ვახტანგ ხაჩიშვილი[1]

სახელმწიფოთა საერთაშორისო სამართლებრივი პასუხისმგებლობა კიბერსივრცეში განხორციელებულ მავნე ქმედებებზე: გამოწვევები და პერსპექტივები

აბსტარქტი

კიბეროპერაციები წარმოადგენს ახალ და მზარდ გამოწვევას, რომელსაც საერთაშორისო სამართალი და შიდა სამართალი ვერ შეხვდა მომზადებული. საერთაშორისო ჰუმანიტარული სამართალი გვთავაზობს მხოლოდ საბაზისო საშუალებებს ისეთ კიბერდანაშაულებზე საპასუხოდ, რომლებიც უტოლდება შეიარაღებულ თავდასხმას ან/და მიმდინარეობს ასეთი თავდასხმის კონტექსტში. სახელმწიფოთა შიდა სამართალი, მეორე მხრივ, გვთავაზობს პოტენციურად ძლიერ, კიბერსფეროში გამოსაყენებლ სამართლებრივ მექანიზმებს, თუმცა ისინი ჯერ კიდევ არ არიან მიმართული იმ გამოწვევებთან საბრძოლველად, რაც დაკავშირებულია კიბერ ჯაშუშობასთან და კიბერშეტევებთან.

საკვანძო სიტყვები: *კიბერსივრცე, კიბერ ჯაშუშობა, ინტერნეტი, კიბერთავდასხმები.*

Abstract

Damage due to cyberattacks is tangible. This can manifest itself in financial loss, inaccessibility of information, loss of personal information, reduced trust in the system, and in general, cyberattacks often affect the welfare of the population. Cyber-attacks can escalate into armed conflict as a means of defense when cyber-attacks are regularly carried out against this state.

To establish the liability of States, it must be sufficient to prove the fact that cyber-attacks originate from their territory and that they have breached their obligation to avoid harm. In such cases, states will be held accountable, not only for government-sponsored cyberattacks against another state but also for cyberattacks carried out by an individual, during which the state's cyberinfrastructure is actively used. Cyber operations are a new and growing challenge that international law and domestic law have failed to meet well-prepared. International humanitarian law offers only basic remedies for responding to cybercrime that equates to an armed attack and / or takes place in the context of such an attack. Domestic law, on the other hand, offers potentially robust legal mechanisms to be used in cyberspace, although they are not yet geared to address the challenges associated with cyber espionage and malicious cyberattacks.

[1] თსუ იურუდიული ფაკულტეტის საერთაშორისო სამართლის სამაგისტრო პროგრამის მე-2 კურსის სტუდენტი. ელ. ფოსტა: vakho.khachishvili@gmail.com.

Keywords: *Cyberspace, cyber espionage, Internet, cyberattacks.*

შესავალი

მას შემდეგ, რაც ჩვენს ყოველდღიურ ცხოვრებაში ადგილი დაიმკვიდრა კიბერტექნოლოგიებმა, სახელმწიფოებისთვის კიბეროპერაციები ერთ-ერთ მთავარ პოლიტიკურ იარაღად იქცა. საერთაშორისო თანამეგობრობის მიერ უკვე ფართოდაა მიღებული აზრი, რომ საერთაშორისო სამართლის ზოგადი პრინციპები მოქმედებენ და უნდა მოქმედებდნენ კიბერსივრცეშიც.[2] მრავალი კვლევა და სამეცნიერო სტატია მიეძღვნა კიბერთავდასხმებსა და ოპერაციებს,[3] თუმცა ჯერ კიდევ ბევრი კითხვაა პასუხგაუცემელი, მათ შორის, თუ რა ვალდებულება აკისრია სახელმწიფოს კიბერსივრცესთან მიმართებით და როგორ არეგულირებს სახელმწიფოთა პასუხისმგებლობას საერთაშორისო სამართალი.

ინტერნეტის მასობრივი გამოყენების დასაწყისიდან, ლოგიკურად გაჩნდა კითხვები, თუ რომელი სამართლით მოხდებოდა ინტერნეტ სივრცის რეგულირება: ეს იქნებოდა საერთაშორისო სამართალი თუ ახალი, სპეციალურად კიბერსივრცისთვის შექმნილი სამართალი. *„კიბერსივრცის დამოუკიდებლობის დეკლარაციაში“, ჯ. ბარლოვი* ამტკიცებდა, რომ კიბერსივრცის რეგულაცია მისი მომხმარებლების საქმე და პრივილეგია იყო და მათ ჰქონდათ თავისუფლება, თავად დაემყარებინათ წესრიგი ამ სფეროში.[4] მისი მთავარი არგუმენტი ის გახლდათ, რომ საერთაშორისო სამართალში კიბერსივრცისთვის არ არსებობდა გადაწყვეტილების მიმღები ლეგიტიმური ორგანო.[5] სხვა მკვლევარები ასეთი რადიკალურები არ ყოფილან ამ საკითხზე მსჯელობისას, თუმცა მაინც მიუთითებდნენ, რომ საჭირო იყო ახალი, სპეციალური სამართლის შექმნა ინტერნეტისთვის, რომლითაც გარანტირებული იქნებოდა ინტერნეტის მომხმარებლებისთვის თვითრეგულაციის უფლების განხორციელება. [6] „კიბერსივრცის ავტონომიას“ მრავალი წინააღმდეგი გამოუჩნდა იურისპრუდენციაში და ბევრმა კიბერსივრცეში განსაკუთრებული სამართლებრივი რეჟიმის დანერგვა სრულიად უსარგებლოდ მიიჩნია. [7] როგორც კიბერსივრცის რეგულაციის ამჟამინდელი მდგომარეობა გვაჩვენებს, სამართლებრივი რეჟიმის დადგენის შესახებ კონფლიქტში გაიმარჯვა უფრო ტრადიციულმა მიდგომამ. ამ

[2] Waxman MC, *'Self-defensive Force against Cyber-attacks: Legal, Strategic and Political Dimensions'* (2013) 89 International Law Studies გვ.109, 111.

[3] Glennon MJ, *'The Road Ahead: Gaps, Leaks and Drips'* (2013) 89 International Law Studies გვ.362, 377.

[4] Barlow JP, *'A Declaration of the Independence of Cyberspace'* (1996) Electronic Frontier Foundation <https://projects.eff.org/~barlow/Declaration-Final.html> 1 (ბოლოს ნანახია: აპრილი 14, 2021)

[5] იქვე.

[6] Johnson DR and Post D, *'Law And Borders - The Rise of Law in Cyberspace'* (1995-1996) გვ.48 Stanford Law Review 1367.

[7] Kulesza J, *International Internet Law* (Routledge, ლონდონი 2012), გვ.146.

მიდგომის მიხედვით, კიბერსივრცე უნდა რეგულირდებოდეს საერთაშორისო სამართლის სტანდარტული წესებით, კომპეტენტური სახელმწიფოს შიდა სამართლით და სახელმწიფოთა თანამშრომლობით.

კიბერსივრცის ბოროტად გამოყენება, იგივე კიბერთავდასხმა, წარმოადგენს ტრანსნაციონალურ გამოწვევას. ბოლო ათწლეულებამდე, ადამიანს არ ჰქონია შესაძლებლობა, ელექტრონული კომუნიკაციის საშუალებით ზეგავლენა მოეხდინა სხვა სახელმწიფოს ტერიტორიაზე, რასაც შესაძლოა მოჰყოლოდა მძიმე და დამანგრეველი შედეგი. კიბერთავდასხმები არის გლობალური პრობლემა, დროთა განმავლობაში კი მასთან ბრძოლა სულ უფრო რთულდება, როგორც ტექნოლოგიური, ისე სამართლებრივი გზებით.[8] ხშირად გაურკვევლობაა იმის დასადგენად, კიბერთავდასხმის მონაწილე მხარე სახელმწიფო წარმონაქმნია, თუ არასახელმწიფო წარმონაქმნი (მაგ: ჰაქტივისტები).[9]

წინამდებარე სტატიის მიზანია, სახელმწიფოსთვის კიბერდანაშაულზე საერთაშორისო სამართლებრივი პასუხისმგებლობის დაკისრების მიზნით ბრალეულობის დამტკიცების სირთულეების ანალიზი. სტატიის პირველ ნაწილში განხილული იქნება სახელმწიფოს პასუხისმგებლობის დადგენასთან დაკავშირებული გამოწვევები და სამართლებრივი და ტექნიკური ხარვეზების გამომწვევი მიზეზები. მეორე ნაწილში შემოთავაზებული იქნება ალტერნატიული თეორიები და გამოსავალი სამართლებრივი და ტექნიკური პრობლემიდან. მართლმსაჯულების საერთაშორისო სასამართლოს პრაქტიკაზე მითითებით და ალტერნატიული თეორიების კიბერსივრცეზე მორგებით, სტატიის მიზანი შესრულებული იქნება და დამტკიცდება, რომ სტატიაში განხილული ალტერნატიული გზების გამოყენებით შესაძლებელია სახელმწიფოთა პასუხისმგებლობის დადგენა იმ კიბერდანაშაულებზე, რომლებიც მომდინარეობენ თავიანთი სუვერენული ტერიტორიიდან.

