ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

იურიდიული ფაკულტეტი

სამართლის სადოქტორო პროგრამის დოქტორანტის

გურამ ღვინჯილიას

სადისერტაციო ნაშრომი თემაზე:

კიბეროპერაციები: გამოწვევა ძალის გამოყენების საერთაშორისო სამართლისთვის

ნაშრომი წარმოდგენილია სამართლის დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სამეცნიერო ხელმძღვანელი

პროფესორი, დოქტორი ირინე ქურდაძე

თბილისი

2020

აბსტრაქტი

თანამედროვე ტექნოლოგიების განვითარებასთან ერთად სულ უფრო აქტუალური ხდება საერთაშორისო სამართლის გადაფასების საკითხი. თანამედროვე საერთაშორისო სამართლის ეფექტიანი მოქმედებისთვის აუცილებელი წინაპირობაა, რომ მისი სტატიკური ნორმები ადეკვატურად აწესრიგებდეს თანამედროვე ტექნოლოგიების განვითარებით გამოწვეულ შედეგებს, მათ შორის კიბერსივრცეს. ჯერჯერობით საერთაშორისო სამართალში არ არსებობს კონკრეტული სპეციალიზებული ნორმები, რომლებიც უპასუხებს ტექნოლოგიურ გამოწვევებს.

სად გადის კიბეროპერაციების ზღვარი? რა მომენტიდან შეიძლება გადაიქცეს უბრალო კიბეროპერაცია სერიოზული შედეგების მქონე აქტად ან შეიძლება თუ არა კიბეროპერაცია თავისი არსით გაუთანაბრდეს შეიარაღებულ თავდასხმას? აღნიშნულ შეკითხვებზე პასუხი შედგება რამდენიმე სხვადასხვა ელემენტისგან, რომლებიც ცალ-ცალკე და ერთიანობაში განხილულია ნაშრომში და სათანადო პასუხს სცემს პრობლემურ კითხვებს.

პროგრესთან ერთად იცვლება პოლიტიკის წარმოების გზები. დღესდღეობით პოლიტიკური ზეწოლის განხორციელება გაცილებით მარტივია, როდესაც საქმე გვაქვს კიბერძალასთან ან კიბერძალის მუქარასთან. შესაბამისად ჩნდება საჭიროება, რომ ნებისმიერი ეკონომიკური და სამხედრო სიძლიერის ქვეყანას, მეტ-ნაკლებად განვითარებული ჰქონდეს კიბერუსაფრთხოება, რათა დაცული იყოს პოლიტიკური იძულების საფრთხისგან.

ნაშრომი მიზნად ისახავს არსებული საერთაშორისო სამართლებრივი რეჟიმის განხილვას, რომელიც ვრცელდება კიბეროპერაციებზე. ახალი ნორმების არარსებობის მიუხედავად, კიბეროპერაციები არ რჩება საერთაშორისო სამართლის რეგულირების მიღმა. აღნიშნულის საჩვენებლად, ნაშრომში განხილული იქნება კიბეროპერაციების მიმართება გაერთიანებული ერების ორგანიზაციის ქარტიასთან, ძალის გამოყენების აკრძალვასა და შიდა საქმეებში ჩაურევლობის პრინციპთან. ასევე, განმარტებული იქნება ხელშეკრულების ევოლუციური განმარტების მიმართება კიბეროპერაციებთან. 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. ასევე, ცალკე უნდა გამოიყოს 2019 წლის 28 ოქტომბერს საქართველოზე განხორციელებული კიბერშეტევა.

კიბერშეტევების ფაქტების მომრავლებასთან ერთად, აქტუალური ხდება აღნიშნული შეტევებისგან თავდაცვის მექანიზმების ძიება. ნაშრომში განხილული იქნება კიბერშეტევების მიმართება გაეროს ქარტიის 51-ე მუხლთან, რომელიც გულისხმობს სახელმწიფოთა თავდაცვის უფლებას.

საკვლევი თემის დამუშავებისას გამოყენებულია იურიდიული მეცნიერებისთვის ტრადიციული - დოგმატური და ნორმატიული მეთოდები. ნაშრომში განვითარებული არგუმენტაცია განვითარებულია ჰიპოთეზის წამოყენების, დამუშავებისა და შემოწმების მეთოდით, რაც სხვადასხვა ხარისხით იყენებს ნორმატიულ, ისტორიულ, ანალიტიკურ, სისტემურ, ლოგიკურ და შედარებით მეთოდებს, რათა სრულყოფილად მოხდეს არსებული საერთაშორისო სამართლის კომპლექსური ანალიზი ისეთ ახალ ფენომენთან, როგორიც არის კიბეროპერაციები. შესაბამისი ადგილი ეთმობა პროგნოზირების მეთოდს. ნაშრომი სამართლებრივად და ემპირიულად აანალიზებს სახელმწიფოთა ოფიციალურ პოზიციებს და შედარებითი ანალიზის საფუძველზე, დედუქციისა და ინდუქციის მეთოდების გამოყენებით, მკითხველს სთავაზობს ახალ დასკვნებს. საბოლოოდ, შეფასების მეთოდის საშუალებით, შეფასებულია ნაშრომის კვლევის საგნის მიმართ გაკეთებული მიგნებების მართებულობა.

ნაშრომი სტრუქტურულად შედგება შესავლის, შვიდი ძირითადი თავისგან და დასკვნისაგან.

საერთაშორისო სამართალში დიდი მნიშვნელობას იძენს გარემოება, თუ რამდენად დგება ფიზიკური ზიანი კიბეროპერაციის შედეგად. ასეთ დროს შედარებით ადვილია უკვე არსებული ნორმების ამოქმედება, რადგან, რიგ შემთხვევებში, კიბეროპერაციის შედეგად მიყენებული ზიანი შეიძლება მარტივად გაუტოლდეს შეიარაღებული თავდასხმის შედეგად მიყენებულ ზიანს. დიდი ალბათობით, უახლოეს მომავალში შეიცვლება სახელმწიფოების მიერ აგრესიის

გამოვლინების გზები და მეთოდებიც. გაცილებით ნაკლები ფინანსური დანახარჯის ფონზე იდენტური შედეგის მიღება ნებისმიერი აგრესორისთვის სასურველი ფუფუნებაა და ამ ყველაფრის განხორციელება კიბეროპერაციისას სწორად შერჩეული სამიზნეებით მარტივი იქნება. სწორედ ამიტომ, მსოფლიოს წამყვანმა სახელმწიფოებმა უკვე განსაზღვრეს თავიანთი კრიტიკული ინფრასტრუქტურის სია, ისეთი სისტემების, ნაგებობების თუ დაწესებულებების ჩამონათვალი, რომელთა ფუნქციონირების შეწყვეტა/შეჩერება არსებით ზიანს მიაყენებს სახელმწიფოს.

წარმოდგენილი ნაშრომი არა მხოლოდ საქართველოში, არამედ საერთაშორისო მასშტაბითაც იმ მცირე აკადემიურ ნაშრომთაგანია, რომელიც ცდილობს გამოიკვლიოს საერთაშორისო სამართალში ამჟამად ფორმირებადი ახალი მიმართულება. ნაშრომის მიგნებები პრაქტიკული მნიშვნელობისაა საქართველოსთვის, რომელიც უკვე ორჯერ გახდა კიბერშეტევების მსხვერპლი.

Abstract

With the development of the modern technologies, the necessity of reassessment of international law is becoming more evident. For the effective operation of modern international law, its static norms should be in a position to adequately regulate those technologies. There are no specialized norms to specifically address technological challenges.

What is the threshold for cyber operations? At what time may a mere normal cyber operation turn into a coercive act with serious effects? Can cyber operations amount to the armed attack? Answer to these questions consists of several elements, which are discussed to shed the light on these issues.

Nowadays it is much simpler by employing cyber force or threat of cyber force. Hence, all states find it more than necessary to have developed cyber security systems in order to be safe from any kind of political pressure.

The present dissertation aims to discuss the existing international legal regime applicable to cyber operations. Despite the absence of specific norms, cyber operations do not remain outside the international law. In this regard, the focus will be on the relationship between

cyber operations and the Charter of the United Nations, the prohibition of the use of force, and the principle of non-intervention. Also, the method of evolutionary interpretation of the treaties will be surveyed.

By illegal cyber operations states often violate the cyber space of other states. Examples of such interventions are 2007 cyber-attack against Estonia, against Iran's nuclear power plant in 2010 and against the Georgian cyber space during the 2008 Russian-Georgian armed conflict and in October 2019. With the increase of cyber-attacks, search for mechanism of self-defence from these attacks becomes essential. To this end, correlation between cyber-attacks and article 51 of the Charter of the United Nations will be explored.

The existence of physical damage as the effect of cyber operation has great importance. It is relatively easy to enforce existing norms as damage caused by cyber operation is easily equal to the damage of armed attack. Identical outcome with significantly less financial loss is attractive for every aggressor. All this will be possible by choosing right targets for their cyber operations. That is why powerful states have already defined the list of their critical infrastructure.

The present dissertation is one of few academic works not only in Georgia, but also internationally, which seeks to explore new direction currently emerging in international law. The findings of the paper is of significant practical importance for Georgia, who has already been the victim of cyberattacks on two occasions.

The research outcomes of this paper is produced by using dogmatic and normative research methods, which are traditional for jurisprudence, including historic, analytical, systematic, logical and comparative research methods. Besides, particular importance is assigned to forecasting method. The paper analyzes official positions of the states and based on comparative analysis offers new conclusions to the reader. Finally, through the evaluation method, the validity of the findings in relation to the subject of the research is evaluated.

სარჩევი

აბრევიატურებისა და უცხოენოვანი ტერმინების ნუსხა

A fortiori		მით უმეტეს
De facto		ფაქტობრივად
De jure		სამართლებრივად
ECtHR	European Court of Human Rights	ადამიანის უფლებათა ევროპული სასამართლო
ed(s)	editor(s)	რედაქტორ(ებ)ი
edn	Edition	გამოცემა
et al.	et alia	და სხვები
ICJ	International Court of Justice	მართლმსაჯულების საერთაშორისო სასამართლო
ICRC	International Committee of the Red Cross	წითელი ჯვრის საერთაშორისო კომიტეტი
ICTY	International Criminal Tribunal for the former Yugoslavia	სისხლის სამართლის საერთაშორისო ტრიბუნალი ყოფილი იუგოსლავიისთვის
Inter alia		მათ შორის
International Atomic Energy Agency		საერთაშორისო ატომური ენერგიის სააგენტო
ipso facto		თავად ფაქტიდან გამომდინარე
Jus ad bellum		ძალის გამოყენების სამართალი
jus cogens		სამართლის ნორმა, რომლისგან გადახვევაც კი დაუშვებელია
Jus contra bellum		ძალის გამოყენების აკრძალვის სამართალი
Jus in bello		საერთაშორისო ჰუმანიტარული სამართალი
lex ferenda		სამართალი მომავალში

NATO	North Atlantic Treaty Organization	ჩრდილო ატლანტიკური ხელშეკრულების ორგანიზაცია
No	Number	ნომერი
Obiter dictum		სასამართლოს მიგნება, რომელიც აუცილებელი არ არის განსახილველი საქმის გადაწყვეტისთვის
opinio juris		სამართლებრივი რწმენა
PCIJ	Permanent Court of International Justice	საერთაშორისო მართლმსაჯულების მუდმივმოქმედი სასამართლო
per se		თავისთავად
ratione materiae		მატერიალური შინაარსი
UN	United Nations	გაერთიანებული ერების ორგანიზაცია (გაერო)
UNGA	United Nations General Assembly	გაეროს გენერალური ასამბლეა
UNSC	United Nations Security Council	გაეროს უშიშროების საბჭო
UNTS	United Nations Treaty Series	გაეროს ხელშეკრულებათა სერია
v.	*Versus*	წინააღმდეგ
აშშ		ამერიკის შეერთებული შტატები
იხ.		იხილეთ
მაგ.		მაგალითად
შეად.		შეადარეთ

შესავალი

თანამედროვე ეპოქაში სულ უფრო დიდ მნიშვნელობას იძენს ტექნოლოგიების განვითარება. ამის პარალელურად, შედარებით სტატიკურად იცვლება ის ნორმები, რომლებიც არეგულირებს აღნიშნული ტექნოლოგიებით გამოწვეულ შედეგებს. გასული საუკუნის მიწურულიდან დაიწყო აქტიური დებატები, რომელთა თანახმად, კიბეროპერაციები გარკვეულ ჩარჩოებში უნდა მოქცეულიყო. ამერიკის შეერთებულ შტატებში 11 სექტემბერს მომხდარმა ტერაქტმა გააჩინა შიში, რომ მომავალში შესაძლოა მომხდარიყო კიბერტერორიზმის ზრდა და განვითარება. სახელმწიფოები ხშირად არღვევენ სხვა ქვეყნების კიბერსივრცეს და ვინაიდან ამ დროისთვის არ არსებობს სპეციალური ნორმები, ინტენსიურად კნინდება საერთაშორისო სამართლის როლი. მაგალითად, 2007 წელს ტალინში განხორციელდა მასობრივი კიბერშეტევა, რომელმაც ქვეყნის საბანკო სისტემა დააზარალა. 2010 წელს კომპიუტერულმა ვირუსმა პრობლემები შეუქმნა ირანის ბირთვულ ქარხანას. 2008 წელს კი, რუსეთ-საქართველოს შეიარაღებული კონფლიქტის დროს, ქართული კიბერსივრცე დაზარალდა ჰაკერული შეტევების შედეგად. ძალის გამოყენების თვალსაზრისით, ეს იყო კიბერშეტევის ყველაზე აშკარა მაგალითი: რუსეთის მიერ საქართველოს წინააღმდეგ განხორციელებულ აგრესიას, ყველაფერთან ერთად, თან დაერთო კიბერშეტევათა უპრეცედენტო მასშტაბი. საქართველო იმ მხრივაც გამოირჩევა, რომ მსოფლიოში განხორციელებული რამდენიმე კიბერშეტევიდან ორი მის წინააღმდეგ განხორციელდა. ერთი უკვე ზემონახსენები, 2008 წელს, ხოლო მეორე - 2019 წლის 28 ოქტომბერს. აღნიშნული კიბერშეტევების ფონზე, სახელმწიფოებს სჭირდებათ მყარი სამართლებრივი მექანიზმების შემუშავება, ისეთი ვერაგი მტრისგან დასაცავად და რეაგირებისთვის, როგორებიცაა კიბეროპერაციები.

1. საკვლევი პრობლემა

კაცობრიობა უფრო და უფრო ეჯაჭვება თანამედროვე ტექნოლოგიებს, რომელთა განვითარებასთან ერთად თავს იჩენს ახალი, აქამდე არარსებული საფრთხეებიც. ჯერ კიდევ 30 წლის წინ უცნობი იყო თავად სიტყვა - „კიბერ“, თუმცა დღეს ყველამ იცის

მისი მნიშვნელობა. ტექნოლოგიების განვითარებასთან ერთად მიმდინარეობს ყველა სფეროს მოდერნიზაცია და კიბერნეტიზაცია. იქნება ეს თავდაცვა, შეიარაღება, განათლება, სამართალწარმოება თუ სხვა. თუმცა, ახალი კიბერგამოწვევების ფონზე, საერთაშორისო სამართალში არ შეინიშნება საპასუხო სამართლებრივი სიახლეები. აქედან გამომდინარე, იბადება კითხვა - რატომ ხდება ასე. მიზეზი შეიძლება იყოს როგორც საერთაშორისო სამართლის შენელებული ტემპი და ერთგვარი ჩამორჩენა, ტექნოლოგიურ პროგრესთან შედარებით, ასევე ოპტიმისტური ვარაუდი იმის თაობაზე, რომ არსებული სამართლებრივი ჩარჩო ვრცელდება თანამედროვე კიბერსივრცეზე. ნაშრომის საკვლევი პრობლემაა ძალის გამოყენების თანამედროვე საერთაშორისო სამართლის მიმართება კიბეროპერაციებთან და იმის გარკვევა, თუ რამდენად არეგულირებს არსებული სამართლებრივი ჩარჩო ამ უკანასკნელს და საკმარისია თუ არა, ამჟამად შემუშავებული სამართლებრივი რეგულაციები.

