ნუცა ნებიერიძე I ალექსანდრე ლაცაბიძე
თავისუფალი უნივერსიტეტი
nnebi20@freeuni.edu.ge I a.latsabidze@freeuni.edu.ge

ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცია (NATO) და კიბერუსაფრთხოების გამოწვევები

რეზიუმე

ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაცია (NATO), თავისი არსით ყოველთვის მიმართული იყო საკუთარი წევრების უსაფრთხოების განმტკიცებაზე. შესაბამისად, მის მიერ შემუშავებული თავდაცვის პოლიტიკა უმეტეს სფეროში საკმაოდ წარმატებული იყო, ვიდრე ახალ გამოწვევას, კიბერუსაფრთხოების მიმართულებით არ წააწყდა. სფეროს სიახლიდან გამომდინარე, ქვეყნები და საერთაშორისო ორგანიზაციები ახლა სწავლობენ კიბერსაფრთხეებთან გამკლავების შესაძლო გზებს. მათ შორის, ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციაც, საფრთხის გაჩენის დღიდან ცდილობს წარმატებული კიბერთავდაცვის პოლიტიკის შემუშავებას. ნაშრომი კიბერუსაფრთხოებასა და ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის მოქმედების ევოლუციას იკვლევს. ამ უკანასკნელის თითოეული ეტაპის უკეთ გასაგებად, განხილული არის ცვლილების განმაპირობებელი მასშტაბური კიბერთავდასხმები, რომლებმაც პრეცედენტი შექმნეს და დღეს კონკრეტული ქვეყნებისგან მომავალი კიბერსაფრთხეები პროგნოზირებადი გახადეს.

საკვანძო სიტყვები: კიბერუსაფრთხოება, თავდაცვის პოლიტიკა, კიბერშეტევები, ჩრდილო-ატლანტიკური ხელშეკრულების ორგანიზაცია (NATO).

მსოფლიოში მიმდინარე მოვლენებმა, ნატოს კიბერუსაფრთოების პოლიტიკისა და სტრატეგიის ცვლილება არაერთხელ განაპირობეს. მიუხედავად იმისა, რომ ზემოხსენებული ყოველთვის ცდილობა საკუთარი საკომუნიკაციო და საინფორმაციო სისტემების დაცვის უზრუნველყოფას, უშუალოდ კიბერთავდაცვის საჭიროების საკითხი პირველად, 2002 წლის ნატოს პრაღის სამიტზე გაჟღერდა. ვინაიდან, იმ პერიოდის მსოფლიოსთვის მთავარ გამოწვევას ტერორიზმი წარმოადგენდა, წევრმა სახელმწიფოებმა კიბერსაფრთხეების შესახებ მხოლოდ ინფორმაციის შეგროვება და ერთმანეთთან გაზიარება გადაწყვიტეს (Davis, 2019). შეიძლება ითქვას, რომ თავდაპირველად ზემოხსენებული საფრთხე ნაკლებად სერიოზულად მიაჩნდათ, მაგრამ მდგომარეობა შეიცვალა 2007 წლის ინციდენტის შემდეგ. ამ წელს, ჯგუფებმა, რომლებიც რუსეთის მთავრობასთან მჭიდრო კავშირში მოქმედებენ, ე.წ. DdoS (Disruption of denial-of-system)[1] მეშვეობით, იერიში მიიტანეს ესტონეთის საჯარო და კერძო ინსტიტუტებზე, რითაც მათი ფუნქციონირება შეაფერხეს. ესტონეთის შემთხვევა მსოფლიოში პირველი შემთხვევაა, რომლის დროსაც კიბერაქტორებმა ფიზიკური ინტერვენციის გარეშე, მწყობრიდან გამოიყვანეს ნატოს წევრი ქვეყნისთვის კრიტიკულად მნიშვნელოვანი ინსტიტუტების ვებ-გვერდები (Herzog, 2011). მოცემული მოვლენა საინტერესოა არამხოლოდ იმის გამო, რომ მის შედეგად, ნატომ ესტონეთის მთავრობასთან ერთად, ტალინში ნატოს კოოპერატიული კიბერ თავდაცვის ცენტრი[2]

1 DDoS შეტევა ვებსაიტებსა და სერვერებზე ხორციელდება, ქსელის სერვისების შეფერხებითა და აპლიკაციის რესურსების ამოწურვის მცდელობით. თავდამსხმელები საიტის, არასაჭირო ოპერაციების განხორციელებით, გადატვირთვას ახდენენ, რის შედეგადაც ვებსაიტი ცუდად ფუნქციონირებს ან საერთოდ ითიშება.

2 Cooperative Cyber Defence Centre of Excellence(CCDCOE) - მოცემული დაწესებულება წარმოადგენს ნატოს აკრედიტირებულ კვლევით და ტრენინგ ცენტრს.