კვლევის მიზანია მხოლოდ ისეთი კიბერთავდასხმის ანალიზი, რომელიც თავისი ხასიათით დამაზიანებელია, თუმცა არ აღწევს საერთაშორისო სამართლით დადგენილ ძალის გამოყენების ზღვარს. კვლევის ინტერესის სფეროა სახელმწიფოს, როგორც საერთაშორისო სამართლის სუბიექტის, კიბერსივრცეში განხორციელებულ მავნე მოქმედებებზე პასუხისმგებლობის დადგენა და არ შეეხება ფიზიკურ თუ იურიდიულ პირთა პასუხისმგებლობის საკითხებს.

1. კიბერსივრცეში სახელმწიფოს საერთაშორისო სამართლებრივი პასუხისმგებლობის დადგენასთან დაკავშირებული გამოწვევები

[8] Karanpreet Singh, Paramvir Singh, and Krishan Kumar, *A Systematic Review of IP Traceback Schemes for Denial of Service Attacks, Computer & Security* გვ.111 (2016).

[9] ტერმინი „ჰაქტივისტები“ მომდინარეობს „ჰაკერი“ და „აქტივისტიდან“. ვრცლად იხილეთ: [https://www.dictionary.com/browse/hacktivist] (ბოლოს ნანახია: 1.7.2021.).

სახელმწიფოზე მავნე კიბერთავდასხმის განხორციელებისას, სახელმწიფოთა ურთიერთთანამშრომლობის ერთ-ერთი უმთავრესი დანიშნულება კიბერსფეროში განხორციელებულ ოპერაციებზე - ბრალეული სახელმწიფოს პასუხისმგებლობის დადგენაა. სახელმწიფოთა შორის საქმის წარმოების დროს, რომელიმე სახელმწიფოს უკანონო ქმედების დადასტურებისთვის მტკიცების პროცესის სირთულე, არ არის მხოლოდ კიბეროპერაციების გამოძიებისთვის დამახასიათებელი პრობლემა. [10] ჯერ კიდევ კიბერ ეპოქამდე, გაეროს საერთაშორისო სასამართლომ ნიკარაგუას საქმეში დაადგინა, რომ „პრობლემა არა სახელმწიფოსთვის ქმედებაზე პასუხისმგებლობის დაკისრების სამართლებრივი პროცესის განხორციელებაა, არამედ ამ პროცესამდე მატერიალური მტკიცებულებების შეგროვებაა, რომლითაც მოხდება დამნაშავე მხარის იდენტიფიცირება“. [11] როგორც ამერიკის შეერთებულმა შტატებმა განაცხადა გაეროს გენერალური მდივნის წინაშე ინფორმაციული უსაფრთხოების შესახებ საკუთარ პოზიციაში: „კიბერსივრცეში არსებული ბუნდოვანებები უბრალოდ იმ გამოწვევების სარკეა, რომლებიც არსებობს სხვა მრავალ სამართლებრივ სფეროში“. [12] შეუძლებელია იმის უარყოფა, რომ ეს გამოწვევები მეტად მძაფრია კიბერ სფეროსთვის, სადაც კიბეროპერაციების უკან დამალული აქტორის პოვნა მომეტებულ ტექნიკურ სირთულეს წარმოადგენს.[13]

1.1 კიბერთავდასხმები: საქართველოსა და ესტონეთზე განხორციელებული კიბერთავდასხმების ანალიზი

საკმარისია შევხედოთ სახელმწიფოთა წინააღმდეგ განხორციელებულ სამ ყველაზე ცნობილ კიბერთავდასხმის საქმეს, რომ მივხვდეთ, თუ როგორი ეკლიანი გზა არის გასავლელი კიბეროპერაციებში სახელმწიფოთა პასუხისმგებლობის მტკიცების პროცესის ეტაპზე. სტატიაში განხილული კიბერთავდასხმები არის მცირე მაგალითი იმ თავდასხმებისა, რომელიც ყოველდღიურად მიმდინარეობს მსოფლიოში. აღნიშნული საქმეების არჩევა მოხდა იმის საილუსტრაციოდ, თუ როგორ ხდება DDoS [14] შეტევების

[10] Michael N. Schmitt ed. *Tallin Manual on the International Law Applicable to Cyber Warfare*, 2013, გვ. 234.

[11] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U. S.), Judgment, 1986 I.C.J. 14, პარაგ. 57.

[12] გაეროს გენერალური სამდივნო, Developments in the Field of Information and Telecommunications in the Context of International Security: Rep. of the Secretary-General, 18, U.N. Doc. A/66/152 (ივლ. 15, 2011).

[13] Fireeye, Digital Bread Crumbs: *Seven Clues to Identifying Who's Behind Advanced Cyber-Attacks* (2014), ხელმისაწვდომია <https://www.fireeye.com/resources/pdfs/digital-breadcrumbs.pdf> (ბოლოს ნანახია: 20.04 2021).

[14] Christos Douligeris and Aikaterini Mitrokotsa, *DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art, 44 Computer Networks*, გვ.643-644. (2004).

გამოყენება რეალური შეიარაღებული კონფლიქტის დაწყებამდე წინმსწრებად, პოლიტიკური მიზნებისთვის თუ კიბერ ჯაშუშობისთვის.

1.1.1 საქართველოს საქმე

რუსეთის მიერ საქართველოს წინააღმდეგ კიბერთავდასხმები დაიწყო 2008 წლის აგვისტოს შეიარაღებული კონფლიქტის დაწყებამდე და გრძელდებოდა შეიარაღებული კონფლიქტის მიმდინარეობისას. საქართველოს წინააღმდეგ 2008 წელს განხორციელებული კიბერთავდასხმები წარმოადგენს პირველ რეგისტრირებულ საქმეებს, როდესაც კიბერთავდასხმა წარმოადგენდა შეიარაღებული კონფლიქტის ნაწილს, მუქარასა და ძალის დემონსტრირებას.[15]

რუსეთის მხრიდან განხორციელებული კიბერთავდასხმები მიმართული იყო საქართველოს მთავრობისა და სამოქალაქო ინფრასტრუქტურის წინააღმდეგ. მათ მიზანს კი, ქართული საკომუნიკაციო სისტემების ჩახშობა წარმოადგენდა. [16] კიბერთავდასხმების შედეგად, საქართველოს სამხედრო ძალისთვის შეუძლებელი გახდა ბრძანებების მიღება და კოორდინაცია ინტერნეტ-საკომუნიკაციო საშუალებებით. ამასთან ერთად, კიბერთავდასხმების მიზანი იყო ქართულ-რუსული კონფლიქტის შესახებ ინფორმაციის კონტროლი და ამით ქართული საზოგადოების აზრთა მანიპულირება. [17] ამ ოპერაციების განმავლობაში, რუსულმა მხარემ ასევე უკანონოდ მოიპოვა ქართული სამხედრო სადაზვერვო ინფორმაცია. [18] საქართველოს წინააღმდეგ კიბერშეტევები რუსეთმა დაიწყო შეიარაღებული დაპირისპირებიდან დაახლოებით 3 კვირით ადრე.

რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებული კიბერთავდასხმების სერიაში, გამოაშკარავდა, რომ საქართველოს წინააღმდეგ კიბერთავდასხმაში ჩართული რუსი ჰაკერები და თავდასხმის კოორდინაცია წარიმართა ძირითადად რუსულ ენაზე. ყოველი შეტევა უფრო დახვეწილი იყო და თავდამსხმელის კიბერსაშუალებებიც მეტად ვითარდებოდა.[19]

საქართველოს წინააღმდეგ განხორციელებული კიბერთავდასხმები არასდროს ყოფილა რომელიმე სახელმწიფოს პასუხისმგებლობას სამართლებრივად მიკუთვნებული. რუსეთმა უარყო ყოველგვარი სახელმწიფო მონაწილეობა ამ თავდასხმებში. ამის მიუხედავად, მრავალი

[15] Andreas Hagen, *The Russo-Georgian War 2008, in, A Fierce Domain: Conflict in Cyberspace*, *1986-2012*, გვ.194-196 (Jason Healey ed., 2013). (დეკემბერი, 24, 2014).
[16] იქვე, გვ. 195.
[17] Andreas Hagen, *The Russo-Georgian War 2008*, გვ. 196.
[18] იქვე. გვ.194-196.
[19] David Hollis, *Cyberwar Case Study: Georgia 2008*, Small Wars J. (2011), William C. Ashmore, *Impact of Alleged Russian Cyber Attacks*, გვ. 11 (2009).

ექსპერტი სწორედ რუსეთის სახელმწიფოს აკუთვნებს ამ დანაშაულებზე პასუხისმგებლობას სხვადასხვა მიზეზის გამო. პირველი სამხილის მიხედვით, თავდასხმა მომდინარეობდა რუსული IP მისამართებიდან და თავდასხმის კოორდინაციაც მხოლოდ რუსულ ენაზე იმართებოდა. სხვა ფაქტების მიხედვით, თავდასხმა იყო დროში სწორად გათვლილი და დახვეწილი გეგმის მიხედვით შესრულებული, რაც რუსეთის მიერ გაკეთებული განცხადების საპირისპიროზე მეტყველებს.[20] თუმცა, ვინაიდან კიბერთავდასხმების დროს აშკარად არ იკვეთებოდა მათზე რუსეთის მთავრობის ეფექტური კონტროლი, საერთაშორისო ჩვეულებითი სამართლის მიხედვით, ეს საკმარისი არაა რუსეთის პასუხისმგებლობის დასადგენად.

საქართველოს წინააღმდეგ განხორციელებულმა კიბერშეტევებმა მსოფლიო ახალი საფრთხის წინაშე დააყენა: ნათელი გახდა, რომ კიბერთავდასხმები შეიძლება გამოყენებული იქნეს სამხედრო დაპირისპირების დროს დამხმარე საშუალებად და გაგრძელდეს მშვიდობიანობის პერიოდშიც.

1.3.2 ესტონეთის საქმე

საერთაშორისო საზოგადოების მიერ მიჩნეულია, რომ რუსეთის ფედერაცია ესტონეთის წინააღმდეგ 2007 წლის DDoS თავდასხმების უკან იდგა.[21] აღნიშნული ბრალდებები ეფუძნება შემდეგ ფაქტებს: ესტონეთის საქმეში ჰაკერები თავს მიიჩნევდნენ რუსეთის მოქალაქეებად, ხოლო შეტევის იარაღი აღმოჩენილ იქნა რუსულ ელექტრონულ გვერდებსა და ფორუმებზე, ამასთან თავდასხმის პიკი იყო 9 მაისს, როდესაც რუსეთი ზეიმობს მეორე მსოფლიო ომში გამარჯვებას.[22] მიუხედავად იმისა, რომ ბოტნეტების წარმომავლობა იკვეთებოდა სხვადასხვა ქვეყნიდან, გარკვეული რაოდენობის თავდასხმები მომდინარეობდა რუსული IP მისამართებიდან, რომელთა შორისაც ჭარბობდა სახელმწიფო ინსტიტუტების IP მისამართები.[23] ესტონეთის თავდაცვის მინისტრის განცხადებით, თავდასხმები იყო „უჩვეულოდ კარგად კოორდინირებული და საჭიროებდნენ ისეთ რესურსებს,

[20] Jason Healey, Concluding Remarks, 265-278, in, *A Fierce Domain: Conflicts in Cyberspace*, 1986 -2012 (Jason Healey ed., 2013).

[21] Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, THE GUARDIAN, მაისი 16, 2007, ხელმისაწვდომია <http://www.theguardian.com/world/2007/may/17/topstories3.russia>. (ბოლოს ნანახია: 3.5.2021.).

[22] William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., *COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 173 box 3.4*, გვ.235, Marco Roscini, 2009.

[23] იქვე.

რაც არ იქნებოდა ხელმისაწვდომი ჩვეულებრივი მოქალაქეებისთვის".[24] DDoS შეტევა დაიწყო მას შემდეგ, რაც ტალინის ცენტრიდან აიღეს რუსეთის ომის მემორიალი.

რუსეთმა არ გამოთქვა სურვილი ეთანამშრომლა ესტონეთთან, რომ ერთობლივი ძალებით გასულიყვნენ თავდასხმაზე პასუხისმგებელი პირების კვალზე, ასევე რუსეთის პროკურატურამ არ დააკმაყოფილა ორმხრივი გამოძიების მოთხოვნა, რომელიც მომდინარეობდა ქვეყნებს შორის გაფორმებული „ორმხრივი სამართლებრივი ხელშეკრულებიდან". [25] საქართველოსა და ესტონეთზე განხორციელებული კიბერთავდასხმები ნათელი მაგალითია იმისა, თუ რაოდენ რთულია და რა გამოწვევებია საერთაშორისო სამართალში სახელმწიფოს პასუხისმგებლობის მტკიცების პროცესში.

2. სახელმწიფოს პასუხისმგებლობის მტკიცების სამართლებრივი გამოწვევები

სახელმწიფოს პასუხისმგებლობის თეორიის მიხედვით, სახელმწიფო შესაძლოა პასუხისმგებელი იყოს სხვა სახელმწიფოს წინაშე, მრავალი სახელმწიფოს წინაშე ან „მთლიანად საერთაშორისო საზოგადოების წინაშე".[26] როგორც წესი, საერთაშორისო სამართალი მონაწილეობს ძირითადად სახელმწიფოთა შორის ურთიერთობებში. ზოგადად, არასახელმწიფოებრივი სუბიექტი, კერძო პირი არ არის ჩართული საერთაშორისო სამართლებრივ ურთიერთობებში, გარდა იმ შეთხვევებისა, როდესაც იგი მოქმედებს ამ სახელმწიფოს სახელით, როგორც სახელმწიფოს აგენტი, წარმომადგენელი. საერთაშორისოდ აღიარებული უკანონო ქმედება შეიძლება გამოიხატოს სახელმწიფოს მხრიდან, როგორც მოქმედებით, ისე უმოქმედობით. საერთაშორისო ჩვეულებითი სამართალი სახელმწიფოს აკისრებს პასუხისმგებლობას ისეთ ქმედებებში, რომელებიც მან განახორციელა და ისეთი უმოქმედობის დროს, როდესაც სახელმწიფოს სამართლებრივად ჰქონდა მოქმედების მოვალეობა. [27] სახელმწიფოს სახელით განხორციელებული აქტიური ქმედებით სახელმწიფოს პასუხისმგებლობა ეკისრება ისეთ შემთხვევებში, როგორებიცაა საერთაშორისო ხელშეკრულების დარღვევა, ძალის გამოყენება ან/და საერთაშორისო ჩვეულებითი სამართლის დარღვევა. სახელმწიფოს მხრიდან პასიური ქმედება შესაძლოა

[24] Strategic Impact of Cyber-attacks, Address before the Royal College of Defence Studies, ხელმისაწვდომია < www.irl.ee/en/articles/strategic-impactof-cyber-attacks > (ბოლოს ნანახია: 3.5.2021.),

[25] Scott J. Shackelford, From Nuclear War to Net War: *Analogizing Cyber-attacks in International Law*, 27 BERKELEY J. INT'L L. გვ. 192, 208 (2009).

[26] Edith Brown Weiss, *Invoking State Responsibility in the Twenty-First Century*, გვ. 798, 798 (2002).

[27] Oona A. Hathaway., *Ensuring Responsibility: Common Article 1 and State Responsibility for Non-State Actors*, გვ. 539, 545-547 (2017).

გულისხმობდეს უკონტროლობას ისეთ სფეროებზე, როგორებიცაა ბუნების დაბინძურების აღკვეთა, ტერორისტული აქტების შეჩერება, ქვეყნის შიდა არეულობის მართვა და მისთ. [28] სახელმწიფოს უმოქმედობის გამო პასუხისმგებლობის დადგენა მეტად რთულია, რადგან შესაძლოა მან არ იცოდა, რომ ჰქონდა ამ საქმეზე მოქმედების ვალდებულება. ნაშრომში სახელმწიფოს ვალდებულებაში იგულისხმება როგორც აქტიური ქმედებით, ისე უმოქმედობით განხორციელებული ქმედების გამო დაკისრებული პასუხისმგებლობა.