2. კვლევის მნიშვნელობა

წინამდებარე ნაშრომი იკვლევს საკითხს, რომელიც ქართულ სამეცნიერო სივრცეში ჯერჯერობით შეუსწავლელია. საერთაშორისო დონეზეც კი მწირია ავტორთა პუბლიკაციები, რომლებშიც ფოკუსირებულად იკვლევენ კიბეროპერაციებს, ძალის გამოყენების აკრძალვის კონტექსტში. ამდენად, კიბეროპერაციები მომავლის თემაა, რომელსაც მეტ-ნაკლებად ვაწყდებით ჩვენს რეალობაში, რასაც ნაშრომში წარმოდგენილი ფაქტობრივი მაგალითებიც ამტკიცებს. ტექნოლოგიების განვითარებასთან ერთად კიბეროპერაციების რეგულირება, პრევენცია, მათგან თავის დაცვა, სამართლებრივ ჩარჩოში მოქცევა დროდადრო უფრო გაძნელდება. ამიტომ მნიშვნელოვანია, რომ ამ უკანასკნელის განვითარების საწყის ეტაპებიდანვე ვიცოდეთ მისი ადგილი საერთაშორისო სამართლის სისტემაში და გვესმოდეს, როგორ ხდება მისი რეგულაცია. სამართლებრივ კვლევასთან ერთად, ნაშრომში გაანალიზებულია მსოფლიოს წამყვანი სახელმწიფოების მიდგომები და პრაქტიკა კიბეროპერაციებთან მიმართებით. აღნიშნული ანალიზი გვიჩვენებს ერთიან სურათს, რამდენად რეალურ საფრთხედ აღიქვამენ სახელმწიფოები კიბეროპერაციებს/კიბერშეტევებს და რა მიმართებით უნდა გაძლიერდეს ესა თუ ის სახელმწიფო, რათა შეძლოს

კიბეროპერაციის შედეგებისგან ეფექტიანად თავის დაცვა. საქართველოს შემთხვევაში, ეს ყოველივე სასიცოცხლოდ მნიშვნელოვანია, თუ გავითვალისწინებთ იმ ფაქტს, რომ მსოფლიოს ოთხი ყველაზე ფართომასშტაბიანი კიბერშეტევიდან ორი საქართველოს წინააღმდეგ განხორციელდა.

3. კვლევის მიზანი

წარმოდგენილი სადისერტაციო ნაშრომის კვლევის მიზანია კიბეროპერაციები, როგორც ახალი გამოწვევა ძალის გამოყენების აკრძალვის საერთაშორისო სამართლის დონეზე. ნაშრომის ამოცანაა, გამოკვლეულ და შესწავლილ იქნეს ის სამართლებრივი რეჟიმი, რომელიც ამჟამად ვრცელდება კიბეროპერაციებსა და მის სხვადასხვა ფორმაზე. ძალის გამოყენების აკრძალვა საკმაოდ ფართო საკითხია, რომელიც აქამდე საზოგადოებისთვის ცნობილი იყო მისი კონვენციური გაგებით. ნაშრომი კი იკვლევს ძალის გამოყენების აკრძალვის ფენომენს კიბერსამყაროში - იქნება ეს კიბერძალის აკრძალვა, კიბერძალის მუქარის აკრძალვა, კიბერსაფრთხეები თუ სხვა. კვლევის მიზანია, ზემოხსენებულ სახელმწიფოთა პრაქტიკის ანალიზის მეშვეობით, განსაზღვროს კიბერსივრცეში აქტუალური სფეროები და მიმართებები.

ნაშრომი ასევე დეტალურად მიმოიხილავს კიბეროპერაციის ძალის გამოყენებად და შეიარაღებულ თავდასხმად დაკვალიფიცირების საკითხებს. რა კრიტერიუმები უნდა დააკმაყოფილოს კიბეროპერაციებმა აღნიშნული კვალიფიკაციების მისაღებად და რამდენად ხშირი და რეალურია მსგავსი შემთხვევები. გარდა ამისა, ნაშრომის ფარგლებში და, განსაკუთრებით დასკვნით ნაწილში, წარმოდგენილი იქნება ავტორისეული ხედვა, რეკომენდაციები და მიგნებები კიბეროპერაციებისა და ძალის გამოყენების სხვადასხვა ასპექტის ურთიერთმიმართების თაობაზე.

4. კვლევის მეთოდოლოგია და გამოყენებული წყაროები

საკვლევი თემის დამუშავებისას გამოყენებულია იურიდიული მეცნიერებისთვის ტრადიციულ-დოგმატური და ნორმატიული მეთოდები. ნაშრომში წარმოდგენილი

არგუმენტაცია განვითარებულია ჰიპოთეზის წამოყენების, დამუშავებისა და შემოწმების მეთოდით, რომელიც სხვადასხვა ხარისხით იყენებს ნორმატიულ, ისტორიულ, ანალიტიკურ, სისტემურ, ლოგიკურ და შედარებით მეთოდს, რათა კომპლექსურად გაანალიზდეს არსებული საერთაშორისო სამართალი ისეთ ახალ ფენომენთან მიმართებით, როგორებიც კიბეროპერაციებია. შესაბამისი ადგილი ეთმობა პროგნოზირების მეთოდსაც. ნაშრომი სამართლებრივად და ემპირიულად აანალიზებს სახელმწიფოთა ოფიციალურ პოზიციებს და, შედარებითი ანალიზის საფუძველზე, დედუქციისა და ინდუქციის მეთოდების გამოყენებით, მკითხველს სთავაზობს ახალ დასკვნებს. საბოლოოდ, შეფასების მეთოდის საშუალებით წარმოდგენილია ნაშრომის კვლევისას გაკეთებული მიგნებების მართებულობა.

ნაშრომში გამოყენებულია საკვლევი თემის გარშემო არსებული უახლესი უცხოენოვანი აკადემიური ლიტერატურა (წიგნები, მონოგრაფიები, კრებულები, სტატიები), რომელთა ძირითადი ნაწილი მოპოვებულია ელექტრონული რესურსის სახით. გარდა ამისა, წყაროების მნიშვნელოვანი წილი მოდის მართლმსაჯულების საერთაშორისო სასამართლოს მიერ განხილულ საქმეებსა და საერთაშორისო ორგანიზაციების დოკუმენტებზე. ასევე, გამოყენებულია საკვლევი თემის გარშემო, ინტერნეტის მეშვეობით მოპოვებული სტატიები და სახელმწიფოთა ოფიციალურ წარმომადგენელთა განცხადებები.

5. კვლევის ფარგლები

კვლევა ეხება კიბეროპერაციებს - მხოლოდ *jus ad bellum* კონტექსტში. პარალელები საერთაშორისო ჰუმანიტარული სამართლიდან გამოყენებულ იქნება მხოლოდ იმ ფარგლებში, რაც საჭიროა კვლევის მთავარ შეკითხვებზე პასუხის გასაცემად. ასევე, შედარებითი ანალიზისთვის, ნაშრომში შეფასებულია შიდა საქმეების ჩაურევლობის პრინციპის მიმართება კიბეროპერაციებთან.

6. ნაშრომის სტრუქტურა

ნაშრომი შედგება შესავლის, ძირითადი ნაწილისა და დასკვნისგან.

ძირითადი ნაწილი მოიცავს შვიდ თავს:

1. პირველი თავი ეხება კიბერშეტევებს ძალის გამოყენების აკრძალვის კონტექსტში, რომელშიც საუბარია საერთაშორისო სამართლის ევოლუციურ ინტერპრეტაციასა და ამ უკანასკნელის მიერ კიბერშეტევების საკუთარ სამართლებრივ ჩარჩოში ინკორპორირებაზე. განხილულია საერთაშორისო ჩვეულებითი სამართლისა და ტალინის სახელმძღვანელო პრინციპების როლი კიბეროპერაციების სამართლებრივ რეგულირებაში. ასევე, დეტალურად არის წარმოდგენილი დღესდღეობით არსებული კიბერშეტევების კონკრეტული მაგალითები და ამერიკის შეერთებული შტატების, როგორც წამყვან კიბერშესაძლებლობათა მქონე სახელმწიფოს მიდგომა კიბერშეტევების მიმართ.
2. მეორე თავი ეხება კიბერშეტევების კორელაციას ძალის გამოყენების გამონაკლისებთან, კერძოდ კი, გაეროს ქარტიის 51-ე მუხლთან, რომელიც ითვალისწინებს თავდაცვის უფლებას და გაეროს ქარტიის VII თავთან, რომელიც გაეროს უშიშროების საბჭოს ანიჭებს ძალის გამოყენების ავტორიზაციის უფლებას. ამასთან, განხილულია კიბეროპერაციების მიმართება სახელმწიფოთა შიდა საქმეებში ჩაურევლობის პრინციპთან.
3. მესამე თავი ეხება კიბეროპერაციების ზღვარს და *jus contra bellum-ს,* ახსნილია, რას ნიშნავს კიბერძალა და რა შემთხვევაში შეიძლება ეწოდოს სახელმწიფოს ქმედებებს კიბერშეიარაღებული თავდასხმა. წარმოდგენილია ამჟამად არსებული მიდგომები, რომლებსაც მიმართავენ კიბეროპერაციების ძალის გამოყენებად დაკვალიფიცირებისთვის. ასევე, ყურადღება ეთმობა კრიტიკულ ინფრასტრუქტურას, კერძოდ, რას წარმოადგენს იგი და რატომ არის სახელმწიფოებისთვის მნიშვნელოვანი გამართული, დაცული, კრიტიკული ინფრასტრუქტურის არსებობა.
4. მეოთხე თავი ეთმობა იძულებითი ხასიათის კიბერაქტივობების განხორციელებასა და სახელმწიფოს განზრახვას ასეთ დროს. განხილულია, თუ რა შემთხვევაშია შესაძლებელი, სახელმწიფომ განახორციელოს კიბერშეტევა სხვა რომელიმე ქვეყანაზე ისე, რომ თავად არ ფლობდეს ამის შესახებ ინფორმაციას. ასევე, ყურადღება გამახვილებულია განხორციელებული კიბერაქტივობის გარემოებებსა და მნიშვნელობაზე, თუ რამდენად ბევრს წყვეტს

გარემო ფაქტორები კიბეროპერაციისთვის კვალიფიკაციის მინიჭებისას. ამავე თავში გამოკვეთილია კიბერაქტივობების გასაჯაროვების სირთულეები და მიზეზები, თუ რატომ შეიძლება არ აძლევდეს ხელს კიბერშეტევის მსხვერპლ სახელმწიფოს მომხდარის გასაჯაროვება.

5. მეხუთე თავში განმარტებულია, რას წარმოადგენს კიბერსაფრთხე და კიბერძალის გამოყენების საფრთხე. განხილულია ძალის გამოყენების მუქარის მახასიათებლები, კიბერძალის მუქარა, ძალის გამოყენების ღია მუქარა და ძალის დემონსტრირება კიბერსამყაროში. ასევე, ნაჩვენებია, რომ კიბერ შესაძლებლობათა განვითარება არ წარმოადგენს აკრძალული ძალის გამოყენების მუქარას. ასევე, აქამდე არსებული ფაქტობრივი მაგალითების გამოყენებით, განხილულია, როგორ მუშაობს ძალის გამოყენების მუქარის ელემენტი კიბერსივრცეში.
6. მეექვსე თავი ეთმობა კიბერშეიარაღებულ თავდასხმასა და კიბერაგრესიას. განხილულია, რა ურთიერთმიმართება გააჩნია ძალის, აგრესიისა და შეიარაღებული თავდასხმის ცნებებს. ასევე, ყურადღება გამახვილებულია კიბეროპერაციების ფიზიკური შედეგების არსებობა/არარსებობის საკითხსა და მის მნიშვნელობაზე. აღნიშნული თავი ასევე ეხება კიბეროპერაციების შეკრებითობის თეორიასა და კიბეროპერაციის შესაძლო ავტორებს. გამახვილებულია ყურადღება კრიტიკულ ინფრასტრუქტურაზე, როგორც კიბეროპერაციის სამიზნეზე.
7. ბოლო, მეშვიდე თავში გაანალიზებულია წამყვანი სახელმწიფოების მიდგომები და პრაქტიკა კიბეროპერაციებთან მიმართებით, ვინაიდან სწორედ სახელმწიფოთა პრაქტიკა ასახავს ყველაზე კარგად კიბეროპერაციების ადგილს თანამედროვე რეალობაში. აღნიშნულ თავში წარმოდგენილია სახელმწიფოთა ვალდებულებები კიბერსივრცეში. ყურადღება გამახვილებულია ისეთ ძირეულ მიმართულებებზე, როგორებიცაა: სუვერენიტეტი, შიდა საქმეებში ჩაურევლობა, ძალის გამოყენების აკრძალვა და თავდაცვის სფეროები. ამასთანავე, თითოეულ მიმართულებაზე განხილულია მიგნებები და რეკომენდაციები.

I. კიბეროპერაციები და გამოსაყენებელი საერთაშორისო სამართლის პრობლემა

1. შესავალი

წინამდებარე თავის მიზანია, გამოიკვლიოს არსებული საერთაშორისო სამართლებრივი ჩარჩო, რომელიც ვრცელდება კიბეროპერაციებზე. ამ მხრივ, ყურადღება გამახვილდება გაეროს ქარტიაზე და შეფასებულ იქნება გაეროს ქარტიის ევოლუციური ინტერპრეტაციის შესაძლებლობა, რათა პასუხი გაეცეს შეკითხვებს: 1) არსებობს თუ არა სპეციალიზებული ნორმები კიბერშეტევებთან მიმართებით? 2) არსებობს თუ არა საერთაშორისო ჩვეულებითი სამართალი, რომელიც ვრცელდება კიბერშეტევებზე?

ამ კითხვებზე პასუხის გასაცემად ნაშრომში მნიშვნელოვანი ყურადღება ეთმობა სახელმწიფოთა პრაქტიკასა და კონკრეტულ მაგალითებს, რათა უკეთ გაანალიზდეს ჩვეულებითი სამართალი, რომელიც ვრცელდება კიბერშეტევებზე.

2. გამოსაყენებელი სამართალი კიბერშეტევებთან დაკავშირებით

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

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

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

ჯერ კიდევ 2000-იანი წლებიდან, გაეროს გენერალურმა ასამბლეამ არაერთ რეზოლუციაში აღნიშნა, რომ თანამედროვე ტექნოლოგიების გამოყენების რეგულირება მთელი საერთაშორისო თანამეგობრობის ინტერესებს ეხება.[2] ასევე ისიც, რომ მათ დანაშაულებრივ გამოყენებას 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 კიბეროპერაციები“ მზარდ ტრანსნაციონალურ საფრთხედ“ მოიხსენიეს.[6] იმავე წლის ნოემბერში ნატომ განაცხადა, რომ კიბერშეტევებმა შესაძლოა, რიგ შემთხვევაში, 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. სავარაუდოდ, წარუმატებლობის მიზეზად იქცა პოლიტიკური ნების ნაკლებობა. ინიციატორ სახელმწიფოთა ჩამონათვალიდან ირკვევა, რომ აღნიშნული

[2] იხ. მაგალითად: 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; 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.

რეზოლუციის პროექტი შემუშავებულ იქნა რუსეთის ფედერაციისა და მის მხარდამჭერ სახელმწიფოთა მიერ. პროექტი მიუღებელი აღმოჩნდა აშშ-ისა და რიგი დასავლური სახელწიფოებისთვის. შედეგად, კენჭისყრაზე რეზოლუციის მიღებას ნაკლები მომხრე აღმოაჩნდა, ვიდრე მოწინააღმდეგე და, შესაბამისად, პროექტიც ჩავარდა.

აღნიშნულის თანახმად, შესაძლებელია ითქვას, რომ საერთაშორისო საზოგადოება ბევრად მეტ ყურადღებას აქცევს კიბეროპერაციების საკითხს და არც ისე შორსაა ის დღე, როცა შემუშავდება უნივერსალური და სპეციალური, მბოჭავი ძალის დოკუმენტი. ამ მიმართებით, რეგიონულ დონეზე, შეინიშნება კიდეც გარკვეული მცდელობები, მაგალითად - ევროპის საბჭოს კონვენცია კიბერდანაშაულის შესახებ.[9] ასევე, 2001 წელს დაკარის სამიტზე მიიღეს ალჟირის კონვენციის დამატებითი ოქმი ტერორიზმთან ბრძოლისა და პრევენციის შესახებ, აფრიკის კავშირის ეგიდით. აღნიშნული ოქმი ეხება კიბერშეტევებსაც.[10] მიუხედავად ამისა, დღეს სპეციალური და სამართლებრივად მბოჭავი სახის დოკუმენტი, კიბეროპერაციებთან დაკავშირებით, არ არსებობს.

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

კიბერსფეროში სპეციალური სახელშეკრულებო ნორმების არარსებობა ლოგიკურად აჩენს შემდეგ შეკითხვას – მოიცავს თუ არა არსებული საერთაშორისო სამართლებრივი რეჟიმი კიბეროპერაციებსაც? დღეს 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 მოქმედებს ყველა ის შეზღუდვა, რაც ნებისმიერ

[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.

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 პასუხის გაცემა არსებითად მნიშვნელოვანია წინამდებარე კვლევისთვის, წინააღმდეგ შემთხვევაში, ყოველგვარი შემდგომი მსჯელობა საფუძველსმოკლებული იქნება.

