cyber Defence factsheet, December 2017)

5. ლიტერატურის მიმოხილვა

ძალიან მნიშვნელოვანია იმის გარკვევა და ანალიზი თუ მკლევარებსა და პოლიტიკის შემქმნელებს როგორ ესმით და იზიარებენ ტექნოლოგიურ მახასიათებლებსა და იმ გამოწვევებს, რასაც ინტერნეტი და ციფრული და საკომუნკაციო ტექნოლოგიები უქმნიან ეროვნულ და საერთაშორისო უსაფრთხოებას. როგორც აკადემიური წრეებში, ასევე სამთავრობო უწყებებში დღემდე დიდი დავა და განხილვა, ასევე აზრთა სხვადასხვაობაა როგორც კიბერ სივრცის, ასევე კიბერ სივრციდან მომდინარე საფრთხეების განმარტებასა და კონცეპტუალიზაციათან დაკავშირებით.

წინამდებარე ქვეთავში შევეცდები გავაანალიზო და მიმოვიხილო რამდენიმე მნიშვნელოვანი ნაშრომი, მკვლევართა და ექსპერტთა შეფასება და დამოკიდებულება, რომელიც შეესაბამება საკველევ კითხვასა და ჰიპოთეზას. ასევე გავაანალიზებ მსოფლიო ლიდერებისა და პოლიტიკოსების განცხადებებს საკვლევი საკითხთან მიმართებაში.

როდესაც ცალკეული სახელმწიფო, სახელმწიფოთა გაერთიანება თუ მთლიანი საერთაშორისო საზოგადოება დგას დილემის წინაშე, როგორ დაიცვას თავი შესაძლო კიბერ-საფრთხეებისგან, აკადემიური წრეების წარმომადგენლები, საგნის მკვლევარები

თუ უბრალოდ პოლიტიკოსები სხვადასხვაგვარ დამოკიდებულებას ამჟღავნებენ. მაგალითად, ზოგიერთს მიაჩნია, კიბერ-შეტევებისა და პროგრამული ვირუსების შესაჩერებლად უნდა შექმნას ძლიერი თავდაცვითი სტრუქტურები, რადგან მსგავსი ტიპის საფრთხეები თავიდან აცილებული იქნას (Averbuch & Siboni, 2013); მაგრამ, როგორც პრაქტიკა და საერთაშორისო გამოცდილება გვიჩვენებს, ასეთი ტრადიციული მიდგომა არის მოწყვლადი და ვერანაირად შეაჩერებს თავმდასხმელს. თან იმასაც თუ გავითვალისწინებთ, რომ როცა სახელმწიფო ან თუნდაც ორგანიზაცია ავითარებს თავის ტექნოლოგიურ შესაძლებლობებს, პარალელურად მეტოქეც ძლიერდება, იმავე ტექნოლოგიური ინოვაციების საშუალებით.

ინფორმაციის ხელმისაწვდომობის გაზრდა მეწარმეებსა და ინოვატორებს შესაძლებლობას აძლევს ითანამშრომლონ ახალი ტექნოლოგიების განვითარებასა და არსებულის გაუმჯობესებაში. თუმცა, პოტენციურ მოწინააღმდეგეებს შეუძლიათ გამოიყენონ იგივე ტექნოლოგიები, რომელიც ტერორის ექსპორტს უწყობს ხელს მთელი მსოფლიოს მასშტაბით. (Pavel Macko, Armed Forces in the 21st Century, 2014, გვ.219)

მოწინავე ინდუსტრიული ქვეყნებისთვის კიბერ-ომი არის როგორც კარგი შესაძლებლობა, ასევე უზარმაზარი საფრთხე. პრინციპული კიბერ-თავდასხმები, რომლის სამიზნეც მაგალითად ირანი გახდა 2010 წელს Stuxnet-ის კიბერ თავდასხმით, მტრის ინსდუსტრიული და სამხედრო ობიექტების განადგურების საშუალებას იძლევა, მაგრამ დასავლური ქვეყნების ხელმძღვანელებშიც კი კოშმარულ განცდებს იწვევს ის, რაც მათ მშობლიურ ქვეყნებში კომპიუტერული სისტემების დაუცველობას უკავშირდება (Rachman, 2010).

კიბერუსაფრთხოება ხშირად განიხილება როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. ახალი ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეები, რომლებიც დიდ ზიანს აყენებს კიბერსივრცეს და მის მომხმარებელს. სახელმწიფოს და სახელისუფლებო ორგაონოებს პირველ რიგში ადარდებთ ეროვნული უსაფრთხოების უზრუნველყოფა,

კრიტიკული ინფორმაციისა და ინფორმაციული ინფრასტრუქტურის დაცვა როგორც უცხო სახელმწიფოს, ისე არასამთავრობო სუბიექტებისა და დაჯგუფებების მხრიდან ხელყოფისგან, რათა თავიდან იქნას აცილებული ინფორმაციის მოპარვა ან/და გადაცემა, ქსელის დაზიანება ან/და საერთოდ განადგურება. სახელმწიფოს უსაფრთხოების რეალურ საფრთხეს წარმოადგენს კიბერშეტევები, რომლებიც მიმართულია ისეთი სასიცოცხლო მნიშვნელობის მქონე ინფრასტრუქტურის განადგურებისკენ, როგორებიცაა სატელეკომუნიკაციო ქსელების, ენერგოგენერირებისა და ნავთობგადამამუშავებელი სიმძლავრეების სისტემები, ასევე ელექტრომომარაგების, საფინანსო, ჯანდაცვისა და სატრანსპორტო სისტემები. (ვლადიმერ სვანაძე, 2015)

კიბერსივრცე დღესდღეისობით არსებული მდგომარეობით ნაკლებად დაცულია, რასაც ხელს უშლის სახელმწიფო და კერძო სექტორებს შორის ნაკლები კომუნიკაცია და იმ განსვავებული მოტივაციის, ინტერესებისა და მიზნების არსებობა, რაც ახასიათებს თითოეულ სექტორს. ყოველივეს ემატება ის გარემოებაც, რომ ტექნოლოგიური განვითარების პარალელურად ვითარდება ასევე კიბერდანაშაულებები, ვინაიდან ისინი ყოველი ნოუ ჰაუს აქტიური მომხმარებლები არიან. (ვლადიმერ სვანაძე, 2015)

ის რომ კიბერ უსაფრთხოება როგორც ეროვნული ისე საერთაშორისო უსაფრთხოების მნიშვნელოვან საკითხად იქცა, ამას ადასტურებს როგორც მსოფლიო ლიდერების განცხადებები, ასევე წამყვანი სახელმწიფოების დღის წესრიგში საკითხის მნიშვნელოვან ნაწილად წამოწევა.