დააარსა, არამედ იმიტომ, რომ რუსეთის კიბერაქტივობა მეტად პროგნოზირებადი გახდა თავდასხმის სპეციფიკის შესწავლის შემდეგ (Oja, 2020). აღნიშნული აისახა 2008 წელს, როდესაც საქართველოს წინააღმდეგ, რუსეთმა კვლავ ზემოხსენებული კიბერტაქტიკა გამოიყენა და DdoS-ის მეშვეობით საქართველოს კრიტიკულად მნიშვნელოვანი ინსტიტუტების მუშაობა შეაფერხა (Andria Gotsiridze, 2019). ეს მოვლენა გარდამტეხი აღმოჩნდა, ნატოსთვის და სრულიად მსოფლიოსთვის იმის გასააზრებლად, რომ კიბერშესაძლებლობების გამოყენება უკვე კონვენციურ ომშიც იყო შესაძლებელი, რაც ჰიბრიდულ ომს ახალ უცნობ და საკმაოდ სახიფათო სივრცეს უმატებდა. შესაბამისად, ალიანსის მიერ, იმაზე მეტის გაკეთება გახდა საჭირო ვიდრე, მხოლოდ კვლევითი ცენტრის დაარსება იყო. 2008 წლის ბუქარესტის სამიტზე ნატომ დაამტკიცა თავისი პირველი კიბერთავდაცვის პოლიტიკა და მოუწოდა წევრებს თავიანთი ტერიტორიების შიგნით, კიბერთავდაცვის გაძლიერების მექანიზმის ძიება დაეწყოთ (NATO, Bucharest Summit Declaration, 2008).

2010 წელს მსოფლიო, მანამდე სრულიად წარმოუდგენელი მასშტაბის კიბერთავდასხმის - Stuxnet-ის[3] მოწმე გახდა. ვირუსი ე.წ. USB-ის მეხსიერების ბარათის მეშვეობით მოხვდა ირანის ისლამური რესპუბლიკის, ქ. ნათანზის ქარხნის საოპერაციო ქსელში, მწყობრიდან გამოიყვანა ათასობით ცენტრიფუგა, საბოლოოდ კი გაურკვეველი მიზეზებით, ქარხნის გარეთაც გავრცელდა. მკვლევართა მტკიცებით, ზემოხსენებულმა ვირუსმა, ირანის ატომური პროგრამა სულ ცოტა ორი წლით უკან დააბრუნა (Baezner & Robin, 2017). აღნიშნული მოვლენის შემდეგ, საკუთარი წევრების უსაფრთხოების დაცვის მიზნით, ნატომ გადაწყვიტა მიდგომა კიდევ უფრო დაეხვეწა. შედეგად, 2014 წლის ნატოს უელსის სამიტზე მოკავშირეებმა მხარი დაუჭირეს კიბერთავდაცვის ახალ პოლიტიკას, რომელშიც კიბერთავდაცვა აღიარებული იყო ნატოს კოლექტიური თავდაცვის მთავარი ამოცანის ნაწილად. ეს იმას ნიშნავდა, რომ კიბერშეტევა შეიძლებოდა გამხდარიყო ნატოს ხელშეკრულების მე-5 მუხლის ამოქმედების მიზეზი, რაც ნატოს კიბერუსაფრთხოებისადმი დამოკიდებულების სერიოზულობას უსვამდა ხაზს. გარდა ამისა, ცვლილება შევიდა მესამე მუხლშიც და წევრებს საკუთარი ფინანსური რესურსების გარკვეული ნაწილის კიბერთავდაცვის სრულყოფისთვის გამოყოფა დაევალათ (NATO, Wales Summit Declaration, 2014). ნატოს კიბერთავდაცვის პოლიტიკის განვითარების შემდეგი ეტაპი, 2016 წლის თებერვალში დადგა, ვარშავის სამიტზე, როდესაც მოკავშირე სახელმწიფოთა მეთაურებმა კიდევ ერთხელ დაადასტურეს ორგანიზაციის თავდაცვითი მანდატი და კიბერსივრცე ოპერაციების ერთ-ერთ იმ სფეროდ[4] აღიარეს, რომელშიც ნატოს თავი უნდა დაეცვა (NATO, Cyber Defence Pledge, 2016). გარდა ამისა, ნატომ და ევროკავშირმა დადეს ტექნიკური შეთანხმება კიბერთავდაცვის შესახებ, კიბერშეტევებთან მიმართებით მნიშვნელოვანი გეგმის შემუშავებისთვის[5] (Stoltenberg, 2016). ზემოხსენებული ფაქტი, ადასტურებს კიბერუსაფრთხოების კონცეფციის მნიშვნელობას, რადგან სწორედ მის გარშემო გაერთიანდნენ საერთაშორისო ორგანიზაციები და წარმატებულად შეიმუშავეს კიბერთავდაცვისკენ მიმართული სპეციალური გეგმა. 2021 წელს, ნატოს წევრი სახელმწიფოების მორიგ შეკრებაზე, ბრიუსელში, შემუშავდა ახალი პოლიტიკა სამი ძირითადი ამოცანის მხარდასაჭერად, რომლის მიხედვითაც ნატოს უნდა შეეკავებინა, დაეცვა და დაპირისპირებოდა კიბერსაფრთხეების სრულ სპექტრს ნებისმიერ დროს - პოლიტიკურ, სამხედრო და ტექნიკურ დონეზე (NATO, Brussels Summit Communiqué, 2021).