საერთაშორისო სახელშეკრულებო სამართალში ხშირად დგება ამა თუ იმ ხელშეკრულების ევოლუციური ინტერპრეტაციის საკითხი. ვინაიდან ზოგჯერ ხელშეკრულება აღარ პასუხობს მოცემული მომენტისთვის არსებულ გამოწვევებს, მათ შორის, ტექნოლოგიური წინსვლის გამო. ხელშეკრულებათა შეცვლა ან სულაც ანულირება და ახლით ჩანაცვლება, ძალიან დიდ სიძნელეებსა და გაჭიანურებულ პროცედურებთან არის დაკავშირებული. ასეთ დროს, განსაკუთრებული ყურადღება ექცევა არსებული ხელშეკრულების განმარტების საკითხს, რაც სამეცნიერო წრეებში ევოლუციურ ინტერპრეტაციად არის ცნობილი.[13] სასამართლომ *ნაოსნობის უფლებების* საქმეში აღნიშნა - მხარეები შეთანხმების დროს აცნობიერებდნენ გარემოებას, რომ, დროთა განმავლობაში, ხელშეკრულების გაგება განიცდიდა ევოლუციას და ვინაიდან ის განუსაზღვრელი ვადით იქნა დადებული, იძლეოდა იმის პრეზუმფციას, რომ ხელშეკრულების პირობებს ჰქონდა ევოლუციური ხასიათი.[14] მნიშვნელოვანია, რომ ევოლუციურ განმარტებას, სასამართლოს გარდა, აქტიურად იყენებს ადამიანის უფლებათა ევროპული სასამართლოც, რომელმაც არაერთ საქმეში

[11] დაწვრილებით იხ., *Scmitt, M. N.,* Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, 84, 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. იხ., ასევე *Bjorge, E.*, The Evolutionary Interpretation of Treaties, Oxford University Press, 2014, 1-22.

აღნიშნა, რომ კონვენცია არის „ცოცხალი დოკუმენტი, რომელიც უნდა განიმარტოს თანამედროვეობის ჭრილში“.[15]

ამრიგად, საერთაშორისო სამართლის კოდიფიცირება/განვითარებაში უმნიშვნელოვანეს როლს ასრულებს საერთაშორისო ხელშეკრულებათა ევოლუციური განმარტება. ამგვარი განმარტებისას განსაკუთრებით მნიშვნელოვანია სასამართლოს როლი. მართალია, უშუალოდ კიბეროპერაციებთან დაკავშირებით ჯერჯერობით არ არსებობს გაეროს მართლმსაჯულების საერთაშორისო სასამართლოს ან სხვა საერთაშორისო სასამართლოს 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, არსებობს 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“.[16] ჩვეულებითი სამართალი, რომელიც, ძირითადად,

[15] იხ. მაგალითად: *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.

[16] მართლმსაჯულების საერთაშორისო სასამართლოს სტატუტი, მუხლი 38.

დაუწერელი ფორმით არსებობს,[17] 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".[18]

პირველ რიგში, პასუხი უნდა გაეცეს შეკითხვას - არსებობს თუ არა კიბერსპეციფიკური[19] ნორმები საერთაშორისო ჩვეულებით სამართალში? ამ მხრივ, საინტერესოა ტალინის სახელმძღვანელო პრინციპების შესავალი, რომელშიც აღნიშნულია - „იმის გამო, რომ სახელმწიფოთა კიბერპრაქტიკა და *opinio juris* არაერთგვაროვანია, ზოგიერთ შემთხვევაში, რთულია იმის დასკვნა, რომ საერთაშორისო ჩვეულებით სამართალში არსებობს რაიმე კიბერსპეციალური ნორმა".[20]

მიუხედავად ამისა, არ იქნება მართებული, დავასკვნათ, რომ რადგან 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. სამხედრო სახელმძღვანელოების მნიშვნელოვანი როლი ამა თუ იმ ნორმის ჩვეულებითი ხასიათის განსაზღვრისთვის, ასევე, აღიარა ყოფილი იუგოსლავიის სისხლის

---

[17] ცხადია, არსებობს მრავალი კონვენცია, რომელიც ასახავს ჩვეულებით სამართალს ან თავად არის ქცეული ჩვეულებითი სამართლის ნაწილად. მაგალითად, ვენის კონვენცია საერთაშორისო ხელშეკრულებების შესახებ, ასევე ჰააგის 1907 კონვენციები და ჟენევის 1949 წლის ოთხი კონვენცია.

[18] *North Sea Continental Shelf* (Germany v. Denmark and 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.

[19] ინგლისურად "Cyber-specific".

[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, 2013, 89, 280.

სამართლის ტრიბუნალმა *Tadic*-ის საქმეში.[23] მართალია, ამგვარ დოკუმენტთა რაოდენობა ჯერ არ არის შთამბეჭდავი, თუმცა, ჩვეულებითი ნორმის ჩამოყალიბება არ ითხოვს აბსოლუტურად ყველა სახელმწიფოს მხრივ 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] შესაბამისად, სახელმწიფოთა მხრივ, კონკრეტულ საკითხზე დუმილი ან მისი არგაპროტესტება წარმოადგენს თანხმობას. საილუსტრაციოდ, შეგვიძლია მოვიყვანოთ იმ ქვეყნებისა და საერთაშორისო ორგანიზაციების ჩამონათვალი, რომლებიც აღიარებენ კიბერშეტევებს, როგორც თავდაცვის უფლების გამოყენების წინაპირობას. ესენია: აშშ, ჩინეთი, ავსტრალია,[25] კუბა,[26] უნგრეთი, იტალია, ირანი, მალი,[27] ნიდერლანდები, ყატარი,[28] რუსეთის ფედერაცია, გაერთიანებული სამეფო და ევროკავშირი.[29] აღსანიშნავია, რომ ჯერჯერობით არ არსებობს რაიმე სახის წინააღმდეგობა, რომელიც ხელს შეუშლიდა კიბერშეტევის, როგორც ძალის გამოყენების აკრძალვის ან კიბერშეტევის საპასუხოდ თავდაცვის უფლების ამოქმედების ჩვეულებით ნორმად ჩამოყალიბებას.

ამრიგად, აშკარაა სახელმწიფოთა მზარდი პრაქტიკა, რომლის მიხედვითაც სულ უფრო მეტი სახელმწიფო ასახავს კიბეროპერაციებს საკუთარ სამხედრო სახელმძღვანელოებში. რაც შეეხება ჩვეულებითი სამართლის მეორე ელემენტს, მართალია, *opinion juris*-ის სრულყოფილად არსებობა არ დასტურდება, თუმცა, სახელმწიფოთა მხრივ არ გაპროტესტება გვიბიძგებს, ვიფიქროთ, რომ დუმილით გამოიხატება ერთგვარი თანხმობა, რამაც შესაძლოა, უბიძგოს კიბერ საერთაშორისო

[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] Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, UNGA A/66/152, 15 July 2011, 6.

[26] Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, Addendum, UNGA A/57/166/Add.1, 29 August 2002, 3.

[27] Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, Addendum, UNGA A/64/129/Add.1, 9 September 2009, 7.

[28] Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, Addendum, UNGA A/65/154, 20 July 2010, 9-10.

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

ჩვეულებითი სამართლის ჩამოყალიბებასაც. ამ ყველაფერში შესაძლოა, განსაკუთრებული როლი შეასრულოს „რბილმა სამართალმაც“, რომლის შესახებაც შემდგომ ქვეთავში ვიმსჯელებთ. აქედან გამომდინარე, შეიძლება ითქვას, 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,[30] ნატომ ჩამოაყალიბა კოოპერაციული კიბერთავდაცვის უპირატესი ცენტრი. 2009 წელს ნატომ მოიწვია საერთაშორისო სამართლის 20 გამორჩეული მეცნიერი, რათა შემუშავებულიყო ის სახელმძღვანელო პრინციპები, რომლებიც, არსებული საერთაშორისო სამართლის მიხედვით, გამოიყენებოდა კიბეროპერაციებისას, როგორც *jus ad bellum*, ისე *jus in bello*-ს შემთხვევებში. შედეგად, შემუშავდა „ტალინის სახელმძღვანელო პრინციპები კიბერბრძოლისას გამოსაყენებელი საერთაშორისო სამართლის შესახებ“.

ტალინის სახელმძღვანელო პრინციპები ერთადერთი სპეციალური, კოდიფიცირებული დოკუმენტია კიბერბრძოლასთან დაკავშირებით და აუცილებელია მისი ბუნების განსაზღვრა. კერძოდ, არის ის მხოლოდ 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.[31] რბილი სამართალი, უპირველესად, ასოცირდება საერთაშორისო სამთავრობათაშორის ორგანიზაციებსა და მათ მიერ

[30] იხ. ქვეთავი 3.1.

[31] *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.

მიღებულ გადაწყვეტილებათა იურიდიულ ძალასთან (როგორც წესი არასავალდებულო ხასიათის). თავის მხრივ, რბილი სამართალი შეგვიძლია, დავყოთ შემდეგ სახეებად: საერთაშორისო ორგანიზაციათა არასავალდებულო ხასიათის დოკუმენტები, სახელმწიფოთა შორის არსებული მბოჭავი ძალის არმქონე შეთანხმებები[32] და სავალდებულო სახელმწიფოთაშორის შეთანხმებათა (მაგალითად, საერთაშორისო ხელშეკრულებათა) არასავალდებულო ნაწილები.[33]

რბილ სამართალს ხშირად განიხილავენ *lex ferenda*-ს ჭრილში, ერთგვარ მიმართებად, რომლითაც უნდა განვითარდეს საერთაშორისო სამართალი.[34] რბილ სამართალს ახასიათებს გარკვეული თავისებურებაც. კერძოდ, ის შეიძლება განხილულ იქნეს საერთაშორისო სამართლის ტრადიციული წყაროების გამყარების საშუალებად.[35] ამ მხრივ, განსაკუთრებით საინტერესოა მიმართება საერთაშორისო ჩვეულებით სამართალთან. მაგალითად, საერთაშორისო გარემოს დაცვით სამართალსა და ფინანსურ საერთაშორისო ორგანიზაციებში რბილ სამართალს გადამწყვეტი როლი ენიჭება, როგორც *de facto* მბოჭავ ეფექტს[36] და, ამავდროულად, ხელს უწყობს ჩვეულებითი ნორმის დაჩქარებულ ჩამოყალიბებას. რბილი სამართლის არსებობა და მისი მხედველობაში მიღების სავალდებულოობა ირიბად აღიარა კიდეც სასამართლომ *ნავთობის პლატფორმების* საქმეში. კერძოდ, ირანმა სასამართლოს იურისდიქცია დააფუძნა 1955 წელს ირანსა და აშშ-ს შორის გაფორმებულ ორმხრივ შეთანხმებაზე,[37] რომლის 21-ე მუხლი აღიარებს სასამართლოს იურისდიქციას შეთანხმებასთან დაკავშირებული დავის შემთხვევაში. ამავე შეთანხმების პირველი მუხლი ადგენს, რომ მხარეებს შორის უნდა იყოს „მტკიცე და განგრძობადი მშვიდობა და გულწრფელი მეგობრობა“. სასამართლომ დაადგინა, რომ შეთანხმების პირველი მუხლი არ იყო კონკრეტული ვალდებულებების წარმომშობი.[38] მიუხედავად ამისა,

---

[32] მაგალითად, ჰელსინკის 1975 წლის დასკვნითი აქტი, თავისი ბუნებით, რბილი სამართალია, Final Act, Conference On Security and Co-Operation in Europe, 1975.

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

[34] *Thirlway, H.*, The Sources of International Law, Oxford University Press, 2014, 165.

[35] *იქვე.*

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

[37] The Treaty of Amity, Economic Relations and Consular Rights between the United States and Iran (ხელმოწერის თარიღი: 15.08.1955; ძალაში შესვლის თარიღი: 16.06.1957).

[38] *Oil Platforms case (Iran v. USA)*, ICJ, Preliminary Objection, 12 December 1996, §52.

სასამართლომ ჩათვალა, რომ პირველი მუხლი ადგენდა შეთანხმების მიზანს, ამიტომ სხვა დებულებები უნდა განმარტებულიყო ამ მუხლის ჭრილში.[39] ერთ-ერთი შეფასების თანახმად, სასამართლომ გამოიყენა ნორმა, რომელიც იყო რბილი სამართლის ნაწილით.[40]

აღნიშნულ მსჯელობას გადამწყვეტი მნიშვნელობა აქვს ტალინის სახელმძღვანელო პრინციპების სამართლებრივი ბუნების დადგენისთვის. ერთი შეხედვით, ეს დოკუმენტი საყოველთაოდ აღიარებულ მეცნიერთა ნაშრომია, თუმცა, ხაზგასასმელია ის ფაქტი, რომ ის შედგენილი და ჩამოყალიბებულია ნორმატიული ენით. ამასთან, აღსანიშნავია, რომ შემუშავდა ნატოს ეგიდით, რომელიც, თავის მხრივ, წარმოადგენს საერთაშორისო [სახელმწიფოთაშორის] ორგანიზაციას და, ამდენად, გვევლინება საერთაშორისო სამართლის სრულფასოვან სუბიექტად. აშკარაა, ტალინის სახელმძღვანელო პრინციპები მეტია, ვიდრე უბრალოდ მეცნიერთა ნაშრომი. ყოველ შემთხვევაში, ის, სულ ცოტა, განხილულ უნდა იქნეს საერთაშორისო სამართლის დამხმარე წყაროდ და განთავსდეს იმ წყაროთა ჩამონათვალში, რომელსაც გვთავაზობს სასამართლოს სტატუტის 38-ე მუხლი. აქვე, აღსანიშნავია, რომ მეცნიერთა ერთი ნაწილის თვალთახედვით, საერთაშორისო სამართლის წყაროებს შორის არ არსებობს ფორმალური იერარქია.[41] ამას გარდა, ტალინის სახელმძღვანელო პრინციპები შეიძლება ჩაითვალოს რბილი სამართლის ნაწილადაც, რომელიც, შესაძლოა, წარმოადგენს ამ მიმართებით ჩვეულებითი სამართლის ჩამოყალიბების წინარე სტადიასაც. აღნიშნულ მოსაზრებას ამყარებს არსებული საერთაშორისო სამართლებრივი პრაქტიკა. მაგალითად, სან რემოს სახელმძღვანელო პრინციპები, ზღვაში შეიარაღებულ კონფლიქტთან დაკავშირებით[42], შემუშავებულია წითელი ჯვრის საერთაშორისო კომიტეტის მიერ, როგორც რბილი სამართლის ნაწილი, თუმცა,

[39] იქვე.
[40] *Thirlway, H.*, The Sources of International Law, Oxford University Press, 2019, 190, სქოლიო 106.
[41] დაწვრილებით იხ., *Thirlway, H.,* The Sources of International Law, Oxford University Press, 2014 117-128.
[42] 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].

დღეს აქტიურად გამოიყენება სახელმწიფოთა მიერ და ჩვეულებითი სამართლის ხასიათი აქვს.[43] ამავე კატეგორიაში შეიძლება მოვიაზროთ სხვა დოკუმენტებიც.[44]

2.5. ტალინის სახელმძღვანელო პრინციპებით დადგენილი ფაქტორები

ტალინის სახელმძღვანელო პრინციპების შემუშავებაში ჩართულნი იყვნენ კიბერ საკითხებზე მომუშავე სამართლის აღიარებული მეცნიერები და სამართლის პრაქტიკოსები. მათ მეთაურობდა მაიკლ შმიტი, შემადგენლობა კი დაკომპლექტებული იყო ევროპის, ჩრდილოეთ ამერიკისა და ავსტრალიის წამყვანი უნივერსიტეტებისა და კოლეჯების პროფესორების მიერ. ისინი წარმოადგენენ ნატოს ეგიდით ჩამოყალიბებულ ექსპერტთა საერთაშორისო ჯგუფს. მათი მიზანი კიბეროპერაციებსა და კიბერომთან საერთაშორისო სამართლის მიმართების კვლევაა.

ექსპერტთა საერთაშორისო ჯგუფის თანახმად, კიბერშეტევათა ძალის გამოყენებად შეფასებისას, სახელმწიფოებმა უნდა გაითვალისწინონ შემდეგი ფაქტორები: სიმწვავე, იმწუთიერობა, პირდაპირობა, შემტევი ხასიათი, ეფექტების გაზომვადობა, სამხედრო ხასიათი, სახელმწიფოს ჩართულობა, ლეგალურობის პრეზუმფციის არარსებობა.[45]

ჩამოთვლილი ფაქტორებიდან, ყველაზე მნიშვნელოვანია სიმწვავე. ცხადია, კიბერშეტევა, რომელსაც ახლავს ფიზიკური ზიანი,[46] რაც შეიძლება გამოიხატოს ნგრევით ან სულაც ადამიანების სიკვდილით, წარმოადგენს ძალის გამოყენებას. იმ

---

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

[44] მაგალითად, დროთა განმავლობაში საერთაშორისო ჩვეულებითი სამართლის ამსახველ დოკუმენტებად იქცა საერთაშორისო ორგანიზაციების მიერ არასავალდებულო ფორმით მიღებული რეზოლუციები, როგორებიცაა: ადამიანის უფლებათა საყოველთაო დეკლარაცია (UNGA Res 217 A, 10 December 1948), დეკლარაცია საერთაშორისო სამართლის პრინციპების შესახებ (UNGA Res 2625 (XXV), 24 October 1970), რეზოლუცია აგრესიის დეფინიციის შესახებ (UNGA Res 3314 (XXIX), 14 December 1974). გარდა რეზოლუციებისა, უნდა აღინიშნოს მაღალი დონის შეხვედრებზე მიღებული არასავალდებულო ხასიათის შეთანხმებები, რომლებიც ხელს უწყობს ჩვეულებითი სამართლის წარმოქმნას. ასეთი დოკუმენტის ყველაზე ნათელი მაგალითია ე.წ. ჰელსინკის დასკვნითი აქტი (Final Act of the Helsinki Conference for Security and Cooperation in Europe, 1 August 1975).