საერთაშორისო ჩვეულებითი სამართლის მიხედვით, სახელმწიფო ვალდებულია ნათლად დაადასტუროს, რომ ბრალდებული სახელმწიფო არის პასუხისმგებელი სადავო დარღვევაზე. აღნიშნული პრინციპი ხშირად იწვევს დაბნეულობასა და კითხვებს საერთაშორისო სამართალში, თუ როგორი და რა მასშტაბის სამხილებია მეორე სახელმწიფოს პასუხისმგებლობის სადემონსტრაციოდ ბრალდების მხრიდან წარსადგენი.

იმის გათვალისწინებით, რომ მტკიცებულებათა საკითხები საკმაოდ კომპლექსურია კიბერსივრცეში, ძირითადი სამუშაოები საერთაშორისო სამართალში მიმართულია იმისკენ, თუ კიბეროპერაციების დროს, რამდენად დაცულია საერთაშორისო სამართლის ნორმები და რამდენადაა ის კანონიერი თუ უკანონო. ამ დროს საერთაშორისო საზოგადოების მხრიდან ნაკლები ყურადღება ეთმობა[29] მტკიცებულებების შეგროვების ეტაპს, რის შედეგადაც დაზარალებულმა სახელმწიფომ საერთაშორისო სასამართლოს თუ საზოგადოების წინაშე უნდა დაამტკიცოს, რომ მის წინააღმდეგ განხორციელებული კიბერთავდასხმის უკან რომელიმე სხვა სახელმწიფო დგას. როგორც პრაქტიკა გვიჩვენებს და როგორც წინა თავებში წარმოდგენილ საქმეებში იკვეთება, სახელმწიფოები ნაკლებად გამოთქვამენ თანამშრომლობის სურვილს, როდესაც საქმე ეხება კიბერშეტევებს, განსაკუთრებით კი მაშინ, თუკი მათ სავარაუდო მონაწილეობაში სდებენ ბრალს. ეს გამოწვევა პირდაპირ დაკავშირებულია კიბერსფეროში საერთაშორისო მტკიცებულებების სამართალთან.

კიბერთავდასხმის უკან მდგომი სახელმწიფოს ბრალის დადგენა, დიდი გამოწვევაა საერთაშორისო სამართალში. მტკიცების ტვირთი, როგორც წესი, აკისრია მოსარჩელეს, რომელსაც საჭირო სამხილების წარდგენის შემდგომ ეხსნება აღნიშნული ტვირთი და ინაცვლებს მოპასუხესთან, რომელმაც უნდა ამტკიცოს საპირისპირო.[30] მხარე, რომელიც გარკვეულ ფაქტებზე აფუძნებს მის მოსაზრებას, ვალდებულია დაამტკიცოს იგი.[31] ეს არის ერთ-ერთი მთავარი

[28] Gordon A. Christenson, *Attributing Acts of Omission to the State*, გვ. 312 (1990).

[29] Robin Geiß & Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat- Prevention, in Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (Katharina Ziolkowski Ed., 2013).

[30] Roger B. Dworkin, *Easy Cases, Bad Law, and Burdens of Proof*, გვ. 1151, 1159 (1972).

[31] Pulp Mills on the River Uruguay (Arg. v. Uru.), Judgment, 2010 I.C.J. 14, პარაგ. 162 (20 აპრილი).

პრინციპი, რომელიც ხშირად გამოყენებულია გაეროს საერთაშორისო სასამართლოსა და სხვა საერთაშორისო სასამართლოებისა თუ ტრიბუნალების მიერ.[32] მხარე, რომელსაც აკისრია მტკიცების ტვირთი, არ არის აუცილებლად მოსარჩელე მხარე, არამედ იგი შეიძლება იყოს მოპასუხე, რომელმაც „წამოწია გარკვეული საკითხი და მასზე ამყარებს თავის პოზიციას“. [33] მაგალითად, მხარეს რომელიც მის ქმედებას კანონიერად მიიჩნევს იმ გამონაკლისის საფუძველზე, რომელიც მოიცავს თავდაცვის უფლებას, ეკისრება მტკიცების ტვირთი, რათა წარადგინოს ფაქტები, რომლითაც დადასტურდება გამონაკლისი წესიდან. [34] ასევე აღსანიშნავია ისიც, რომ ორ სახელმწიფოს შორის საერთაშორისო დავების დროს, ყოველთვის არ არის ნათელი თუ ვინ არის მოსარჩელე და მოპასუხე სახელმწიფო, განსაკუთრებით მაშინ, როდესაც სასამართლოში საქმე მხარეებს შორის გაფორმებული სპეციალური ხელშეკრულებითაა შეტანილი.[35]

ზემოთ განხილულ მტკიცების ტვირთის გადანაწილების პრინციპს გააჩნია სამი გამონაკლისი. პირველი გამონაკლისი მდგომარეობს იმაში, რომ მხარეებს არ სჭირდებათ ისეთი ფაქტების მტკიცება, რომელსაც ისინი არ ხდიან სადავოდ ან წინასწარ შეჯერდნენ მის ჭეშმარიტებაზე. [36] მეორე გამონაკლისი გულისხმობს სასამართლოს მიერ მხარისთვის მტკიცების ტვირთის მოხსნას ისეთი ფაქტების დადასტურებისაგან, რომელიც სახალხოდ ცნობილი და აშკარაა. [37] საყოველთაოდ ცნობილი ფაქტების რაოდენობა მუდმივად იზრდება, განსაკუთრებით მას შემდეგ, რაც ფართოდ ხელმისაწვდომი გახდა ინტერნეტი და სხვა საკომუნიკაციო საშუალებები. ისეთი კომპანიები, როგორებიცაა McAfee, Symantee, Mandiant და NATO-ს ცენტრი კიბერთავდაცვის სფეროში თანამშრომლობისთვის (CCD COE) პერიოდულად აქვეყნებენ კიბერინციდენტების შესახებ ანგარიშებს. [38] აღნიშნული ანგარიშები, როგორც წესი შეიცავს კიბერინციდენტების ტექნიკურ ანალიზს, ამასთან, ბევრად ხშირად ხდება კიბერინციდენტების გაშუქება მასმედიით, რაც ხელს უწყობს გარკვეული რაოდენობის ფაქტების საზოგადოდ ცნობილ ფაქტებად აღიარებას. თუმცა, ნიკარაგუას საქმეში ICJ-მ განაცხადა, რომ „ფაქტის შესახებ ფართოდ გავრცელებული ცნობების უკეთესი გამოკვლევის შედეგად შესაძლებელია აღმოჩნდეს, რომ ეს ცნობები მხოლოდ

[32] Ruth Teitelbaum, *Recent Fact-Finding Developments at the International Court of Justice*, 6 L. & PRAC. INT'L CTS. & TRIBUNALS 119, 151 (2007).

[33] Anna Riddell & Brendan Plant, *Evidence before the International Court of Justice*. გვ.142-43 (2009).

[34] Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, para. 57 (ნოემბერი. 6).

[35] Andrés Aguilar Mawdsley, *Evidence Before the International Court of Justice*, გვ. 533, 538 (Ronald St. John Macdonald ed., 1994).

[36] Rüdiger Wolfrum, *International Courts and Tribunals, Evidence*, in 5 THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 552, 567–69 (Rüdiger Wolfrum ed., 2012)

[37] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, para. 92 (ივნისი 27).

[38] MANDIANT, 2020 THREAT REPORT, ხელმისაწვდომია https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html (ბოლოს ნანახია: 12.6.2021.).