ამერიკის შეერთებული შტატების პრეზიდენტი დონალდ ტრამპი ცალსახად აფიქსირებს თავის დამოკიდებულებას, რომ კიბერუსაფრთხოება წარმოადგენს ეროვნული თავდაცვის პრიორიტეტს. 2017 წლის დეკემბერში კი გამოქვეყნებულ ახალი სტრატეგიული დოკუმენტის მიხედვით, თეთრი სახლი გარკვევით აფიქსირებს თავის პოზიციას: „საფრთხე კიბერუსაფთხოებისთვის, არის საფრთხე ამერიკის სტაბილურობისთვის“. პრეზიდენტ ტრამპის ადმინისტრაცია სტრატეგიულ დოკუმენტში რამდენჯერმე ხაგზასმით გამოჰყოფს კიბერუსაფრთხოებასთან

დაკაშირებულ საკითხებს და ასევე, არ ერიდება, დაასახელოს ის ქვეყნები რომლებიც მოსალოდნელია რომ იყენებენ ან გამოიყენებენ კომპიუტერულ ქსელებს იარაღად აშშ-ს წინააღმდეგ. საპასუხოდ, დოკუმენტში აღნიშნულია, რომ „ამერიკის შეერთებული შტატები შეაკავებს, დაიცავს და, საჭიროების შემთხვევაში, დაამარცხებს მავნე, ვირუსულ აქტორებს, რომლებიც აშშ-ს წინააღმდეგ კიბერ-შესაძლებლობებს იყენებენ.“ National Security Strategy of the United States of America, December 2017

რაც შეეხება თავად ნატოს ლიდერების დამოკიდებულებას და განცხადებებს კიბერ უსაფრთხოების საკითხთან მიამრთებაში, 2017 წლის ნოემბერში, პრე-მინისტერიალის პრენსკონფერნეციაზე ნატოს გენერალურმა მდივანმა იანს სტოლტენბერგმა ყურადღება გაამახვილა კიბერუსაფრთხოების შესახებ და აღნიშნა, რომ ეს საკითხი დღის წესრიგის მნიშვნელოვან საკითხს წარმოადგენდა. (North Atlantic Treaty Organization) შედეგად, 2017 წლის ნოემბრის მინისტერიალზე, კიბერ-შეტევებიდან მომდინარე მზარდი საფრთხეების გათვალისწინებით, ნატოს წევრი ქვეყნების თავდაცვის მინისტრებმა დაამტკიცეს ერთგვარი პრინციპების ნაკრები, თუ ალიანსს როგორ შეუძლია სამხედრო ოპერაციებში ალიანსის კიბერ-შესაძლებლობების ინტეგრირება. მინსიტრები ასევე შეთანხმდნენ ახალი კიბერ-ოპერაციების ცენტრის შექმნაზე, რათა დაეხმარონ კიბერის ინტეგრირებას ნატოს დაგეგმვისა და ოპერაციების ყველა დონეზე. ეს კი იყო შემდეგი ნაბიჯი მას შემდეგ, რაც 2016 წელს ნატოს წევრებმა კიბერი აღიარეს როგორც სამქომედო განზომილებად მსგავსად ხმელეთის, ზღვისა და ჰაერისა. (North Atlantic Treaty Organization)

გარდა ზემოთ აღნიშნულისა, ნატოს გენერალურმა მდივანმა მის ერთ-ერთ ინტერვიუში გერმანულ გაზეთთან "Die Welt", განაცხადა, რომ გასულ წელს ნატოში კიბერ-შეტევის რაოდენობა მნიშვნელოვნად გაიზარდა. ალიანსის ხელმძღვანელი შიშობს, რომ კიბერ-თავდასხმებს სასიცოცხლო და კრიტკული მნიშვნელობის ინფრასტრუქტურაზე შესაძლებელია განსაკუთრებით გამანადგურებელი ხასიათი ჰქონდეს. გენერალური მდივნის განცხადებით, ასევე, 2016 წელს 500-მდე საშიში კიბერ-შეტევა განხორციელდა

ნატოს სხვადასხვა მნიშვნელოვან ობიექტებზე ყოველთვიურად; რაც წარმოადგენდა წინა წელთან შედარებით 60%-იან ზრდას. სტოლტენბერგმა, ასევე, დაამატა, რომ ალიანსის მონაცემთა ქსელებზე თავდასხმების უმრავლესობა სახელმწიფო ინსტიტუტების მიერ ფინანსდება ვიდრე, კერძო პირების მიერ. (http://p.dw.com/p/2W1fe)

ნატოს გენერალური მდივნის იენს სტოლტენბერგის განცხადებით, უსაფრთხოების კუთხით ალიანსის მიერ განხორციელებული ქმედებები კიბერსივრცეზეც გავრცელდება, რომელიც ბოლო პერიოდში საფრთხის შემცველი გახდა როგორც მთლიანად ორგანიზაციისთვის, ისე მისი ცალკეული წევრი ქვეყნისთვის. სტოლტენბერგმა ამის საჭიროებისთვის მაგალითად მოიყვანა 2017 წლის მაისში განხორციელებული მასშტაბური კიბერ-შტევები, რომელმაც და რომლის მსგავსმა თავდასხმებმაც შესაძლებელია საფრთხე შეუქმნას და მოწყვალდი გახადოს ალიანსის კიბერ თავდაცვის სისტემა. შესაბამისად, სტოლტენბერგმა კიდევ ერთხელ აღნიშნა, რომ კიბერსივრცე სამხედრო მოქმედებათა ისეთივე სფერო გახდა, როგორიც ხმელეთი, ზღვა და ჰაერი. მისი თქმით, ნატოს ნებისმიერ წევრ ქვეყანაზე კიბერშეტევის შემთხვევაში შესაძლოა ამოქმედდეს ჩრდილოატლანტიკური ხელშეკრულების მე-5 მუხლი, რომლის თანახმადაც ალიანსის ერთ წევრზე თავდასხმა ყველა წევრზე თავდასხმად განიხილება. (North Atlantic Treaty Organization)

ასევე, 2017 წლის მიწურულს, ნატოს გენერალური მდივნის მოადგილე, როუზ გოტმიოლერი დაესწრო ნატოს კიბერ უსაფრთხოების კონფერენციას მონსში, ბელგიაში, სადაც ისაუბრა კიბერუსაფრთხოების სასიცოცხლო მნიშვნელობის შესახებ. „კიბერ-თავდასხმები არის სერიოზული. მათ გააჩნიათ პოტენციალი რომ ძირი გამოუთხაროს ნატოს მისიასა და ძირითად ამოცანებს მსოლიოს მასშტაბით და ხელი შეუშალონ ჩვენს შესაძლებლობას, ვუზრუნველყოთ კოლექტიური თავდაცვა. სწორედ ამიტომ, კიბერუსაფრთხოება წარმაოდგენს ნატოსა და ნატოს მოკავშირეებისთვის უმთავრეს პრიორიტეტს“. (North Atlantic Treaty Organization)

6. თეორიული ჩარჩო

წინამდებარე თავში განხილული იქნება საერთაშორისო ურთიერთობების თეორიული მიდგომა, რომელიც მიესადაგება ჩემს კვლევას და ქვემოთ განხილული თეორიით შევეცდები ავხსნა ნაშრომში წარმოდგენილი ჰიპოთეზა.

როგორც უკვე არაერთგზის ვახსენეთ, აღნიშნული ნაშრომი მიზნად ისახავს კვლევის პროცესში დაამტკიცოს ჰიპოთეზა, რომ საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებამ ნატოს სამხედრო პოლიტიკური სტაბილურობა თანამედროვე გამოწვევების წინაშე მოწყვლადი გახადა და ალიანსის დღის წესრიგისა და ძირითადი ამოცანების ტრანსფორმაცია განაპირობა.

ნაშრომში თეორიულ ჩარჩოდ გამოყენებული მაქვს ლიბერული ინსტიტუციონალიზმი და ურთიერთდამოკიდებულების ლიბერალური თეორია.

ლიბერალური ინსტიტუციონალიზმის მიხედვით, რომელიც წარმოადგენს თანამედროვე საერთაშორისო ურთიერთობების თეორიას და თავის მხრივ ემყარება ლიბერალურ თეორიას, ომები და კონფლიქტები არ არის გარდაუვალი. მიუხედავად იმისა, რომ აღნიშნული მიდგომა იზიარებს რეალიზმის ძირითად დებულებას იმის შესახებ, რომ საერთაშორისო სისტემაში სახელმწიფოები არიან მთავარი აქტორები, ლიბერალური ინსტიტუციონალიზმის მიხედვით – საერთაშორისო ურთიერთობებში არის საკმარისი სივრცე და საშუალება რათა სახელმწიფოებმა ითანამშრომლონ, ინსტიტუტები და ორგანიზაციები კი ამ წარმატებული თანამშრომლობის საშუალებას იძლევა.