3 Stuxnet დახვეწილი კიბერიარაღი იყო, რომელიც სავარაუდოდ აშშ-მ შექმნა ისრაელთან ერთად, ირანის ატომური პროგრამის შეჩერების მიზნით (Fruhlinger, 2022).

4 სახმელეთო, საზღავო და საჰაერო სივრცეს კიბერ სივრცეც დაემატა.

5 ეს ტექნიკური შეთანხმება NCIRC-სა და ევროკავშირის კომპიუტერულ გადაუდებელ სიტუაციებზე რეაგირების გუნდს (CERT-EU) შორის უზრუნველყოფს ინფორმაციის გაცვლისა და საუკეთესო პრაქტიკის გაზიარებას, საგანგებო სიტუაციებზე რეაგირების გუნდებს შორის.

დასკვნა

ნატოს 2021 წლის კიბერთავდაცვის პოლიტიკამ მის წევრ სახელმწიფოებს მრავალი კიბერთავდასხმა თავიდან აარიდა, შესაბამისად ეს საკითხი ნაკლებად აქტუალური გახადა. მიუხედავად ამისა, 2022 წლის რუსეთ-უკრაინის ომის წინ აღმოჩენილმა მსოფლიომ, კვლავ დღის წესრიგში დააბრუნა კიბერუსაფრთხოების აქტუალობა. 2023 წლის ვილნიუსის სამიტზე, ხაზი გაესვა კიბერთავდაცვის გაძლიერების მნიშვნელობას სამხედრო, პოლიტიკურ, ტექნიკურ ასპექტებში და სხვა საერთაშორისო ორგანიზაციებთან ერთად, კერძო კომპანიებთან კოოპერირების აუცილებლობას. წევრმა სახელმწიფოებმა გამოთქვეს სურვილი, საკუთარი ფინანსებით ჩამოეყალიბებინათ, კიბერინციდენტების ვირტუალური დამხმარე მექანიზმი-VCISC[6], რომელიც უმნიშვნელო თავდასხმის იდენტიფიცირებასაც კი მოახდენს და ინფორმაციას ყველა წევრს გაუზიარებს, რაც თავდაცვის მექანიზმების გაუმჯობესება-სრულყოფის საშუალებას წარმოადგენს (NATO, Vilnius Summit Communiqué, 2023). შესაბამისად, ძირითადი ამოცანების, კოლექტიური თავდაცვის, კრიზისების მართვისა და კოოპერატიული უსაფრთხოების უზრუნველყოფის მიზნით, ნატო აგრძელებს ცვალებადი კიბერსაფრთხეების შემცველ გარემოსთან ადაპტირებასა და კიბერთავდაცვის პოლიტიკის დახვეწას.

ბიბლიოგრაფია

Andria Gotsiridze, C. S. (2019). *The Cyber Dimension of the 2008 Russia-Georgia War.* Retrieved from Rondeli Foundation: https://gfsis.org.ge/cbgl/blog/view/970

Baezner, M., & Robin, P. (2017). *Stuxnet.* Zürich: Center for Security Studies (CSS), ETH Zürich.

Davis, S. (2019). *NATO IN THE CYBER AGE:STRENGTHENING SECURITY & DEFENCE, STABILISING DETTERENCE.* SCIENCE AND TECHNOLOGY COMMITTEE (STC).

Fruhlinger, J. (2022). *Stuxnet explained: The first known cyberweapon.* Retrieved from CSO: https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html#:~:text=Stuxnet%20is%20a%20powerful%20computer,about%20its%20design%20and%20purpose.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, 49-54.

NATO. (2008, April 3). *Bucharest Summit Declaration.* Retrieved from NATO: https://www.nato.int/cps/en/natolive/official_texts_8443.htm

NATO. (2014, September 5). *Wales Summit Declaration.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

NATO. (2016, July 8). *Cyber Defence Pledge.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2021, June 14). *Brussels Summit Communiqué.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/news_185000.htm

NATO. (2023). *ALLIED COMMAND TRANSFORMATION NATO's Strategic Warfare Development Command*. Retrieved from https://www.act.nato.int/article/nato-centres-of-excellence-cooperative-cyber-defence-ccd-coe/

NATO. (2023, July 11). *Vilnius Summit Communiqué.* Retrieved from NATO: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

6 Virtual Cyber Incident Support Capability

Oja, M. (2020). History Education: The Case of Estonia. In M. Oja, *Pedagogy and Educational Sciences in the Post-Soviet Baltic States, 1990–2004: Changes and Challenges* (pp. 143-165). Talinn.

Stoltenberg, J. (2016). *JOINT DECLARATION BY THE PRESIDENT OF THE EUROPEAN COUNCIL THE PRESIDENT OF THE EUROPEAN COMMISSION, AND THE SECRETARY GENERAL OF THE NORTH ATLANTIC TREATY ORGANIZATION.*