ივანე ჯავახიშვილის სახელობის
თბილისის სახელმწიფო უნივერსიტეტი
იურიდიული ფაკულტეტი

სამართლის ჟურნალი

№1, 2020

უნივერსიტეტის
გამომცემლობა

გურამ ღვინჯილია*

კიბერშეტევა ძალის გამოყენების აკრძალვის კონტექსტში – საჭიროებს თუ არა საერთაშორისო სამართალი ახლებურ გააზრებას?

თანამედროვე ტექნოლოგიების განვითარებასთან ერთად სულ უფრო აქტუალური ხდება საერთაშორისო სამართლის გადაფასების საკითხი, რათა შესაძლებელი გახდეს საერთაშორისო სამართლის სტატიკური ნორმების მიერ ტექნოლოგიების ადეკვატური რეგულირება. ერთ-ერთი ასეთი საკითხია კიბერსივრცე. არამართლზომიერი კიბეროპერაციებით სახელმწიფოები ხშირად არღვევენ სხვა სახელმწიფოების კიბერსივრცეს, რომლის ნათელი მაგალითებია 2007 წლის კიბერშეტევა ესტონეთზე, 2010 წელს ირანის ბირთვული სადგურის კომპიუტერულ სისტემაში აღმოჩენილი ვირუსი და 2008 წელს რუსეთ-საქართველოს შეიარაღებული კონფლიქტის დროს ქართულ კიბერსივრცეზე განხორციელებული თავდასხმა. ვინაიდან ამჟამად არ არსებობს კიბერსივრცეზე მორგებული სპეციალური რეგულაციები, ხშირად კნინდება საერთაშორისო სამართლის როლი.

ნაშრომი მიზნად ისახავს არსებული საერთაშორისო სამართლებრივი რეჟიმის განხილვას, რომელიც ვრცელდება კიბეროპერაციებზე. ამ კუთხით, ყურადღება გამახვილდება კიბეროპერაციების ურთიერთმიმართებაზე გაერთიანებული ერების ქარტიასთან, ძალის გამოყენების აკრძალვისა და სახელმწიფოთა შიდა საქმეებში ჩაურევლობის პრინციპებთან. სახელმწიფოთა პრაქტიკის ანალიზი აჩვენებს, რომ კიბერშეტევები სახელმწიფოების მიერ აღიქმება ძალის გამოყენების დამოუკიდებელ ფორმად და მათ სამართლებრივ შეფასებას ცდილობენ დღეს არსებული საერთაშორისო სამართლის ფარგლებში. ასევე, შეიმჩნევა კიბერშეტევების სპეციალიზებული ნორმებით მოწესრიგების ტენდენცია.

კიბერშეტევები საჭიროებს ახლებურ გააზრებას საერთაშორისო სამართლის ჭრილში. თუმცა, ეს არ ნიშნავს, რომ კიბერშეტევები ვერ ექცევა დღეს არსებული საერთაშორისო სახელშეკრულებო და ჩვეულებითი სამართლის ჩარჩოში და სცდება მისი რეგულირების ფარგლებს. ახლებური გააზრება საჭიროა მხოლოდ იმ ფარგლებში, რაც აუცილებელია კიბერშეტევების უკვე არსებულ საერთაშორისო სამართლებრივ ჩარჩოში ინკორპორაციისთვის.

საკვანძო სიტყვები: *კიბერშეტევა, კიბეროპერაცია, კიბერსივრცე, ძალის გამოყენება, საერთაშორისო ჩვეულებითი სამართალი, საერთაშორისო სახელშეკრულებო სამართალი, ევოლუციური განმარტება, ტალინის სახელმძღვანელო პრინციპები, შიდა საქმეებში ჩარევა.*

1. შესავალი

თანამედროვე ეპოქაში სულ უფრო დიდ მნიშვნელობას იძენს ტექნოლოგიების განვითარება. ამის პარალელურად, შედარებით სტატიკურად იცვლება ის ნორმები, რომლებიც მათ არეგულირებენ. გასული საუკუნის მიწურულიდან დაიწყო აქტიური დებატები, რომლის თანახმად უნდა მომხდარიყო კიბეროპერაციათა გარკვეულ ჩარჩოებში მოქცევა. ამერიკის შეერთებულ შტატებში (შემდგომში - აშშ) 11 სექტემბერს მომხდარმა ტერაქტმა გააჩინა შიში, რომ მომავალში შესაძლოა მოხდეს კიბერტერორიზმის ზრდა და განვითარება. სახელმწიფოები ხშირად არღვევენ სხვა სახელმწიფოთა კიბერსივრცეს და ვინაიდან ამ დროისთვის არ არსებობს სპეციალური რეგულაციები, ხშირად ხდება საერთაშორისო სამართლის როლის დაკ-

* ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტის იურიდიული ფაკულტეტის დოქტორანტი. თსუ-ის იურიდიული ფაკულტეტის მოწვეული ლექტორი.

ნინებაც. მაგალითად, 2007 წელს ესტონეთში განხორციელდა მასობრივი კიბერშეტევა, რომელმაც ქვეყნის საბანკო სისტემა დააზარალა; 2010 წელს კომპიუტერულმა ვირუსმა პრობლემები შეუქმნა ირანის ბირთვულ სადგურს; მანამდე კი, 2008 წელს, რუსეთ-საქართველოს შეიარაღებული კონფლიქტის დროს ქართული კიბერსივრცე გახდა ჰაკერული შეტევების მსხვერპლი. ძალის გამოყენების კონტექსტში, ეს იყო კიბერშეტევის ყველაზე აშკარა და თვალსაჩინო მაგალითი: რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებული აგრესია, რომელსაც, ყველაფერთან ერთად, თან ერთვოდა კიბერშეტევათა უპრეცედენტო მასშტაბი.

ნაშრომის მიზანია, გამოიკვლიოს არსებული საერთაშორისო სამართლებრივი მექანიზმები, რომლებიც ვრცელდება კიბეროპერაციებზე და საერთაშორისო ხელშეკრულებათა, მათ შორის, გაერთიანებული ერების (შემდგომში - გაერო) ქარტიის ევოლუციური ინტერპრეტაციის შესაძლებლობა, რათა პასუხი გაეცეს შეკითხვებს, ვრცელდება თუ არა ძალის გამოყენების აკრძალვა კიბერშეტევებზე? საჭიროებს თუ არა საერთაშორისო სამართალი ახლებურ გააზრებას კიბეროპერაციებთან, განსაკუთრებით კი კიბერშეტევების მიმართებით? და არსებობს თუ არა საერთაშორისო სამართლის სხვა დამცავი წესები ისეთი კიბერშეტევებისგან დასაცავად, რომელიც ვერ შეფასდება ძალის გამოყენებად გაეროს ქარტიის ფარგლებში?

ამ კითხვებზე პასუხის გასაცემად ნაშრომში მნიშვნელოვანი ყურადღება ეთმობა სახელმწიფოთა პრაქტიკისა და კონკრეტულ მაგალითებს, რათა უკეთ მოხდეს ჩვეულებითი სამართლის ანალიზი, რომელიც ვრცელდება კიბერშეტევებსა და ოპერაციებზე.

აქვე, უნდა აღინიშნოს, რომ კვლევა ეხება კიბეროპერაციათა მხოლოდ *jus ad bellum* კონტექსტში ანალიზს. პარალელები საერთაშორისო ჰუმანიტარული სამართლიდან გამოყენებული იქნება მხოლოდ იმ ფარგლებში, რაც საჭიროა კვლევის მთავარ შეკითხვებზე პასუხის გასაცემად.

2. გამოსაყენებელი სამართალი კიბერშეტევებთან დაკავშირებით

2.1. არსებობს თუ არა სპეციალური სახელშეკრულებო ხასიათის ნორმები კიბერშეტევებთან მიმართებით?

საერთაშორისო სამართლის ნორმები, იყოფა ორ კატეგორიად, პირველადი ნორმები, რომლებიც ადგენენ სახელმწიფოთა ქცევის ზოგად წესებს და მეორადი, იგივე სახელმწიფოთა პასუხისმგებლობის დამდგენი ნორმები.[1] აუცილებელია, პასუხი გაეცეს შემდეგ შეკითხვებს - საერთაშორისო სამართლის რა ნორმები გამოიყენება კიბერშეტევების დასარეგულირებლად? და თუ არ არსებობს სპეციალური ნორმები, მაშინ შეიძლება თუ არა, არსებული საერთაშორისო ხელშეკრულებები გავრცელდეს კიბერშეტევებზეც?

ჯერ კიდევ 2000 წლიდან, გაეროს გენერალურმა ასამბლეამ, თავის არაერთ რეზოლუციაში აღნიშნა, რომ თანამედროვე ტექნოლოგიების გამოყენების რეგულირება მთელი საერთაშორისო თანამეგობრობის ინტერესებს ეხება.[2] ასევე ისიც, რომ მათ დანაშაულებრივ გამო-

[1] *Cassese A., (ed.),* The Oxford Companion to International Criminal Justice, Oxford University Press, 2009, 19-20.

[2] იხ. მაგ.: United Nations General Assembly (UNGA) Resolutions 55/28 of 20 November 2000; 56/19 of 29 November 2001; 59/61 of 3 December 2004; 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 5 December 2007;

ყენებას შესაძლოა დიდი გავლენა ჰქონდეს ყოველ სახელმწიფოზე,[3] უფრო მეტიც, ამან შესაძლოა, საერთაშორისო სტაბილურობასა და უსაფრთხოებას შეუქმნას მნიშვნელოვანი საფრთხე.[4] ჟენევასა და ტუნისში 2003 და 2005 წლებში, გენერალური ასამბლეის ეგიდით, ორი მსოფლიო სამიტი ჩატარდა, რომლებიც ეხებოდა კიბერუსაფრთხოების საკითხებს.[5] 2010 წელს, ასტანაში, ეუთოს მემორიალურ დეკლარაციაში კიბეროპერაციებინ მზარდ ტრანსნაციონალურ საფრთხედო მოიხსენიეს.[6] იმავე წლის ნოემბერში, ნატომ განაცხადა, რომ კიბერშეტევებმა შესაძლოა, რიგ შემთხვევებში, მიაღწიოს იმ ზღვარს, რომელიც ალიანსის უსაფრთხოებასა და სტაბილურობას საფრთხის ქვეშ დააყენებს.[7] 2011 წელს, ჩინეთის, რუსეთის ფედერაციის, ტაჯიკეთისა და უზბეკეთის ერთობლივი ინიციატივით შემუშავდა გაეროს რეზოლუციის პროექტი ინფორმაციული უსაფრთხოების საერთაშორისო კოდექსის შესახებ,[8] თუმცა მცდელობა წარუმატებელი აღმოჩნდა, რადგან რეზოლუციის მიღება ვერ მოხერხდა.

აღნიშნული ადასტურებს, რომ საერთაშორისო საზოგადოება უფრო და უფრო მეტ ყურადღებას აქცევს კიბეროპერაციების საკითხს და რომ არც ისე შორსაა ის დღე, როცა შემუშავდება უნივერსალური და სპეციალური, მბოჭავი ძალის დოკუმენტი. ამ მიმართულებით რეგიონალურ დონეზე არის კიდეც გარკვეული მცდელობები. მაგალითად, ევროპის საბჭოს კონვენცია კიბერდანაშაულის შესახებ.[9] ასევე, 2001 წელს, დაკარის სამიტზე მიღებულ იქნა ალჟირის კონვენციის დამატებითი ოქმი ტერორიზმთან ბრძოლისა და პრევენციის შესახებ, აფრიკის კავშირის ეგიდით. აღნიშნული ოქმი ასევე ეხება კიბერშეტევებსაც.[10] მიუხედავად ამისა, დღეს კონკრეტული სპეციალური და სამართლებრივად მბოჭავი სახის დოკუმენტი კიბეროპერაციებთან დაკავშირებით, არ არსებობს.

2.2. საერთაშორისო ხელშეკრულებათა ევოლუციური განმარტება: ვრცელდება თუ არა არსებული სამართლებრივი რეჟიმი კიბეროპერაციებზეც?

კიბერსფეროში სპეციალური სახელშეკრულებო ნორმების არარსებობა ლოგიკურად აჩენს შემდეგ შეკითხვას – მოიცავს თუ არა არსებული საერთაშორისო სამართლებრივი რე-

63/37 of 2 December 2008; 64/25 of 2 December 2009; 65/41 of 8 December 2010; 66/24 of 2 December 2011; 67/27 of 3 December 2012.

3 UNGA Resolutions 55/63 of 4 December 2000; 56/121 of 19 December 2001, პრეამბულა.

4 UNGA Resolutions 58/32 of 8 December 2003; 59/61 of 3 December 2004; 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 5 December 2007; 63/37 of 2 December 2008; 64/25 of 2 December 2009; 65/41 of 8 December 2010; 66/24 of 2 December 2011; 67/27 of 3 December 2012.

5 *Roscini M*., Cyber Operations and the Use of Force in International Law, Oxford University Press*,* 2014, 3-4.

6 OSCE, Astana Commemorative Declaration — Towards a Security Community, SUM.DOC/ 1/10/Corr.1, 3 December 2010, § 9, <http://www.osce.org/cio/74985?download=true> [16.05.2020].