ინსტიტუტები სიცოცხლისუნარიანნი არიან, ამასთან, გაცილებით ადვილია, საჭიროების შემთხვევაში, მათი გარდაქმნა, ვიდრე ახლის ჩამოყალიბება. შესაბამისად, იმ შემთხვევაში, თუ ორგანიზაციის წინაშე ახალი გამოწვევა შეიქმნება, ისეთი, როგორიც მისი შექმნისას გათვალისწინებული არ იყო, ქვეყნები ორგანიზაციის დაშლის

და სხვა ინსტიტუტის ჩამოყალიბების ნაცვლად, არსებულის მოდიფიკაციას ახდენენ, რათა მოარგონ თანამედროვე გამოწვევებს. (Robert Keohane, 1984)

თუმცა, მნიშვნელოვანია გავითვალისწინოთ ის მნიშვნელოვანი გარემოება, რომ ინსტიტუტის არსებობა შესაძლებელია მხოლოდ იმ პირობებში, როდესაც ორგანიზაცია ემსახურება მასში შემავალ ქვეყნებს. ინსტიტუტებს გააჩნიათ თუ არა ადაპტირების უნარი, დამოკიდებულია იმაზე, მისი საშუალებები – კონკრეტული თუ ზოგადი - ნორმების, წესებისა და პროცედურების ჯამი, რამდენად შეესაბამება წევრი სახელმწიფოების ინტერესებს. (Celeste Wallander, 2000, გვ.705-706)

ცივი ომის დასრულების შემდგომ, ნატოს წევრმა ქვეყნებმა, შექმნილი უსაფრთხოების პრობლემის გადაჭრა კვლავ ალიანსის საშუალებით მოახერხეს, ორგანიზაციის უკვე კარგად ჩამოყალიბებული ზოგადი საშუალებებისა და მათი ახალი მიზნებისთვის გამოყენების გზით. ნატო-ს ცალკეულმა სტრუქტურებმა ტრანსფორმაცია განიცადა.

ვოლანდერის მიხედვით, ნატოს სიცოცხლისუნარიანაობის ახსნა, შესაძლებელია ალიანსში არსებული შემდეგი ფაქტორების გათვალისწინებით: გამჭვირვალობა წევრ სახელმწიფოთა შორის, სამხედრო ძალების მაღალი სამოქალაქო კონტროლი, კონსულტაციების პრაქტიკა, ინტეგრირებული სარდლობის სტრუქტურა, წევრ-სახელმწიფოთა შესაბამისობა, საერთო ლოჯისტიკა და საჰაერო თავდაცვა. ასევე, მნიშვნელოვანია საერთო ეკონომიკური ინფრასტრუქტურა. (Celeste Wallander, 2000, გვ.705-706)

რობერტ მაკკალას მიხედვით, რომელიც ნატოს გაფართოების ანალიზს ასევე ლიბერალური ინსტიტუციონალიზმის საშუალებით ახდენს, ჯერ კიდევ 1996 წელს, მაშინ, როდესაც ნატოს გაფართოება არ იყო ისეთი მასშტაბური, აცხადებდა, რომ ბანაკების აკეცვის, გამარჯვების გამოცხადების და ახალი ინსტიტუტის მშენებლობის მაგივრად, წევრი ქვეყნები ალიანსს ახალ მიმართულებას მისცემენ, არსებული მექანიზმების და პროცედურების გამოყენებით, ზედ დააშენებენ წარსულ წარმატებებს,

რათა გაუმკლავდნენ ახალ პრობლემებს. მაკკალა თავის ნაშრომში აღწერს თუ როგორ გაინთავისუფლა ნატომ თავი ცივი ომის დროინდელი ინსტიტუტებისგან და ჩაანაცვლა ისინი ახალი მექანიზმებით, რომლებიც საჭირო იყო ახალ საფრთხეებთან გასამკლავებლად. (Robert McCalla, 1996, გვ.646)

მიუხედავად იმისა, რომ მაკკალა ინსტიტუციონალისტური მიდგომით ნატოს ტრანსფორმაცას ხსნის, იგი ასევე დასძენს, რომ ეს არ არის საკმარისი, რადგან ეს არ არის სრულყოფილი ანალიზი პროცესისა. ავტორის აზრით, მნიშვნელოვანი ფაქტორია წევრ სახელმწიფოთა ურთიერთობები და მიმდნარე პროცესები, რადგან საბოლოო ჯამში, სწორედ წევრი სახელმწიფოები არიან ის დონორები, რომლებიც განაპირობებენ ინსტიტუტებისა და საერთაშორისო ორგანიზაციების ფუნქციონირებას. (Robert McCalla, 1996, გვ.646)

ზემოთ განხილული მსჯელობა კი გვაძლებს იმის მტკიცების შესაძლებლობას, რომ დღეს ყველაფერი უწყობს ხელს ნატოს, რომ კიდევ ერთხელ ტრანსფორმირდეს თანამედროვე გამოწვევების შესაბამისად.

ასევე უნდა განვიხილოთ ურთირთდამოკიდებულის ლიბერალური თეორიის ისეთი წარმომადგენლების დამოკიდებულება წინამდებარე ნაშრომის კვლევის პროცესში, როგრებიც არიან ჯოზეფ ნაი და რობერტ კიოჰანი და მათი ნაშრომი „ძალა და ურთიერთდამოკიდებულება“ (1977). მათი მტკიცებით, მეორე მსოფლიო ომის შემდგომი საერთაშორისო ურთიერთობები უფრო კომპლექსური და გაცილებით რთულია, ვიდრე ეს ასე იყო. ადრე თუ ერთადერთი საშუალება ძალის გამოყენება იყო წამოჭრილი პრობლემების გადასაჭრელად, დღეს სამხედრო ძალა და შეიარაღება უკვე ნაკლებად გამოყენებადი ინსტრუმენტია.

მოდერნიზაციის გავლენის გამოძახილია ნაის და კიოჰეინის უახლესი ნაშრომი ამ თემაზე, ,,ძალა და ურთიერთდამოკიდებულება საინფორმაციო საუკუნეში,” რომელიც

ავტორებმა 1998 წელს სტატიის სახით დაბეჭდეს ცნობილ ჟურნალ საგარეო ურთიერთობებში (Foreign Affairs). ამ სტატიის სიახლე ისაა, რომ ნაი და კიოჰენმა ყურადღება მიაპყრეს საერთაშორისო ურთიერთობებში ინფორმაციის მნიშვნელობას და გვამცნეს, რომ ,,სავარაუდოა რომ ახალ საუკუნეში სინფორმაციო ტექნოლოგია იქნეს ყველაზე მნიშვნელოვანი რესურსი (power resource).” მათი თქმით, უკვე დაიწყო ახალი ხანა, ე.წ. ,,საინფორმაციო რევოლუცია” რომელიც ჯერ კიდევ საწყის ეტაპზეა, მაგრამ უკვე იქონია დიდი ზეგავლენა კომპლექსური ურთიერთდამოკიდებულების სამ ძირითად კომპონენტებზე:

1. საზოგადოებათაშორისი კონტაქტები;

2. სამხედრო ძლიერების როლის შესუსტება;

3. უსაფრთხოება, როგორც ნაკლებ მნიშვნელოვანი საკითხი. (აკობია ეკა, საერთაშორისო ურთიერთობების თეორია, 2006).