[45] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 54-55.

[46] ფიზიკური ზიანი გულისხმობს ადამიანისთვის ან დაწესებულებისთვის/ნაგებობისთვის მიყენებულ ფიზიკურ დაზიანებას.

შემთხვევაში, თუ არ იკვეთება ამგვარი ფიზიკური ხასიათის ზიანი ან ზარალი,[47] კიბერშეტევა მაინც შეიძლება ჩაითვალოს ძალის გამოყენებად, მხოლოდ ამ დროს, მხედველობაში მიიღება შეტევის ფარგლები, ხანგრძლივობა, ინტენსივობა და ა.შ.[48] 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 აშკარაა, როცა მიყენებული ზარალის აღწერა ობიექტურად შესაძლებელია. ცალკე უნდა აღინიშნოს ლეგალურობის პრეზუმფციის ფაქტორი, რომელიც, წინა ფაქტორებისგან განსხვავებით, არ იკვეთება. როგორც წესი, ერთი სახელმწიფოს მიერ მეორისადმი ეკონომიკური ზეწოლის განხორციელება ექცევა ლეგალურობის პრეზუმფციის ფარგლებში, რაც ნიშნავს იმას, რომ არ არღვევს საერთაშორისო სამართლის ნორმებს. მსგავს შემთხვევაში, ქარტიის მე-2(4) მუხლზე საუბარიც კი ზედმეტია. რაც შეეხება სახელმწიფოს ჩართულობას, იგულისხმება, რომ კიბეროპერაციას უნდა ახორციელებდეს სახელმწიფო ან მასთან დაკავშირებული არასახელმწიფო აქტორი. და ბოლოს, მნიშვნელოვანი ფაქტორია ისიც, რომ კიბერშეტევა უნდა იყოს სამხედრო ხასიათის. თუმცა, ეს არ უნდა იქნეს აღქმული მხოლოდ სამხედრო ობიექტებზე თავდასხმად.[49]

აღსანიშნავია, რომ 2007 წელს ესტონეთზე განხორციელებული კიბერთავდასხმა შეიძლება შეფასდეს, როგორც ძალის გამოყენება, თუმცა, პრობლემას ის ქმნის, რომ ვერ ხერხდება კიბერშეტევის რუსეთიდან დაგეგმვის/ორგანიზების დამტკიცება.

[47] ზარალი გულისხმობს დაწესებულებისთვის/ნაგებობისთვის ფიზიკური ზიანის შედეგად მიყენებულ გაზომვად დანაკარგს.

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

[49] იქვე, 1115-1116.

3. კიბერშეტევების მაგალითები სახელმწიფოთა პრაქტიკაში

3.1. ესტონეთი 2007

2007 წლის გაზაფხულზე ესტონეთის მთავრობამ განაცხადა, რომ „რუსი ჯარისკაცის“ ქანდაკებას გადაიტანდა ახალ ლოკაციაზე, ტალინის ცენტრიდან - გარეუბანში. ამის მიზეზად დასახელდა ის, რომ ქანდაკება, რომელიც აღიმართა ნაცისტური გერმანიის წინააღმდეგ, მეორე მსოფლიო ომში დაღუპული საბჭოთა ჯარისკაცთა პატივსაცემად, დიდი ხნის განმავლობაში ასოცირდება უცხოური ოკუპაციის სიმბოლოსთან. აღნიშნულ განცხადებას უკმაყოფილება მოჰყვა ესტონეთში მცხოვრები რუსი მოსახლეობის მხრივ, რაც გადაიზარდა აქციებში. ძალადობრივ პროტესტს თან დაერთო სამთავრობო უწყებებისა და კერძო კომპანიების (ბანკები, მედია) წინააღმდეგ მიმართული კიბერშეტევები. განხორციელდა DDoS (Distributed Denial of Service) ტიპის შეტევები, რაც ნიშნავს, რომ ინტერნეტსაიტზე იგზავნება იმდენად ბევრი მოთხოვნა ინფორმაციის შესახებ, რომ ვებგვერდი ფუნქციონირებს ძალიან ნელა, ან საერთოდ წყვეტს მუშაობას. შედეგად - ლეგიტიმურ მომხმარებლებს ეზღუდებათ წვდომა საიტზე. თავდაპირველად, DDoS-ის აღმოჩენა და მასთან გამკლავება მარტივად შეეძლო კომპიუტერული დაცვის სისტემებს, თუმცა, დროთა განმავლობაში, იმდენად დაიხვეწა, რომ დღესდღეობით ძალიან რთულია მისი მიკვლევა და მასთან ბრძოლა.[50] ასევე გამოყენებულ იქნა ბოტნეტი. ბოტნეტი (Botnet) წარმოადგენს კომპიუტერთა ქსელს, რომელიც გამოიყენება მფლობელის ნებართვის გარეშე. ესტონეთის შემთხვევაში, მფლობელის ნებართვის გარეშე გამოიყენეს დაახლოებით 85 000 კომპიუტერი, რომლებიც ინტერნეტის საშუალებით აგზავნიდნენ მოთხოვნებს ინფორმაციის შესახებ, ესტონეთის სამთავრობო უწყებების საიტებზე. ესტონურმა საიტებმა მსგავს ნაკადს ვერ გაუძლო და გაითიშა.[51] კიბერშეტევები გაგრძელდა დაახლოებით სამი კვირის განმავლობაში (26 აპრილი – 19 მაისი).

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

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

მიუხედავად იმისა, რომ არ დამტკიცდა რუსეთის მხარის პირდაპირი კავშირი კიბერშეტევებთან, ესტონეთის მთავრობა მაინც რუსეთს მიიჩნევს აღნიშნულ შეტევებზე პასუხისმგებლად,[52] რასაც კატეგორიულად უარყოფდნენ რუსეთის ფედერაციის წარმომადგენლები.

შეკითხვა, რომელიც დაისვა როგორც მედიაში, ასევე აკადემიურ წრეებში, იყო შემდეგი: განხორციელებული ტიპის კიბერშეტევა (კონკრეტულად DDoS) ჩაითვლება თუ არა ძალის არამართლზომიერ გამოყენებად? შეიძლება ითქვას, რომ აღნიშნულმა კიბერშეტევებმა მნიშვნელოვანი ზიანი მიაყენა ესტონეთს. ესტონეთის პარლამენტის სპიკერმა 2007 წლის მაისში განხორციელებული შეტევები შეადარა ბირთვული იარაღის გამოყენების შედეგებს და განაცხადა, რომ კიბერშეტევები არ იწვევს სისხლისღვრას, მაგრამ შეუძლია გაანადგუროს ყველა და ყველაფერი.[53]

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

2008 წელი, რუსეთის მიერ საქართველოს მიმართ განხორციელებული სამხედრო ინტერვენციისა და აგრესიის გარდა, აღსანიშნავია ასევე კიბერშეტევის არნახული მასშტაბით, რომელიც რუსეთის ფედერაციამ განახორციელა საქართველოს როგორც საჯარო, ასევე კერძო სივრცეში.

შეტევების პირველი ტალღის (20 ივლისი, 7 აგვისტო) შედეგად გაითიშა სამთავრობო საიტები, შეიცვალა არსებული ინფორმაცია ცრუ შეტყობინებებით. ვრცელდებოდა უამრავი დეზინფორმაცია, რომლის მიზანიც მოსახლეობაში შიშის

[52] 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].

[53] *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].

გაჩენა იყო.[54] საქართველოს მთავრობამ განაცხადა კიდეც, რომ რუსეთი აწარმოებდა კიბერომს.[55]

შეტევების მეორე ტალღა (8-12 აგვისტო) ეხებოდა სამოქალაქო და კერძო საიტების ბლოკირებას. გარკვეული დროის განმავლობაში, მთელი ქვეყნის მასშტაბით, შეუძლებელი იყო წვდომა ინტერნეტთან, რაც მოსახლეობაში ზრდიდა პანიკას და უსუსურობის განცდას.

საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისიის 2009 წლის ანგარიშში („ტალიავინის დასკვნა“) არსებობს შემდეგი ჩანაწერი: „თუ ეს შეტევები მართული იყო მთავრობის ან მთავრობების მიერ, ამ სახის ბრძოლა პირველად იქნა გამოყენებული სახელმწიფოთაშორის შეიარაღებულ კონფლიქტში“.[56]

კიბერშეტევების შესახებ გავრცელებული ინფორმაცია 2008 წლის აგვისტოს რუსეთ-საქართველოს კონფლიქტის ერთ-ერთი განსაკუთრებული მახასიათებელია.[57] აშკარაა, რომ კიბერშეტევები საქართველოს წინააღმდეგ განხორციელდა კონფლიქტის დროს. რუსული აგრესიის პირველ დღეებში საქართველოს მთავრობისა და საინფორმაციო საიტების უმრავლესობა მიუწვდომელი ან დაზიანებული იყო. მოგვიანებით, რამდენიმე ვებგვერდი გადაიყვანეს ამერიკულ, ესტონურ და პოლონურ სერვერებზე.[58] ექსპერტთა ნაწილის აზრით, ამ შეტევებს შეეძლო, შეესუსტებინა საქართველოს მიერ გადაწყვეტილების მიღების უნარი ისევე, როგორც კომუნიკაცია მოკავშირეებთან, რაც, სავარაუდოდ, შეამცირებდა ქართული ძალების ოპერატიულ მოქნილობას. ყველაზე საყურადღებო ქმედებები, რამაც გავლენა იქონია სახელმწიფოს

---

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

[55] *Jon Swaine,* “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].

[56] Report of the Independent Fact-Finding Mission on the Conflict in Georgia, September 2009, Vol. II, 217–219. „ტალიავინის ანგარიშში“ რუსეთის მიერ საქართველოს წინააღმდეგ ძალის გამოყენების თვალსაზრისით მიკვლეული მიგნებების სამართლებრივი ანალიზისთვის იხ., *ალექსიძე, ლ.* საქართველოში კონფლიქტთან დაკავშირებული ფაქტების დამდგენი საერთაშორისო დამოუკიდებელი მისიის მოხსენების საერთაშორისო სამართლებრივი ასპექტები. საერთაშორისო სამართლის ჟურნალი, N2, 2009, N1, 2010, 2010, 5-14.

[57] *Korns, S., W., Kastenberg J., E.,* ‘Georgia's Cyber Left Hook’, Small Wars Journal §meter, 2008-2009 Winter Edition.

[58] მაგ. პოლონური სერვერი www.president.pl.

მდგრადობაზე და რა დროსაც რუსეთის ფედერაცია შეიჭრა საქართველოს სუვერენულ უფლებებში, იყო შემდეგი:[59]

- 20 ივლისს სახელმწიფოს პრეზიდენტის ვებგვერდი 24 საათის განმავლობაში გათიშული იყო;
- 7 აგვისტოს რამდენიმე ქართული სერვერი და ინტერნეტტრაფიკი დაკავებული იყო და ექვემდებარებოდა გარე კონტროლს;
- 8 აგვისტოს დაიწყო ფართომასშტაბიანი კიბერშეტევები საქართველოს საიტების წინააღმდეგ. კიბერშეტევების წყაროები დაუდგენელი იყო. ზოგიერთ მოხსენებაში მათ მიაწერდნენ ორგანიზაციას, სახელად - „Russian Business Network“[60] (რუსეთის ბიზნესქსელი);
- გავრცელდა ცნობა, რომ საქართველოს მთავრობის ყველა ვებგვერდი მიუწვდომელი იყო ამერიკის, დიდი ბრიტანეთისა და ევროპის ინტერნეტ სივრცეებიდან. ამავე ინფორმაციით, 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, რომლებზეც განხორციელდა ვირტუალური შეტევები, იყო შინაგან საქმეთა სამინისტროს, თავდაცვის სამინისტროსა და სანაკოევის პროქართული სამხრეთ ოსეთის დროებითი ადმინისტრაციის ვებგვერდი. ამის გარდა, გავრცელებული ცნობით, დაზიანებული იყო საქართველოს ეროვნული ბანკის ვებგვერდი და საქართველოს ახალი ამბების პორტალები, DDoS (distributed denial of service) - შეტევებით;

[59] *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].

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

- 12 აგვისტოსთვის საქართველოს პრეზიდენტისა და პოპულარული ქართული სატელევიზიო მაუწყებლის, „რუსთავი 2“-ის 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.

მაღალია იმის ალბათობა, რომ ქართული მხარის წინააღმდეგ განხორციელებული კიბერშეტევები იმართებოდა რუსეთის ხელისუფლის მიერ. ასეთ შემთხვევაში, შესაძლებელია თქმა, რომ სახელმწიფოთა შეიარაღებულ კონფლიქტში პირველად მიმართეს კიბერშეტევების, როგორც ომის წარმოების ფორმის გამოყენებას. შესაბამისი რესურსის არსებობის შემთხვევაში, მარტივია მსგავსი შეტევების განხორციელება და საკმაოდ რთული 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, რომლებსაც იწვევს კონკრეტული თავდასხმა. ტალიავინის დასკვნაში გამოთქმული ვარაუდი, რომ კიბეროპერაციები საქართველოს წინააღმდეგ რუსეთის მიერ იყო მართული, ბევრ რამეს ჰფენს ნათელს.

აშკარაა, ინტერნეტის სრული ბლოკირება, დეზინფორმაციის გავრცელება და მოსახლეობაში პანიკის მიზანმიმართული დათესვა სხვა არაფერია, თუ არა სახელმწიფოში არეულობის მოწყობა და წესრიგის დაცვის შესაძლებლობის მოსპობა. ეს ყოველივე კი უშუალო სასიცოცხლო რისკს უქმნიდა ასიათასობით ადამიანს, რომელთა სახლები ყოველდღე რუსული თვითმფრინავების მიერ იბომბებოდა. გორის გადაკეტვამ გამოიწვია აღმოსავლეთ და დასავლეთ საქართველოს დამაკავშირებელი ცენტრალური მაგისტრალის პარალიზება. ამის ფონზე, რუსული კიბერშეტევების შედეგად მნიშვნელოვნად შეფერხდა ადამიანებს შორის თითქმის ყველანაირი სახის კომუნიკაცია. კომუნიკაციის შეფერხებას განსაკუთრებული მნიშვნელობა ენიჭება, როდესაც საქმე ეხება სახელმწიფოს ინსტიტუტებს შორის კომუნიკაციის მოსპობას და ამ გზით თავდაცვის შესაძლებლობების შესუსტებას. მართლაც, ამგვარი ზიანი მსოფლიოში განხორციელებული კიბეროპერაციების შემთხვევებს შორის უპრეცედენტოა. მეტიც, თვით ესტონეთზე განხორციელებული 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 აგრესიისა და ძალის არამართლზომიერი გამოყენების კიდევ ერთ შემთხვევას. შეიარაღებული თავდასხმის პარალელურად და წინსწრებით განხორციელებული კიბერშეტევები მიმართული იყოს საქართველოს თავდაცვის შესაძლებლობების შესუსტებისა და მოსახლეობაში პანიკის დათესვისკენ. ამასთან, წინსწრებით განხორციელებული კიბერშეტევები შეგვიძლია, მივიჩნიოთ ძალის გამოყენების მუქარად, რომელიც განხორციელდა კიბერძალის დემონსტრირების გზით.

3.3. ირანი 2010

2010 წლის ივლისში ირანის მთავრობამ აღმოაჩინა მათ კუთვნილ კომპიუტერებზე დაინსტალირებული ვირუსი, რომელიც შემდეგ ცნობილი გახდა სახელით - Stuxnet. ვირუსმა ირანის სხვადასხვა კომპიუტერულ სისტემაში შეაღწია. მისი ეპიცენტრი ნატანზის (Natanz) ბირთვული სადგური იყო.

ნატანზი ირანის მოწინავე ბირთვული სადგურია და გამოიყენება ურანის გამდიდრებისთვის. ირანის მთავრობა აცხადებდა, რომ მათი ბირთვული პროგრამის მიზნები მშვიდობიანი, კონკრეტულად კი - ატომური ელექტროენერგიის წარმოებაა. თუმცა, საერთაშორისო თანამეგობრობა ეჭვობდა, რომ ბირთვული მასალა გამოყენებული იქნებოდა მასობრივი განადგურების იარაღის შესაქმნელად.[61]

როგორც ცნობილია, ურანის გამდიდრებისთვის საჭიროა პირობების ზედმიწევნით დაცვა. პირველ რიგში, ურანი უნდა იყოს სუფთა, მინარევების გარეშე, რის შემდეგაც იგი თავსდება ცენტრიფუგებში და, შესაბამისი ტემპერატურისა და წნევის პირობებში, ტრიალებს ზუსტად განსაზღვრული სიჩქარით.

[61] United Nations Security Council (UNSC) Resolution 1696, 31 July 2006.