7 NATO, Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, November 2010, §§ 7, 12, <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf> [26.05.2020].

8 UN Doc A/66/359, 14 September 2011.

9 კონვენცია კიბერდანაშაულის შესახებ, ევროპის საბჭო, ETS No. 185, (მიღების თარიღი: 23.11.2001; ძალაში შესვლის თარიღი: 01.07.2004).

10 *Salinas de Frias A. M., et al. (ed.),* Counter-Terrorism: International Law and Practice, Oxford University Press, 2012, 1005-1006.

ჟიმი კიბეროპერაციებსაც? დღეს უკვე დავის საგანს აღარ წარმოადგენს ის, რომ საერთაშორისო ჰუმანიტარული სამართალი, იგივე, *jus in bello*, კერძოდ, ჟენევის 1949 წლის კონვენციები და მისი 1977 წლის დამატებითი ოქმები, სრულად ვრცელდება კიბეროპერაციებზეც და აქ მოქმედებს ყველა ის შეზღუდვა, რაც ზოგადად მოქმედებს ნებისმიერ იარაღსა თუ მეთოდთან დაკავშირებით.[11] ამ მიდგომას ამყარებს მართლმსაჯულების საერთაშორისო სასამართლოს (შემდგომში – სასამართლო) ცნობილი საკონსულტაციო დასკვნა ბირთვულ იარაღებთან დაკავშირებით, რომლის თანახმადაც, მარტენსის დათქმა ვრცელდება და არის „განსაკუთრებით ეფექტური სამხედრო ტექნოლოგიის განვითარებასთან მიმართებით“.[12] ისმის კითხვა, შესაძლებელია თუ არა, ევოლუციური ინტერპრეტაციის გზით, გაეროს ქარტია და სხვა შესაბამისი საერთაშორისო სამართლებრივი დოკუმენტები სრულად გავრცელდეს კიბეროპერაციებზეც? ამ შეკითხვაზე დადებითი პასუხის გაცემა ძალიან მნიშვნელოვანია, რადგან, წინააღმდეგ შემთხვევაში, ყოველგვარ შემდგომ მსჯელობაზე, საუბარი ზედმეტი იქნება.

საერთაშორისო სახელშეკრულებო სამართალში ხშირად დგება ამა თუ იმ ხელშეკრულების ევოლუციური ინტერპრეტაციის საკითხი. ვინაიდან ზოგჯერ ხელშეკრულება აღარ პასუხობს რეალობას და კარგავს ადეკვატურობას ტექნოლოგიური წინსვლის თუ სხვა ფაქტორთა გამო. ხელშეკრულებათა შეცვლა ან სულაც, ანულირება და ახლით ჩანაცვლება, ძალიან დიდ სიძნელეებთან და გაჭიანურებულ პროცედურებთან არის დაკავშირებული. ასეთ დროს, განსაკუთრებული ყურადღება ექცევა არსებული ხელშეკრულების ახლებურად განმარტების საკითხს, რაც სამეცნიერო წრეებში ევოლუციურ ინტერპრეტაციად არის ცნობილი.[13] სასამართლომ *ნაოსნობის* უფლებების საქმეში აღნიშნა, რომ მხარეები შეთანხმების დროს აცნობიერებდნენ იმას, რომ დროთა განმავლობაში ხელშეკრულების გაგება განიცდიდა ევოლუციას და ვინაიდან ის განუსაზღვრელი ვადით იქნა დადებული, იძლეოდა იმის პრეზუმფციას, რომ ხელშეკრულების პირობებს ჰქონდათ ევოლუციური ხასიათი.[14] ეს წარმოადგენს სასამართლოს მიერ ხელშეკრულების ევოლუციურად განმარტების ერთ-ერთ თვალსაჩინო მაგალითს.[15] აღსანიშნავია, რომ ევოლუციურ განმარტებას სასამართლოს გარდა, ასევე და უფრო აქტიურად იყენებს ადამიანის უფლებათა ევროპული სასამართლო, რომელმაც არაერთ საქმეში აღნიშნა, რომ კონვენცია არის „ცოცხალი დოკუმენტი, რომელიც უნდა განიმარტოს თანამედროვეობის ჭრილში“.[16]

ამრიგად, საერთაშორისო სამართლის კოდიფიცირება/განვითარებაში უმნიშვნელოვანეს როლს ასრულებს საერთაშორისო ხელშეკრულებათა ევოლუციური განმარტება. ამგვარი განმარტებისას განსაკუთრებით მნიშვნელოვანია სასამართლოს როლი. მართალია, კიბეროპერაციებთან დაკავშირებით ჯერჯერობით არ არსებობს გაეროს ან სხვა საერთაშორისო სა-

---

11 დაწვრილებით იხ. *Scmitt M. N.,* Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, Vol. 84, Issue 846, 2002, 365-399.

12 *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §78.

13 *Cannizzaro E., (ed.),* The Law of Treaties Beyond the Vienna Convention, Oxford University Press, 2011, 125.

14 *Dispute Regarding Navigational and Related Rights* (*Costa Rica v. Nicaragua*), ICJ, Judgment, 13 July 2009, §§ 49-52, 66.

15 *Bjorge E*., The Evolutionary Interpretation of Treaties, Oxford University Press, 2014, 1-22.

16 იხ. მაგ.: *Rasmussen v Denmark*, ECtHR, Judgment, 28 November 1984, Series A, No. 87, § 40; *Guzzardi v Italy*, ECtHR, Judgment, 6 November 1980, Series A, No. 39, §95; *Rees v the United Kingdom*, ECtHR, Judgment, 17 October 1986, Series A, No. 106, § 47; *Ireland v United Kingdom*, ECtHR, Judgment, 18 January 1978, Series A, No. 25, § 239.

სამართლოს დასკვნა, თუმცა, ეს სრულებითაც არ აკნინებს იმ ფაქტს, რომ დღეს არსებული სამართლებრივი რეჟიმი, გაეროს ქარტიის მეთაურობით, იძლევა დებულებათა ევოლუციური განმარტების საშუალებას, რომელიც სრულებით მოიცავს კიბეროპერაციებსაც, სახელდობრ, კიბერშეტევებს ძალის გამოყენების აკრძალვის კონტექსტში.

2.3. არსებობს თუ არა საერთაშორისო ჩვეულებითი სამართალი, რომელიც ვრცელდება კიბერშეტევებზე?

ევოლუციური ინტერპრეტაციის საკითხის დადებითად გადაწყვეტის შემდეგ, საჭიროა იმის გარკვევაც, არის თუ არა საერთაშორისო ჩვეულებით სამართალში ზოგადი ან სპეციალური ხასიათის ნორმები, რომლებიც ეხება კიბეროპერაციებს? ან უფრო მეტიც, ხომ არ ვართ ახალი ჩვეულებითი ნორმების ჩამოყალიბების პროცესის მომსწრენი?

საერთაშორისო ჩვეულებით სამართალს სასამართლოს სტატუტის 38-ე მუხლი განმარტავს, როგორც „ზოგადი პრაქტიკის მტკიცებულებას, რომელიც აღიარებულია, როგორც სამართალი“.[17] ჩვეულებითი სამართალი, რომელიც ძირითადად, დაუწერელი ფორმით არსებობს,[18] შედგება ორი კუმულაციური ელემენტისგან. ესენია: სახელმწიფოთა პრაქტიკა და ფსიქოლოგიური ელემენტი, *opinio juris ac necessitates,* რომელიც განიმარტება, როგორც „მტკიცებულება რწმენისა, რომ [სახელმწიფოთა] პრაქტიკა არის შესასრულებლად სავალდებულო ხასიათის და განმტკიცებულია სათანადო კანონის უზენაესობის არსებობით“.[19]

პირველ რიგში, პასუხი უნდა გაეცეს შეკითხვას, არსებობს თუ არა კიბერსპეციფიკური ნორმები საერთაშორისო ჩვეულებით სამართალში? ამ მხრივ საინტერესოა ტალინის სახელმძღვანელო პრინციპების შესავალი, სადაც აღნიშნულია - „იმის გამო, რომ სახელმწიფოთა კიბერპრაქტიკა და *opinio juris* არის არაერთგვაროვანი, ზოგიერთ შემთხვევაში რთულია იმის დასკვნა, რომ საერთაშორისო ჩვეულებით სამართალში არსებობს რაიმე კიბერსპეციალური ნორმა“.[20]

მიუხედავად ამისა, არ იქნება სწორი იმ დასკვნის გაკეთება, რომ რახან კიბერსპეციალური ჩვეულებითი ნორმების არსებობა სადავოა, ამიტომ არც არსებული ჩვეულებითი სამართლის ნორმები არ გავრცელდება კიბეროპერაციებზე.[21] როგორც *დინშტაინი* სამართლიანად მიუთითებს, „არ არის აუცილებელი, სახელმწიფოთა პრაქტიკა განვითარდეს ყოველ კონკრეტულ იარაღთან მიმართებით ცალ-ცალკე“.[22] მეტიც, სულ უფრო და უფრო იზრდება იმ სახელმწიფოთა რიცხვი, რომელთა სამხედრო სახელმძღვანელოები ითვალისწინებენ კიბერძალის გამოყენებას, მათ შორის, თავდაცვის უფლების გამოყენების წინაპირობადაც.

---

17 მართლმსაჯულების საერთაშორისო სასამართლოს სტატუტი, მუხლი 38.

18 თუმცა ცხადია, არსებობს მრავალი კონვენცია, რომელიც ახდენს ჩვეულებითი სამართლის ასახვას ან თავად არის ქცეული ჩვეულებითი სამართლის ნაწილად. მაგალითად, ვენის კონვენცია საერთაშორისო ხელშეკრულებების შესახებ, ასევე ჰააგის 1907 და ჟენევის 1949 წლის ოთხი კონვენცია.

19 *North Sea Continental Shelf* (Germany v. Denmark/The Netherlands), ICJ, Judgment of 20 February 1969, §77; *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. US), Merits, ICJ, Judgment of 27 June 1986, § 183.

20 *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 5.

21 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 3-4, 25-26.

22 *Dinstein Y.*, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, International Law Studies, Vol. 89, 2013, 280.

სამხედრო სახელმძღვანელოების მნიშვნელოვანი როლი ამა თუ იმ ნორმის ჩვეულებითი ხასიათის განსაზღვრისთვის, ასევე, აღიარა ყოფილი იუგოსლავიის სისხლის სამართლის ტრიბუნალმა *Tadic*-ის საქმეში.[23] მართალია, ამგვარ დოკუმენტთა რაოდენობა ჯერ არ არის შთამბეჭდავი, თუმცა, ჩვეულებითი ნორმის ჩამოყალიბება არ ითხოვს აბსოლუტურად ყველა სახელმწიფოს მხრიდან მისდამი აშკარა მხარდაჭერის გამოხატვას. როგორც სასამართლომ *ნორვეგიულ თევზჭერის საქმეში* დაასკვნა, სწორი საწყისი ხაზები ჩვეულებითი სამართლის ნაწილი იყო და გაერთიანებულმა სამეფომ, მანამ, სანამ დაიწყებდა აღნიშნული პრინციპის გაპროტესტებას, თავისი დუმილით აღიარა მისი ჩვეულებითი ხასიათი.[24] საილუსტრაციოდ, შეგვიძლია მოვიყვანოთ იმ ქვეყნების და საერთაშორისო ორგანიზაციების ჩამონათვალი, რომლებიც აღიარებენ კიბერშეტევებს, როგორც თავდაცვის უფლების გამოყენების წინაპირობას. ესენია: აშშ, ჩინეთი, ავსტრალია, კუბა, უნგრეთი, იტალია, ირანი, მალი, ნიდერლანდები, ყატარი, რუსეთის ფედერაცია, გაერთიანებული სამეფო და ევროკავშირი.[25] აღსანიშნავია, რომ ჯერჯერობით არ არსებობს რაიმე სახის პროტესტი, რომელიც ხელს შეუშლიდა კიბერშეტევის, როგორც ძალის გამოყენების აკრძალვის ან კიბერშეტევის საპასუხოდ თავდაცვის უფლების ამოქმედების ჩვეულებით ნორმად ჩამოყალიბებას.

ამრიგად, სახეზე გვაქვს სახელმწიფოთა მზარდი პრაქტიკა, რომელიც გამოიხატება კიბეროპერაციების სამხედრო სახელმძღვანელოებში სულ უფრო და უფრო მეტი სახელმწიფოს მიერ შეტანაში. მეტიც, არსებობს კონკრეტული მაგალითებიც, როდესაც სახელმწიფოებმა კიბერშეტევის საპასუხოდ ან პრევენციისთვის გამოიყენეს თავდაცვის უფლება. რაც შეეხება ჩვეულებითი სამართლის მეორე ელემენტს, მართალია, *opinion juris*-ის სრულყოფილად არსებობა არ დასტურდება, თუმცა, სახელმწიფოთა მხრიდან არგაპროტესტება გვიბიძგებს ვიფიქროთ, რომ დუმილით ხდება ერთგვარი თანხმობის გამოხატვაც, რამაც შესაძლოა, ბიძგი მისცეს კიბერ საერთაშორისო ჩვეულებითი სამართლის ჩამოყალიბებასაც. ამ ყველაფერში შესაძლოა, განსაკუთრებული როლი შეასრულოს „რბილმა სამართალმაც“, რომლის შესახებაც შემდგომ ქვეთავში ვიმსჯელებთ. აქედან უნდა გამოვიტანოთ დასკვნა, რომ კიბეროპერაციებზე სრულად ვრცელდება დღეს არსებული ჩვეულებითი საერთაშორისო სამართალი.