როგორც ავტორები აცხადებენ, მიუხედავად იმისა, რომ საინფორმაციო რევოლუციამ საგრძნობლად შეცვალა და გააღრმავა საზოგადოებებს შორის კონტაქტი, სამხედრო სიძლიერისა და უსაფრთხოების მნიშვნელობისა და გავლენის შემცირება ბოლომდე ვერ შეძლეს და ეს ეტაპი ჯერჯერობით საწყის ეტაპზეა.

რომ შევაჯამოთ, აღნიშნულ თავში განხილული თეორიებით შევეცადე ამეხსნა როგორც ალიანსის ტრანსფორმაციის შესაძლებლობა და მისი ბუნება, ასევე საინფორმაციო და საკომუნიკაციო ტექნოლგიების გავლენა ტრადიციული სამხედრო ძლიერების როლის შესუსტებაზე და საერთაშორისო უსაფრთხოების მოწყვლადობაზე.

დღევანდელი გადასახედიდან თუ შევხედავთ, მართალია, რომ სამხედრო სიძლიერე და ეროვნული უსაფრთხოება მნიშვნელოვან რგოლად რჩება, თუმცა ისიც ფაქტია, რომ რაც არ უნდა ძლიერი და მოდერნიზებული სამხედრო შეირაღება გყავდეს, ნებისმიერ დროს

თუ განხოციელდა კიბერ-სივრციდან გამანადგურებული და მასირებული თავდასხმა, მას შეიარაღებული სამხედრო კონტიგენტი ვერ უშველის. შესაბამისად, რომელიმე კონკრეტული ქვეყნის ან მთლინი ალიანსის სტაბილურობა კითხვის ნიშნის ქვეშ დადგება და მას სერიოზული საფრთხე დაემუქრება. ეს იმითაც არის განპირობებული, რომ ვერ მოხდება სწრაფად იმის დადგენაც, ვინაა მტერი, რადგან შეიძლება შეტევის განმახორციელებელი იყოს ერთ კონტინენტზე, IP მისამართი იყოს დარეგისტრირებული მეორე კონტინენტზე, ხოლო დამკვეთი საერთოდ სხვა კონტინენტს წარმოადგენდეს. შესაბამისად, ამ დროს სამხედრო მობილიზება და იერიში ვერ დაიწყება და ვერც იქნება ეფექტური.

7. კიბერუსაფრთხოების გამოწვევები და ნატოს ტრანსფორმაციის უნარი - არის თუ არა ნატოს დღევანდელი როლი და აქტივობები საკმარისი?

წინამდებარე ნაშრომის განმავლობაში, ხშირად აღვნიშნეთ, რომ ნაშრომის მთავრი საკვლევი კითხვა მდგომარეობდა იმაში, თუ როგორი გავლენა მოახდინა კიბერუსაფრთხოების გამოწვევებმა ნატოს დღის წესრიგის ტრანსფორმაციაზე 2002 წლიდან დღემდე. სხვადასხვა სამეცნიერო სტატიის, ოფიციალური დოკუმენტებისა თუ მსოფლიო ლიდერების განცხადებების ანალიზით, დავინახეთ, რომ ჩრდილოატლანტიკური ალიანსის დღის წესრიგში როგორც ტერმინი კიბერი, ასევე კიბერუსაფრთხოების გამოწვევები უმნიშვნელო საკითხიდან ერთ-ერთ უაღრესად დიდი მნიშვნელობის მქონე თემად იქცა, რომელზეც ყურადღება დღითიდღე იზრდება და ნატოს დღის წესრიგშიც და ძირითად ამოცანებშიც მნიშვნელოვან ადგილს იკავებს. იგი უკვე იქცა ნატოს სამიდან ერთ-ერთი უმთავრესი პრინციპის - კოლექტიური

თავდაცვის შემადგენელ ნაწილად. მაგრამ, ამ მსჯელობის პარალელურად, მოვლენების სწორი ანალიზისთვის საჭიროა მეორე მხარის ანალიზიც.

როგორც თემის კვლევის პროცესში და ზემოთ აღნიშნულ მსჯელობებში დავინახეთ, ნატო და მისი წევრი ქვეყნები ყველანაირად ცდილობენ მხარი აუბან ტექნოლოგიურ ცვლილებებს, მოახდინონ სწრაფი ადაპტირება და შესაძლო საფრთხეებზე სწრაფი რეაგირებისთვის ყველანაირად სრულყოფილად დაიცვან თავი შესაძლო კიბერ-საფრთხეებისგან. მაგრამ, მეორე მხარეს გვყავს პოტენციური მეტოქე სახელმწიფოები, როგორებიცაა რუსეთი და ჩინეთი, ასევე, სხვა განვითარებადი სახელმწიფოები, რომლებიც სწორედ ტექნოლოგიური განვითარებების საშუალებით ცდილობენ გაძლიერდნენ და ასე გაუტოლდნენ მათზე ძლიერ და განვითარებულ ქვეყნებს. მაგალითად, ვიცით, რომ, როგორც ნატო ერთიანად, ასევე, თუნდაც მისი წევრები ცალ-ცალკე, მაგალითისთვის, ამერიკის შეერთებული შტატები სამხედრო-პოლიტიკური სიძლიერითა და სტაბილურობით ბევრად აღემტება მის კონკურენტ და მეტოქე სახელმწიფოებეს, თუმცა სწორედ კიბერსივრცე არის ის განზომილება, სადაც მოქმედება და თუნდაც ბრძოლა, ასევე შეიარაღება არის ასიმეტრიული. ასიმეტრიულ სიტუაციაში კი ძნელია განსაზღვრო ვინაა ძლიერი და ვინაა სუსტი, რადგან მეტოქის სიძლიერეს ვერ აფასებ. ასევე, რთულია წინასწარ განსაზღვრო შესაძლო დაპირისპირების შემთხვევაში ვინ იქნება გამარჯვებული. ინტერნეტის იარაღიზაციის საშუალებით პოტენციურად მეტოქე სახელმწიფოები, როგორებიცაა ჩინეთი და რუსეთი, ბევრად უფრო საშიშ ძალას წარმოადგენენ, რადგან ტექნოლოგიური განვითარებით ისინიც ისევე სარგებლობენ, როგორც თუნდაც აშშ და ნატოს სხვა წევრი სახელმწიფოები.

გარდა კიბერსივრცის და კიბერუსაფრთხოების ასიმეტრიულობისა, ასევე, მსურს, ყურადღება გავამახვილო თანამედროვე კიბერ-გამოწვევების წინაშე ნატოს არა მხოლოდ დღის წესრიგის, არამედ მისი სრული ტრანსფორმაციის შესაძლებლობაზე. მართალია, რომ ნატოს დღის წესრიგში კიბერუსაფრთხოების საკითხი