ერთი წყაროდან მოდის. შესაბამისად, ასეთ ფაქტს ორიგინალ წყაროზე მეტი ღირებულება არ ექნება“.[39]

მტკიცების ტვირთის პრინციპიდან მესამე გამონაკლისის მიხედვით, მტკიცების ტვირთის პრინციპი ვრცელდება მხოლოდ ფაქტებზე და არა სამართალზე.[40] თუმცა აღსანიშნავია ის, რომ სახელმწიფოთა შორის საქმის წარმოების დროს, შიდა სამართალი ყოველთვის მტკიცების საგანია, თუკი სახელმწიფო მას ეყრდნობა, როგორც ფაქტს. მაგალითისთვის, ICJ ხშირად ასხვავებს ერთმანეთისგან სახელშეკრულებო სამართალსა და ჩვეულებით საერთაშორისო სამართალს, განსაკუთრებით მაშინ, როდესაც საქმე რეგიონალური ხასიათის მქონე ჩვეულებას ეხება. Asylum-ის საქმეში, სასამართლომ განმარტა, რომ ჩვეულებითი სამართლის არსებობა მტკიცების საგანია, რადგან მისი შემადგენელი ერთ-ერთი ნაწილი - სახელმწიფოთა პრაქტიკა - ფაქტუალური ხასიათისაა.[41] სახელმწიფო, რომელიც შიდა სამართლიდან გამომდინარე წარმოადგენს ზოგად თუ კიბერსფეროსთან დაკავშირებულ ჩვეულებას თავის სასარგებლოდ, შესაბამისად ეკისრება მტკიცების ტვირთი სასამართლოს წინაშე. გარკვეული ავტორები მხარს უჭერენ მოსაზრებას, რომ სახელმწიფოებს შორის კიბერდანაშაულზე დავისას, მტკიცების ტვირთი უნდა დაეკისროს იმ სახელმწიფოს, საიდანაც განხორციელდა თავდამსხმელი პროგრამის გაშვება.[42] აღნიშნული მიდგომით გამარტივდება იდენტიფიკაციასთან დაკავშირებული პრობლემები, საერთაშორისო სამართალი მოსთხოვს დაცვის მხარეს ამტკიცოს, რომ კიბერთავდასხმისას იგი არ იყო ჩართული ამ ოპერაციაში ან/და მან გულგრილობით არ დაუშვა თავდასხმისთვის საჭირო ინფრასტრუქტურის გამოყენება. ამის მსგავსად, ბევრ მკვლევარს მიაჩნია, რომ თუკი კიბერთავდასხმა განხორციელდა ისეთი საინფორმაციო ინფრასტრუქტურით, რომელიც სახელმწიფოს კონტროლის ქვეშაა, ეს თავისთავად გულისხმობს, რომ სახელმწიფომ იცოდა ამ კიბერინციდენტის შესახებ და არის მასზე პასუხისმგებელი.[43] თუმცა, აღნიშნული მიდგომა არასწორია. კორფუს არხის საქმეში, ICJ-მ დაადგინა, რომ მიუხედავად სახელმწიფოს მიერ ტერიტორიაზე განხორციელებული ექსკლუზიური კონტროლისა, იგი არაა პასუხისმგებელი ყველა უკანონო ქმედებაზე, რაც ამ ტერიტორიაზე ხდება და მტკიცების ტვირთი ბრალდების/მოსარჩელეს მხრიდან არ უნდა გადავიდეს დაცვის მხარეზე.[44] შეიარაღებული აქტივობის საქმეში, ICJ-მ მტკიცების ტვირთი არ დააკისრა მხარეს, რადგან სახელმწიფოს მხრიდან მის ტერიტორიაზე

[39] Nicar. v. U.S., Judgment, 1986 I.C.J. para. 63.

[40] Wolfrum, იქვე. გვ.557.

[41] Asylum Case (Colom. v. Perú), Judgment, 1950 I.C.J. 266, 276–77 (ნოემბერი. 20); Rights of Nationals of the United States of America in Morocco (Fr. v. U.S.), Judgment 1952 I.C.J. 176, 200 (აგვისტო. 27).

[42] Richard A. Clarke & Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about it* გვ. 249 (2010).

[43] Daniel J. Ryan, Maeve Dion, Eneken Tikk & Julie J. C. H. Ryan*, International Cyberlaw: A Normative Approach*,. გვ. 1161, 1185 (2011).

[44] Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 18 (აპრილი. 9).

არსებული აჯანყებული ჯგუფების არ ჩახშობა არ ნიშნავდა მათ მხარდაჭერას და წახალისებას.[45]

თუ ამ მიგნებების გადმოტანა მოხდება კიბერსფეროში, მხოლოდ ის ფაქტი, რომ სახელმწიფოს აქვს „ექსკლუზიური“ ტერიტორიული კონტროლი იმ კიბერინფრასტრუქტურაზე, საიდანაც იკვეთება კიბეროპერაციის წარმოშობა, ავტომატურად არ ნიშნავს, რომ მტკიცების ტვირთი გადადის ამ სახელმწიფოზე და სწორედ ეს სახელმწიფო დგას შეტევის უკან. [46] კიბერდანაშაულში საერთაშორისოდ აღიარებული უკანონო აქტების სუბიექტური ელემენტების დასადგენად საჭიროა სამი დონის სამხილი, რომლითაც კიბეროპერაცია დაუკავშირდება სახელმწიფოს პასუხისმგებლობას. 3 დონის სამხილის პრინციპის მიხედვით:[47]

1. უნდა დადგინდეს იმ კომპიუტერების ან/და სერვერების მისამართები, საიდანაც განხორციელდა კიბეროპერაცია;
2. შესაძლებელი უნდა იყოს ქმედების განმახორციელებელი პირის ვინაობის დადგენა;
3. უნდა დასაბუთდეს, რამდენად მოქმედებდა კიბეროპერაციის განმახორციელებელი პირი სახელმწიფოს სახელით.

ტერიტორიული პრინციპის მიღმაც, მხოლოდ ის ფაქტი, რომ საჭირო სამხილები მოპასუხე სახელმწიფოს ხელშია ავტომატურად არ ნიშნავს, რომ ამ სახელმწიფოზე გადადის მტკიცების ტვირთი. *ავენას* საქმეში, ICJ-მ განაცხადა, რომ სასამართლოსთვის მიუღებელი იყო მექსიკისთვის, როგორც ბრალდებული სახელმწიფოსთვის, მტკიცებულებების წარმოდგენის დავალება, მხოლოდ იმიტომ, რომ ეს მტკიცებულებები მის ტერიტორიაზე იყო. ეს აშშ-ს ვალდებულება იყო, რომ თავად მოეპოვებინა მტკიცებულებები, რითიც დაამტკიცებდა მექსიკის მიერ ვალდებულებების დარღვევას. სასამართლომ გადაწყვეტილებაში აღნიშნა, რომ ამერიკის შეერთებულმა შტატებმა, ვერ წარადგინა საკმარისი მტკიცებულებები საქმეში, რითაც დადასტურდებოდა, რომ მექსიკელი მოქალაქეები ასევე ამერიკის შეერთებული შტატების მოქალაქეებიც იყვნენ.[48] ის ფაქტი, რომ 2008 წელს საქართველოს წინააღმდეგ განხორციელებულ კიბერთავდასხმას რუსეთის მხრიდან ძალის გამოყენება მოჰყვა ავტომატურად არ ახდენს მტკიცების

[45] Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, para. 301 (დეკემბერი. 19).

[46] David J. Betz & Tim Stevens, *Analogical Reasoning and Cyber Security*, 44 SECURITY DIALOGUE გვ. 147, 151 (2013).

[47] Marco Roscini, Cyber *Operations and the Use of Force in International Law*, Oxford University Press, გვ. 38, (2014).

[48] Avena and Other Mexican Nationals (Mex. v. U.S.), Judgment, 2004 I.C.J. 12, პარაგ. 57 (მარტი. 31.).

ტვირთის მოქმედებაზე ზეგავლენას. [49] *ელ სალვადორის* საქმეში, სასამართლომ განაცხადა შემდეგი: სასამართლოს სრულიად ესმის ელ სალვადორისთვის ქვეყანაში ძალადობრივი აქტების გამო სამხილების შეგროვების სირთულე და გამოწვევების არსებობა. ამის მიუხედავად, სასამართლო ვერ ჩათვლის, რომ სამხილების არსებობის შემთხვევაში, ისინი კონკრეტული მხარის პოზიციის დასადასტურებლად გამოდგებოდა.[50]