2.4. 2009 წლის ტალინის სახელმძღვანელო პრინციპები, როგორც რბილი სამართალი

2007 წელს, ესტონეთზე განხორციელებული მასობრივი კიბერშეტევის საპასუხოდ,[26] ნატომ ჩამოაყალიბა კოოპერაციული კიბერთავდაცვის უპირატესი ცენტრი. 2009 წელს ნატომ მოიწვია საერთაშორისო სამართლის 20 გამორჩეული მეცნიერი, რათა შეემუშავებინათ ის სახელმძღვანელო პრინციპები, რომლებიც არსებული საერთაშორისო სამართლის მიხედვით, გამოიყენებოდა კიბეროპერაციებისას, როგორც *jus ad bellum*, ისე *jus in bello*-ს შემთხვევებში.

---

23 *The Prosecutor v. Dusko Tadic,* ICTY, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case IT-94-1, 2 October 1995, § 99.

24 *Fisheries Case (United Kingdom v. Norway)*, ICJ, Judgment, 18 December 1951.

25 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 21-23.

26 იხ. ქვეთავი 3.1.

შედეგად, შემუშავდა „ტალინის სახელმძღვანელო პრინციპები კიბერბრძოლისას გამოსაყენებელი საერთაშორისო სამართლის შესახებ“.

რამდენადაც ტალინის სახელმძღვანელო პრინციპები არის ერთადერთი სპეციალური, კოდიფიცირებული დოკუმენტი კიბერბრძოლასთან დაკავშირებით, აუცილებელია მისი ბუნების განსაზღვრა. კერძოდ, არის ის უბრალოდ მეცნიერთა მოსაზრება და ამდენად, წარმოადგენს საერთაშორისო სამართლის დამხმარე წყაროს, სასამართლოს სტატუტის 38(1)(დ) მუხლის მიხედვით, თუ საქმე გვაქვს „რბილ სამართალთან“, რომელიც ასევე შესაძლოა განვიხილოთ, როგორც საერთაშორისო ჩვეულებითი სამართლის ფორმირების წინარე ეტაპი.

ტერმინი „რბილის სამართალი“ პირველად გამოიყენა ლორდმა მაკნირმა, რათა აღეწერა ირიბად მბოჭავი დოკუმენტები.[27] რბილი სამართალი უპირველესად ასოცირდება საერთაშორისო სამთავრობათაშორის ორგანიზაციებთან და მათ მიერ მიღებულ გადაწყვეტილებათა იურიდიულ ძალასთან (როგორც წესი არასავალდებულო ხასიათის). გარდა ამისა, თავის მხრივ, რბილი სამართალი შეგვიძლია დავყოთ შემდეგ კატეგორიებად, ესენია: საერთაშორისო ორგანიზაციათა არასავალდებულო ხასიათის დოკუმენტები (რეზოლუციები), სახელმწიფოთა შორის არსებული მბოჭავი ძალის არმქონე შეთანხმებები[28] და სავალდებულო სახელმწიფოთაშორის შეთანხმებათა (მაგალითად, საერთაშორისო ხელშეკრულებათა) არასავალდებულო ნაწილები.[29]

რბილ სამართალს ხშირად განიხილავენ *lex ferenda-ს* ჭრილში, რომელიც არის ერთგვარი მიმართულება, რომლითაც უნდა განვითარდეს საერთაშორისო სამართალი.[30] ამასთან ერთად, რბილ სამართალს ახასიათებს გარკვეული თავისებურებაც. კერძოდ, ის შეიძლება განხილულ იქნას საერთაშორისო სამართლის ტრადიციული წყაროების გამყარების საშუალებად.[31] ამ მხრივ, განსაკუთრებით საინტერესოა მიმართება საერთაშორისო ჩვეულებით სამართალთან. მაგალითად, საერთაშორისო გარემოს დაცვით სამართალში რბილ სამართალს გადამწყვეტი როლი ენიჭება, რადგან იგი ატარებს *de facto* მბოჭავ ეფექტს[32] და ამავდროულად, ხელს უწყობს ჩვეულებითი ნორმის დაჩქარებულ ჩამოყალიბებას. აქვე აღსანიშნავია, რომ ეს მიდგომა არ შემოიფარგლება მხოლოდ გარემოსდაცვითი სამართლით. რბილი სამართლის არსებობა და მისი მხედველობაში მიღების სავალდებულოობა ირიბად აღიარა კიდეც სასამართლომ *ნავთობის პლატფორმების* საქმეში. კერძოდ, ირანმა თავისი კომპრომისი დააფუძნა 1955 წელს მასსა და აშშ-ს შორის გაფორმებულ ორმხრივ შეთანხმებაზე, სადაც ხაზი გაესვა მხარეებს შორის მშვიდობისა და თანამშრომლობის აუცილებლობას. საქმე იმაშია, რომ ეს დოკუმენტი, თავისი შინაარსით, არ იყო საერთაშორისო ხელშეკრულება და წარმოადგენდა რბილი სამართლის ნაწილს, თუმცა სასამართლომ ის მხედველობაში მაინც მიიღო და

---

27 *Thurer D.,* Soft Law. Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009, §5; *Roscini M.*, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 45.

28 მაგალითად, ჰელსინკის 1975 წლის დასკვნითი აქტი, თავისი ბუნებით, არის რბილი სამართალი, Final Act, Conference On Security and Co-Operation in Europe, 1975.

29 *Thurer D.*, Soft Law, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009, §§ 9, 15.

30 *Thirlway H.*, The Sources of International Law, Oxford University Press, 2014, 165.

31 იქვე.

32 *Beyerlin U., Stoutenburg J. G.*, International Protection of Environment, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2015, §§ 2, 8, 21, 30.

აღნიშნა, რომ მართალია, დოკუმენტი არ არის სავალდებულო ძალის, მაგრამ ის მაინც უნდა იქნას გამოყენებული მხარეთა ქმედებების ინტერპრეტაციისა და შეფასებისთვის.[33]

აღნიშნულ მსჯელობას გადამწყვეტი მნიშვნელობა აქვს ტალინის სახელმძღვანელო პრინციპების სამართლებრივი ბუნების დადგენისათვის. ერთი შეხედვით, ეს დოკუმენტი არის საყოველთაოდ აღიარებულ მეცნიერთა ნაშრომი, თუმცა, ხაზგასასმელია ის ფაქტი, რომ ის შედგენილი და ჩამოყალიბებულია ნორმატიული ენით. ამასთან, აღსანიშნავია, რომ მისი შემუშავება მოხდა ნატოს ეგიდით, რომელიც თავის მხრივ, წარმოადგენს საერთაშორისო [სახელმწიფოთაშორის] ორგანიზაციას და ამდენად, გვევლინება საერთაშორისო სამართლის სრულფასოვან სუბიექტად. ფაქტია, ტალინის სახელმძღვანელო პრინციპები მეტია, ვიდრე უბრალოდ მეცნიერთა ნაშრომი. ყველა შემთხვევაში, ის, როგორც მინიმუმ, უნდა განხილულ იქნეს საერთაშორისო სამართლის დამხმარე წყაროდ და ამდენად, მოთავსდეს იმ წყაროთა ჩამონათვალში, რასაც გვთავაზობს სტატუტის 38-ე მუხლი. აქვე, აღსანიშნავია, რომ მეცნიერთა ერთი ნაწილის თვალთახედვით, საერთაშორისო სამართლის წყაროებს შორის არ არსებობს ფორმალური იერარქია.[34] ამას გარდა, ტალინის სახელმძღვანელო პრინციპები შეიძლება ჩაითვალოს რბილი სამართლის ნაწილადაც, რომელიც შესაძლოა, წარმოადგენს ამ მიმართულებით ჩვეულებითი სამართლის ჩამოყალიბების წინარე სტადიასაც. აღნიშნულ მოსაზრებას ამყარებს ისტორიული ფაქტებიც. მაგალითად, სან რემოს სახელმძღვანელო პრინციპები ზღვაში შეიარაღებულ კონფლიქტთან დაკავშირებით[35] შემუშავდა წითელი ჯვრის საერთაშორისო კომიტეტის მიერ, როგორც რბილი სამართლის ნაწილი, თუმცა, დღეს აქტიურად გამოიყენება სახელმწიფოთა მიერ და ჩვეულებითი სამართლის ხასიათი აქვს.[36]

3. კიბერშეტევების მაგალითები სახელმწიფოთა პრაქტიკაში

3.1. ესტონეთი 2007

2007 წლის გაზაფხულზე, ესტონეთის მთავრობამ განაცხადა, რომ „რუსი ჯარისკაცის“ ქანდაკებას გადაიტანდა ახალ ლოკაციაზე, ტალინის გარეუბანში. ამის მიზეზად დასახელდა ის, რომ ქანდაკება, რომელიც აღიმართა ნაცისტური გერმანიის წინააღმდეგ მეორე მსოფლიო ომში დაღუპული საბჭოთა ჯარისკაცების საპატივცემულოდ, უკვე დიდი ხნის განმავლობაში ასოცირდება უცხოური ოკუპაციის სიმბოლოსთან. აღნიშნულ განცხადებას უკმაყოფილება მოჰყვა ესტონეთში მცხოვრები რუსი მოსახლეობის მხრიდან, რაც გადაიზარდა აქციებში. ძალადობრივ პროტესტს თან დაერთო სამთავრობო უწყებებისა და კერძო კომპანიების (ბანკები, მედიამაუწყებლობები) წინააღმდეგ მიმართული კიბერშეტევები. ადგილი ჰქონდა DDoS (Distributed Denial of Service) ტიპის შეტევებს, რაც ნიშნავს, რომ ინტერნეტსაიტზე იგზავნება იმდენად ბევრი მოთხოვნა ინფორმაციის შესახებ, რომ საიტი ან ძალიან ნელა მუშაობს, ან საერ-

33 *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, §52; იხ. ასევე *Thirlway H.*, The Sources of International Law, Oxford University Press, 2014, 167.

34 დაწვრილებით იხ. *Thirlway H.,* The Sources of International Law, Oxford University Press, 2014, 117-128.

35 San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994, ICRC. <https://www.icrc.org/ihl/INTRO/560?OpenDocument> [25.05.2020].

36 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 32-33.

თოდ წყვეტს ფუნქციონირებას. შედეგად, ლეგიტიმურ მომხმარებლებს ეზღუდებათ წვდომა საიტზე. თავდაპირველად DDoS იყო მოუქნელი და მარტივად ასარიდებელი[37], თუმცა მალე დაიხვეწა და გახდა უფრო ორგანიზებული და რთული გამოსაკვლევი. ასევე გამოყენებული იქნა ბოტნეტი. ბოტნეტი (Botnet) წარმოადგენს კომპიუტერთან ქსელს, რომელიც გამოიყენება მფლობელის ნებართვის გარეშე. ესტონეთის შემთხვევაში მფლობელის ნერბართვის გარეშე გამოყენებულ იქნა დაახლოებით 85 000 კომპიუტერი, რომლებიც ინტერნეტის საშუალებით აგზავნიდნენ მოთხოვნებს ინფორმაციის შესახებ ესტონეთის სამთავრობო უწყებების საიტებზე. ესტონურმა საიტებმა მსგავს ნაკადს ვერ გაუძლო და გაითიშა.[38] კიბერშეტევები გაგრძელდა დაახლოებით 3 კვირის განმავლობაში (26 აპრილი – 19 მაისი). მიუხედავად იმისა, რომ არ დამტკიცდა რუსეთის მხარის პირდაპირი კავშირი კიბერშეტევებთან ესტონეთის მთავრობა, მაინც რუსეთს თვლის აღნიშნულ შეტევებზე პასუხისმგებლად,[39] რასაც კატეგორიულად უარყოფდა ეს უკანასკნელი.

შეკითხვა, რომელიც დაისვა, როგორც მედიაში, ასევე აკადემიურ წრეებში, იყო შემდეგი: განხორციელებული ტიპის კიბერშეტევა (კონკრეტულად DDoS) ჩაითვლება თუ არა ძალის არამართლზომიერ გამოყენებად. ცალსახად შეიძლება ითქვას, რომ აღნიშნულმა შეტევებმა მნიშვნელოვანი ზიანი მიაყენა ესტონეთს. ესტონეთის პარლამენტის სპიკერმა 2007 წლის მაისში განხორციელებული შეტევები შეადარა ბირთვულ იარაღის გამოყენების შედეგებს და განაცხადა, რომ კიბერშეტევები არ იწვევს სისხლისღვრას, მაგრამ მას შეუძლია გაანადგუროს ყველა და ყველაფერი.[40]

3.2. 2008 წლის აგვისტოში რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევების საერთაშორისო სამართლებრივი შეფასება და ტალიავინის დასკვნა

2008 წელი, რუსეთის მიერ საქართველოს მიმართ განხორციელებული აგრესიის გარდა, აღსანიშნავი იყო ასევე კიბერშეტევის იმ არნახული მასშტაბით, რომელიც რუსეთის ფედერაციამ განახორციელა საქართველოს როგორც საჯარო, ასევე კერძო სივრცეში.