Stuxnet ვირუსის მოქმედებით ცენტრიფუგების სიჩქარე ერთდროულად მკვეთრად იზრდებოდა და მცირდებოდა. ტექნოლოგიები არ მიუთითებდა გაუმართავ მუშაობაზე და, მონაცემთა მიხედვით, პროცესი მიმდინარეობდა გეგმის მიხედვით.[62]

ირანის მთავრობამ არ გაახმაურა კონკრეტული დეტალები, თუ რა სახის გავლენა მოახდინა Stuxnet ვირუსმა. ირანის ატომური ენერგიის ორგანიზაციის იმდროინდელმა მმართველმა განაცხადა, რომ ვირუსი დროულად აღმოჩნდა, ვიდრე შეაღწევდა მოწყობილობებში.[63] განსხვავებული მოსაზრება გამოთქვა ირანის პრეზიდენტმა, რომელმაც აღნიშნა, რომ ვირუსმა პრობლემები შეუქმნა რამდენიმე ცენტრიფუგის ფუნქციონირებასა და ელექტრონულ მოწყობილობებზე არსებული პროგრამული უზრუნველყოფის გამართულ მუშაობას.[64]

სხვა ანგარიშების თანახმად, ვირუსის მიერ მიყენებული ზიანი ბევრად ფართო მასშტაბის იყო, ვიდრე ამას ასახელებდნენ ირანის მთავრობის წარმომადგენლები. მეცნიერებისა და საერთაშორისო უსაფრთხოების ინსტიტუტის განცხადებით,[65] ვირუსის მოქმედებას შეეძლო, დაეზიანებინა არა მხოლოდ გასამდიდრებელი ურანი, არამედ თავად ცენტრიფუგებიც. საერთაშორისო ატომური ენერგიის სააგენტოს მიერ მიწოდებული მტკიცებულების თანახმად, ირანმა 2009 წლის ბოლოსა და 2010 წლის დასაწყისში ნატანზის (Natanz) ბირთვულ სადგურში გამოცვალა დაახლოებით 1 000 ცენტრიფუგა. აღნიშნული ცვლილებების ლოგიკური ახსნა იქნებოდა სწორედ ვირუსი Stuxnet.[66]

იმის გათვალისწინებით, რომ ქარტიის 2(4) მუხლი ემხრობა შედეგზე დამყარებულ აკრძალვას, ირანზე განხორციელებული შეტევის ძალის არაკანონიერ გამოყენებად შეფასება რთულია, ვინაიდან შეტევის განმავლობაში არ მომხდარა ვირუსის იდენტიფიცირება და გამოვლენა. ირანის პრეზიდენტის განცხადების თანახმად, ვირუსის შეტევამ გამოიწვია ცენტრიფუგების გაუმართავი ფუნქციონირება და ვერ

---

[62] *Shakarian, P.*, Stuxnet: Cyberwar Revolution in Military Affairs. Small Wars Journal, 2011, 7, 1.

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

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

[65] *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].

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

მოხერხდა ურანის გამდიდრება. ამდენად, აღნიშნული კიბერშეტევა ვერ ჩაითვლება ძალის არაკანონიერ გამოყენებად, რადგან არ დაზიანებულა მატერიალური საკუთრება.[67] თუმცა, მეტ-ნაკლებად სანდო წყაროების ინფორმაციით, ვირუსმა პირდაპირ გამოიწვია ფიზიკური ზიანი ცენტრიფუგების განადგურებით.[68] ლოგიკურია, რომ ირანს არ სურდა მომხდარი ფაქტის გასაჯაროვება და ცდილობდა მაქსიმალურად მცირე დეტალების გახმაურებას. აქედან გამომდინარე, შეგვიძლია ვივარაუდოთ, რომ ირანის წარმომადგენელთა საჯარო განცხადებები არ ასახავდა სრულ რეალობას.

არადა, სავსებით რეალურია, ყოფილიყო სწორედ ზემოხსენებული კიბერშეტევა.

მატერიალური ზიანის დადგომის შემთხვევაში, შედარებით ადვილია ირანზე განხორციელებული შეტევის სახით გაეროს ქარტიის 2(4) მუხლის დარღვევა, რადგან დაკმაყოფილებულია ფაქტობრივი შედეგის არსებობის წინაპირობა. ძალის გამოყენების საერთაშორისო სამართლებრივი კონტექსტისთვის კი, საინტერესოა მხოლოდ რეალურად განხორციელებული კიბეროპერაცია, რომელსაც შედეგად მოჰყვა ფიზიკური ზიანი.

3.4. აშშ-ის მიდგომა კიბერშეტევების მიმართ

კიბერშეტევებით განსაკუთრებით დიდი ზიანის მიყენების პოტენციურ მაგალითად გამოდგება აშშ-ის მიდგომის განხილვა, რომელიც, სამხედრო სისტემების თვალსაზრისით, დიდწილადაა დამოკიდებული საინფორმაციო სისტემებზე.[69] როგორც პრეზიდენტ ობამას დროს მიღებული 2010 წლის „ეროვნული უსაფრთხოების სტრატეგია“ ცხადყოფს:

> „ზუსტად ის ტექნოლოგიები, რომლებიც გვაძლიერებს, რათა ვიყოთ მოწინავეები და შემოქმედები, ასევე აძლიერებს მათ, ვინც

[67] *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].

[68] *Stiennon R.* A Short History of Cyber Warfare, Cyber Warfare: A Multidisciplinary Analysis, *Green J.A.*,(ed), Routledge, 2015, 22.

[69] *Sharp W. G. Sr.*, The Past, Present, and Future of Cybersecurity. Journal of National Security Law & Policy, 2010, 4, 13. <http://jnslp.com/wp-content/uploads/2010/08/03_Sharp.pdf> [30.06.2020].

> მოგვაყენებდა ზიანს და გაგვანადგურებდა. ეს ტექნოლოგიები გვაძლევს სამხედრო უპირატესობის საშუალებას და... ჩვენი ყოველდღიური ცხოვრება და საჯარო წესრიგი დამოკიდებულია ელექტრონულ სისტემებზე. თუმცა, პოტენციურ მოწინააღმდეგეებს შეუძლიათ, გამოიყენონ კიბერსისუსტეები, რათა ზიანი მოგვაყენონ მასიური მასშტაბით.“

კიბერსივრცეში მასშტაბური ზიანის მიყენების ასეთი შესაძლებლობა ბადებს კითხვას, გავრცელდება თუ არა ასეთ ოპერაციებზე გაეროს ქარტიის აკრძალვები იმის გათვალისწინებით, რომ ქარტიის შეზღუდვები ჩამოყალიბდა კონვენციური ომის მახასიათებლების გათვალისწინებით.

დომინანტური შეხედულების მიხედვით, 2(4)-ე მუხლის აკრძალვები და 51-ე მუხლის ფარგლები ეხება მხოლოდ შეიარაღებულ ძალას ან სამხედრო თავდასხმებს,[70] მაგრამ, თუ ამოვალთ 2(4)-ე მუხლის მიზნებიდან და ზოგადი არსიდან, ცხადია, ის კრძალავს ქმედებას, რომელიც, სულ ცოტა, მოიცავს „ძალადობისა“ და „იძულების“ ელემენტებს. ასეთ განმარტებას ავითარებს აშშ-ის მთავრობა.

კერძოდ, აშშ-ის ხელისუფლებას საჯაროდ არ გამოუთქვამს პოზიცია გაეროს ქარტიისა და კიბერშეტევების ურთიერთმიმართებაზე. თუმცა, უდავოა, რომ შიდა დონეზე აშშ იხრება 2(4)-ე მუხლის ფართო განმარტებისკენ და ცდილობს, დაასაბუთოს, რომ კიბერშეტევა, რომელიც გამოიწვევს სამხედრო ძალის გამოყენების ტოლფას ზიანს, უნდა მოექცეს 2(4)-ე მუხლში. მაგალითად, კვლევის ეროვნულმა საბჭომ (The National Research Council) მოიწვია სპეციალური კომიტეტი, რომელსაც უნდა შეესწავლა კიბერშეტევები. საბოლოო დასკვნის სახით კომიტეტმა განაცხადა, რომ კიბერშეტევები უნდა შეფასდეს გაეროს ქარტიისა და ძალის გამოყენების სამართლის ჩვეულებითი პრინციპების მიხედვით და იმის გათვალისწინებით, უტოლდება თუ არა კიბერშეტევები სამხედრო შეტევებს.[71] მაიკლ შმიტი მიუთითებს, რომ კიბერშეტევის ძალის გამოყენებად შეფასება დამოკიდებულია სხვადასხვა

---

[70] *Waxman, M. C.*, Cyber Attacks as Force under UN Charter Article 2(4), International Law and the Changing Character of War: Part III: The Changing Character of the Battlefield: The Use of Force in Cyberspace, 2011, 45. <http://unstudies.ir/static/fckimages/files/vol-87_III_waxman_cyberattacks.pdf> [30.06.2020].

[71] *National Research Council's Committee on Offensive Information Warfare's.*, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. The National Academies Press, 2009, 33-34. <http://www.steptoe.com/assets/attachments/3785.pdf> [30.06.2020].

ფაქტორზე, რომლებიც, თავის მხრივ, ახასიათებს სამხედრო თავდასხმებს. მათ შორისაა - სიმწვავე, იმწუთიერობა, შეტევის პირდაპირი ხასიათი, მასშტაბურობა, შეტევის გაზომვადობა და ა.შ.[72] მსგავსი კრიტერიუმები გვხვდება სამართლის სხვა ექსპერტების მოსაზრებებშიც.[73] იდენტური დასკვნები გამოაქვთ აშშ-ის სამხედრო ექსპერტებს, აშშ-ის თავდაცვის დოქტრინის ფარგლებში არსებული კიბერშეტევების მიმართ: კიბერშეტევები შეიძლება, განხილულ იქნეს ფიზიკურ ძალად, რომელიც იძლევა ასეთივე ძალით რეაგირების საშულებას [ე.წ. კიბერეკვივალენტურობის მიდგომა].[74]

კიბერეკვივალენტურობის მიდგომის მხარდაჭერა შეიმჩნევა აშშ-ის მთავრობის მაღალი თანამდებობის პირთა განცხადებებშიც. მაგალითად, 1999 წელს თავდაცვის დეპარტამენტის გენერალური მრჩევლის ოფისის (Defense Department's Office of the General Counsel) მიერ მომზადებული ანგარიშის თანახმად:

> *„თუ ყურადღებას გავამახვილებთ გამოყენებულ საშუალებებზე, შეიძლება, დავასკვნათ, რომ ადამიანის მიერ არააღქმადი ელექტრონული სიგნალები საერთოდ არ ჰგავს ბომბებს, ტყვიებს ან სამხედრო ძალებს. მეორე მხრივ, ლოგიკურია, რომ საერთაშორისო საზოგადოებას უფრო მეტად დააინტერესებს კომპიუტერულ ქსელებზე შეტევების შედეგები, ვიდრე მისი მექანიზმები.“*[75]

ანგარიში უფრო შორს წავიდა და კიბერშეტევები მოიაზრა თავდაცვის უფლების განხორციელების წინაპირობადაც,[76] ანუ შესაძლებლად მიიჩნია მათი შეფასება, როგორც „შეიარაღებულ თავდასხმად“.

2010 წელს სახელმწიფო მდივანმა, ჰილარი კლინტონმა, განაცხადა, რომ აშშ კიბერუსაფრთხოებას დაიცავდა ისევე, როგორც სამხედრო უსაფრთხოებას:

---

[72] *Schmitt, M. N.,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 37, 1999, 914-15. [HeinOnline], <http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/cjtl37&div=39&id=&page=> [30.06.2020].

[73] *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, Computer Network Attack and International Law, *Schmitt, M. N., O'Donnell, B. T (eds.)*, US Naval War College, 76, 2002, 92, <https://archive.org/details/computernetworka76nava> [30.06.2020].

[74] *Clarke, R. A., Knake, R. K.,* Cyber War: The Next Threat to National Security and What to Do about It, Harper Collins, 2010, 178.

[75] *Schmitt, M. N., O'Donnell, B. T (eds.),* Computer Network Attack and International Law, US Naval War College, 2002, 76, 459, 483: <https://archive.org/details/computernetworka76nava> [30.06.2020].

[76] *იქვე.*

„სახელმწიფოებმა, ტერორისტებმა... უნდა იცოდნენ, რომ შეერთებული შტატები დაიცავს საკუთარ ქსელებს... ქვეყნები ან კერძო პირები, რომლებიც ჩაერთვებიან კიბერშეტევებში, აღმოჩნდებიან საერთაშორისო დაგმობის წინაშე. ურთიერთდაკავშირებულ მსოფლიოში ერთი სახელმწიფოს ქსელებზე თავდასხმა შეიძლება იყოს თავდასხმა თითოეულ მათგანზე.“[77]

სენატის წინაშე გამოსვლისას, პენტაგონის კიბერმეთაურობის უფროსმა, ლეიტენანტ-გენერალმა, კით ალექსანდერმა განმარტა: „არ არსებობს კიბერსივრცეში ან მის მიღმა ძალის გამოყენების საერთაშორისო ერთმნიშვნელოვანი დეფინიცია. შესაბამისად, კონკრეტულმა სახელმწიფოებმა შეიძლება, ამტკიცონ სხვადასხვა დეფინიცია და გამოიყენონ სხვადასხვა სტანდარტი, თუ რა წარმოადგენს ძალის გამოყენება.“[78] თუმცა, მოგვიანებით, განაცხადა: „თუ პრეზიდენტი ჩათვლის, რომ კიბერშემთხვევა ვერ აკმაყოფილებს ძალის გამოყენების/შეიარაღებული თავდასხმის სტანდარტს, მას შეუძლია, მიიჩნიოს, რომ ასეთი ქმედება არის ისეთი მასშტაბის, ხანგრძლივობის ან ინტენსივობის, რომ ამართლებს თავდაცვის უფლების განხორციელებას ან/და საბრძოლო მოქმედებების დაწყებას, როგორც სათანადო რეაგირებას.“[79] აქედან შეგვიძლია, დავასკვნათ, რომ „ძალის“ ცნება, გარკვეულწილად, დამოკიდებულია ქმედებათა ეფექტსა და შედეგებზე.

აშშ-ის მთავრობა მიანიშნებს „ეფექტებზე დაფუძნებულ“ ან „შედეგებზე დაფუძნებულ“ მიდგომაზე, რომლის ფარგლებშიც მოხდება „ძალის“ ან „შეიარაღებული თავდასხმის“ ინტერპრეტაცია, კიბერშეტევების კონტექსტში. ამგვარი მიდგომა, გარკვეულწილად, სასარგებლოა, რადგან კომპიუტერულ სისტემებზე დაფუძნებული ჯაშუშობა, სადაზვერვო ინფორმაციის შეგროვება ან პრევენციული კიბეროპერაციები, მოწინააღმდეგის საინფორმაციო სისტემების წყობიდან გამოყვანის

---

[77] Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom at the Newseum, Washington, D.C., 21 January 2010.

[78] Responses by Lieutenant General Keith Alexander, Nominee for Commander, United States Cyber Command to Senate Armed Services Committee Advance Questions, 15 April 2010, 11. ციტირებული: *Waxman M. C.*, Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 36, 2011, 421.

[79] *იქვე*, 12.

მიზნით, არ ჩაითვლებოდა ძალის გამოყენებად და მით უფრო შეიარაღებულ თავდასხმად (არც კიბერეკვივალენტურობის მიდგომის თანახმად), რადგან ასეთი მოქმედებები ვერ გამოიწვევს პირდაპირ და უშუალო გამანადგურებელ შედეგებს, სამხედრო ოპერაციების მსგავსად.[80]

3.5. 2019 წლის 28 ოქტომბრის კიბერშეტევა საქართველოზე

2019 წლის 28 ოქტომბერს ფართომასშტაბიანი კიბერშეტევა განხორციელდა ქართული ვებსაიტებისა და სერვერების წინააღმდეგ. აღნიშნული კიბერშეტევის სამიზნეს წარმოადგენდა სამთავრობო უწყებების, სასამართლოების, მუნიციპალური დაწესებულებების, კერძო სექტორისა და მედიის ვებგვერდები და სერვერები. კიბერშეტევის შედეგად არსებითად დაზიანდა სამიზნეთა სერვერები და შეფერხდა მათი ფუნქციონირება. შეტევის განხორციელებისას ჯერ კიდევ უცნობი იყო მისი წარმოშობა.

კიბერშეტევიდან ოთხი თვის თავზე, 2020 წლის 20 თებერვალს, ქართულმა მხარემ, განხორციელებული გამოძიების საფუძველზე, ოფიციალურად განაცხადა, რომ კიბერშეტევა დაგეგმილი და განხორციელებული იყო რუსეთის სამხედრო დაზვერვის სამსახურის, იმავე „გრუ-ს“ მიერ.[81] ამასთან, დიდი ბრიტანეთის გაერთიანებული სამეფოს ეროვნულმა კიბერუსაფრთხოების ცენტრმა საქართველოზე განხორციელებულ თავდასხმაზე პასუხისმგებლად „გრუ“ დაასახელა.[82] რუსეთი, რა თქმა უნდა, უარყოფს აღნიშნულ კიბერშეტევასთან კავშირს და აცხადებს, რომ საქართველოსა და დიდი ბრიტანეთის გაერთიანებული სამეფოს პოზიციები პოლიტიკურად მოტივირებული, უსაფუძვლო ბრალდებებია და ემყარება მხოლოდ ვარაუდებს.[83]

---

[80] National Research Council's Committee on Offensive Information Warfare's, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. The National Academies Press, 2009, 259-261. <http://www.steptoe.com/assets/attachments/3785.pdf> [30.06.2020].