მკვლევარები მიიჩნევენ, რომ ბრალდებულ სახელმწიფოზე მტკიცების ტვირთის გადაკისრების თეორია საერთაშორისო ეკოლოგიურ სამართალში არსებულ წინდახედულობის პრინციპიდან მომდინარეობს. [51] წინდახედულობის პრინციპი გულისხმობს „სახელმწიფოს ვალდებულებას, მიიღოს ყველა შესაბამისი ზომა, რათა ადრეულ ეტაპზევე აირიდოს კონკრეტული ზიანის გამომწვევი რისკები“. [52] ამ პრინციპის კიბერსფეროში ანალოგიით გადმოტანის შემთხვევაში, სახელმწიფოები ვალდებულნი იქნებიან, გაატარონ ისეთი ზომები, რომლითაც თავიდან აიცილებენ მათი კიბერინფრასტრუქტურის უკანონო გამოყენებას. [53] მიუხედავად იმისა, გავრცელდება თუ არა წინდახედულობის პრინციპი კიბერსფეროზე, აღნიშნული მაინც არ გამოიწვევს მტკიცების ტვირთის გადაკისრებას განმცხადებელი სახელმწიფოდან იმ სახელმწიფოზე, საიდანაც მომდინარეობდა კიბერშეტევები. ICJ-ს გადაწყვეტილებებში ნათლად ჩანს, რომ იგი არ უჭერს მხარს მტკიცების ტვირთის გადაკისრებას: „მტკიცების ტვირთის გადაკისრებით მარტივი იქნება არასწორ და ზოგჯერ აბსურდულ შედეგებამდე მისვლა, იმის გათვალისწინებით, რომ ხშირად ხდება კიბეროპერაციების გადამისამართება სხვადასხვა ქვეყნის კიბერინფრასტრუქტურის გავლით. ასეთ დროს მტკიცების ტვირთი დაეკისრება სრულიად უდანაშაულო სახელმწიფოებს“. [54] ამის საილუსტრაციოდ, საკმარისია კიდევ ერთხელ გავიხსენოთ ესტონეთის წინააღმდეგ 2007 წელს განხორციელებული DDoS კამპანია, რომელში ჩართული ბოტი კომპიუტერებიც განთავსებული იყო არა მხოლოდ რუსეთში, არამედ ამერიკის შეერთებულ შტატებში, ევროპაში, ბრაზილიაში, კანადაში, ვიეტნამში და სხვა ქვეყნებში.

---

[49] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14 (ივნისი 27).

[50] Land, Island and Maritime Frontier Dispute (El Sal. /Hond.: Nicar. intervening), Judgment, 1992 I.C.J. 351, პარაგ. 63 (სექტემბერი. 11).

[51] Thilo Marauhn, *Customary Rules of International Environmental Law – Can They Provide Guidance for Developing a Peacetime Regime for Cyberspace?* სტატია PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE -დან. გვ.475

[52] Katharina Ziolkowski, *General Principles of International Law as Applicable in Cyberspace*, სტატია PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE - დან, გვ. 169.

[53] იქვე.

[54] Robin Geiß & Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat* გვ. 621 (Katharina Ziolkowski Ed., 2013).

3. სახელმწიფოს კიბერდანაშაულთან დაკავშირების ტექნიკური მხარე

ინტერნეტსა და კიბერსფეროს არ გააჩნიათ დადგენილი საზღვრები და არ არიან დაკავშირებული რომელიმე სახელმწიფოსთან. [55] თვითონ სახელმწიფოს ტერიტორია და მის შიგნით არსებული კიბერინფრასტრუქტურის მდებარეობა უცვლელია, თუმცა ამ ინფრასტრუქტურის მიერ კიბერსივრცეში დატოვებულ ნაკვალევს შესაძლოა კავშირი ჰქონდეს სხვა მრავალ სახელმწიფოსთან. მაგალითისთვის: სახელმწიფოს შესაძლოა ჰქონდეს საკუთარი ვებ საიტები, კომერციული გადარიცხვების სერვისები, ელექტრონული საფოსტო სერვისები, თუმცა მათი ფიზიკური სერვერები მესამე სახელმწიფოში იყოს განთავსებული. შესაბამისად, თუკი მოხდა პირველი სახელმწიფოს სამთავრობო სერვისებზე კიბერთავდასხმა, პროცესში ჩართული იქნება მესამე სახელმწიფოს სუვერენიტეტიც.

გამოწვევები, რომელიც დაკავშირებულია სუვერენიტეტთან, გულისხმობს იმ ფაქტს, რომ თავდამსხმელისთვის უმჯობესია გამოიყენოს მესამე სახელმწიფოს კიბერინფრასტრუქტურა, ვიდრე საკუთარი, რადგან მარტივი იქნება ბრალის გადაკისრება უდანაშაულო სახელმწიფოზე. [56] ზოგჯერ აღნიშნული შემთხვევები ხდება ინტერნეტ მარშრუტიზატორების მიერ თავდასხმის განხორციელება მესამე სახელმწიფოს კიბერინფრასტრუქტურის გავლით. თუკი მესამე სახელმწიფო ნებაყოფლობითაა ჩართული ამ პროცესში, მაშინ ის თავდასხმის თანამონაწილედ უნდა ჩაითვალოს, სხვა შემთხვევაში ასეთი სახელმწიფო უდანაშაულოა, თუ არ დამტკიცდა, რომ მან იცოდა ასეთი თავდასხმის განხორციელების შესახებ, თუმცა არ შეაჩერა იგი. აღნიშნული პრობლემა განხილულია ტალინის სახელმძღვანელოში, სადაც ექსპერტთა ჯგუფის დასკვნის მიხედვით, კიბერთავდასხმის მესამე სახელმწიფოს კიბერინფრასტრუქტურაში გადამისამართება, ავტომატურად არ იწვევს ამ სახელმწიფოს ბრალეულობის საკითხს. [57] თუმცა, თუკი სახელმწიფოს აქვს ინფორმაცია ასეთი თავდასხმის მიმდინარეობის შესახებ, მან ყველა ტექნიკური საშუალებით უნდა შეაჩეროს აღნიშნული თავდასხმა. თუ სახელმწიფოს არ გააჩნია საკმარისი ტექნიკური ცოდნა ან რესურსი თავდასხმის შესაჩერებლად, მას შეუძლია თავისუფალი ნებით ჩართოს სხვა სახელმწიფოები დასახმარებლად.[58]

---

[55] Zhiqianq Gao and Nirwan Ansari, *Tracing Cyber Attacks from The Practical Perspective* გვ. 123, (მაისი 2005).

[56] Ashley Deeks, *The Geography of Cyber Conflict: Through A Glass Darkly*, გვ. 89 Int'l L. Studies 1, 5 (2013).

[57] Tallinn Manual on the International Law Applicable to Cyber Warfare 36 (Michael N. Schmitt ed. 2013), Rule 8.

[58] Louis Arimatsu, *The Law of State Responsibility in Relation to Border Crossings: An Ignored Legal Paradigm*, 89 Int'l L. Studies გვ. 21, 36 (2013).

3.1 ინტერნეტის როლი სახელმწიფოთა სუვერენიტეტში

კიბერთავდასხმებზე სახელმწიფოთა პასუხისმგებლობის მტკიცების პროცესს თან ახლავს როგორც სამართლებრივი, ისე ტექნიკური გამოწვევები. მავნე კიბერთავდასხმების დაკავშირება მის შემსრულებელ პირთან საკმაოდ დიდ პრობლემას წარმოადგენს, თუმცა მეტად დიდი პრობლემაა ფიზიკური პირის ქმედების რომელიმე სახელმწიფოს პასუხისმგებლობასთან დაკავშირება. არსებობს რამდენიმე ფაქტორი, რაც გავლენას ახდენს მავნე კიბერთავდასხმის განმახორციელებელი სახელმწიფოს პასუხისმგებლობის მტკიცების სამართლებრივ და ტექნიკურ პროცესზე, ესენია: (1). მავნე კიბერხელსაწყოების მოცულობა და მავნე კოდების ნაირფეროვნება. McAfee-ს მონაცემებით,[59] ყოველდღიურად ასობით ათასზე მეტი ახალი მავნე კოდია აღმოჩენილი ინტერნეტში. (2). მავნე კიბერთავდასხმების განხორციელება შესაძლებელია ნებისმიერი კომპიუტერული მოწყობილობით, რომელიც დაკავშირებულია ინტერნეტთან. ამასთან, არსებობს უამრავი საშუალება, რითიც ხდება შეტევის განხორციელების მისამართის შეცვლა ან დამალვა. ასევე, ისიც უნდა აღინიშნოს, რომ კიბერთავდასხმების განხორციელება შესაძლებელია ინტერნეტ კავშირის გარეშეც, ფიზიკურ მოწყობილობებზე დატანილი მავნე კოდით.[60] (3). განსხვავებით შეიარაღებული თავდასხმისგან, რომლის დროსაც შესაძლებელია გამოყენებულ იარაღზე დაკვირვებით დადგინდეს მფლობელის ვინაობა, კიბერშეტევების დროს გამოყენებულ იარაღში (მავნე კომპიუტერულ კოდში) არ ინახება პირის საიდენტიფიკაციო საშუალებები, თავდასხმის განხორციელების ადგილი და დრო, თუკი თვითონ თავდამსხმელს არ სურს ეს. პირიქით, კოდში შესაძლებელია ჩაწერილი იყოს ისეთი მინიშნებები, რომლებიც შეცდომით, უდანაშაულო აქტორის კვალზე გავა. აღნიშნული მავნე კოდის მოხმარება შეუძლია ერთდროულად უამრავ პირს.[61] (4). მავნე კოდი შესაძლოა შენახული იყოს მსხვერპლის კომპიუტერში და გააქტიურდეს დისტანციურად თავდამსხმელისთვის საჭირო დროს.[62] კიბერშეტევით დაზარალებული სახელმწიფოს ვალდებულება, რომ დაამტკიცოს სახელმწიფოს ეფექტური კონტროლი კიბერშეტევის განმახორციელებელ არასახელმწიფოებრივ თუ სახელმწიფოებრივ აქტორზე, არის უმძიმესი მტკიცების ტვირთი, რომლის გადალახვასაც სახელმწიფოები თითქმის ვერ ახერხებენ. საერთაშორისო ჩვეულებითი სამართლით წამოყენებულია წინაპირობა, რაც გულისხმობს, რომ მხარემ უნდა დაამტკიცოს