შეტევების პირველი ტალღის შედეგად, გაითიშა სამთავრობო საიტები, შეიცვალა იქ არსებული ინფორმაცია ცრუ შეტყობინებებით. ვრცელდებოდა უამრავი დეზინფორმაცია, რომლის მიზანი იყო სამოქალაქო მოსახლეობაში შიშის გაჩენა.[41] საქართველოს მთავრობამ განაცხადა კიდეც, რომ რუსეთი აწარმოებდა კიბერომს.[42]

---

37 *Tikk E., Kasha K., Vihul L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 19.

38 *Steed D.,* The Strategic Implications of Cyber Warfare, Cyber Warfare: A Multidisciplinary Analysis, *Green J. A.*, Routledge, 2015, 78.

39 Russia Accused of Unleashing Cyberwar to Disable Estonia. The Guardian (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia#maincontent> [09.05.2020].

40 *Ergma E.,* Speaker of the Estonian Parliament, ციტირებულია: *Davis J.,* Hackers Take Down the Most Wired Country in Europe, Wired Magazine (21 August 2007) <https://www.wired.com/2007/08/ff-estonia/> [23.05.2020].

41 *Markoff J.,* "Before the Gunfire, Cyberattacks", The New York Times, 2008. <http://www.nytimes.com/2008/-08/13/technology/13cyber.html?_r=0> [17.05.2020].

42 *Swaine J.,* "Georgia: Russia 'Conducting Cyber War'", The Telegraph, 2008. <http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> [17.05.2020].

შეტევების მეორე ტალღა ეხებოდა სამოქალაქო და კერძო საიტების ბლოკირებას. გარკვეული პერიოდის განმავლობაში შეუძლებელი იყო წვდომა ინტერნეტზე მთელი ქვეყნის მასშტაბით, რაც მოსახლეობაში კიდევ უფრო ზრდიდა პანიკასა და უსუსურობის განცდას.

აღსანიშნავია, რომ 2009 წელს „ტალიავინის დასკვნის“ სახელწოდებით ცნობილ დოკუმენტში, რომელიც წარმოადგენდა 2008 წლის ომის ფაქტების დამდგენ კომისიის დასკვნას, არსებობს შემდეგი ჩანაწერი: „თუ ეს შეტევები მართული იყო მთავრობის ან მთავრობების მიერ და აღსანიშნავია, რომ ამ სახის ბრძოლა პირველად იქნა გამოყენებული სახელმწიფოთაშორის შეიარაღებულ კონფლიქტში.[43]

კიბერშეტევების შესახებ მოხსენებები 2008 წლის აგვისტოს რუსეთ-საქართველოს კონფლიქტის ერთ-ერთი განსაკუთრებული მახასიათებელია.[44] აშკარაა, რომ კიბერშეტევები საქართველოს წინააღმდეგ განხორციელდა კონფლიქტის მსვლელობისას. კონფლიქტის პირველ დღეებში საქართველოს მთავრობისა და საინფორმაციო საიტების უმრავლესობა მიუწვდომელი ან დაზიანებული იყო. მოგვიანებით, რამდენიმე ვებგვერდი გადაიყვანეს ამერიკულ, ესტონურ და პოლონურ სერვერებზე.[45] ზოგი ექსპერტი თვლის, რომ ამ შეტევებს შეეძლო შეესუსტებინა საქართველოს მიერ გადაწყვეტილების მიღების უნარი ისევე, როგორც მისი კომუნიკაციის უნარი მოკავშირეებთან, რაც სავარაუდოდ, შეამცირებდა ქართული ძალების ოპერატიულ მოქნილობას. ყველაზე საყურადღებო ქმედებები, რომელმაც გავლენა იქონია სახელმწიფოს მდგრადობაზე და რა დროსაც რუსეთის ფედერაცია შეიჭრა საქართველოს სუვერენულ უფლებებში იყო შემდეგი:[46]

- 20 ივლისს, სახელმწიფოს პრეზიდენტის ვებგვერდი 24 საათის განმავლობაში გათიშული იყო;
- 7 აგვისტოს რამდენიმე ქართული სერვერი და ინტერნეტტრაფიკი დაკავებული და გარე კონტროლს დაქვემდებარებული იყო;
- 8 აგვისტოს დაიწყო ფართომასშტაბიანი კიბერშეტევები საქართველოს საიტების წინააღმდეგ. კიბერშეტევების წყაროები დაუდგენელი იყო. ზოგიერთ მოხსენებაში მათ მიაწერდნენ ორგანიზაციას, სახელად “Russian Business Network”[47] (რუსეთის ბიზნესქსელი);
- გავრცელდა ცნობა, რომ საქართველოს მთავრობის ყველა ვებგვერდი მიუწვდომელი იყო ამერიკის, დიდი ბრიტანეთის და ევროპის ინტერნეტსივრცეებიდან. გავრცელებული ცნობით, კავკასიაში ტრაფიკის ერთ-ერთი საროუტერო პუნქტი თურქული AS9121 TTNet სერვერ დაბლოკილი იყო კავკასიაში ტრაფიკისთვის, სავარაუდოდ, COMSTAR-ის მიერ;
- 9 აგვისტოს, ჰაკერებმა დააზიანეს საქართველოს საგარეო საქმეთა სამინისტროს ვებგვერდი და ჩაანაცვლეს ის შეურაცხმყოფელი ფოტოსურათებით. იმ ქართულ ვებგვერდებს შორის, რომლებიც განიცდიდნენ ვირტუალურ შეტევებს ასევე იყო შინაგან საქმეთა სამინისტროს, თავდაცვის სამინისტროსა და სანაკოევის პრო-ქართული სამხრეთ ოსეთის

---

43 Report of the Independent Fact-Finding Mission on the Conflict in Georgia, September 2009, Vol. II, 217–219.

44 *Korns S. W., Kastenberg J. E.,* Georgia's Cyber Left Hook, Small Wars Journal Parameter, Winter Edition, 2008-2009.

45 მაგ. პოლონური სერვერი www.president.pl[25.05.2020].

46 RFERL, საქართველოს მთავრობა ადანაშაულებს რუსეთს „ვირტუალური ცეცხლის“ წამოწყებაში, 12.08.2008, <http://www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html>; <http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html> [25.05.2020].

47 Report of the Independent Fact-Finding Mission on the Conflict in Georgia, Vol. II, September 2009, 218.

დროებითი ადმინისტრაციის ვებგვერდი. ამის გარდა, გავრცელებული ცნობით, დაზიანებული იყო საქართველოს ეროვნული ბანკის ვებგვერდი და საქართველოს ახალი ამბების პორტალები DDoS (distributed denial of service)-ის შეტევებით;

• 12 აგვისტოსთვის საქართველოს პრეზიდენტის და პოპულარული ქართული სატელევიზიო მაუწყებლის ვებგვერდი გადაყვანილ იქნა Tulip Systems-ზე, რომელზეც მცირე პერიოდის შემდეგ ასევე განხორციელდა შეტევა;

• 12-13 აგვისტოს შინაგან საქმეთა და თავდაცვის სამინისტროების ვებგვერდებმა განიცადეს ძლიერი კიბერშეტევები.

აღნიშნულ პერიოდში დაფიქსირდა რუსული საიტის მიმართაც განხორციელებული კიბერშეტევა, თუმცა მისი მასშტაბები და მნიშვნელობა გაცილებით მცირე იყო (10 საათის განმავლობაში დაიხურა РИА Новости-ის ვებგვერდი).

დიდია იმის ალბათობა, რომ ქართული მხარის წინააღმდეგ განხორციელებული კიბერშეტევები იმართებოდა რუსეთის ხელისუფლის მიერ. ასეთ შემთხვევაში შეგვეძლება ვთქვათ, რომ სახელმწიფოთა შეიარაღებულ კონფლიქტში პირველად მოხდა კიბერშეტევების, როგორც ომის წარმოების ფორმის გამოყენება. აქვე უნდა ითქვას, რომ მარტივია მსგავსი შეტევების განხორციელება და საკმაოდ რთულია მათი თავიდან არიდება ან შეტევის წყაროს მიკვლევა.

როგორც ნაშრომში აღინიშნა, კიბერშეტევის ძალის გამოყენებად შეფასებისას უპირველესად ყურადღება უნდა გამახვილდეს შეტევისა და მიყენებული ზიანის მასშტაბზე, ასევე იმ ეფექტებზე, რასაც იწვევს კონკრეტული შეტევა. ტალიავინის დასკვნაში ნახსენები ვარაუდი, რომ კიბეროპერაციები საქართველოს წინააღმდეგ რუსეთის მიერ იყო მართული, ბევრ გარემოებას ჰფენს ნათელს.

ცალსახაა, რომ ინტერნეტის სრული ბლოკირება, დეზინფორმაციის გავრცელება და მოსახლეობაში პანიკის მიზანმიმართული დათესვა სხვა არაფერია თუ არა სახელმწიფოში არეულობის მოწყობა და წესრიგის დაცვის შესაძლებლობის ანულირება. ეს ყოველივე კი უშუალო სასიცოცხლო რისკს უქმნიდა ასიათასობით ადამიანს, რომელთა სახლები ყოველ დღე რუსული თვითმფრინავების მიერ იბომბებოდა. გორის გადაკეტვამ გამოიწვია აღმოსავლეთ და დასავლეთ საქართველოს დამაკავშირებელი ცენტრალური მაგისტრალის პარალიზება. რუსული კიბერშეტევების შედეგად კი მნიშვნელოვნად შეფერხდა ადამიანებს შორის ყველანაირი სახის კომუნიკაცია. მართლაც, ამგვარი ზიანი მსოფლიოში განხორციელებული კიბეროპერაციების შემთხვევებში უპრეცედენტოა. მეტიც, თვით ესტონეთზე განხორციელებულ კიბერშეტევაც კი ვერ მიუახლოვდება სიმძაფრითა და მასშტაბებით, საქართველოზე რუსეთის მიერ პირდაპირ განხორციელებულ შეტევებს.

ამრიგად, რუსეთის მიერ 2008 წლის აგვისტოში, საქართველოს მიმართ განხორციელებული კიბერშეტევათა მთელი ციკლი წარმოადგენდა აგრესიის და ძალის არამართლზომიერი გამოყენების კიდევ ერთ შემთხვევას.

3.3. ირანი 2010

2010 წლის ივლისში ირანის მთავრობამ აღმოაჩინა მათ კომპიუტერებზე დაინსტალირებული ვირუსი, რომელიც შემდეგ ცნობილი გახდა სახელით: Stuxnet. მიუხედავად იმისა,

რომ აღნიშნული ვირუსი ირანის სხვადასხვა კომპიუტერულ სისტემებში იქნა აღმოჩენილი, მისი ეპიცენტრი იყო ნატანზის (Natanz) ბირთვული სადგური.

ნატანზი არის ირანის მოწინავე ბირთვული სადგური და გამოიყენება ურანის გამდიდრებისთვის. ირანის მთავრობა აცხადებდა, რომ მათი ბირთვული პროგრამის მიზნები მშვიდობიანია, კონკრეტულად კი ატომური ელექტროენერგიის წარმოება. თუმცა, საერთაშორისო თანამეგობრობაში არსებობს ეჭვი, რომ ბირთვული მასალა გამოყენებულ იქნება მასობრივი განადგურების იარაღის შესაქმნელად.[48]

ურანის გამდიდრებისათვის საჭიროა პირობების ზედმიწევნით დაცვა. პირველ რიგში ურანი უნდა იყოს სუფთა ზედმეტი მინარევებისგან, რის შემდეგაც, იგი თავსდება ცენტრიფუგებში და კონკრეტული ტემპერატურისა და წნევის პირობებში ტრიალებს ზუსტად განსაზღვრული სიჩქარით.