[81] <https://twitter.com/MFAgovge/status/1230479514431631363> [15.07.2020].

[82] UK condemns Russia's GRU over Georgia cyber-attacks (20 February 2020), <https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks> [30.05.2020].

[83] Comment by the Information and Press Department on accusations against Russia of carrying out large-scale cyberattacks on Georgian websites <https://www.mid.ru/ru/foreign_policy/news/-

საქართველოს პოზიცია გაიზიარა არაერთმა სახელმწიფომ და საერთაშორისო ორგანიზაციამ, მათ შორის: ამერიკის შეერთებულმა შტატებმა,[84] დიდმა ბრიტანეთმა,[85] ავსტრალიამ,[86] უკრაინამ,[87] მონტენეგრომ,[88] ავსტრიამ,[89] ნიდერლანდებმა,[90] პოლონეთმა,[91] ლატვიამ,[92] ლიეტუვამ,[93] ესტონეთმა,[94] დანიამ,[95] შვედეთმა,[96] ნორვეგიამ,[97] ჩეხეთმა,[98] რუმინეთმა,[99] ისლანდიამ,[100] სუამმა[101], ევროკავშირმა.[102]

/asset_publisher/cKNonkJE02Bw/content/id/4050783?p_p_id=101_INSTANCE_cKNonkJE02Bw&_101_INSTANCE_cKNonkJE02Bw_languageId=en_GB> [15.07.2020].

[84] The United States Condemns Russian Cyber Attack Against the Country of Georgia (February 20, 2020), <https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/?fbclid=IwAR0RICJwF5Um_djH3cxZPbPXaoQ8i4Sfy56BARRXgy8eSFYyaS2rwh28dqU> [15.07.2020].

[85] UK condemns Russia's GRU over Georgia cyber-attacks (20 February 2020), <https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks> [30.05.2020].

[86] Attribution of malicious cyber activity in Georgia by Russian Military Intelligence <https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-malicious-cyber-activity-georgia-russian-military-intelligence?fbclid=IwAR30-b2Ei4r0x3lGOaVM9IWIz1Sj8i_LJKrPMeZAAQPThmv3XdrKvW_h5s8> [15.07.2020].

[87] Коментар МЗС України щодо кібератак, вчинених Російською Федерацією проти Грузії <https://mfa.gov.ua/news/komentar-mzs-ukrayini-shchodo-kiberatak-vchinenih-rosijskoyu-federaciyeyu-proti-gruziyi> [15.07.2020].

[88] <https://twitter.com/MFA_MNE/status/1230534482081525762> [15.07.2020].

[89] <https://twitter.com/MFA_Austria/status/1230880949610721280> [15.07.2020].

[90] The Netherlands considers Russia's GRU responsible for cyber attacks against Georgia (20-02-2020) <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia?fbclid=IwAR0gmhX1vWkbss7KMe6Id7tFjuKTRVBpl4nbt60rZgTyQZ4jILS3A31_PTg> [15.07.2020].

[91] Statement of the Polish MFA on cyberattacks against Georgia (20.02.2020) <https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia> [15.07.2020].

[92] Latvia condemns cyber-attack against Georgia (21.02.2020) <https://www.mfa.gov.lv/en/news/latest-news/65504-latvia-condemns-cyber-attack-against-georgia> [15.07.2020].

[93] <https://twitter.com/LT_MFA_Stratcom/status/1230485445798219777> [15.07.2020].

[94] Statement of the Foreign Minister of the Republic of Estonia Urmas Reinsalu (20 February 2020) <https://vm.ee/en/news/statement-foreign-minister-republic-estonia-urmas-reinsalu> [15.07.2020].

[95] <https://twitter.com/DanishMFA/status/1230483524123320322> [15.07.2020].

[96] <https://twitter.com/AnnLinde/status/1230496401873887233> [15.07.2020].

[97] <https://twitter.com/NorwayMFA/status/1230487577502855169> [15.07.2020].

[98] <https://twitter.com/CzechMFA/status/1230491060150964230> [15.07.2020].

[99]<http://mae.ro/node/51739?fbclid=IwAR1xakYudOR6D4OU4GVL7Fz6SHTESyKmHvYXGUemRAKez1WDWnygUBHKhmk> [15.07.2020].

[100] <https://twitter.com/GudlaugurThor/status/1230527048906682369> [15.07.2020].

[101] <https://twitter.com/GUAMSecretariat/status/1230542765345398784> [15.07.2020].

[102] Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace (21.02.2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/?fbclid=IwAR1xbr-X62Nz_xjVpNXaAwFA0k-7h8wXhUCvIKmD51tNmAaTzgKbgnjihSQ> [15.07.2020].

საქართველოს მიმართ 2019 წლის 28 ოქტომბერს განხორციელებულმა კიბერშეტევამ მნიშვნელოვანი სიახლე წარმოაჩინა სახელმწიფოთა მიდგომაში, უმრავლესობამ კიბერშეტევის კანონიერება შეაფასა არა საერთაშორისო სამართლის, არამედ „კიბერსივრცეში პასუხისმგებლიანი სახელმწიფოს ქცევის“ კონტექსტში.[103] რას წარმოადგენს „პასუხისმგებლიანი სახელმწიფოს ქცევა კიბერსივრცეში“? წესების ეს ჩარჩო არ განსაზღვრავს კიბერსივრცეში არსებული ვალდებულებების იძულებით აღსრულების სპეციალურ მექანიზმს ან პროცედურებს.

„პასუხისმგებლიანი სახელმწიფოს ქცევა კიბერსივრცეში“ მხოლოდ იმეორებს საერთაშორისო სამართლით უკვე აღიარებულ სამართლებრივ ჭეშმარიტებას, რომ საერთაშორისო სამართლით არსებული სამართლებრივი ჩარჩო ვრცელდება კიბეროპერაციებზეც. პასუხი კითხვაზე - ვრცელდება თუ არა საერთაშორისო სამართალი კიბეროპერაციებზე, არ დგას დღის წესრიგში. საკითხავია, რა სახით, როგორ ვრცელდება საერთაშორისო სამართალი კიბეროპერაციებზე. კითხვაზე პასუხის გაცემას ართულებს ისიც, რომ, როდესაც კიბერშეტევა ხორციელდება სამოქალაქო ინფრასტრუქტურის ან მოსახლეობის წინააღმდეგ, მშვიდობიან დროს და არ ექცევა შეიარაღებული კონფლიქტის ფარგლებში, დაბალი ინტენსივობის გამო არ კვალიფიცირდება ძალის გამოყენებად ან მის მუქარად.

ბევრად მარტივია დემონსტრირება იმისა, რომ მსგავსი სახელმწიფოთაშორისი კიბერშეტევები არღვევს სახელმწიფოს სუვერენიტეტს, შიდა საქმეებში ჩაურევლობასა და ტერიტორიულ მთლიანობას, პოლიტიკურ დამოუკიდებლობას ან უბრალოდ შეუსაბამოა გაეროს ქარტიის მიზნებთან.

„პასუხისმგებლიანი სახელმწიფოს ქცევა კიბერსივრცეში“, თავის მხრივ, კონკრეტული სამართლებრივი რეჟიმის ჩამოყალიბებას ვერ ახერხებს, მაგრამ სახელმწიფოებისთვის ქმნის შესაძლებლობას, გამოიყენონ ერთიანი კონცეპტუალური და ტერმინოლოგიური ჩარჩო, კიბერშეტევებზე რეაგირებისას.

---

[103] *Nakashidze G.,* Cyberattack against Georgia and International Response: Emerging Normative Paradigm of 'Responsible State behavior in Cyberspace'?, EJIL: Talk!, 28 February 2020, <https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative§digm-of-responsible-state-behavior-in-cyberspace/> [15.07.2020].

4. დასკვნა

ტექნოლოგიების განვითარების კვალდაკვალ, სულ უფრო მეტად აქტუალურდება 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.

შეიმჩნევა ტენდენცია, რომ კიბერშეტევების რეგულირება განისაზღვროს სპეციალიზებული ნორმებით. ამის კარგი მაგალითია ტალინის სახელმძღვანელო პრინციპები, რომლებიც შემუშავდა ისეთი საერთაშორისო ორგანიზაციის ეგიდით, როგორიცაა - ნატო, რაც, თავის მხრივ, ზრდის ამ დოკუმენტის სანდოობას. აღნიშნული დოკუმენტი, საყოველთაოდ აღიარებულ მეცნიერთა ნაშრომი, ჩამოყალიბებულია ნორმატიული ენით, რაც კიდევ უფრო ზრდის მის, როგორც რბილი სამართლის წყაროს, ავტორიტეტს.

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.

საქართველოს, ესტონეთისა და ირანის მაგალითებზე კარგად ჩანს, თუ რაოდენ დიდი დარტყმა შეიძლება მიადგეს სახელმწიფოს, 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 გადაიტანს რეაგირების მექანიზმებისა და სახელმწიფოთა პასუხისმგებლობის საკითხებზე. ამასთან, მოსალოდნელია, ასეთი ახალი დარგი ვერ აღმოჩნდეს უნივერსალური და მოხდეს დარგის ფრაგმენტაცია, საერთაშორისო სამართლის უკვე არსებული დარგების მიხედვით. მაგალითად, ცალკე განვითარდება

კიბერძალის გამოყენების საერთაშორისო სამართალი, რაც დიდწილად დაეფუძნება გაეროს ქარტიასა და აგრესიის საერთაშორისო სამართლებრივ ჩარჩოს. ასევე შესამჩნევია ტენდენცია - დიდი ყურადღება ეთმობა საერთაშორისო ჰუმანიტარული სამართლის კიბეროპერაციების კონტექსტში განვითარებას. ინდივიდის უფლებების დაცვის თვალსაზრისით, არსებობს ხელშესახები პრაქტიკა ადამიანის უფლებათა საერთაშორისო სამართალში. ამგვარი ტენდენცია მისასალმებელია იმდენად, რამდენადაც გაადვილდება XX საუკუნეში ჩამოყალიბებული საერთაშორისო სამართლის კონსერვატიული ნორმების ადაპტაცია XXI საუკუნის ტექნოლოგიურ სიახლეებთან.

II. კიბერშეტევების მიმართება ძალის გამოყენების გამონაკლისებთან: გაეროს ქარტიის 51-ე მუხლი და VII თავი

1. შესავალი

წინამდებარე თავი მიმოიხილავს კიბერშეტევების მიმართებას ძალის გამოყენების გაეროს ქარტიის მიხედვით გათვალისწინებულ ორ გამონაკლისთან - თავდაცვის უფლების განხორციელება და უშიშროების საბჭოს მიერ VII თავის ფარგლებში მოქმედება.

2. ითვალისწინებს თუ არა გაეროს ქარტია კიბერძალის გამოყენების აკრძალვას?

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

გაეროს ქარტიის მე-2(4) მუხლი,[104] *ნიკარაგუის გადაწყვეტილებაში,* სასამართლომ ქარტიის ქვაკუთხედად მოიხსენია.[105] აღნიშნული ნორმა, რომელიც, ცხადია, ჩვეულებითი ხასიათისაა,[106] წარმოადგენს ასევე, *jus cogens*[107] ნორმას. როგორც წინა თავში აღინიშნა, საერთაშორისო ხელშეკრულებებზე, მათ შორის, გაეროს ქარტიაზე, შესაძლოა, გავრცელდეს ევოლუციური ინტერპრეტაცია. თუმცა, მოცემულ თავში პასუხი უნდა გაეცეს შემდეგ შეკითხვებს - იკრძალება თუ არა კიბერშეტევების განხორციელება ქარტიის მიხედვით? მიიჩნევა თუ არა კიბერშეტევა ძალის გამოყენებად? თუ ასეა, მაშინ რა სახის შეტევები უნდა ჩაითვალოს ასეთად და როგორ

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

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

[106] *იქვე,* §§187-190.

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

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.[108] ეს შეხედულება გამომდინარეობს *ბირთვული იარაღის შესახებ* სასამართლოს საკონსულტაციო დასკვნის ანალიზიდან, რომლის მიხედვითაც, თავდაცვის უფლება გამოიყენება „ნებისმიერი ძალის გამოყენების საპასუხოდ, იმის მიუხედავად, რომელი იარაღით განხორციელდა შეტევა".[109] ვინაიდან თავდაცვის უფლების გამოყენება შეუძლებელია ქარტიის მე-2(4) მუხლის კონტექსტის გარეშე და, რადგან „ნებისმიერ იარაღში" შესაძლოა, იგულისხმებოდეს, როგორც ელექტრონული საშუალებები, ისე - კიბერშეტევაც, ამიტომ, თანამედროვე ეპოქაში *jus ad bellum*-ზე საუბრისას შეუძლებელია, არ იქნეს გათვალისწინებული კიბერშეტევების კონტექსტიც. კიბერსივრცეში მოქმედებისას ერთი სახელმწიფოს მიერ მეორის მიმართ განხორციელებული კიბერშეტევა აღქმული უნდა იქნეს, როგორც ქმედება, ხოლო ელექტრონული საშუალებები კი - ამ ქმედების განხორციელების ინსტრუმენტი.

აღსანიშნავია, რომ გაეროს ქარტიის კომენტარები არ უარყოფს იმ მოსაზრებას, რომ სავსებით შესაძლებელია, „კომპიუტერულ ქსელზე შეტევა, რომელსაც აქვს იარაღის მსგავსი დამანგრეველი ეფექტი", ჩაითვალოს ძალის გამოყენებად ქარტიის მე-2(4) მუხლის კონტექსტში,[110] მეტიც, რიგ შემთხვევაში, შესაძლოა, „შეიარაღებული შეტევაც", რაც გამოიწვევს თავდაცვის უფლების ამოქმედებას[111].

კიბერშეტევა რომ შეფასდეს ძალის გამოყენებად, სამი წინაპირობა უნდა იყოს გათვალისწინებული: ა) შეტევას უნდა ახორციელებდეს სახელმწიფო; ბ) კიბეროპერაცია უნდა აღიქმებოდეს ძალის გამოყენებად ან მის მუქარად მაინც; გ)

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

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

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

[111] იქვე.

ძალის გამოყენება ან მისი მუქარა უნდა განხორციელდეს საერთაშორისო ურთიერთობების ფარგლებში.[112]

პირველ კრიტერიუმში შეიძლება, მოიაზრებოდეს არა მხოლოდ სახელმწიფოს ოფიციალური *(de jure)*,[113] არამედ მისი *de facto* ორგანოებიც,[114] ასევე არასახელმწიფო დაჯგუფებათა ქმედებებიც, რომლებიც იმყოფებიან სახელმწიფოს ეფექტური კონტროლის ქვეშ.[115]

რაც შეეხება ძალის გამოყენების ან მისი მუქარის არსებობას, ტალინის სახელმძღვანელო პრინციპების თანახმად, ეს წინაპირობა აშკარაა, როცა კიბეროპერაციის მასშტაბები და ეფექტები შეიძლება, შეედაროს [ტრადიციული], არაკიბერიარაღების მიერ მიყენებულ ზიანს, რომელიც საკმარისი იქნებოდა ქმედების ძალის გამოყენების შესაფასებლად.[116]

ძალის გამოყენება ან მისი მუქარა უნდა განხორციელდეს საერთაშორისო ურთიერთობების ფარგლებში, რათა მოექცეს ქარტიის 2(4) მუხლის მოქმედების ქვეშ. ეს ნიშნავს, რომ საერთაშორისო სამართალში არსებული ძალის გამოყენების აკრძალვა არ მოქმედებს ერთ სახელმწიფოში განვითარებულ მოვლენებზე. აქ არ იგულისხმება ძალის გამოყენება სახელმწიფოს ტერიტორიაზე მყოფი სხვა ქვეყნის შეიარაღებული ძალების წინააღმდეგ, რომელთაც აქვთ ტერიტორიაზე ყოფნის უფლება. შეჯამების სახით შეიძლება ითქვას, რომ *jus ad bellum* არ ვრცელდება ისეთ დროს, როდესაც ძალის გამოყენების ადრესატს არ გააჩნია სხვა სახელმწიფოს ოფიციალური წარმომადგენლის სტატუსი.

ერთია, რომ შესაძლოა, კიბეროპერაციებზეც გავრცელდეს ქარტიის მე-2(4) მუხლი და მეორეა ის ფაქტი, რომ არ არსებობს თავად ძალის გამოყენების ოფიციალური დეფინიცია. ამგვარ შემთხვევებში, ვენის 1969 წლის კონვენციის 31-ე მუხლი, რომელიც

---

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

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

[114] 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.