[59] McAfee-ის 2019 წლის აგვისტოს ანგარიში. ხელმისაწვდომია: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf ბოლოს (ნანახია: 20.6.2021.).

[60] Neil C. Rowe, *The Attribution of Cyber Warfare, in, Cyber Warfare: A Multidisciplinary Analysis* 61-72 (James A. Green ed., 2015).

[61] იქვე. 61-72.

[62] იქვე. გვ.71.

სახელმწიფოს ეფექტური კონტროლი არასამთავრობო პირზე, რომელმაც განახორციელა კიბერთავდასხმა, რათა შესაძლებელი იყოს ამ სახელმწიფოზე პასუხისმგებლობის დაკისრება.[63] ამ წინაპირობის გამო სამართლებრივად ბრალის დადასტურება ხშირად შეუძლებელი ხდება, ამის მიზეზი კი არა მხოლოდ სამართლებრივი, არამედ ტექნიკური გამოწვევებიცაა.

4. კიბერდანაშაულის მიზეზ-შედეგობრიობასთან დაკავშირებული გამოწვევები

ტექნიკური საშუალებით კიბერდანაშაულის მიზეზ-შედეგობრიობის დადგენა თეორიულად შესაძლებელია, თუმცა პრაქტიკაში ის მოითხოვს ხანგრძლივ დროს და დამოკიდებულია სახელმწიფოს ექსპერტიზის კვალიფიკაციაზე. ამ დრომდე არ არსებობს ტექნიკური საშუალებები, რომლითაც შესაძლებელი იქნება კიბერთავდასხმის ავტორის ვინაობის დადგენა, იმ კომპიუტერულ მოწყობილობებზე ფიზიკური კონტროლის გარეშე, რომლებშიც თავდასხმისთვის გამოყენებული მავნე კოდი დაიწერა.[64] ამასთან, სათუო იქნება წაშლილი მავნე კოდის (დაფარული კვალის) აღდგენა. აქედან გამომდინარე, კიბერდანაშაულში სახელმწიფოს პასუხისმგებლობის დასადგენად ტექნიკური საშუალებით შეგროვებული ინფორმაცია შესაძლოა იყოს: IP მისამართები, გეოლოკაცია და სხვადასხვა სამხილი, რომელიც შეგროვდა კიბერიარაღების ანალიზითა და არაპირდაპირი წყაროებით. აღნიშნული სამხილები არ იქნება საკმარისი სახელმწიფოს პასუხისმგებლობის დასადგენად, რადგან წინა პლანზე ინაცვლებს ისეთი სამართლებრივი საკითხები, როგორებიცაა: მტკიცების ტვირთი, სამხილთა წონა და დასაშვებობა და სხვა დაკავშირებული პრობლემები.

საინტერესოა, რა ტიპის სამხილები იქნება საკმარისი და სანდო მტკიცების ტვირთის სტანდარტების დასაკმაყოფილებელად და იმის დასადგენად, რომ კიბეროპერაცია ნამდვილად განხორციელდა, დადგა ზიანი და ქმედება დაკავშირებულია სახელმწიფოს პასუხისმგებლობასთან? სამხილთან წარმოების წესები რეგულირდება ICJ-ს სტატუტის 48-ე და 52-ე მუხლებით და სასამართლოს წესებით. თუმცა, არ არსებობს მტკიცების მეთოდების სახელმძღვანელო მხარეებისთვის და არც ამ მეთოდების იურიდიულ ძალაზე აქვთ მხარეებს ინფორმაცია. როგორც წამყვანი სამართლის მეცნიერები აღნიშნავენ, „გაეროს საერთაშორისო სასამართლოს არ გააჩნია სტატუტში აკრძალვითი ნორმები მტკიცების მეთოდების

[63] David D. Clark and Susan Landau, *Untangling Attribution, 25 Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (2010).

[64] უნდა აღინიშნოს, რომ კვლევის დროს გაცნობიერებულია ის ფაქტი, რომ შესაძლოა ა.შ.შ-ს, გაერთიანებულ სამეფოსა და სხვა სუპერსახელმწიფოებს გააჩნდეთ თავდამსხმელის ვინაობის დამდგენი ტექნიკური საშუალება, მოწყობილობებზე ფიზიკური წვდომის გარეშე, თუმცა კვლევაში განხილულია მხოლოდ საჯაროდ ცნობილი ტექნიკა და მეთოდები.

შერჩევასთან დაკავშირებით, რადგან ამით სასამართლო მხარეებს აძლევს თავისუფლებას, წარადგინონ ნებისმიერი კანონიერი სამხილი სასამართლოს მიერ განსაზღვრულ ვადებში“. [65] გარდა მხარეების ვალდებულებისა, წარადგინონ სამხილები იმ ფაქტებთან დაკავშირებით, რაზეც დამყარებულია მათი პოზიცია, სასამართლომაც შესაძლოა დამატებით მოითხოვოს დოკუმენტების წარდგენა, ექსპერტებისა და მოწმეების მოწვევა, ტერიტორიის დათვალიერება და გამოითხოვოს საჭირო ინფორმაცია საერთაშორისო ორგანიზაციებიდან.[66]

5. სახელმწიფოთა საერთაშორისო სამართლებრივი პასუხისმგებლობა კიბერსივრცეში განხორციელებულ მავნე ქმედებებზე: საერთაშორისო სამართლის პრინციპებით დასახული პერსპექტივები

საერთაშორისო ეკოლოგიური სამართლიდან ნასესხები ზიანის მიუყენებლობის მოვალეობის თეორიის საშუალებით, შესაძლებელი იქნებოდა სახელმწიფოს პასუხისმგებლობის დაკისრება დამდგარი ზიანის გამო, როდესაც კიბერშეტევები მომდინარეობდა მისი სუვერენული ტერიტორიიდან და მან იცოდა ან უნდა სცოდნოდა ამ კიბერდანაშაულის შესახებ. ზიანის მიუყენებლობის თეორია დიდი ხანია აღიარებულია საერთაშორისო სამართლის მიერ და საკმაოდ მოქნილია, რათა შესაძლებელი იყოს ანალოგიით მისი გამოყენება ზიანის დასაფარად, რომელიც გამოწვეულია სახელმწიფოდან მომდინარე კიბერშეტევების მიერ.

კიბერთავდასხმებმა შესაძლოა დაარღვიონ სახელმწიფოების შიდა საქმეებში ჩაურევლობის პრინციპი. ამ პრინციპის მიხედვით, სახელმწიფოებისთვის წინასწარი უფლებამოსილების ან გამართლების გარეშე აკრძალულია მეორე სახელმწიფოთა საშინაო თუ საგარეო საქმეებში ჩარევა.[67] თუმცა ზიანი, რომელიც მომდინარეობს ასეთი ინტერვენციით, განსხვავდება იმ ზიანისგან, რომელიც განხილული იყო წინა თეორიებში. სახელმწიფოს შიდა საქმეებში ჩარევით გამოწვეული ზიანის დათვლა შეუძლებელია, რადგან ასეთი ზიანი შეიძლება იყოს, მაგალითად, სახელმწიფოს დამოუკიდებლობის შებღალვა. ამასთან, ზიანი, რომელიც მომდინარეობს სახელმწიფოში უკანონო პოლიტიკური ინტერვენციისგან, პირდაპირ დაკავშირებულია გაეროს წესდების მე-2(1) მუხლთან, რომლის მიხედვითაც გაერთიანებული ერების ორგანიზაცია დაფუძნებულია მისი წევრების თანაბარი სუვერენიტეტის პრინციპზე. [68] შესაბამისად, როდესაც ერთი სახელმწიფო უკანონოდ ერევა

[65] Durward V. Sandifer, *Evidence before International Tribunals 184* (rev. ed. 1975).