უმნიშვნელოვანეს ადგილს იკავებს, მაგრამ, რეალურად, რამდენად შეიცვალა თავად ორგანიზაცია, ან რამდენად მდგრადია ალიანსი და მისი სტრუქტურა კიბერ-საფრთხეების წინაშე, ესეც კითხვის ნიშნის ქვეშ დგას. რეალურად, ჩვენ ზემოთ მსჯელობისას უკვე განვიხილეთ საერთაშორისო ურთიერთობებში და კიბერსივრცეში მომხდარი მნიშვნელოვანი და ყურადსაღები კიბერ-ინციდენტები და მათი გავლენა როგორც ცალკეული ქვეყნების, ასევე სახელმწიფოთა გაერთიანებებსა და მათ ქმედებებზე, მაგრამ, მეორე მხრივ, ფაქტი სახეზეა, რომ ისტორიაში არ ყოფილა პრეცედენტი იმისა, რომ მომხდარიყო ფატალური შედეგის კიბერ-თავდახმა, რომელიც კატასტროფულ შედეგს გამოიწვევდა. მართალია, იყო მრავალი შემთხვევა, რომელიც ამის საშიშროების წინაშე აყენებდა საერთაშორისო საზოგადოებას, თუმცა, ჯერ რეალობაში მსგავსი კატასტროფა არ მომხდარა. პირადად ჩემი მოსაზრებაა, რომ ახლო მომავალში შესაძლებელია მსგავსი პრეცედენტიც ვიხილოთ, თუმცა, დღემდე მსგავსი რამ რომ არ ყოფილა ეს ნათელია. შესაბამისად, ამ შემთხვევაში, თუ ნატოს და მის წევრი ქვეყნების მოქმედებებს განვიხილავთ, დავინახავთ, რომ სიტყვიერად თუ წერილობით თითოეული წვერისა თუ ალიანსის დღის წესრიგში საკითხი ზემდეტად აქტუალურიცაა, ლიდერები არც ხმამაღალ განცხადებებს ერიდებიან და ეროვნული უსაფრთხოების სტრატეგიებშიც მნიშვნელოვან ადგილს უთმობენ; ასევე, აღიარებენ კოლექტიური თავდაცვის კომპონენტად. მაგრამ ფაქტი ჯიუტია: მიუხედავად იმისა, რომ ბოლო წლებში მრავალი ვირუსული კიბერ-თავდასხმები განხორციელდა, პრაქტიკაში განხორციელებული მნიშვენლოვანი საპასუხო ქმედებები არ ჩანს. ეს შესაძლებელია იმითაც იყოს განპირობებული, რომ მოწინააღმდეგეს არც სურდა ამ დრომდე მოვლენები ზედმეტად სახიფათო / დამანგრეველ ეტაპზე გადაეყვანა. შესაბამისად, როცა რეალობა დადგება ფაქტის წინაშე, რთული სათქმელია, თუ როგორ მოიქცევა ალიანსი და რამდენად შეძლებს აღნიშნულ შესაძლო საფრთხესთან გამკლავებას. მართალია, ნატო ცდილობს აღიჭურვოს და თანამედროვე ტექნოლოგიური გამოწვევების წინაშე მომზადებული იყოს, მაგრამ მეორე მხრივ, არ ვიცით რას გვიმზადებს მოწინააღმდეგე და მისი ვირტუალური შესაძლებლობები.

გარდა ამისა, უნდა აღვნიშნოთ კიბერსივრცეში საერთაშორისო სამართლის მისადაგება. რამდენადაც ნატო და მისი წევრი ქვეყნები აღიარებენ რა კიბერსივრცეს მეხუთე განზომილებად და უშვებენ მოვლენათა იმ განვითარებას, რომ ომი განხორციელდეს კიბერსივრცეში და საერთაშორისო სამართალი, მათ შორის გაეროს ქარტია მიესადაგებოდეს კიბერსივრცეს, სანამ საერთაშორისო სამართლით და სამართლებრივი ნორმებით ყველაფერი არ იქნება მიღებული და საერთაშორისო თანამეგობრობის მიერ აღიარებული, ალიანსს და მის წევრებს თავისუფლად მანევრირების შესაძლებლობა კიბერსივრცეში მაინც არ ექნებათ.

თემის კვლევის პროცეში მრავალ ნაშრომს, განცხადებას თუ აკადემიურ სტატიას გავეცანი, ასევე კონსულტაციები და დისკუსიები მქონდა საქართველოში კიბერუსაფრთხოების საკითხზე მომუშავე პირებთან. მუშაობის პროცესში კი დავინახე, რომ სივრცე, რომელსაც ვიკვლევთ, არის უაღრესად ასიმეტრიული და ზუსტი დასკვნების გამოტანა და პროგრნოზირება არც თუ ისე მარტივია. ნაშრომში განხილული იყო ალიანსის მიერ გადადგუმლი ნაბიჯები კიბერუსაფრთხოების საჭიროებებიდან გამომდინარე; ასევე, კვლევის პროცესში აქტიურად ვეცნობოდი როგორც ნატოს წევრი ქვეყნების, ასევე პარტნიორი ქვეყნების ეროვნული უსაფრთოხებისა და კიბერუსაფრთოხების სტრატეგიებს. ისეთი დასკვნა გამოვიტანე, რომ დღეს თუ კონკრეტულ ქვეყანაზე კიბერ-თავდასხმა განხორციელდება, მათთან ბრძოლა და პრობლემის გადაჭრა დამოუკიდებლად უფრო ეფექტური შეიძლება იყოს, ვიდრე კოლექტიური თავდაცვის პრინციპის მიხედვით. ეს იმით არის განპირობებული, რომ სახელმწიფოებრივ დონეზე ეს საკითხი შედარებით უფრო მაღლა ჰყავთ აყვანილი და შიდა კანონმდებლობითაა დარეგულირებული, როცა ნატოს კიდევ უფრო მეტი ეტაპის გავლა, კონსულტაციები და კონსესუსი ჭირდება შესაძლო პრობლემის გადასაჭრელად.

კიდევ ერთი მნიშვნელოვანი პრობლემა, რასაც ჩრდილოატლანტიკური ალიანსი ჯერ პირისპირ არ შეჯახებია არის ტექნოლოგიების გამოყენებით ვირტუალურ სივრცეში

განხორციელებული ტერორისტული აქტი. მოსალოდნელია, რომ ალიანსი მსგავსი გამოწვევის წინაშე უახლოეს პერიოდში დადგება. ხოლო როგორ გაუმკლავდება მსგავსი ტიპის გამოწვევას, რომელმაც შესაძლოა ფატალური შედეგი გამოიწვიოს, დღეისათვის მარტივად პროგნოზირებადი არაა. თუმცა ფაქტი სახეზა, ასეთ მოვლენას უდიდესი გავლენა ექნება როგორც ნატოს მდგრადობაზე, ასევე საერთაშორისო უსაფრთხოებაზე.

8. დასკვნა

წინამდებარე ნაშრომში განხილული იყო კიბერუსაფრთხოების გავლენა ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის დღის წესრიგზე და ალიანსის ტრანსფორმაციის უნარზე მის წინაშე მდგარი გამოწვევების მიმართ. წარმოდგენილი იყო ჰიპოთეზა: საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებამ ნატოს სამხედრო-პოლიტიკური სტაბილურობა მოწყვლადი გახადა თანამედროვე გამოწვევების წინაშე და ალიანსის ძირითადი ამოცანების ტრანსფორმაცია განაპირობა.

საკვლევი საკითხის ირგვლივ არსებული ლიტერატურის, პირველადი წყაროების, კვლევითი ცენტრებისა და უნივერსიტეტების მუშაობის ანგარიშების, სტატიების, ოფიციალური დოკუმენტების, სახელმწიფოს პირველ პირთა და ოფიციალური წარმომადგნელების მიერ გაკეთებული განცხადებებისა და ნაშრომში თეორიულ ჩარჩოდ გამოყენებული ლიბერალური ინსტიტუციონალიზმის და ურთიერთდამოკიდებულების ლიბერალური თეორიების განხილვის შედეგად, შეგვიძლია დავასკვნათ, რომ 2002 წლიდან დღემდე, ნატოს დღის წესრიგმა მნიშვნელოვანი ტრანსფორმაცია განიცადა; კიბერუსაფრთხოებამ და კიბერსივრციდან მომდინარე საფრთხეებმა ალიანსისა და მისი წევრი სახელმწიფოების განსაკუთრებული ყურადღება გამოწვია. კიბერ-გამოწვევებმა კი სამხედრო-პოლიტიკური ალიანსი

ერთგვარი გარდაუვალი აუცილებლობისა და დილემის წინაშე დააყენა - ინსტიტუტისა და მისი დღის წესრიგის ტრანსფორმირების საჭიროება.