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

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

თავის მხრივ, უმეტესწილად, ჩვეულებით სამართალს დაეყრდნო, ითვალისწინებს ინტერპრეტაციისას კონტექსტური ანალიზის მნიშვნელობას. აღსანიშნავია, რომ სიტყვა - „ძალა“ ნახსენებია ქარტიის პრეამბულაში (41-ე, 44-ე და 46-ე მუხლები). თითოეულ მათგანში, გარდა მე-2(4) მუხლისა, „ძალას“ წინ უძღვის სიტყვა - „შეიარაღებული“, 44-ე მუხლი კი, საერთოდ, მხოლოდ შეიარაღებული ძალის გამოყენების საკითხებს ეხება. ეს ყოველივე ქმნის აზრთა სხვადასხვაობას, რადგან ყველა სხვა შემთხვევაში, „ძალის გამოყენება“ განიხილება შეიარაღებულ კონტექსტში, იგივე ვრცელდება მე-2(4) მუხლზეც. თუმცა, ასეთივე წარმატებით შეიძლება, ითქვას, საპირისპიროც, რომ ტერმინი - „შეიარაღებული“ - ზემოხსენებულ მუხლებში გათვალისწინდა განზრახ, მე-2(4) მუხლი ბევრად ვრცელია და მოიცავს სხვა „არაშეიარაღებულ“ შემთხვევებსაც. ამ უკანასკნელი არგუმენტის სასარგებლოდ მიუთითებს თავად გაეროს ქარტიის სულისკვეთებაც, დაიცვას თაობები ომის სისასტიკისგან.[117] 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 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; ქმედების ეფექტების მიხედვით შეფასება. სამეცნიერო წრეებში ეს უკანასკნელი მიდგომაა მხარდაჭერილი, რომელიც გულისხმობს, რომ ძალის გამოყენებას უნდა ჰქონდეს პირდაპირი დამანგრეველი ეფექტი საკუთრებისა და ადამიანებისთვის.[118]

[117] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 45.
[118] იქვე, 47.

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

კიბერსივრცეში ჩადენილი ქმედება შეიძლება წარმოადგენდეს შიდა საქმეებში ჩარევას. თუმცა, რიგ შემთხვევაში, შესაძლოა, რომ კიბეროპერაციები ვერ აღწევდეს იმ ზღვარს, რომელიც საჭიროა მისი ძალის გამოყენებად შეფასებისთვის. მიუხედავად ამისა, მსგავსი ქმედებები საერთაშორისო სამართლის მიღმა მაინც არ რჩება.

ასეთ შემთხვევებში, აშკარა იქნება სახელმწიფოს შიდა საქმეებში ჩარევა, რაც, თავის მხრივ, დაარღვევს დაზარალებული სახელმწიფოს სუვერენიტეტსა და ასევე საერთაშორისო სამართალში განმტკიცებულ[119] შიდა საქმეებში ჩაურევლობის პრინციპს, რომელსაც ჩვეულებითი სამართლის ძალა აქვს.[120]

ასეთ დროს, როდესაც ირღვევა საერთაშორისო სამართლის პირველადი ნორმები, ამოქმედდება მეორადი ნორმები, რომლებიც წამოჭრის 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.[121]

შიდა საქმეებში ჩაურევლობის პრინციპის შეფასება ტრადიციულად მიმდინარეობდა ძალის გამოყენების ჭრილში.[122] თუმცა, სასამართლომ ნიკარაგუის საქმეში აღნიშნა, რომ ძალის გამოყენება „განსაკუთრებით ნათელი მაგალითია“

---

[119] 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).

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

[121] Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001.

[122] *Damrosch, L.,* Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs, American Journal of International Law, 83, 1989, 3.

უკანონო ჩარევის.[123] მიუხედავად იმისა, რომ ჩარევასთან დაკავშირებული საერთაშორისო სამართლის ჩვეულებით წესებს აქვს შესამჩნევი ფარგლები, რათა განხილულ იქნეს ძალის გამოყენების ზოგად აკრძალვასთან ერთად, ჩარევა მაინც წარმოადგენს ცალკეულ კონცეფციას.[124] როგორც მოსამართლე ჯენინგსმა განაცხადა, „უდავოა, რომ შიდა საქმეებში ჩაურევლობის პრინციპი წარმოადგენს ჩვეულებითი სამართლის ავტონომიურ პრინციპს“.[125]

შიდა საქმეებში ჩაურევლობის პრინციპი შეიძლება განვიხილოთ, როგორც სასარგებლო სამართლებრივი მექანიზმი, რომლის საფუძველზეც შესაძლოა, სახელმწიფოებმა თავი დაიცვან ისეთი კიბერშეტევებისგან, რომლებიც არ იწვევს ფიზიკურ ზიანს, თუმცა, მოაქვს უარყოფითი შედეგები.

საინტერესოა, რატომ არ ექცევა დიდი ყურადღება ჩაურევლობის პრინციპს კიბერშეტევების კონტექსტში?

ეს 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“.[126]

სუვერენიტეტის ამგვარი განსაზღვრება გავლენას ახდენს შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლებზე, რომლებიც მიიჩნევა სუვერენიტეტის პრინციპის თანმდევად.[127] რაც შეეხება სუვერენიტეტის ტერიტორიული გაგების გავლენას, უკანონო ჩარევა განხორციელდება მხოლოდ მაშინ, როცა ჩარევა მოხდება სახელმწიფოს ფიზიკურად არსებულ ტერიტორიაზე ან მის მიმართ.[128]

---

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

[124] *Jennings, R., Watts, A.,* Oppenheim's International Law (9th Edition): Volume 1 Peace, Oxford University Press, 2008, 429.

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

[126] იქვე, § 212.

[127] იქვე, § 202.

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

ამ ფონზე, კიბერსივრცე მიიჩნევა სფეროდ, რომელზეც სახელმწიფო ვერ განახორციელებს ტერიტორიულ კონტროლს. საერთაშორისო ჰუმანიტარული სამართლის ინსტიტუტის მოსაზრების თანახმად, „კიბერსივრცის გამორჩეული მახასიათებელია ის, რომ ეს არის ცნების დონეზე არსებული გარემო ნებისმიერ სახელმწიფოს იურისდიქციის მიღმა“.[129]

საპირისპირო მიდგომას ავითარებს აშშ-ის თავდაცვის დეპარტამენტი, რომელიც მიიჩნევს, რომ კიბერსივრცე არის საერთო სივრცე, როგორც ღია ზღვა, საჰაერო სივრცე და კოსმოსი.[130]

ზემოაღნიშნულიდან 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 სახელმწიფოს არამატერიალურ კატეგორიებში, როგორებიცაა - რადიაცია ან ელექტროენერგია, ჩაითვალოს სახელმწიფოს წინააღმდეგ განხორციელებულ დარღვევად.[131]

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 უნარსა და პოლიტიკის შემუშავების პროცესებზე, შიდა და გარე საქმეებთან მიმართებით.

სუვერენიტეტის ბევრად ფართო გაგების მხარდამჭერი მიდგომა გამოხატა სასამართლომ. *ნიკარაგუის საქმეში*, ჩაურევლობის პრინციპის ჩვეულებითი სამართლის სტატუსისა და ფარგლების დადგენისას, სასამართლომ აღნიშნა:

> *„აკრძალული ჩარევა, რომელიც ეხება საკითხებს, რომელთა გადაწყვეტა სახელმწიფოს, სახელმწიფო სუვერენიტეტიდან გამომდინარე, შეუძლია თავისუფლად. ერთ-ერთია პოლიტიკური,*

[129] *International Humanitarian Law Institute,* Rules of Engagement Handbook. September 2009, 15.
[130] *US Department of Defense,* The Strategy for Homeland Defense and Civil Support, June 2005, 12.
[131] *Kanuck, S.,* Recent Development: Information Warfare: New Challenges for Public International Law, Harvard International Law Journal, 37, 1996, 288.

ეკონომიკური, სოციალური და კულტურული სისტემების არჩევა. ჩარევა მართლსაწინააღმდეგოა, როცა მას ახლავს იძულების მეთოდები. ასეთ არჩევანი უნდა იყოს თავისუფალი... იძულების ელემენტი განსაზღვრავს და რეალურად წარმოადგენს აკრძალული ჩარევის არსს."[132]

შესაბამისად, აკრძალული ჩარევა ისეთი აქტებია, რომლებიც შეფასდება ძალადობრივად. აქედან გამომდინარე, მოექცევა შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლებში. ამ კონტექსტში კარგი მაგალითია ისეთი ჩარევა, რომელიც მიზნად ისახავს სამიზნე სახელმწიფოს იძულებას, შეცვალოს პოლიტიკა.[133] აღსანიშნავია, რომ მხოლოდ იძულება არ არის საკმარისი. *ნიკარაგუის* საქმიდან გამომდინარე, ასეთი იძულება უნდა ეხებოდეს ისეთ საკითხს, რომლის გადაწყვეტაში სახელმწიფოს აქვს ფართო დისკრეცია. ამ ელემენტზე ყურადღება გამახვილებულია სამეცნიერო ლიტერატურაშიც.[134] ამ ელემენტების გათვალისწინება საჭიროა იმ მიზნით, რომ შეიძლება ჩარევის ყველა ფორმა არ აიკრძალოს საერთაშორისო ჩვეულებითი სამართლით, რადგან სახელმწიფოებმა თავიანთი პრაქტიკით შეიძლება შეცვალონ შიდა საქმეებში ჩაურევლობის პრინციპის ფარგლები. მაგალითად, ნიკარაგუის საქმეში სასამართლოს მოუწია, ემსჯელა, ხომ არ არსებობდა სახელმწიფოთა პრაქტიკა ისეთი *opinio juris*-ით, რომელიც ითვალისწინებდა სახელმწიფოთა ჩარევის ზოგადი 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.[135] თუმცა, სასამართლომ მიუთითა, რომ თანამედროვე საერთაშორისო სამართალში არ არსებობდა ასეთი ჩარევის უფლება.[136] ამ მიდგომის მნიშვნელობა მდგომარეობს იმაში, რომ ჩაურევლობის პრინციპის ფარგლების

---

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

[133] *Jamnejad, M., Wood, M.,* The Principle of Non-Intervention, Leiden Journal of International Law, 22, 2009, 348.

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

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

[136] იქვე, § 207.

ცვლილებაზე საუბარი შეიძლება იმ შემთხვევაშიც, 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 სამართლის მიხედვით, შიდა საქმეებში ჩაურევლობის პრინციპის განხილვის მიზანია იმის ჩვენება, რომ ეს მოქმედებს კიბერშეტევების საწინააღმდეგოდ მაშინ, როცა არსებობს კიბერშეტევის ძალის გამოყენების შეფასების ეჭვი. ამდენად, ზემოთ მოცემული ანალიზიდან გამომდინარე, საჭიროა დადგინდეს ა) კიბერშეტევის მიზანს წარმოადგენს თუ არა სამიზნე სახელმწიფოს იძულება, შეცვალოს პოლიტიკა; ბ) გამოკვეთილია თუ არა იძულების/ძალადობრივი მეთოდის გამოყენება. დადებითი პასუხის შემთხვევაში, უნდა შეფასდეს, რამდენად ეხება კიბერშეტევა იმ საკითხებს, რომლებიც სახელმწიფოს შეუძლია, გადაწყვიტოს. პირველის 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 აეძულებინა ესტონეთის მთავრობა, შეეცვალა პოლიტიკა. ასევე უნდა შეფასდეს, თუ რა სირთულის პრობლემები შექმნა ამ კიბერშეტევებმა. 2007 წელს ესტონეთი იყო ყველაზე დიდი ინტერნეტქსელის მქონე სახელმწიფო ევროპაში, ეგრეთ წოდებული, ერთგვარი „ინფორმაციული საზოგადოება“.[137] შესაბამისად, მთავრობა, კერძო სექტორი და მოქალაქეები ინტენსიურად იყენებდნენ ინტერნეტ-მომსახურებას. მაგალითად, 2007 წელს საბანკო ოპერაციების 95% ხორციელდებოდა ელექტრონულად.[138] შეტევების შედეგად, მოწინავე ბანკების საიტების მოშლამ მასშტაბურად შეაფერხა ეკონომიკური აქტივობები.

შეტევები მიიტანეს მედიის ვებგვერდებზეც. მთავარი საინფორმაციო საიტების ქსელიდან გამორთვის გამო, მოქალაქეებს არ მიეწოდებოდათ ინფორმაცია კიბერშეტევის მასშტაბისა და შედეგების შესახებ. უფრო მეტიც, როცა აღმოაჩინეს, რომ

[137] *Tikk, E., Kasha, K., Vihul, L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence, 2010, 16.
[138] იქვე, 17.

შეტევები ხორციელდებოდა საზღვარგარეთიდან, პრევენციის მიზნით, გამორთეს შემომავალი ინტერნეტტრაფიკი და ესტონეთი აღმოჩნდა მსოფლიოსგან მოწყვეტილი.

შეტევების უარყოფითი შედეგი აისახა საჯარო სექტორზეც, პრემიერმინისტრისა და მისი პოლიტიკური პარტიის, პრეზიდენტის აპარატის, პარლამენტისა და სახელმწიფო აუდიტის ვებგვერდებზე. სრულად უფუნქციო საიტებზე შეუძლებელი იყო ინფორმაციის განახლება და ელექტრონული ფოსტით კომუნიკაციის შენარჩუნება.[139]

და ბოლოს, მნიშვნელოვანია იმის აღნიშვნა, რომ შეტევები საჯარო და კერძო სექტორის მიმართ გაგრძელდა სამი კვირის განმავლობაში. მისი ინტენსივობისა და დროის გათვალისწინებით, შეიძლება იმის მტკიცება, რომ ამ ქმედებებს თან ახლდა იძულების ელემენტი, რათა ესტონეთის მთავრობა წასულიყო დათმობაზე და არ შეეცვალა ბრინჯაოს ჯარისკაცის ქანდაკების ლოკაცია. ეს გარემოება ადვილად ექცევა კიბერიძულების განსაზღვრებაში, რომელიც გულისხმობს „კიბერ-შესაძლებლობების გამოყენებას, მოწინააღმდეგის იძულების მიზნით, შეასრულოს ისეთი ქმედება, რომლის განხორციელების სურვილი მას ჩვეულებრივ არ ექნებოდა.“[140]

რაც შეეხება მეორე საკითხს - უკავშირდება თუ არა იძულება იმ სფეროს, სადაც სახელმწიფოს შეეძლო თავისუფალი არჩევანი? - ცხადია, არ არსებობს უფლება, ერთი სახელმწიფო იძულების გზით ჩაერიოს მეორე სახელმწიფოს საქმეებში, როცა სურს განსაკუთრებული მნიშვნელობის ქანდაკების ან მემორიალის ლოკაციის ცვლილება. ამდენად, ეს არის სფერო, სადაც სახელმწიფოს სრული ფარგლებით იცავს შიდა საქმეებში ჩაურევლობის პრინციპი.

ასეთი დარღვევის დადგენა მნიშვნელოვანია იმ კუთხით, რომ სახელმწიფოს მიეცეს უფლება, მოითხოვოს უკანონო ქმედების აღკვეთა, გარანტიები, ასეთი ქმედების ხელახალი განმეორების თავიდან აცილების მიზნით და რეპარაციები.[141] გარდა ამისა, საერთაშორისო ჩვეულებითი სამართალი საშუალებას აძლევს

---

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

[140] *Hodgson, Q. E.*, Understanding and Countering Cyber Coercion, 10th International Conference on Cyber Conflict, *T. Minárik, R. Jakschis, L. Lindström (eds.)*, NATO CCD COE Publications, 2018, 73.

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

სახელმწიფოს, გამოიყენოს კონტრზომები, განგრძობადი დარღვევის შემთხვევაში.[142] ასეთი კონტრზომები უნდა იყოს აუცილებელი და პროპორციული.[143]

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

3. „შეიარაღებული შეტევა“ - როგორც ასეთი

გაეროს ქარტიის 51-ე მუხლით კოდიფიცირებული თავდაცვის უფლება მოიცავს როგორც ინდივიდუალურ, ასევე კოლექტიური თავდაცვის უფლებას. ქარტია მას „თანდაყოლილ უფლებად“[144] მოიხსენიებს. სასამართლო, *ნიკარაგუის საქმეში*, მას „წინარე [ქარტიამდელ] ჩვეულებითი სამართლის ნორმას“ უწოდებს.[145] მიუხედავად იმისა, რომ თავდაცვის უფლება განმტკიცებულია საერთაშორისო სამართალში, გარკვეულ შეზღუდვებსაც ექვემდებარება. დოქტრინის განსაკუთრებით მნიშვნელოვან და საკამათო წინაპირობას წარმოადგენს „შეიარაღებული შეტევის“ არსებობა, რომლის გარეშეც, ქარტიის თანახმად, სახელმწიფოს არ შეუძლია, მითითება თავდაცვის უფლებით სარგებლობაზე. *ნიკარაგუის საქმეში* სასამართლომ ყურადღება გაამახვილა ასევე სახელმწიფოთა პასუხისმგებლობის სამართალსა და გენერალური ასამბლეის 1974 წლის ცნობილ რეზოლუციაზე, რომლის მიხედვითაც განიმარტა აგრესიის დეფინიცია,[146] რის გამოც მეცნიერთა ერთი ნაწილი შეიარაღებულ შეტევას აგრესიის კატეგორიად მოიხსენიებს. ამ მოსაზრებას მკვლევართა უმეტესობა

[142] იქვე, მუხლი 49.
[143] იქვე, მუხლი 51.
[144] ინგლისურად - „Inherent right“.
[145] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 94.
[146] *Crawford, J.*, Brownlie's Principles of Public International Law (8th Edition), Oxford University Press, 2013, 748.