Stuxnet ვირუსის მოქმედებით ცენტრიფუგების სიჩქარე მკვეთრად იზრდებოდა და მცირდებოდა, ამავდროულად ტექნოლოგიები არ მიუთითებდნენ გაუმართავ მუშაობაზე და მონაცემების მიხედვით პროცესი მიმდინარეობდა გეგმის მიხედვით.[49]

ირანის მთავრობამ არ გაახმაურა კონკრეტული დეტალები, თუ რა სახის გავლენა მოახდინა Stuxnet ვირუსმა. ირანის ატომური ენერგიის ორგანიზაციის იმდროინდელმა მმართველმა განაცხადა, რომ მათ მიერ ვირუსის აღმოჩენა მოხდა იმ მომენტამდე, სანამ ვირუსი შეაღწევდა მოწყობილობებში.[50] განსხვავებული განცხადება გააკეთა ირანის პრეზიდენტმა, რომელმაც აღნიშნა, რომ ვირუსმა პრობლემები შეუქმნა რამდენიმე ცენტრიფუგის ფუნქციონირებას და ელექტრონულ მოწყობილობებზე არსებული პროგრამული უზრუნველყოფის გამართულად მუშაობას.[51]

სხვა ანგარიშების მიხედვით ვირუსის მიერ მიყენებული ზიანი უფრო ფართო მასშტაბების იყო, ვიდრე ამას ასახელებენ ირანის მთავრობის წარმომადგენლები. მეცნიერებისა და საერთაშორისო უსაფრთხოების ინსტიტუტის განცხადებით,[52] ვირუსის მოქმედებას შეიძლება დაეზიანებინა არა მხოლოდ გასამდიდრებელი ურანი, არამედ თავად ცენტრიფუგებიც. საერთაშორისო ატომური ენერგიის სააგენტოს მიერ მიწოდებული მტკიცებულების თანახმად, ირანმა 2009 წლის ბოლოს და 2010 წლის დასაწყისში ნატანზის (Natanz) ბირთვულ სადგურში გამოცვალა დაახლოებით 1 000 ცენტრიფუგა. აღნიშნული ცვლილებების ლოგიკური ახსნა იქნებოდა სწორედ ვირუსი Stuxnet.[53]

იმის გათვალისწინებით, რომ ქარტიის 2(4) მუხლი წარმოადგენს შედეგზე დამყარებულ აკრძალვას, ირანზე განხორციელებული შეტევის ძალის არაკანონიერ გამოყენებად შეფასება რთულია, ვინაიდან შეტევის მანძილზე არ მომხდარა ვირუსის ზუსტად იდენტიფიცირება და

---

48 United Nations Security Council (UNSC) Resolution 1696, 31 July 2006.

49 *Shakarian P.*, Stuxnet: Cyberwar Revolution in Military Affairs. Small Wars Journal, Vol. 7, 2011, 1.

50 "Iran Briefly Halted Enrichment", Aljazeera (23 November 2010). <http://www.aljazeera.com/news/middleeast/2010/11/201011231936673748.html> [11.05.2020].

51 "Iran says Cyber Foes Caused Centrifuge Problems" Reuters (29 November 2010). <http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129> [24.05.2020].

52 *Albright D., Brannan P., Walrond C.,* Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 2010, <http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf> [22.05.2020].

53 *Katz Y.,* Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years. Jerusalem Post, Jerusalem, 15 December, 2010, <http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475> [26.05.2020].

გამოვლენა. ირანის პრეზიდენტის განცხადების თანახმად, ვირუსის შეტევამ გამოიწვია ცენტრიფუგების გაუმართავი ფუნქციონირება და შედეგად ვერ მოხერხდა ურანის გამდიდრება. აღნიშნული კიბერშეტევა ვერ ჩაითვლება ძალის არაკანონიერ გამოყენებად, რადგან არ დაზიანებულა მატერიალური საკუთრება.[54] თუმცა, თუ დავეყრდნობით მეცნიერებისა და საერთაშორისო უსაფრთხოების ინსტიტუტის ანგარიშებს, შეიძლება ითქვას, რომ ვირუსმა გამოიწვია ცენტრიფუგების განადგურება და ასეთი მატერიალური ზიანი აუცილებელია, რათა დადგინდეს გაერო-ს ქარტიის 2(4) მუხლის დარღვევა.

4. ითვალისწინებს თუ არა გაეროს ქარტია კიბერძალის გამოყენების აკრძალვას?

4.1. მიმართება გაეროს ქარტიის მე-2(4) მუხლთან

გაეროს ქარტიის მე-2(4) მუხლი,[55] *ნიკარაგუას გადაწყვეტილებაში, სასამართლომ ქარტიის ქვაკუთხედად მოიხსენია.*[56] აღნიშნული ნორმა, რომელიც ცხადია, ჩვეულებითი ხასიათისაა,[57] წარმოადგენს ასევე, *jus cogens*[58] ნორმას. როგორც წინა თავში აღინიშნა, საერთაშორისო ხელშეკრულებებზე, მათ შორის გაეროს ქარტიაზე, შესაძლოა გავრცელდეს ევოლუციური ინტერპრეტაცია. თუმცა მოცემულ თავში უნდა გაეცეს პასუხი შემდეგ შეკითხვებს – აკრძალულია თუ არა კიბერშეტევების განხორციელება ქარტიის მიხედვით? ითვლება თუ არა კიბერშეტევა ძალის გამოყენებად? თუ ასეა, მაშინ რა სახის შეტევები უნდა ჩაითვალოს ასეთად და როგორ განვსაზღვროთ აკმაყოფილებს თუ არა კონკრეტული კიბერშეტევა ძალის გამოყენების კრიტერიუმებს?

ტალინის სახელმძღვანელო პრინციპების შემმუშავებელ ექსპერტთა საერთაშორისო ჯგუფის მოსაზრებით, *jus ad bellum* აუცილებლად უნდა გავრცელდეს კიბეროპერაციათა გარკვეულ კატეგორიაზე.[59] ეს მოსაზრება გამომდინარეობს *ბირთვული იარაღების შესახებ* სასამართლოს საკონსულტაციო დასკვნის ანალიზიდან, რომლის მიხედვითაც, თავდაცვის უფლება გამოიყენება „ნებისმიერი ძალის გამოყენების საპასუხოდ, იმის მიუხედავად, რომელი იარაღით განხორციელდა შეტევა“.[60] ვინაიდან თავდაცვის უფლების გამოყენება შეუძლებელია ქარტიის მე-2(4) მუხლის კონტექსტის გარეშე და რადგან „ნებისმიერ იარაღში“ შესაძლოა თავისუფლად იგულისხმებოდეს, როგორც ელექტრონული საშუალებები, ისე კიბერშეტევაც,

---

54 *Woltag J. C.,* Computer Network Operations below the Level of Armed Force, European Society of International Law Conference Paper Series, 2011, 1. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1967593> [26.05.2020].

55 „ყველა წევრმა, საერთაშორისო ურთიერთობების განხორციელებისას, თავი უნდა შეიკავოს ძალის გამოყენებისგან ან მისი მუქარისგან, ნებისმიერი სახელმწიფოს ტერიტორიული მთლიანობის ან პოლიტიკური დამოუკიდებლობის წინააღმდეგ, ან ნებისმიერი სხვა ქმედებისგან, რომელიც ეწინააღმდეგება გაეროს მიზნებს“.

56 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, §§ 188–190.

57 იქვე, §§187-190.

58 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 44.

59 *Weller M., (ed.),* The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, 1112.

60 *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §39.

ამიტომ ცალსახაა, რომ თანამედროვე ეპოქაში *jus ad bellum*-ზე საუბრისას შეუძლებელია არ იქნას გათვალისწინებული კიბერშეტევების კონტექსტიც. კიბერსივრცეში მოქმედებისას ერთი სახელმწიფოს მიერ მეორეს მიმართ განხორციელებული კიბერშეტევა აღქმული უნდა იქნას, როგორც ქმედება, ხოლო ელექტრონული საშუალებები კი - ამ ქმედების განხორციელების საშუალება.

აღსანიშნავია, რომ გაეროს ქარტიის კომენტარები არ უარყოფს იმ მოსაზრებას, რომ სავსებით შესაძლებელია, „კომპიუტერული ქსელის შეტევა, რომელსაც აქვს იარაღის მსგავსი დამანგრეველი ეფექტი“, ჩაითვალოს ძალის გამოყენებად ქარტიის მე-2(4) მუხლის კონტექსტში,[61] მეტიც, რიგ შემთხვევებში, შესაძლოა სახეზე გვქონდეს „შეიარაღებული შეტევაც“, რაც გამოიწვევს თავდაცვის უფლების ამოქმედებას[62].

იმისათვის, რომ კიბერშეტევის შეფასება მოხდეს ძალის გამოყენებად, სამი წინაპირობა უნდა იყოს სახეზე: ა) შეტევას უნდა ახორციელებდეს სახელმწიფო; ბ) კიბეროპერაცია უნდა აღიქმებოდეს ძალის გამოყენებად ან მის მუქარად მაინც; გ) ძალის გამოყენება ან მისი მუქარა უნდა განხორციელდეს საერთაშორისო ურთიერთობების ფარგლებში.[63]

პირველ კრიტერიუმში შეიძლება მოიაზრებოდეს არა მხოლოდ სახელმწიფოს ოფიციალური *(de-jure)*,[64] არამედ, მისი *de facto* ორგანოებიც,[65] ასევე არასახელმწიფო დაჯგუფებათა ქმედებებიც, რომლებიც იმყოფებიან სახელმწიფოს ეფექტური კონტროლის ქვეშ.[66]

რაც შეეხება ძალის გამოყენების ან მისი მუქარის არსებობას, ტალინის სახელმძღვანელო პრინციპების თანახმად, ეს წინაპირობა თვალსაჩინოა, როცა კიბეროპერაციის მასშტაბები და ეფექტები შეიძლება შეედაროს [ტრადიციული], არაკიბერიარაღების მიერ მიყენებულ ზიანს, რომელიც საკმარისი იქნებოდა ქმედების ძალის გამოყენებად შესაფასებლად.[67]

ერთია, რომ შესაძლოა კიბეროპერაციებზეც გავრცელდეს ქარტიის მე-2(4) მუხლი და მეორეა ის ფაქტი, რომ არსად არ არსებობს თავად ძალის გამოყენების ოფიციალური დეფინიცია. ამგვარ შემთხვევებში, ვენის 1969 წლის კონვენციის 31-ე მუხლი, რომელიც თავის მხრივ, უმეტეს შემთხვევებში ჩვეულებით სამართალს დაეყრდნო, ითვალისწინებს ინტერპრეტაციისას კონტექსტური ანალიზის მნიშვნელობას. აღსანიშნავია, რომ სიტყვა „ძალა“ ქარტიაში ნახსენებია ასევე პრეამბულაში, 41-ე, 44-ე და 46-ე მუხლებში. ყველა მათგანში, გარდა მე-2(4) მუხლისა, მოცემულ სიტყვას წინ უძღვის სიტყვა „შეიარაღებული“, 44-ე მუხლი კი საერთოდ, მხოლოდ შეიარაღებული ძალის გამოყენების საკითხებს ეხება. ყოველივე ეს აჩენს აზრთა სხვადასხვაობას. ერთი მხრივ, შესაძლოა ვიფიქროთ, რომ რადგან ყველა სხვა შემ-

---

61 *Simma B., et al (eds.),* The Charter of the United Nations: A Commentary, 3rd ed., Vol. I, Oxford University Press, 2012, 210.

62 იქვე.

63 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 44.

64 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001, მუხლი 4.

65 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001, მუხლი 8. აღსანიშნავია, რომ გაეროს საერთაშორისო სასამართლომ, გენოციდის საქმეში, როგორც მე-4 ასევე მე-8 მუხლები აღიარა ჩვეულებითი სამართლის ნაწილებად. იხ.: *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ, Judgment, 26 February 2007, §§ 385, 398.

66 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986.

67 *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, წესი 11, 45.

თხვევაში „ძალის გამოყენება“ განიხილება შეიარაღებულ კონტექსტში, იგივე ვრცელდება მე-2(4) მუხლზეც. თუმცა, ასეთივე წარმატებით შეიძლება ითქვას, საპირისპიროც, რომ ტერმინი “შეიარაღებული” ზემოხსენებულ მუხლებში ჩადებული იყო განზრახ, ხოლო მე-2(4) მუხლი უფრო ფართოა და ფარავს სხვა „არაშეიარაღებულ“ შემთხვევებსაც. ამ უკანასკნელი არგუმენტის სასარგებლოდ მიუთითებს თავად გაეროს ქარტიის სულისკვეთებაც, დაიცვას თაობები ომის სისასტიკისაგან.[68] მიუხედავად ამისა, საკითხი ვიწროდაც რომ განვიხილოთ და ჩავთვალოთ, მე-2(4) მუხლი ეხება მხოლოდ შეიარაღებული ძალის გამოყენების აკრძალვას, კიბერშეტევებს ამ ჩარჩოდან მაინც ვერ გამოვრიცხავთ, რადგან ის თავისუფლად შეიძლება ჩაითვალოს შეიარაღებული ძალის გამოყენების ანალოგადაც. ერთადერთი შეკითხვა, რაც ამ დროს შეიძლება წარმოიშვას არის ის, თუ რა მასშტაბის უნდა იყოს კიბერშეტევა, რომ ის ჩაითვალოს შეიარაღებულ შეტევად. ამ მხრივ, დოქტრინაში შემუშავებულია სამი მიდგომა: გამოსაყენებელ საშუალებათა შეფასება; სამიზნის მიხედვით შეფასება; და ქმედების ეფექტების მიხედვით შეფასება. სამეცნიერო წრეებში ეს უკანასკნელი მიდგომაა მხარდაჭერილი, რომელიც გულისხმობს, რომ ძალის გამოყენებას უნდა ჰქონდეს პირდაპირი დამანგრეველი ეფექტი საკუთრებისა და ადამიანებისათვის.[69]

4.2. ტალინის სახელმძღვანელო პრინციპებით დადგენილი ფაქტორები

ექსპერტთა საერთაშორისო ჯგუფის თქმით, კიბერშეტევათა ძალის გამოყენებად შეფასებისას, სახელმწიფოებმა უნდა გაითვალისწინონ შემდეგი ფაქტორები: სიმწვავე; იმწუთიერობა; პირდაპირობა; შემტევი ხასიათი; ეფექტების გაზომვადობა; სამხედრო ხასიათი; სახელმწიფოს ჩართულობა; და ლეგალურობის პრეზუმფციის არ არსებობა.[70]