ასევე, ნაშრომზე მუშაობის პროცესში მიღებული ცოდნის, შედეგებისა და გამოცდილების საფუძველზე, შესაძლებელია რამდენიმე მნიშვნელოვანი საკითხი გამოვყოთ დასკვნის სახით.

პირველ რიგში, კვლევის პროცესში გამოიკვეთა, რომ ნატოს დღის წესრიგმა მნიშვნელოვანი ტრანსფორმაცია განიცადა და კიბერუსაფრთხოების საკითხი უმნიშვნელო საკითხიდან ტოპ-პრიორიტეტად იქცა. ამის დასკვნის საშუალება კი რამდენიმე გასათვალისწინებელმა ფაქტორმა განაპირობა, როგორებიცაა ნატოს კოლექტიური თავდაცვის ძირითად კომპონენტად კიბერუსაფრთხოების აღიარება (ხმელეთის, ზღვის, ჰაერისა და კოსმოსის შემდეგ ოპერირების მეხუთე განზომილებად ქცევა) და ნატოს წვერი ქვეყნების შეთანხმება, რომ საჭიროების შემთხვევაში ნატოს დამფუძნებელი ხელშეკრულების მე-5 მუხლი კიბერსივრცეშიც გავრცელდება. თუმცა, თუ რეალურ სურათს დავაკვირდებით, დავინახავთ, რომ მე-5 მუხლის ამოქმედების საკითხი არც თუ ისე მარტივად გადასაწყვეტი იქნება, განსაკუთრებით, იმ გარემოებას თუ დავეყრდნობით, რომ კონვენციური დაპირისპირების შემთხვევაშიც კი ნატოს 70-წლიანი არსებობის პერიოდში აღნიშნული პრინციპი მხოლოდ ერთხელ, 9/11 მოვლენების შემდგომ ამოქმედდა. შესაბამისად, კიბერსივრცეში რამდენად შესაძლებელი იქნება მეხუთე მუხლის ამოქმედება და უახლოეს მომავალში ეს რამდენად მოსალოდნელია, რთული განსასაზღვრია და უამრავ რისკ-ფაქტორებთან არის დაკავშირებულ. მაგრამ მეორე მხრივ, აღნიშნულ მსჯელობას მაინც იმ აზრამდე მივყავართ, რომ ნატოს მთავარი დღის წესრიგი ნამდვილად ტრანსფორმირდა თანამედროვე მნიშვნელოვანი გამოწვევის წინაშე. თუმცა, მეორე მხრივ, რამდენად ნაყოფიერად და სრულყოფილად ტრანსფორმირდა მთლიანად ალიანსი თავისი სამხედრო-პოლიტიკური ბუნებითა და სტრუქტურით ეს კიდევ ცალკე საკითხია და დღეს ამის დასკვნის საშუალება არ გვაქვს. უფრო სწორად, დღევანდელი

გადასახედიდან თუ ვიმსჯელებთ, ნატო სრული ტრანსფორმაციისგან ჯერ მაინც შორსაა, და ამის დანახვის საშუალება მხოლოდ მაშინ გვექნება, როდესაც რეალურად მოუწევს დაუპირისპირდეს ვირტუალურ ომს პირდაპირ და ცხადად. ამის შემდეგ შესაძლებლობა გვექნება, გავიგოთ, თუ რამდენად შეძლო ალიანსმა სრული ტრანსფორმირება. დღევანდელი რეალობიდან თუ შეხვედავთ, ნატო კვლავ რჩება სამხედრო-პოლიტიკურ ალიანსად, რომლის მთავარი საფუძველი კვლავ სამხედრო შეიარაღებასა და სიძლიერეში გამოიხატება. მაგრამ, მეორე მხირვ, ახლო მომავალში მოსალოდნელია ნატოს სამხედრო-პოლიტიკური როლის ერთგვარი დაკნინება და კონვენციური შეიარაღებიდან კიბერ-შეირაღებაზე გადასვლა. ასევე, მოსალოდნელია, რომ შემცირდება ხარჯების გაწევა სამხედრო შეირაღებაზე და გაიზრდება კიბერ-ტექნოლოგიების მიმართულების გაძლიერება.

ასევე, დღევანდელი სურათი იმის დასკვნის საშუალებასაც გვაძლევს, რომ თანამედროვე ინფორმაციული და საკომუნიკაციო ტექნოლოგიები იმდენად სწრაფად ვითარდება და შედარებით იმდენად მცირე ხარჯთან და რესურსებთანაა დაკავშირებული, რომ ეს მტრის გაძლიერებასაც გამოიწვევს. შესაბამისად, უახლოეს პერიოდში უნდა ველოდოთ ტერორიზმს კიბერ-განზომილებაშიც - სხვანაირად რომ განვსაზღვროთ - ტექნოლოგიების გამოყენებით ვირტუალურ სივრცეში ტეროტისტული აქტის განხორციელებას. ჩემი აზრით, კი სწორედ მომავალი საფრთხეები დაგვანახებს თუ რეალურად რამდენად შეძლო ნატომ სრული ტრანსფორმაცია და რამდენად გამოიყენებს თუნდაც 2002 წლიდან დღემდე მიღწეულ პროგრესს, განხორციელებულ რეფორმებსა და დღეს მის ხელთ არსებულ თანამედროვე ტექნოლოგიურ შესაძლებლობებს.

რაც შეეხება საკვლევ კითხვას თუ როგორ შეცვალა კიბერუსაფრთხოების გამოწვევებმა ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის დღის წესრიგი 2002-2017 წლებში და, ზოგადად, რა გავლენას ახდენს კიბერუსაფრთხოება საერთაშორისო ურთიერთობებზე, ფაქტი სახეზე გვაქვს: საინფორმაციო და საკომუნიკაციო

ტექნოლოგიების განვითარებამ როგორც ნატო, ისე მისი წევრი ქვეყნები და პარტნიორები, ასევე, მთლიანი საერთაშორისო საზოგადოება მოწყვლადი გახადა თანამედროვე გამოწვევების წინაშე და როგორც კონკრეტულად ალიანსის, ასევე, ზოგადად საერთაშორისო სისტემის სტაბიულურობას კითხვის ნიშნის ქვეშ აყენებს და მრავალ პასუხგაუცემელ კითხვას ღიად ტოვებს. მოწყვლადობა კი იმაშიც გამოიხატება, რომ ალიანსი, მისი წევრები და პარტნიორები იმდენად შიშობენ მოსალოდნელი საფრთხეების გამო, რომ დღითიდღე ავითარებენ თავიანთ ტექნოლოგიურ შესაძლებლობებს, ზრდიან დაფინანსების ხარჯებს ამ მიმართულებით და უფრო ხმამაღლა და მკაფიოდ როგორც ზეპირ, ისე წერილობით აფიქსირებენ კიბერუსაფრთხოების მნიშვნელობას და კიბერსივრციდან მომდინარე საფრთხეებს ეროვნული და საერთაშორისო უსაფრთხოებისთვის საფრთხის შემცველად ასახელებენ. ასევე, ის რომ რეალურად ჯერ არ განხორციელებულა ისეთი მასშტაბური და გამანადგურებელი კიბერ-შეტევა, რომელიც რეალურად დაგვანახებდა თუ რამდენად მზად არიან სახელმწიფოები თუ სახელმწიფოთა გაერთიანებები რომ ბოლომდე აღკვეთონ და დაამარცხონ კიბერ-თავდასხმები, ამის გათვლისწინებით, ვერ ვიტყვით რამდენად მზად არიან სახელმწიოფები ან ალიანსი წარმატებით გაართვან თავი ამ გამოწვევას. დღემდე განხორცილებული მრავალი კიბერ-შეტევები და მისით გამოწვეული მნიშვნელოვანი ზიანი კი ნათლად წარმოაჩენს საერთაშორისო სტაბილურობის მოწყვლადობას საინფორმაციო და საკომუნიკაციო ტექნოლოგიების განვითარებით წარმოქმნილ კიბერ-საფრთხეების წინაშე.