[66] Statute of the International Court of Justice arts. 49, 50, June 26, 1945, 33 U.N.T.S. 933; Rules of Court, arts. 62, 66, 67, 69, 1978 I.C.J. Acts & Docs. 6.

[67] Phillip Kunig, Prohibition of Intervention, in, Max Planck Encyclopedia of Law (2015), ხელმისაწვდომია: <http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?rskey=4krYZ6&result=5&prd=EPIL> (ბოლოს ნანახია: 20.6.2021.).

[68] იქვე.

მეორე სახელმწიფოს სუვერენიტეტში, ის ამავდროულად ზიანს აყენებს გაეროს მთავარ მიზნებსა და იდეებს. თუმცა, ისიც საკითხავია, როგორ არღვევენ კიბერთავდასხმები სახელმწიფოს შიდა საქმეებში ჩაურევლობის პრინციპს. სახელმწიფოები კიბერთავდასხმის გამოყენებით პრინციპს არღვევენ იმ შემთხვევაში, თუკი თავდასხმა არის პოლიტიკური მიზნით მოტივირებული და გააჩნია ძალის გამოყენებაზე ნაკლები ინტენსივობა, თუმცა მისი დანიშნულებაა აიძულოს მეორე სახელმწიფო მიიღოს გარკვეული ზომები, ან თავდასხმით ჩაერიოს ქვეყნის შიდა საქმეებში, რითიც თავდამსხმელი სახელმწიფო მიიღებს პოლიტიკურ სარგებელს.[69]

2008 წელს მსგავსი თავდასხმა განხორციელდა სწორედ საქართველოზე. თავდასხმებმა გავლენა მოახდინა ქართული კიბერინფრასტრუქტურის თითქმის ყოველ ელემენტზე. როგორც იკვეთებოდა, თავდასხმების მიზანი იყო გავლენა მოეხდინა და ხელი შეეშალა საქართველოსა და მისი მოკავშირეებისთვის გადაწყვეტილების მიღების პროცესში. DDoS შეტევების შედეგად, საქართველო დროულად ვეღარ აწვდიდა მოსახლეობასა და მის მოკავშირე სახელმწიფოებს/ორგანიზაციებს ინფორმაციას. თავდასხმების შედეგად, საქართველოს მოქალაქეებს შეეზღუდათ სახელმწიფო სერვისებისა და ფინანსური მომსახურების მიღება, რითიც თავდამსხმელის მიზანი იყო ქვეყანაში პოლიტიკური რაკურსის შეცვლა. 2008 წლის კიბერშეტევები, ალბათ ერთ-ერთი ყველაზე ნათელი მაგალითია, თუ როგორ შეიძლება კიბერთავდასხმით დაირღვეს შიდა საქმეებში ჩაურევლობის პრინციპი.

6. სახელმწიფოს პასუხისმგებლობის დამდგენი თეორიების პრაქტიკაში აღსრულების პერსპექტივები

მიუხედავად იმისა, რომ საერთაშორისო სამართალში ყოველთვის დიდ გამოწვევას წარმოადგენს აღსრულების ეტაპი, კიბერშეტევებთან დაკავშირებით აღსრულების პრობლემის დასაძლევად შესაძლოა განვიხილოთ სხვადასხვა შესაძლებლობები. ესენია:

1. დიპლომატიური დაცვა და მორიგება ex gratia მოთხოვნით;
2. ფორმალური საერთაშორისო სამართლებრივი სარჩელით;
3. შიდა სასამართლოებში სარჩელის შეტანით, უცხო ქვეყნის სუვერენული იმუნიტეტის გამორიცხვით.

6.1 დიპლომატიური დაცვა და მორიგება

[69] Cf. Rafael Nieto-Navia, *International Peremptory Norms (Jus Cogens) and International Humanitarian Law,* ICCNow, (n.d.), ხელმისაწვდომია: http://www.iccnow.org/documents/WritingColombiaEng.pdf. (ბოლოს ნანახია: 20.6.2021.).

საერთაშორისო სამართლებრივი სარჩელის ჩამოყალიბებისას, პირველ რიგში პრიორიტეტულია დავის ნებაყოფლობით მოგვარებაზე შეთანხმების მიღწევა. *Ex gratia* კომპენსაცია შესაძლოა საკმაოდ ეფექტური იყოს კიბერ კონტექსტში, რადგან ეს საშუალებას აძლევს სახელმწიფოებს, აანაზღაურონ ზიანი მათი ქმედების არაკანონიერებისა თუ გადაცდომის აღიარების გარეშე. აღნიშნული საშუალება შესაძლოა საკმაოდ შედეგიანი აღმოჩნდეს იმ სახელმწიფოსთვის, რომელიც ცდილობს მოსთხოვოს მეორე სახელმწიფოს ზიანის ანაზღაურება, თუმცა ბრალდებული სახელმწიფო თავს იკავებს თანამშრომლობისგან, რადგან არ სურს ბრალის აღიარება. ასეთი შემთხვევა იყო ამერიკის შეერთებული შტატების საქმეზე, როდესაც მან აუნაზღაურა ბირთვული იარაღის ტესტირებით გამოწვეული ზიანი კუნძულ-სახელმწიფოებს საკუთარი ბრალის აღიარების გარეშე.

6.2 ფორმალური საერთაშორისო სამართლებრივი სარჩელი

ისეთ შემთხვევებში, როდესაც შეუძლებელია ნებაყოფლობით კომპენსაციაზე შეთანხმების მიღწევა, საერთაშორისო სასამართლოებს შეუძლიათ მისცენ ასპარეზი ისეთი სარჩელების განხილვას, რომლებიც ეხება სახელმწიფოთა მიერ ზიანის თავიდან აცილების ვალდებულების დარღვევას. მაგალითისთვის: ICJ-მ შესაძლოა უზრუნველყოს მხარეები სამართლებრივი ფორუმით, სადაც მოხდება ფორმალური დიპლომატიური დაცვის სარჩელების განხილვა იმ ზიანთან დაკავშირებით, რომელიც მეორე სახელმწიფომ კიბერშეტევებით მიაყენა მოსარჩელე სახელმწიფოს მოქალაქეებსა და კერძო ინდუსტრიას.

6.3 შიდა სასამართლოებში სარჩელის შეტანა, უცხო ქვეყნის სუვერენული იმუნიტეტის გამორიცხვით.

მრავალი სახელმწიფო ასევე მიმართავს შიდა სასამართლოებს უცხო სახელმწიფოს წინააღმდეგ დელიქტების გამო წაყენებული სარჩელებით. აღნიშნული არის ერთ-ერთი ეფექტური გზა კიბერთავდასხმებისგან გამოწვეული ზიანის გამო კომპენსაციის მისაღებად.[70] მიუხედავად იმისა, რომ უცხო სახელმწიფოს იმუნინეტმა შესაძლოა დააბრკოლოს გარკვეული ტიპის სარჩელები, საერთაშორისო ჩვეულებითმა სამართალმა გამონაკლისების სახით შესაძლოა უგულვებელყოს უცხო სახელმწიფოს იმუნიტეტი ისეთ სარჩელებზე, რომლებიც ეხება ერთი სახელმწიფოს მიერ განხორციელებულ „ტერიტორიულ დელიქტებს“, რომლითაც ზიანდება მეორე სახელმწიფოს ტერიტორია. გაეროს კონვენცია სახელმწიფოთა და მათი საკუთრების სამართლებრივი იმუნიტეტების შესახებ ადასტურებს ამ პრინციპის არსებობას.

[70] Hazel Fox, G.C. & Philippa Webb, *The Law of State Immunity,* გვ.475-83.

Voitia v Federal Republic of Germany -ს საქმეში ნათქვამია, რომ საბერძნეთმა შიდა სასამართლოების გამოყენებით მოითხოვა გერმანიისგან იმ დელიქტებისგან მიყენებული ზიანის ანაზღაურება, რომელიც განხორციელდა საბერძნეთის ტერიტორიაზე.[71]

[71] Voitia v. Federal Republic of Germany [A.P.] [სააპელაციო სასამართლო] 11/2000, გვ. 514 (საბერძნეთი).