ჩამოთვლილი ფაქტორებიდან, ყველაზე მნიშვნელოვანია სიმწვავე. ცხადია, კიბერშეტევა, რომელსაც ახლავს ფიზიკური ზიანი, რაც შეიძლება გამოიხატოს ნგრევაში ან სულაც, ადამიანების სიკვდილშიც, წარმოადგენს ძალის გამოყენებას. იმ შემთხვევაში თუ სახეზე არ არის ამგვარი ფიზიკური ხასიათის ზიანი ან ზარალი, კიბერშეტევა მაინც შეიძლება ჩაითვალოს ძალის გამოყენებად, ოღონდ ამ დროს, მხედველობაში მიიღება შეტევის ფარგლები, ხანგრძლივობა, ინტენსივობა და ა.შ.[71] იმწუთიერობა განისაზღვრება შეტევის დაწყებისა და შედეგების გაცხადებას შორის არსებული პერიოდით. პირდაპირობაში იგულისხმება მიზეზ-შედეგობრივი კავშირი კიბეროპერაციასა და მიყენებულ ზიანს შორის. შემტევი ხასიათი ვლინდება მაშინ, როცა მეორე სახელმწიფოს კიბერსივრცეში შეჭრა ხდება უნებართვოდ. ეფექტების გაზომვადობა თვალსაჩინოა, როცა მიყენებული ზარალის აღწერა ობიექტურად შესაძლებელია. ცალკე უნდა აღინიშნოს ლეგალურობის პრეზუმფციის ფაქტორი, რომელიც წინა ფაქტორებისგან განსხვავებით, სახეზე არ უნდა იყოს. მაგალითად, როგორც წესი, ერთი სახელმწიფოს მიერ მეორისადმი ეკონომიკური ზეწოლის განხორციელება ექცევა ლეგალურობის პრეზუმფციის ფარგლებში, რაც ნიშნავს იმას, რომ ცალსახად არ არღვევს საერთაშო-

68 *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 45.

69 იქვე, 47.

70 *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, წესი 11, § 9(ა-თ), 54-55.

71 *Weller M., (ed.),* The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, 1114.

რისო სამართლის ნორმებს, ხოლო ქარტიის მე-2(4) მუხლზე კი ლაპარაკიც ზედმეტია. და ბოლოს, მნიშვნელოვანი ფაქტორია ისიც, რომ კიბერშეტევა უნდა ატარებდეს სამხედრო ხასიათს. თუმცა, ეს არ უნდა იქნას აღქმული თითქოს მხოლოდ სამხედრო ობიექტებზე თავდასხმა იგულისხმება.[72]

აღსანიშნავია, რომ 2007 წელს ესტონეთზე განხორციელებული კიბერთავდასხმა თავისუფლად შეიძლება შეფასდეს, როგორც ძალის გამოყენება, თუმცა პრობლემა იმაშია, რომ ვერ ხერხდება კიბერშეტევის რუსეთიდან დაგეგმვის/ორგანიზების დამტკიცება.

4.3. შიდა საქმეებში ჩაურევლობის პრინციპი, როგორც ძალის გამოყენების აკრძალვის ალტერნატივა დაბალი ინტენსივობის კიბერშეტევებისთვის

რიგ შემთხვევებში შესაძლოა, რომ კიბეროპერაციები ვერ აღწევდეს იმ ზღვარს, რომელიც საჭიროა მის ძალის გამოყენებად შეფასებისთვის. მიუხედავად ამისა, მსგავსი ქმედებები საერთაშორისო სამართლის მიღმა მაინც არ რჩება.

ასეთ შემთხვევებში სახეზე გვექნება სახელმწიფოს შიდა საქმეებში ჩარევა, რაც თავის მხრივ დაარღვევს დაზარალებული სახელმწიფოს სუვერენიტეტს და ასევე საერთაშორისო სამართალში განმტკიცებულ[73] შიდა საქმეებში ჩაურევლობის პრინციპს, რომელსაც ჩვეულებითი სამართლის ძალა აქვს.[74]

ასეთ დროს, როდესაც ირღვევა საერთაშორისო სამართლის პირველადი ნორმები, ხდება მეორადი ნორმების ამოქმედება, რომლებიც საფუძვლად უდევს პასუხისმგებლობის საკითხს. ცხადია, ისეთი კიბეროპერაციებისას, როდესაც ვერ კმაყოფილდება ძალის გამოყენების ან მისი მუქარის ტესტი, შეუძლებელია მათზე სამხედრო პასუხის გაცემა. თუმცა საკითხი რეგულირდება სხვა, ალტერნატიული მექანიზმებით. ასეთ შემთხვევებში, განსაკუთრებით მნიშვნელოვანია, უკვე ჩვეულებით სამართლად აღიარებული, გაეროს მიერ შემუშავებული 2001 წლის დოკუმენტი საერთაშორისო დარღვევებისთვის სახელმწიფოთა პასუხისმგებლობის შესახებ.[75]

შიდა საქმეებში ჩაურევლობის პრინციპის შეფასება ტრადიციულად ხდებოდა ძალის გამოყენების ჭრილში.[76] თუმცა, სასამართლომ აღნიშნა ნიკარაგუას საქმეში, ძალის გამოყენება

---

72 იქვე, 1115-1116.

73 მაგალითად, იხ., UNGA Resolution 2131(XX) of 21 December 1965, Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, რომელიც გმობს „შეიარაღებულ და ყველა სხვა სახის ჩარევას“ სახელმწიფოთა შიდა საქმეებში. მოცემულ კონტექსტში მნიშვნელოვანია ასევე გენერალური ასამბლეის 1970 წლის რეზოლუცია A/RES/2625(XXV) საერთაშორისო სამართლის პრინციპების შესახებ და 1975 წლის ჰელსინკის დასკვნითი აქტი (Final Act, Conference On Security and Co-Operation in Europe, 1975).

74 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, §202.

75 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001.

76 *Damrosch L.,* Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs, American Journal of International Law, Vol. 83, Issue 1, 1989, 3.

არის „განსაკუთრებით ნათელი მაგალითი“ უკანონო ჩარევის.[77] შესაბამისად, მიუხედავად იმისა, რომ ჩარევასთან დაკავშირებული საერთაშორისო სამართლის ჩვეულებით წესებს აქვს შესამჩნევი ფარგლები, რათა განხილულ იქნას ძალის გამოყენების ზოგად აკრძალვასთან ერთად, ჩარევა მაინც წარმოადგენს ცალკე მდგარ კონცეფციას.[78] როგორც მოსამართლე ჯენინგსმა განაცხადა, „უდავოა, რომ შიდა საქმეებში ჩაურევლობის პრინციპი წარმოადგენს ჩვეულებითი სამართლის ავტონომიურ პრინციპს“.[79]

შიდა საქმეებში ჩაურევლობის პრინციპი შეიძლება განვიხილოთ, როგორც სასარგებლო სამართლებრივი მექანიზმი, რომ სახელმწიფოებმა თავი დაიცვან ისეთი კიბერშეტევებისგან, რომლებიც არ იწვევენ ფიზიკურ ზიანს, თუმცა იწვევენ უარყოფით შედეგებს.

აღსანიშნავია, რომ კიბერშეტევების ლიტერატურაში უმეტესწილად განხილულია ძალის გამოყენების ფარგლებში, შესაბამისად, საინტერესოა, რატომ არ ექცევა დიდი ყურადღება შიდა საქმეებში ჩაურევლობის პრინციპს კიბერშეტევების კონტექსტში?

ეს ფაქტი შეიძლება გამომდინარეობდეს თავად სუვერენიტეტის გაგებიდან, რომელიც წარმოადგენს ტერიტორიული გაგებით არსებულ სამართლებრივ კატეგორიას, რომლის ფარგლები განისაზღვრება გეოგრაფიული საზღვრებით. როგორც სასამართლომ განაცხადა: „სახელმწიფოს სუვერენიტეტის ძირითადი იდეა საერთაშორისო ჩვეულებით სამართალში [...] მოიცავს სახელმწიფოს შიდა წყლებს, ტერიტორიულ ზღვას და საჰაერო სივრცეს მისი ტერიტორიის თავზე“.[80]

სუვერენიტეტის ამგვარი განსაზღვრება გავლენას ახდენს შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლებზე, რომელიც მიიჩნევა სუვერენიტეტის პრინციპის თანმდევად.[81] რაც შეეხება სუვერენიტეტის ტერიტორიული გაგების გავლენას, უკანონო ჩარევა განხორციელდება მხოლოდ მაშინ, როცა ჩარევა მოხდება სახელმწიფოს ფიზიკურად არსებულ ტერიტორიაზე ან მის მიმართ.[82]

ამის ფონზე, კიბერსივრცე მიიჩნევა სფეროდ, რომელზეც სახელმწიფო ვერ განახორციელებს ტერიტორიულ კონტროლს. საერთაშორისო ჰუმანიტარული სამართლის ინსტიტუტის თანახმად, „კიბერსივრცის გამორჩეული მახასიათებელია ის, რომ ეს არის ცნების დონეზე არსებული გარემო ნებისმიერ სახელმწიფოს იურისდიქციის მიღმა“.[83]

თუმცა, საპირისპირო მიდგომას ავითარებს აშშ-ის თავდაცვის დეპარტამენტი, რომელიც თვლის, რომ კიბერსივრცე არის საერთო სივრცე, როგორც ღია ზღვა, საჰაერო სივრცე და კოსმოსი.[84]

ზემოთქმულიდან გამომდინარე, გასაკვირი არ არის, რომ საერთაშორისო სამართლის კომენტატორები თავს არიდებენ იმის მტკიცებას, რომ სახელმწიფოს ვირტუალურ სივრცეში ჩარევა მიჩნეულ იყოს სახელმწიფოს სუვერენიტეტში უკანონო ჩარევად. მაგალითად, კიბერშეტევების კონტექსტში რთულია იმის წარმოდგენა, რომ ერთი სახელმწიფოს ჩარევა მეორე

---

77 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, Merits, ICJ, Judgment, 27 June 1986, § 205.

78 *Jennings R., Watts A.,* Oppenheim's International Law, 9th ed., Vol. 1 Peace, Oxford University Press, 2008, 429.

79 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 534.

80 იქვე, § 212.

81 იქვე, § 202.

82 *SS Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A. No. 10, 18.

83 *International Humanitarian Law Institute,* Rules of Engagement Handbook. September 2009, 15.

84 *US Department of Defense,* The Strategy for Homeland Defense and Civil Support, June 2005, 12.

სახელმწიფოს არამატერიალურ კატეგორიებში, როგორიცაა რადიაცია ან ელექტროენერგია, ჩაითვალოს სახელმწიფოს წინააღმდეგ განხორციელებულ დარღვევად.[85]

მიუხედავად ამისა, შეიძლება იმის მტკიცება, რომ სახელმწიფოს სუვერენიტეტი არ არის მკაცრად ტერიტორიული, რადგან საერთაშორისო ჩვეულებითი სამართალი იცნობს სუვერენიტეტის უფრო ფართო გაგებას. სუვერენიტეტი სახელმწიფოს იცავს გარე ჩარევისგან, რომელიც გავლენას ახდენს სახელმწიფოს მიერ გადაწყვეტილების მიღების უნარზე და პოლიტიკის შემუშავების პროცესებს შიდა და გარე საქმეებთან მიმართებით.

სუვერენიტეტის უფრო ფართო გაგების მხარდამჭერი მიდგომა დააფიქსირა სასამართლომ. ნიკარაგუას საქმეში, შიდა საქმეებში ჩაურევლობის პრინციპის ჩვეულებითი სამართლის სტატუსის და ფარგლების დადგენისას სასამართლომ აღნიშნა:

„აკრძალული ჩარევა უნდა წარმოადგენდეს ისეთს, რომელიც ეხება საკითხებს, რომელთა გადაწყვეტა სახელმწიფოს, სახელმწიფო სუვერენიტეტიდან გამომდინარე, შეუძლია თავისუფლად. ერთ-ერთი მათგანია პოლიტიკური, ეკონომიკური, სოციალური და კულტურული სისტემების არჩევა. ჩარევა მართლსაწინააღმდეგოა, როცა მას ახლავს იძულების მეთოდები ასეთ არჩევანთან დაკავშირებით, რომლებიც უნდა დარჩეს თავისუფალი... იძულების ელემენტი განსაზღვრავს და რეალურად, წარმოადგენს აკრძალული ჩარევის არსს.“ [86]

შესაბამისად, აკრძალული ჩარევა არის ისეთი აქტები, რომლებიც შეფასდება ძალადობრივად და აქედან გამომდინარე, მოექცევა შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლებში. ამ კონტექსტში კარგი მაგალითია ისეთი ჩარევა, რომელიც მიზნად ისახავს სამიზნე სახელმწიფოს იძულებას, შეცვალოს პოლიტიკა.[87] აქვე აღსანიშნავია, რომ მხოლოდ იძულება არ არის საკმარისი. *ნიკარაგუას* საქმიდან გამომდინარე, ასეთი იძულება უნდა ეხებოდეს ისეთ საკითხს, რომლის გადაწყვეტაში სახელმწიფოს აქვს დიდი მოცულობის დისკრეცია. ამ ელემენტზე ხაზგასმაა ლიტერატურაშიც.[88] ამ ელემენტების გათვალისწინება საჭიროა იმ მიზნით, რომ შეიძლება ჩარევის ყველა ფორმა არ იყოს აკრძალული საერთაშორისო ჩვეულებითი სამართლით, რადგან სახელმწიფოებმა თავიანთი პრაქტიკით შეიძლება შეცვალონ შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლები. მაგალითად, ნიკარაგუას საქმეში სასამართლოს მოუწია ემსჯელა, ხომ არ არსებობდა სახელმწიფოთა პრაქტიკა ისეთი *opinio juris*-ით, რომელიც ითვალისწინებდა სახელმწიფოთა ჩარევის ზოგად უფლების არსებობას, პირდაპირ ან არაპირდაპირ, ძალის გამოყენებით ან მის გარეშე, სახელმწიფოს შიგნით არსებული ოპოზიციური ძალის დახმარების მიზნით, როცა ასეთ ჩარევას გააჩნდა სათანადო პოლიტიკური ან მორალური საფუძველი.[89] თუმცა, სასამართლომ მიუთითა, რომ თანამედროვე საერთაშორისო სამართალში არ არსებობდა ასეთი ჩარევის უფლება.[90] ამ მიდგომის მნიშვნელობა მდგომარეობს იმაში, რომ ჩაუ-

---

85 *Kanuck S.,* Recent Development: Information Warfare: New Challenges for Public International Law, Harvard International Law Journal, Vol. 37, 1996, 288.