ზემოთ აღნიშნული მსჯელობების საფუძველზე, თავისუფლად შეგვიძლია დავსკვნათ, რომ ბოლო ათწლეულში საინფორმაციო და კომპუტერული ტექნოლოგიების განვითარების ხარისხის უმაღლეს დონემდე მიღწევამ განაპირობა არამარტო ინდივიდების, არამედ სახელმწიფოების დაყრდნობა ინტერნეტზე და კომპუტერულ ტექნოლოგიებზე. მასზე არის დამოკდებული როგორც უსაფრთხოებისა და თავდაცვის სისტემები, ასევე სასიციცხოლოდ მნიშვნელოვანი დაწესებულებები; ინტერნეტის

საშუალებით წარმოებს მნიშვნელოვანი პოლიტიკური, ეკონომიკური, ფინანსური, თუ სავაჭრო ოპერაციები. ასეთი დამოკიდებულება კი მოწყვლადს ხდის საერთაშორისო უსაფრთხოების სტაბილურობას. კვლევისას გამოჩნდა, რომ რაც უფრო აუმჯობესებენ კიბერ-ტექნოლოგიებს ქვეყნები და სახელმწიფოთა გაერთიანებები, მით უფრო მოწყვლადები ხდებიან მის მიმართ. შესაბამისად, პრობლემასთან სათანადოდ დასაპირისპირებლად საჭიროა სწორად ადაპტირება და სტრუქტურული, ფუნქციური და თვისებრივი ტრანსფორმაცია.

ბიბლიოგრაფია

1. ზურაბიშვილი , თინათინ . თვისებრივი მეთოდები სოციალურ კვლევაში . თბილისი : სოციალურ მეცნიერებათა ცენტრი , 2006

2. ეკონომიკური ნატო ანალიტიკური დოკუმენტი N1, ჰიბრიდული ომი და ევრო-ატლანტიკური სივრცის უსაფრთხოების ლანდშაფტის ცვლილება პოლიტიკური და ეკონომიკური შედეგები; თბილისი, 2016

3. რა არის NATO? საინფორმაციო ცენტრი ნატოსა და ევროკავშირის შესახებ; http://infocenter.gov.ge/eng-nato-structure/#1 accessed 28.12.2017

4. საქართველოს თავდაცვის სამინისტრო სსიპ - კიბერუსაფრთხოების ბიუროკიბერ თავდაცვაკიბერსივრცის მთავარი მოთამაშეები. კიბერუსაფრთხოებისპოლიტიკა, სტრატეგია და გამოწვევები(ნაშრომების და სტატიების კრებული), თბილისი, 2015

5. ნატო-ს ვარშავის სამიტის დეკლარაციის მოკლე მიმოხილვა (გავლენა საქართველოზე); საქართველოს უსაფრთხოების და განვითარების ცენტრი, 2016, გვ.6

6. რა არის გამომძალველი ვირუსი Petya და როგორ დავიცვათ მისგან კომპიუტერები? https://imedinews.ge/ge/theme/7/ra-aris-gamomdzalveli-virusi-petya-da-rogor-davitsvat-misgan-kompiuterebi accessed 11.02.218

7. Betz, David J.; 2012. “Cyberpower and International Security”. The Foreign Policy Research Institute;

8. Clarke, Richard and Knake,Robert; Cyber War: The Next Threat to National Security and What to Do About It (New York: Harper Collins, 2010), p. 6.

9. Copeland,Thomas E.; 2011. “The Information Revolution and National Security”. Publisher: University Press of the Pacific

10. Cyberlaw - კიბერსივრცის სამართალი

11. Council of the EU, Cyber attacks: EU ready to respond with a range of measures, including sanctions. http://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/ accessed 10.02.2018

12. Celeste Wallander, "Institutional Assets and Adaptability: NATO after the cold war"(2000): 83.705-706

13. Department of Defense, Strategy for Operating in Cyberspace, July 2011

14. Explore Terms: A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies. Available from http://niccs.us-cert.gov/glossary#cybersecurity accessed 15.01.2018

15. Farrel, Henry; "The political science of cybersecurity III – How international relations theory shapes U.S. cybersecurity doctrine"; Feb 20, 2014 - washingtonpost.com © 1996-2014 The Washington Post http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/02/20/the-political-science-of-cybersecurity-iii-how-international-relations-theory-shapes-u-s-cybersecurity-doctrine/ accessed 16.01.2018

16. Hoffman, Frank, Center for Security StudiesOn Not-So-New Warfare: Political Warfare vs. Hybrid Threats, 2014

17. McGuinness, Damien, How a cyber attack transformed Estonia, http://www.bbc.com/news/39655415 accessed 25. 01.2018

18. National Security Strategy of the United States of America, N S. S of the United States of America. DECEMBER 2017

19. North Atlantic Treaty Organization www.nato.int accessed 27. 12.2017

20. NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/news/2014.html accessed 27. 12.2017

21. Ondrejcsák, Robert, Introduction to Security Studies, Bratislava 2014 Centre for European and North Atlantic Affairs (CENAA), 2014

22. Qualitative Methods, Spring 2004; Newsletter of the American Political Science Association Organized Section on Qualitative Methods; Spring 2004, Vol. 2, No. 1

23. Robert Keohane, After Hegemony: Discord and Cooperation in International Political Economy, 1984

24. Robert McCalla "NATO's persistence after the Cold War" (1996) გვ. 464

25. Sanger, David E. and Markoff, John, "I.M.F. Reports Cyberattack Led to 'Very Major Breach'," New York Times, June 11, 2011, http://www.nytimes.com/2011/06/12/world/12imf.html.

26. Schjolberg, Stein. 2012. Peace and Justice in Cyberspace Potential new global legal mechanisms against global cyberattacks and other global cybercrimes. An International Criminal Tribunal for Cyberspace (ICTC). Pp.3. Available from http://cybersummit2012.com/sites/cybersummit2012.com/files/EWICybersecuritySummit.pdf accessed 05.01.2018

27. Stoltenberg warns of spike in cyberattacks on NATO, http://p.dw.com/p/2W1fe

28. Tosbotn, Roger André, NATO and Cyber Security:Critical Junctures as Catalysts for ChangeMA International Relations

29. The Tech Terms Computer Dictionary. Cyberspace. Available from http://www.techterms.com/definition/cyberspace accessed 06.01.2018

30. Web ტერმინები და მათი განმარტება. რა არის ჰოსტი, სერვერი Available from https://sites.google.com/site/chemiproekti/web-terminebi-da-mati-ganmarteba accessed 11.01.2018

დანართი: #1

ტერმინთა განმარტება

Computer System - კომპიუტერული სისტემა - ნებისმერი მოწყობილობა ან ურთიერთ დაკავშირებულ ხელსაწყოთა ჯგუფი, რომელთაგან ერთ-ერთი მაინც ასრულებს მონაცემების ავტომატურ გადაცემას პროგრამის საშუალებით. (National Initiative for Cybersecurity Careers and Studies)

Information System - საინფორმაციო სისტემა - სისტემა, რომელიც განკუთვნილია საპროცესო მონაცემის გენერირების, გაგზავნის, მიღების ან შენახვისათვის. (National Initiative for Cybersecurity Careers and Studies)