86 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 205.

87 *Jamnejad M., Wood M.,* The Principle of Non-Intervention, Leiden Journal of International Law, Vol. 22, 2009, 348.

88 *Damrosch L.,* Politics Across Borders: Nonintervention and Non-forcible Influence of Domestic Affairs. American Journal of International Law, Vol. 83, 1989, 2.

89 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 206.

90 იქვე, § 207.

რევლობის პრინციპის ფარგლების ცვლილებაზე საუბარი შეიძლება იმ შემთხვევაში, როცა არსებობს სახელმწიფოთა სათანადო პრაქტიკა და თანმდევი *opinio juris*.

იმის გათვალისწინებით, რომ წინამდებარე ნაშრომის მიზანი არ არის შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლების დადგენა თანამედროვე საერთაშორისო სამართალში, შიდა საქმეებში ჩაურევლობის პრინციპის განხილვის მიზანია იმის ჩვენება, რომ ეს პრინციპი მოქმედებს კიბერშეტევების მიმართ მაშინ, როცა არსებობს კიბერშეტევის ძალის გამოყენებად შეფასების ეჭვი. ამისათვის, ზემოთ მოცემული ანალიზიდან გამომდინარე, საჭიროა დადგინდეს ა) კიბერშეტევის მიზანს წარმოადგენს თუ არა სამიზნე სახელმწიფოს იძულება, შეცვალოს პოლიტიკა და ბ) თვალსაჩინოა თუ არა იძულების/ძალადობრივი მეთოდის გამოყენება. თუ პასუხი დადებითია, შემდეგი ნაბიჯის სახით უნდა შეფასდეს, რამდენად ეხება კიბერშეტევა იმ საკითხებს, რომელიც სახელმწიფოს შეუძლია თავისუფლად გადაწყვიტოს. პირველი საკითხის გადაწყვეტა მოითხოვს სამიზნე სახელმწიფოზე განხორციელებული გავლენის შეფასებას. მეორე საკითხი უკავშირდება ჩარევის მიზნის დადგენას.

ამ კონტექსტში საინტერესოა, წარმოადგენს თუ არა ესტონეთის 2007 წლის კიბერშეტევები აკრძალულ ჩარევას. ამისთვის საჭიროა დადგინდეს, განხორციელდა თუ არა კიბერშეტევები იმ მიზნით, რომ ეიძულებინა ესტონეთის მთავრობა შეეცვალა პოლიტიკა. ამისთვის უნდა შეფასდეს, თუ რა მასშტაბის პრობლემები წარმოშვა შედეგად აღნიშნულმა კიბერშეტევებმა. 2007 წელს ესტონეთი იყო ყველაზე დიდი ქსელის მქონე სახელმწიფო ევროპაში, ერთგვარი „ინფორმაციული საზოგადოება“.[91] შესაბამისად, მთავრობა, კერძო სექტორი და მოქალაქეები ძლიერ ეყრდნობოდნენ ინტერნეტმომსახურებას. მაგალითად, 2007 წელს საბანკო ოპერაციების 95% ხორციელდებოდა ელექტრონულად.[92] ამის შედეგად, შეტევების მიერ მოწინავე ბანკების საიტების მოშლამ დიდი მასშტაბით შეაფერხა ეკონომიკური აქტივობები.

შეტევების ქვეშ მოექცა მედია სადგურებიც. ეს გამოწვეული იყო იმით, რომ მედიაზე წვდომა ესტონეთში ძირითადად ხორციელდება ინტერნეტით. შესაბამისად, მთავარი საინფორმაციო საიტების ქსელიდან გამორთვის გამო მოქალაქეებს არ მიეწოდებოდა ინფორმაცია კიბერშეტევის მასშტაბისა და შედეგების შესახებ. უფრო მეტიც, როცა აღმოაჩინეს, რომ შეტევები ხორციელდებოდა საზღვარგარეთიდან, შემდგომი შეტევების პრევენციის მიზნით, მოხდა გარედან შემომავალი ინტერნეტტრაფიკის გამორთვა. შედეგად, ესტონეთი აღმოჩნდა მსოფლიოსგან მოწყვეტილი.

შეტევების უარყოფითი შედეგი, ასევე, დიდი იყო საჯარო სექტორში, რადგან შეტევები ხორციელდებოდა ძირითად სამთავრობო საიტებზე, როგორიცაა პრემიერ-მინისტრის და მისი პოლიტიკური პარტიის, პრეზიდენტის აპარატის, პარლამენტის და სახელმწიფო აუდიტის საიტები. აღნიშნული საიტები გახდა სრულად უფუნქციო, რის გამოც შეუძლებელი გახდა ამ საიტებზე ინფორმაციის განახლება და ელექტრონული ფოსტით კონტაქტის შენარჩუნება.[93]

და ბოლოს მნიშვნელოვანია იმის აღნიშვნა, რომ შეტევები საჯარო და კერძო სექტორის მიმართ გაგრძელდა სამი კვირის განმავლობაში. ამ დროისა და მისი ინტენსივობის გათვა-

---

91 *Tikk E., Kasha K., Vihul L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 16.

92 იქვე, 17.

93 *Woltag J. C.,* Computer Network Operations below the Level of Armed Force, European Society of International Law Conference Paper Series, 2011, 5.

ლისწინებით, შეიძლება იმის მტკიცება, რომ მათ თან ახლდა იძულების ელემენტი, რათა ესტონეთის მთავრობას შეეცვალა ბრინჯაოს ჯარისკაცის ქანდაკების ლოკაცია.

რაც შეეხება მეორე საკითხს – უკავშირდებოდა თუ არა იძულება იმ სფეროს, სადაც სახელმწიფოს შეუძლია გააკეთოს თავისუფალი არჩევანი? ცხადია, რომ არ არსებობს უფლება, ერთი სახელმწიფო იძულების გზით ჩაერიოს მეორე სახელმწიფოს საქმეებში, როცა მას სურს განსაკუთრებული მნიშვნელობის ქანდაკების ან მემორიალის ლოკაციის ცვლილება. სხვა სიტყვებით, ეს არის სფერო, სადაც სახელმწიფოს სრული ფარგლებით იცავს შიდა საქმეებში ჩაურევლობის პრინციპი.

დასკვნის სახით შეიძლება ითქვას, რომ ესტონეთის მიმართ განხორციელებული კიბერშეტევები წარმოადგენდა ესტონეთი სუვერენიტეტის და შიდა საქმეებში ჩაურევლობის პრინციპის დარღვევას.

ასეთი დარღვევის დადგენა მნიშვნელოვანია იმ კუთხით, რომ სახელმწიფოს მიეცემა უფლება, მოითხოვოს უკანონო ქმედების აღკვეთა, ასეთი ქმედების არგამეორების გარანტიები და, როცა შესაძლებელია, რეპარაციები.[94] გარდა ამისა, საერთაშორისო ჩვეულებითი სამართალი საშუალებას აძლევს სახელმწიფოს, გამოიყენოს კონტრზომები განგრძობადი დარღვევის შემთხვევაში.[95] ასეთი კონტრზომები უნდა იყოს აუცილებელი და პროპორციული.[96]

ყოველივე ზემოთქმულიდან გამომდინარეობს, რომ შიდა საქმეებში ჩაურევლობის პრინციპი ქმნის იმ სამართლებრივ ჩარჩოს, რომელსაც შეუძლია დაიცვას სახელმწიფოები კიბერშეტებისგან იმ შემთხვევებში, როცა კიბერშეტევა ვერ ექცევა ძალის გამოყენების აკრძალვის ფარგლებში, მაგრამ შედეგად იწვევს სახელმწიფოს იძულებას შიდა საქმეების ისეთ საკითხთან დაკავშირებით, რომლის გადაწყვეტა სახელმწიფოს შეუძლია სრულიად თავისუფლად.

5. დასკვნა

ტექნოლოგიების განვითარების კვალდაკვალ, სულ უფრო და უფრო აქტუალური ხდება საერთაშორისო სამართლის კონსერვატიული ხედვის გადაფასების საკითხი. ამ პროცესის დაწყების ერთ-ერთი მნიშვნელოვანი ფაქტორი კი სწორედ საერთაშორისო განზომილებაში წარმოებული კიბეროპერაციების სამართლებრივი რეგულირების საჭიროებაა, რადგან სახელმწიფოს უსაფრთხოებაში სულ უფრო დიდ ადგილს იკავებს კიბერუსაფრთხოება.

სტატიის შესავალში დასმულ შეკითხვებზე პასუხები, წარმოდგენილი ანალიზიდან გამომდინარე, შესაძლებელია შეჯამდეს შემდეგი სახით:

1) კიბერშეტევები შეიძლება მოვიაზროთ გაეროს ქარტიის 2(4)-ე მუხლით აკრძალული ძალის გამოყენების ფარგლებში, რადგან:

• ქმედების ძალის გამოყენებად შეფასება ხორციელდება შედეგობრივი მაჩვენებლების მიხედვით. იმ შემთხვევაში, თუ კიბერშეტევები გამოიწვევს ისეთივე შედეგებს, რასაც გამო-

94 Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001, მუხლები 30, 31.

95 იქვე, მუხლი 49.

96 იქვე, მუხლი 51.

იწვევდა შეიარაღებული თავდასხმები, მაშინ, კიბერეკვივალენტურობის მიდგომის თანახმად, არაფერი არ უშლის ხელს, რომ ასეთი კიბერშეტევა ჩაითვალოს ძალის გამოყენებად;

• ძალის გამოყენების კონცეფცია არ არის მკაცრად შეზღუდული „შეიარაღებულის“ კრიტერიუმით, როგორც, მაგალითად, გაეროს ქარტიის 51-ე მუხლში ნახსენები „შეიარაღებული თავდასხმა“;

• 2(4)-ე მუხლი წარმოადგენს სახელშეკრულებო ნორმას, რომელზეც თავისუფლად შეიძლება გავრცელდეს ხელშეკრულების ევოლუციური ინტერპრეტაცია – ამ მუხლის მიზანი იყო, აეკრძალა იძულების ელემენტის მატარებელი მოქმედებები სახელმწიფოთაშორის ურთიერთობებში. გაეროს ქარტიის მიღების დროს შეუძლებელი იყო, რომ ხელშეკრულების შემდგენლებს ძალის გამოყენებაში მოეაზრებინათ კიბერშეტევები. ერთი მხრივ, ამ ხარვეზის აღმოსაფხვრელად და, მეორე მხრივ, ამ მუხლის თვითმიზანის შესრულების კუთხით, ევოლუციური ინტერპრეტაცია წარმოადგენს სამართლებრივად რელევანტურ მექანიზმს. შესაბამისად, დღეის მდგომარეობით, კიბერშეტევები, გარკვეული წინაპირობების არსებობისას (სიმძიმე, მასშტაბურობა, ინტენსივობა და ა.შ.) თავისუფლად შეიძლება ჩაითვალოს გაეროს ქარტიის 2(4)-ე მუხლით აკრძალულ ქმედებად.

2) მეორე მხრივ, თუ კიბერშეტევა ვერ მიაღწევს იმ სტანდარტს, რაც საჭიროა მის ძალის გამოყენებად შეფასებისთვის, საერთაშორისო სამართალი სამართლებრივი დაცვის გარეშე არ ტოვებს დაზარალებულ სახელმწიფოს, რადგან ამ შემთხვევაში ამოქმედდება შიდა საქმეებში ჩაურევლობის პრინციპი. ამ პრინციპით გათვალისწინებული დაცვით სარგებლობისთვის კი საჭიროა, რომ

• ჩარევის მიზანს წარმოადგენდეს სამიზნე სახელმწიფოს იძულება, შეცვალოს პოლიტიკა;

• იძულების/ძალადობრივი მეთოდის გამოყენება უნდა ეხებოდეს იმ საკითხებს, რომელიც სახელმწიფოს შეუძლია თავისუფლად გადაწყვიტოს.