კრიტიკული ინფრასტრუქტურა - სისტემები და აქტივები, იქნება ეს ფიზიკური თუ ვირტუალური, იმდენად მნიშვნელოვანია საზოგადოებისთვის, რომ მის უუნარობას, გაუამრთაობას ან განადგურებას ექნება დამასუსტებელი გავლენა უსაფრთხოებაზე, ეკონომიკაზე, ჯანდაცვაზე, გარემოსა და სხვა მსგავსი კომბინაციის და მნიშვნელობის საკითხებზე.(National Initiative for Cybersecurity Careers and Studies)

Software - პროგრამა - ანგარიშებისა და ინსტრუქციების კრებული, რომელიც გამოიყენება კომპიუტერის მიერ შესაბამისი შედეგის მიღწევის მიზნით. (National Initiative for Cybersecurity Careers and Studies)

Domain - დომენი - ინტერნეტში ჩართული ერთი ან მეტი კომპიუტერი, რომლებსაც სპეციფიკური მისამართი და IP აქვს. (Mediapedia)

Unauthorized Access - არაავტორიზებული წვდომა - შესაბამისი ავტორიზაციის გარეშე დაცულ კომპიუტერში შეჭრა, შეღწევა. (Cyberlaw - კიბერსივრცის სამართალი)

Virus - ვირუსი - დაწერილი კოდი, რომლის მიზანიცაა საკუთარი თავის გამრავლება. ვირუსი ცდილობს კომპიუტერიდან კომპიუტერში გავრცელებას პროგრამაზე მიბმის საშუალებით და შეუძლია ზიანი მიაყენოს მყარ ტექნიკას, პროგრამას ან მონაცემს.

(National Initiative for Cybersecurity Careers and Studies)

Hacking - ჰაკერობა - ზოგადი ცნება, რომელიც მოიცავს კომპიუტერში ან კომპიუტერულ ქსელში ნებისმიერი სახის არაავტორიზებულ შეღწევას. (Cyberlaw - კიბერსივრცის სამართალი)

Bot - ბოტი - პროგრამული აგენტი, რომელიც წარმოადგენს გაფილტრული პროგრამის ნაწილს, მოქმედებს, როგორც რეალური პიროვნება და ავტომატური დავალებების შედეგად ახდენს ინფორმაციის გამოთხოვასა და მიწოდებას. (Cyberlaw - კიბერსივრცის სამართალი)

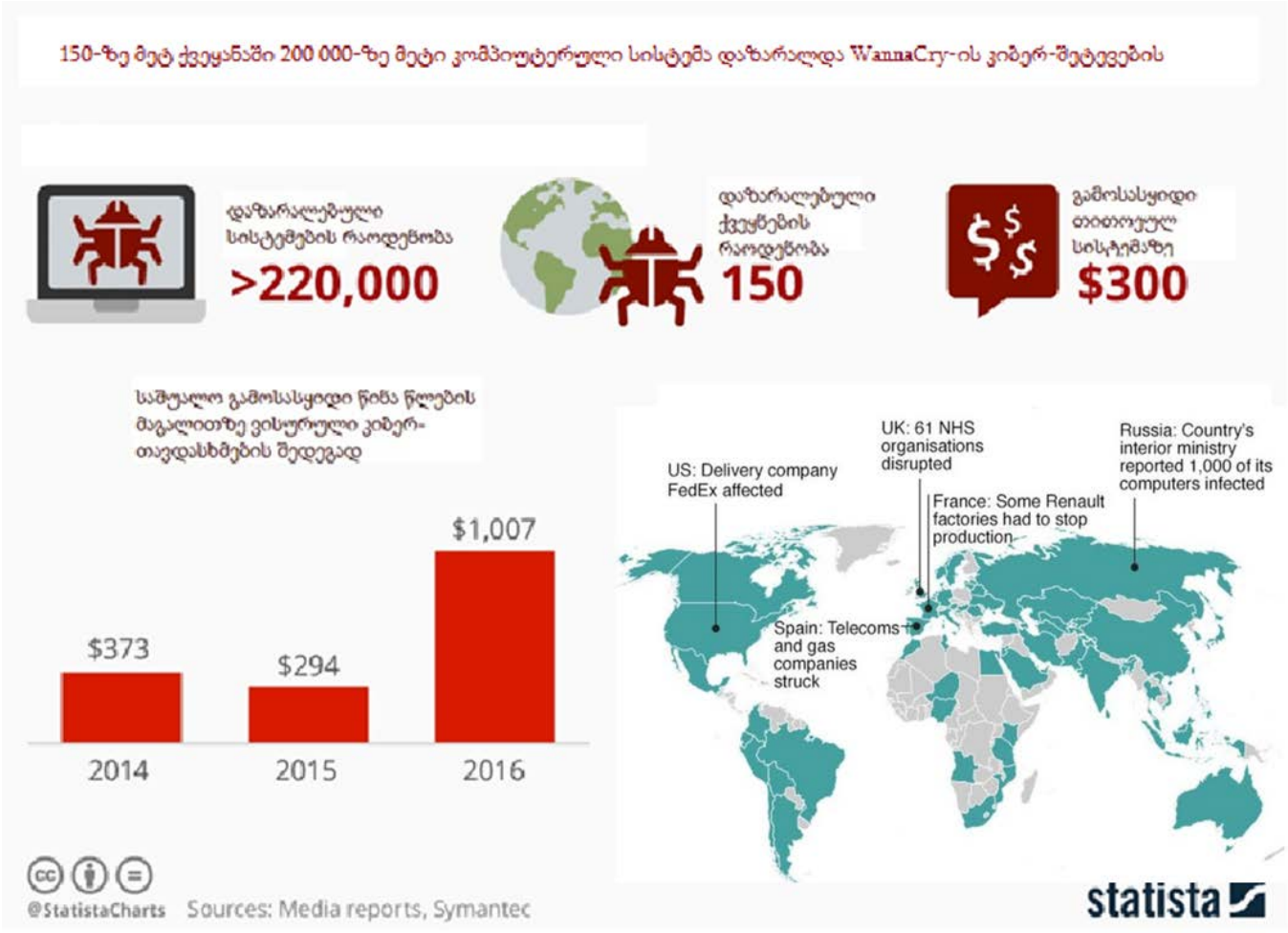
Malicious Code - საზიანო კოდი - პროგრამა ან კოდი, რომელიც ცვლის, ანადგურებს ან იპარავს მონაცემს ან იძლევა არაავტორიზებული შეღწევის შესაძლებლობას, უწევს ექსპლუატაციას ან აზიანებს სისტემას ისე, როგორც მომხმარებლის მიერ არ იყო განზრახული. (National Initiative for Cybersecurity Careers and Studies)

Anonymity - ანონიმურობა - იმ ნებისმიერი განმასხვავებელი ნიშნის არარსებობა, რომლითაც შესაძლებელია ქმედების ჩამდენის ამოცნობა. (Cyberlaw - კიბერსივრცის სამართალი)

Server - "**სერვერი**" გამოიყენება ორი მნიშვნელობით: 1) სერვერი არის კომპიუტერი, რომლის გამოყენება ქსელში ბევრ მომხმარებელს შეუძლია. 2)სერვერი არის პროგრამა, რომელიც ემსახურება სხვა პროგრამებს - კლიენტებს. ინტერნეტი შედგება სერვერებისაგნ ორივე მნიშვნელობით. (Web ტერმინები და მათი განმარტება)

დანართი #2

2017 წელს მასშტაბური კიბერ-თავდასხმის awannaCry-ის გავრცელების არეალი და სტატისტიკა



დანართი #3

Ivane Javakhishvili Tbilisi State University

Mariam Gigauri

The role of cyber security in International Relations - Impact of cyber security on the transformation of the NATO agenda

Diplomacy and International Politics

The Thesis is submitted in partial fulfillment of the requirements for a degree of

Master of Diplomacy and International Politics

Supervisor: Ms. Eka Akobia

Associated Professor

Doctor of International Relations

Tbilisi 2018