3) ამის ფონზე, შეიმჩნევა ტენდენცია, რომ კიბერშეტევების რეგულირება მოხდეს უფრო სპეციალიზებული ნორმებით. ამის კარგი მაგალითია ტალინის სახელმძღვანელო პრინციპები, რომელიც შემუშავდა ისეთი საერთაშორისო ორგანიზაციის ეგიდით, როგორიცაა ნატო, რაც თავის მხრივ, ზრდის ამ დოკუმენტის ავტორიტეტს. აღნიშნული დოკუმენტი, რომელიც წარმოადგენს საყოველთაოდ აღიარებულ მეცნიერთა ნაშრომს, ჩამოყალიბებულია ნორმატიული ენით, რაც კიდევ უფრო ზრდის მის, როგორც რბილი სამართლის წყაროს ავტორიტეტს.

4) გარდა ამისა, მნიშვნელოვან როლს თამაშობს სახელმწიფოთა პრაქტიკა და მათი ხედვა კიბერშეტევების შესახებ. სამხედრო სახელმძღვანელოებისა და სახელმწიფოთა მზარდი პრაქტიკის ანალიზი გვიჩვენებს, რომ კიბერშეტევები სახელმწიფოების მიერ აღიქმება ძალის გამოყენების დამოუკიდებელ ფორმად და მათ სამართლებრივ შეფასებას ცდილობენ დღეს არსებული საერთაშორისო სამართლის ფარგლებში.

5) საქართველოს, ესტონეთის და ირანის მაგალითებზე კარგად ჩანს, თუ რაოდენ დიდი დარტყმა შეიძლება მიადგეს სახელმწიფოს მის კიბერსივრცეზე განხორციელებული შეტევის შედეგად. ყოველივე ამის ფონზე, შეგვიძლია, ვივარაუდოთ, რომ ძალიან მალე ჩამოყალიბდება ახალი დარგი, სახელწოდებით, კიბეროპერაციების საერთაშორისო სამართალი, რომელიც, სახელმწიფო უსაფრთხოების ინტერესებიდან გამომდინარე, აქცენტს გააკეთებს რეაგირების მექანიზმებისა და სახელმწიფოთა პასუხისმგებლობის საკითხებზე.

6) მართლმსაჯულების საერთაშორისო სასამართლოს პოზიციის მიხედვით, ხელშეკრულების ნორმის გაგებამ დროთა განმავლობაში შეიძლება განიცადოს ევოლუცია, იძლევა საშუალებას, რომ კიბერშეტევებზე გავრცელდეს უკვე არსებული ნორმები. ეს მიდგომა, თავის მხრივ, მიანიშნებს საერთაშორისო სამართლის ახლებურ გააზრებაზე კიბერშეტევების მიმართ.

საბოლოო შეჯამების სახით და ნაშრომის მიერ დასმულ კითხვაზე პასუხის გაცემის მიზნით, შეიძლება ითქვას, რომ კიბერშეტევები საჭიროებს ახლებურ გააზრებას საერთაშორის სამართლის ჭრილში, თუმცა, ეს არ ნიშნავს, რომ კიბერშეტევები ვერ ექცევა დღეს არსებული საერთაშორისო სახელშეკრულებო და ჩვეულებითი სამართლის ჩარჩოში (ძალის გამოყენების აკრძალვა და შიდა საქმეებში ჩაურევლობის პრინციპი) და სცდება მისი რეგულრების ფარგლებს. ახლებური გააზრება საჭიროა მხოლოდ იმ ფარგლებში, რაც აუცილებელია, ერთი მხრივ, კიბერშეტევების უკვე არსებულ საერთაშორისო სამართლებრივ ჩარჩოში ინკორპორაციისთვის.

ბიბლიოგრაფია:

1. გაერთიანებული ერების ორგანიზაციის ქარტია (მიღების თარიღი: 26.06.1945; ძალაში შესვლის თარიღი: 24.10.1945).
2. მართლმსაჯულების საერთაშორისო სასამართლოს სტატუტი.
3. კონვენცია კიბერდანაშაულის შესახებ, ევროპის საბჭო, ETS No. 185, (მიღების თარიღი: 23.11.2001; ძალაში შესვლის თარიღი: 01.07.2004).
4. RFERL, საქართველოს მთავრობა ადანაშაულებს რუსეთს „ვირტუალური ცეცხლის“ წამოწყებაში, 12.08.2008. <http://www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html> [25.05.2020].
5. United Nations General Assembly Resolution 2131(XX) of 21 December 1965.
6. United Nations General Assembly Resolution 2625(XXV) of 24 October 1970.
7. United Nations General Assembly Resolution 55/28 of 20 November 2000.
8. United Nations General Assembly Resolution 56/19 of 29 November 2001.
9. United Nations General Assembly Resolution 59/61 of 3 December 2004.
10. United Nations General Assembly Resolution 60/45 of 8 December 2005.
11. United Nations General Assembly Resolution 61/54 of 6 December 2006.
12. United Nations General Assembly Resolution 62/17 of 5 December 2007.
13. United Nations General Assembly Resolution 63/37 of 2 December 2008.
14. United Nations General Assembly Resolution 64/25 of 2 December 2009.
15. United Nations General Assembly Resolution 65/41 of 8 December 2010.
16. United Nations General Assembly Resolution 66/24 of 2 December 2011.
17. United Nations General Assembly Resolution 67/27 of 3 December 2012.
18. United Nations General Assembly Resolution 55/63 of 4 December 2000.
19. United Nations General Assembly Resolution 56/121 of 19 December 2001.
20. United Nations General Assembly Resolution 58/32 of 8 December 2003.
21. United Nations General Assembly Resolution 59/61 of 3 December 2004.
22. United Nations General Assembly Resolution 60/45 of 8 December 2005.
23. United Nations General Assembly Resolution 61/54 of 6 December 2006.
24. United Nations General Assembly Resolution 62/17 of 5 December 2007.

25. United Nations General Assembly Resolution 63/37 of 2 December 2008.
26. United Nations General Assembly Resolution 64/25 of 2 December 2009.
27. United Nations General Assembly Resolution 65/41 of 8 December 2010.
28. United Nations General Assembly Resolution 66/24 of 2 December 2011.
29. United Nations General Assembly Resolution 66/359 of 14 September 2011.
30. United Nations General Assembly Resolution 67/27 of 3 December 2012.
31. United Nations Security Council (UNSC) Resolution 1696, 31 July 2006.
32. Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001.
33. OSCE, Astana Commemorative Declaration — Towards a Security Community, SUM.DOC/ 1/10/Corr.1, 3 December 2010, § 9, <http://www.osce.org/cio/74985?download=true> [16.05.2020].
34. NATO, Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, November 2010, §§ 7, 12, <http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf> [26.05.2020].
35. San Remo Manual on International Law Applicable to Armed Conflicts at Sea, 12 June 1994, ICRC. <https://www.icrc.org/ihl/INTRO/560?OpenDocument> [25.05.2020].
36. Final Act, Conference on Security and Co-Operation in Europe, 1975.
37. International Humanitarian Law Institute, Rules of Engagement Handbook. September 2009, 15.
38. *US Department of Defense,* The Strategy for Homeland Defense and Civil Support, June 2005, 12.
39. *Albright D., Brannan, P., Walrond, C.,* Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 2010, <http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf> [22.05.2020].
40. *Beyerlin U., Stoutenburg J. G.*, International Protection of Environment, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2015, §§ 2, 8, 21, 30.
41. *Bjorge E*., The Evolutionary Interpretation of Treaties, Oxford University Press, 2014, 1-22.
42. *Cannizzaro E., (ed.),* The Law of Treaties Beyond the Vienna Convention, Oxford University Press, 2011, 125.
43. *Cassese A., (ed.),* The Oxford Companion to International Criminal Justice, Oxford University Press, 2009, 19-20.
44. Cyber Attacks Disable Georgian Websites, Ministry of Foreign Affairs of Georgia <http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html> [25.05.2020].
45. *Damrosch L.,* Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs, American Journal of International Law, Vol. 83, 1989, 2-3.
46. *Dinstein Y.*, Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference, International Law Studies, Vol. 89, 2013, 280.
47. *Ergma E.,* Speaker of the Estonian Parliament, ციტირებული: *Davis, J.,* Hackers Take Down the Most Wired Country in Europe, Wired Magazine (21 August 2007) <https://www.wired.com/2007/08/ff-estonia/> [23.05.2020].
48. "Iran Briefly Halted Enrichment", Aljazeera (23 November 2010). <http://www.aljazeera.com/news/middleeast/2010/11/201011231936673748.html> [11.05.2020].
49. "Iran says Cyber Foes Caused Centrifuge Problems" *Reuters* (29 November 2010). <http://www.reuters.com/article/iran-ahmadinejad-computers-idAFLDE6AS1L120101129> [24.05.2020].
50. *Jamnejad M., Wood, M.,* The Principle of Non-Intervention, Leiden Journal of International Law, Vol. 22, 2009, 348.
51. *Jennings R., Watts A.,* Oppenheim's International Law, 9th ed., Vol. 1 Peace, Oxford University Press, 2008, 429.
52. *Katz Y.,* Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years. Jerusalem Post, Jerusalem, 15 December, 2010, <http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475> [26.05.2020].

53. *Kanuck S.,* Recent Development: Information Warfare: New Challenges for Public International Law, Harvard International Law Journal, Vol. 37, 1996, 288.
54. *Korns S. W., Kastenberg J. E.,* Georgia's Cyber Left Hook, Small Wars Journal Parameter, Winter Edition, 2008-2009.
55. *Markoff J.,* "Before the Gunfire, Cyberattacks", The New York Times*,* 2008, <http://www.nytimes.-com/2008/08/13/technology/13cyber.html?_r=0> [17.05.2020].
56. Report of the Independent Fact-Finding Mission on the Conflict in Georgia, Vol. II, September 2009, 217–219.
57. Russia Accused of Unleashing Cyberwar to Disable Estonia*.* The Guardian (17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia#maincontent> [09.05.2020].
58. *Roscini M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 3-4, 21-23, 25-26, 32-33, 44-45, 47.
59. *Salinas de Frias, A. M., et al. (ed.),* Counter-Terrorism: International Law and Practice, Oxford University Press, 2012, 1005, 1006.
60. *Schmitt M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 5, 45, 54-55.
61. *Scmitt M. N.,* Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, Vol 84, Issue 846, 2002, 365-399.
62. *Shakarian P.*, Stuxnet: Cyberwar Revolution in Military Affairs. Small Wars Journal, 2011, 1, 7.
63. *Simma B., et al (eds.),* The Charter of the United Nations: A Commentary, Vol. I, 3rd ed., Oxford University Press, 2012, 210.
64. *Steed D.,* The Strategic Implications of Cyber Warfare, Cyber Warfare: A Multidisciplinary Analysis, *Green J., A.*, Routledge, 2015, 78.
65. *Swaine J.,* "Georgia: Russia 'Conducting Cyber War'", The Telegraph, 2008. <http://www.tele-graph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html> [17.05.2020].
66. *Thurer D.,* Soft Law. Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009, §§5, 9, 15.
67. *Thirlway H.*, The Sources of International Law, Oxford University Press, 2014, 117-128, 165.
68. *Tikk E., Kasha K., Vihul L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 16-17, 19.
69. *Weller M., (ed.),* The Oxford Handbook of the Use of Force in International Law, Oxford University Press, 2015, 1112, 1114-1116.
70. *Woltag J. C.,* Computer Network Operations below the Level of Armed Force, European Society of International Law Conference Paper Series, 2011, 1, 5. <https://papers.ssrn.com/sol3/papers.cfm?abstract-id=1967593> [26.05.2020].
71. *Dispute Regarding Navigational and Related Rights* (*Costa Rica v. Nicaragua*), ICJ, Judgment, 13 July 2009, §§ 49-52, 66.
72. *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, ICJ, Judgment, 26 February 2007, §§ 385, 398.
73. *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, §52.
74. *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §§ 39, 78.
75. *The Prosecutor v. Dusko Tadic,* ICTY, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case IT-94-1, 2 October 1995, § 99.
76. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, §§ 187–190, 202, 205- 207, 212, 534.
77. *Rees v the United Kingdom*, ECtHR, Judgment, 17 October 1986, Series A, No. 106, § 47.

78. *Rasmussen v Denmark*, ECtHR, Judgment, 28 November 1984, Series A, No. 87, § 40.
79. *Guzzardi v Italy*, ECtHR, Judgment, 6 November 1980, Series A, No. 39, §9.
80. *Ireland v United Kingdom*, ECtHR, Judgment, 18 January 1978, Series A, No. 25, § 239.
81. *North Sea Continental Shelf* (Germany v. Denmark/The Netherlands), ICJ, Judgment of 20 February 1969, §77.
82. *Fisheries Case (United Kingdom v. Norway)*, ICJ, Judgment, 18 December 1951.
83. *SS Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A. No. 10, 18.