არ იზიარებს.[147] ფრაზა - „თუკი ხდება შეიარაღებული შეტევა“[148] - გულისხმობს მომხდარ ან მიმდინარე შეიარაღებულ შეტევებს.[149] დინშტაინი ავითარებს ე.წ. „ჩამჭრელი თავდაცვის“[150] დოქტრინას, რომლის მიხედვით, არ არის აუცილებელი უკვე შემდგარი შეტევა. საკმარისია ცოდნა მისი დაწყების თაობაზე, რომელიც სახელმწიფოს აძლევს თავდაცვის უფლების გამოყენებას.[151] დინშტაინი იმოწმებს ჰიპოთეტურ მაგალითს, რომლის თანახმადაც, პერლ-ჰარბორის დაბომბვამდე, ღია ცაში, ამერიკელებს რომ გაეცათ იაპონელებისთვის სათანადო პასუხი, ეს თავდაცვის უფლების გამოყენების სამართლებრივ საფუძველს არ გასცდებოდა.[152] რაც მთავარია, უნდა გაიმიჯნოს ერთმანეთისგან ჩამჭრელი თავდაცვის უფლება წინასწარი[153] ან უპირატესი[154] თავდაცვის უფლებისგან, რომელთა შესახებ ნაშრომის მომდევნო თავებში ვისაუბრებთ.

კიბერკონტექსტში განსაკუთრებულ მნიშვნელობას იძენს ტერმინ „შეიარაღებულის“ ანალიზი, რაც გამოწვეულია იმით, რომ ნებისმიერი შეიარაღებული შეტევა - *ipso facto* - გულისხმობს ძალის გამოყენებას, ნებისმიერი ძალის გამოყენება კი, თავის მხრივ, არ ნიშნავს შეიარაღებულ შეტევას.[155] ნიკარაგუის საქმეში სასამართლო ამ ორ შემთხვევას ერთმანეთისგან ასხვავებს „მასშტაბებისა და ეფექტების“ შეფასებათა მიხედვით.[156] ტალინის ექსპერტთა ჯგუფი კიბეროპერაციას შეიარაღებულ შეტევად იმ შემთხვევაში მოიხსენიებს, თუ ის იწვევს მნიშვნელოვან ფიზიკურ ზიანს, მაგალითად, ადამიანთა სიკვდილს.[157] დოქტრინაში მოყვანილია ამგვარი შეტევის ჰიპოთეტური მაგალითი - კიბერშეტევის შედეგად კაშხლის დამცავი სისტემის მოშლა, თანმდევი

[147] *Zemanek, K.*, Armed Attack, Max Planck Encyclopedia of Public International Law. Oxford University Press, 2013, § 2.
[148] ინგლისურად „if an armed attack occurs“.
[149] *Zemanek, K.*, Armed Attack, Max Planck Encyclopedia of Public International Law. Oxford University Press, 2013, § 4.
[150] ინგლისურად: „Interceptive Self-Defence“.
[151] *Dinstein, Y.*, War, Aggression and Self-Defence (4th ed.), Cambridge University Press, 2005, 187 *et seq.*
[152] *იქვე,* 190.
[153] ინგლისურად: „Anticipatory“.
[154] ინგლისურად: „Pre-emptive“.
[155] *Weller, M. (ed.),* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 1119.
[156] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* ICJ, Judgment, 27 June 1986, §195.
[157] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 54-60.

კატასტროფული შედეგებით, რომელიც მართლაც ფასდება „შეიარაღებულ შეტევად“, რის შემდეგაც დაზარალებულ სახელმწიფოს ეძლევა თავდაცვის უფლება.[158] სხვა შემთხვევაში, ეს შეიძლება ჩაითვალოს „უბრალოდ, სასაზღვრო ინციდენტის“[159] ანალოგად.[160]

თანამედროვე საერთაშორისო სამართალი იცნობს ისეთ მაგალითსაც, როცა სახელმწიფომ კიბერშეტევის საპასუხოდ მიიღო თავდაცვითი სამხედრო ზომები. 2007 წელს, სირიის მიერ განხორციელებულმა კიბერშეტევამ დააზიანა ისრაელის ანტისაჰაერო სისტემის ნაწილი, რის საპასუხოდაც, ისრაელმა დაბომბა სირიის ატომური სადგური.[161] აღნიშნული შემთხვევის სამართლებრივი შეფასებისას გამოყენებულ უნდა იქნეს ორი კრიტერიუმი: აუცილებლობა და პროპორციულობა. კერძოდ, უნდა შეფასდეს:

- რამდენად აუცილებელი იყო ისრაელის მიერ კიბერშეტევის საპასუხოდ და მის აღსაკვეთად სირიის ატომური სადგურის დაბომბვა;
- რამდენად წარმოადგენდა აღნიშნული ქმედება პროპორციულ ზომას.

თუ რას გულისხმობს აუცილებლობისა და პროპორციულობის ტესტი, დეტალურად იხილეთ შემდეგ ქვეთავში.

3.1. აუცილებლობისა და პროპორციულობის ტესტი

ჩვეულებითი საერთაშორისო სამართლის თანახმად, ნებისმიერი თავდაცვითი ქმედება, იქნება ეს კიბეროპერაცია თუ კიბერშეტევაზე განხორციელებული არა კიბერ სახის თავდაცვა, ექვემდებარება ორ კუმულაციურ წინაპირობას: აუცილებლობასა და

[158] *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 1120.

[159] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* ICJ, Judgment, 27 June 1986, §195. ასევე, ამავე საქმეში, სასამართლომ ერთმანეთისგან განასხვავა მძიმე ინციდენტი ნაკლებად მძიმე ინციდენტისგან (*იქვე*, §191).

[160] *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 1120.

[161] *Roscini, M.*, Cyber Operations and the Use of Force in International Law, Oxford Unviersity Press, 2014, 7.

პროპორციულობას,[162] რომელთა ჩვეულებით ხასიათზეც მიუთითებს სასამართლო თავის არაერთ გადაწყვეტილებაში.[163]

აუცილებლობის პრინციპის თანახმად, თავდაცვის უფლების მიზნით, ძალის გამოყენება მხოლოდ იმ შემთხვევაშია დასაშვები, თუ, სხვა, არაძალისმიერი მეთოდები არ აღმოჩნდება საკმარისი კიბერშეტევის მოგერიებისას. მაგალითად, თუ ერთი რომელიმე სახელმწიფოს კიბერთავდაცვის სისტემების სისუსტით ისარგებლებს სხვა სახელმწიფო, დაზარალებულ მხარეს არ აქვს უფლება, საპასუხოდ განახორციელოს შეიარაღებული შეტევა.[164] ასეთ ვითარებაში გამოსავალი იქნება საკუთარი კიბერთავდაცვის გაძლიერება, არასამხედრო ხასიათის კონტრზომების გატარება, მათ შორის, დიპლომატიური პროტესტი, სხვადასხვა სანქცია და სხვ.

აუცილებლობის პრინციპი პასუხს სცემს კითხვას, უფლებამოსილია თუ არა სახელმწიფო, გამოიყენოს ძალა. *პროპორციულობის პრინციპი* კი განსაზღვრავს, რა ფარგლებში შეუძლია სახელმწიფოს ძალის გამოყენება. პროპორციულობის პრინციპის თანახმად, კიბერშეტევის საპასუხოდ დასაშვებია მხოლოდ იმ ოდენობის ძალის გამოყენება, რაც საჭიროა ამგვარი შეტევის დასასრულებლად.[165] სახელმწიფო არ არის უფლებამოსილი, მიმდინარე კიბერშეტევის საპასუხოდ, დამრღვევი სახელმწიფოს წინააღმდეგ ტოტალური სამხედრო შეტევა განახორციელოს, მიუხედავად იმისა, რომ მას აქვს თავდაცვის უფლების გამოყენების შესაძლებლობა. აქვე უნდა აღინიშნოს, რომ ხშირად პროპორციულობის პრინციპი არასწორად არის აღქმული, თითქოსდა ის საპასუხოდ გულისხმობდეს აგრესორი სახელმწიფოს წინააღმდეგ ადეკვატური ძალის გამოყენებას.[166] პროპორციულობის პრინციპი ეხება იმ საკითხს, თუ რამდენად საკმარისია კონკრეტული იძულებითი ზომა შეტევის მოსაგერიებლად/დასასრულებლად და არა იმას, თუ რა ოდენობისა და როგორი

---

[162] *იქვე,* 1124.

[163] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, §§174, 196; *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, §41; *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, §§43, 73, 74, 76.

[164] *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 1124.

[165] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 61-63.

[166] *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 1125.

იარაღით განხორციელდება თავდაცვა. საერთაშორისო სამართალი ასევე ითვალისწინებს თავდაცვითი ძალის გამოყენების დროით შეზღუდვასაც.[167]

3.2. შეიძენს თუ არა განზრახვის ელემენტი განსაკუთრებულ მნიშვნელობას კიბერშეტევათა ძალის გამოყენებად შეფასებისას?

ნავთობის პლატფორმების ცნობილ საქმეში სასამართლომ შემოიღო „სპეციალური განზრახვის“ დამატებითი კრიტერიუმი. სასამართლოს თქმით, არ დადგინდა, ირანის მიერ ამერიკული გემის ჩაძირვა წინასწარ განზრახულობით, ანუ იმ მიზნით, რომ ზიანი მიეყენებინა აშშ-თვის. შესაბამისად, ირანის მიერ ამერიკული გემის ჩაძირვა ვერ შეფასდებოდა შეიარაღებულ შეტევად.[168] მნიშვნელოვანია, რომ სასამართლომ ამგვარი კრიტერიუმი, ძალის გამოყენების კონტექსტში, პირველად შემოიღო, რამაც გამოიწვია არა მხოლოდ აშშ-ის, არამედ მეცნიერთა ნაწილის უკმაყოფილებაც და წარმოშვა აზრთა სხვადასხვაობა.[169]

საინტერესოა, რომ თუ ძალის გამოყენების სამართლის კონვენციური გაგებისთვის *ნავთობის პლატფორმების* საქმეში შემოტანილი კრიტერიუმი არ იმსახურებს ფართო მხარდაჭერას, ის შესაძლოა, გადამწყვეტი ფაქტორი აღმოჩნდეს, სამომავლოდ, კიბერშეტევის საპასუხოდ, თავდაცვითი ძალის გამოყენების ლეგიტიმურობის შესამოწმებლად. კიბეროპერაციათა კონტექსტში, მეცნიერთა შორის დამკვიდრებულია მოსაზრება, რომლის თანახმადაც, უბრალო დანაშაულებრივ აქტსა და სახელმწიფოს პასუხისმგებლობას შორის განმასხვავებელია უშუალოდ ქმედების მოტივი - რამ განამაპირობა კონკრეტული კიბერშეტევა.[170]

თუმცა, საეჭვოა, რამდენად პრაქტიკული იქნება მიზნის კრიტერიუმის დამატება კიბეროპერაციათა კონტექსტში, რადგან პრაქტიკაში სახელმწიფოს მოქმედების ისეთი სუბიექტური ელემენტის მტკიცება, როგორიც მიზანია, თითქმის შეუძლებელია.

---

[167] ვრცლად იხ.: *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 737-750.

[168] *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, §64.

[169] *Gray, C.,* International Law and the Use of Force (3rd ed.), Oxford University Press, 2008, 143-148.

[170] *Roscini, M.*, Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 34-35.

სახელმწიფო ორგანიზაციული სტუქტურაა, რომელიც შეიძლება, არც მოქმედებდეს გაცხადებული მიზნებით.

4. კიბერშეტევების მიმართება გაეროს ქარტიის VII თავთან

გაეროს ქარტიის თანახმად, უშიშროების საბჭოს ეკისრება პირველადი პასუხისმგებლობა[171] მსოფლიოში მშვიდობისა და უსაფრთხოების შესანარჩუნებლად. უშიშროების საბჭოსვე ენიჭება ფართო, მაგრამ არა აბსოლუტური დისკრეცია,[172] მიიღოს ყველა სათანადო ზომა, რათა მშვიდობა და უსაფრთხოება იქნეს დაცული.

თეორიულად, თითქოს მართალაც არაფერი უდგას წინ იმას, რომ უშიშროების საბჭომ VII თავის მიხედვით მიიღოს რეზოლუცია, რომლითაც მოიპოვებს კონკრეტული კიბეროპერაციის ლეგიტიმაციას. აღნიშნულ აზრს იზიარებს ტალინის ექსპერტთა საერთაშორისო ჯგუფიც.[173] თუმცა, აზრთა სხვადასხვაობას იწვევს საკითხი, რა სახის იქნება უშიშროების საბჭოს მიერ კიბეროპერაციაზე ნებართვის გაცემა? იქნება ეს ძალისმიერი თუ არაძალისმიერი მეთოდი? კერძოდ, ქარტიის 41-ე მუხლი, რომლითაც განისაზღვრება არაძალისმიერი მექანიზმები, მიუთითებს შემდეგს: „მთლიანი ან ნაწილობრივი შეზღუდვა ეკონომიკური ურთიერთობებისა, ისევე, როგორც სარკინიგზო, საჰაერო, საზღვაო, საფოსტო, სატელეგრაფო, რადიო და სხვა სახის კომუნიკაციებისა და ასევე დიპლომატიური ურთიერთობების გაწყვეტა“. მოცემული ამონარიდი, გარკვეულწილად, მოიცავს კიბეროპერაციებსაც, რადგან ითვალისწინებს ელექტრონულ და ციფრულ კომუნიკაციაზე შეზღუდვების დაწესებას. მკვლევართა უმეტესობის აზრით, ქარტიის აღნიშნულ მუხლში ნახსენები „სხვა სახის კომუნიკაციებში“ კიბეროპერაციები მხოლოდ იმ შემთხვევაში იგულისხმება, თუ დამრღვევი სახელმწიფოს მიერ განხორციელებული ქმედებები არ/ვერ აღწევს იმ ზღვარს, რომ შეფასდეს ძალის გამოყენებად, ქარტიის მე-2(4) მუხლის

[171] გაერთიანებული ერების ორგანიზაციის ქარტიის 24(1)-ე მუხლი.
[172] *Prosecutor v. Dusko Tadic,* Decision on the Defence Motion For Interlocutory Appeal on Jurisdiction, ICTY, Appeals Chamber, 2 October 1995, §28.
[173] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 69.

თანახმად.[174] სხვა შემთხვევაში, უშიშროების საბჭოს ექნებოდა შესაძლებლობა, გაეცა ნებართვა კიბეროპერაციების ძალისმიერი მექანიზმების ამოქმედების თაობაზე.

5. კიბერტერორიზმი და უპირატესი თავდაცვის დოქტრინა – წინასწარი/ პრევენციული თავდაცვის წარმატებული რეინკარნაცია?

უპირატესი თავდაცვის დოქტრინას[175] უკავშირებენ ტერორიზმის წინააღმდეგ ბრძოლასა და ე. წ. „ბუშის დოქტრინას".[176] მიუხედავად იმისა, რომ დოქტრინამ კონცეპტუალური მხარდაჭერა სწრაფადვე მოიპოვა და წარმოადგენს ე.წ. „მყისიერი ჩვეულების" ჩამოყალიბების ნიმუშს,[177] მისი კრიტერიუმები მაინც არ არის სრულყოფილად მხარდაჭერილი. მაგალითად, დიდი ბრიტანეთის გაერთიანებული სამეფოს წარმომადგენელთა თქმით, უპირატეს თავდაცვას განიხილავდა წინასწარი თავდაცვის ჭრილში და მის არსებობას აღიარებდა მხოლოდ იმ შემთხვევაში, როცა აშკარა იქნებოდა შეიარაღებული შეტევის „იმწუთიერი საფრთხე".[178] გაეროს გენერალურმა მდივანმა მოხსენებაში („უკეთესად დაცული მსოფლიო: ჩვენი საზიარო ვალდებულება")[179] აღნიშნა:

> *„საფრთხის წინაშე მყოფ სახელმწიფოს, დიდი ხნის დამკვიდრებული საერთაშორისო სამართალის თანახმად, შეუძლია გამოიყენოს სამხედრო ზომა მანამ, სანამ საფრთხე არის იმწუთიერი, სხვა არც ერთი საშუალებით არ შეიძლება მისი არიდება. გამოყენებული ძალა უნდა იყოს პროპორციული."*[180]

---

[174] *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 1118.

[175] ინგ: pre-emptive self-defence.

[176] დამატებით იხ. The Bush Administration's Doctrine of Preemption (and Prevention): When, How, Where?" Council on Foreign Relations, 2004. <http://www.cfr.org/world/bush-administrations-doctrine-preemption-prevention-/p6799> [30.06.2020].

[177] *Langille, B.,* It's 'Instant Custom': How the Bush Doctrine Became Law after the Terrorist Attacks of September 11, 2001, Boston College International & Comparative Law Review, 26, 2001, 145-156.

[178] *Greenwood, C.*, Self-Defence, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011, §47.

[179] A More Secure World: Our Shared Responsibility. Report of the Secretary-General's High-level Panel on Threats, Challenges and Change, 2004.

[180] *იქვე,* §188.

მოცემული შეფასებები სხვა არაფერია, თუ არა უპირატესი თავდაცვის დოქტრინის ტოტალური შემოფარგვლა წინასწარი თავდაცვის დოქტრინით. მეტიც, როგორც ბრიტანული მხარის, ასევე გენერალური მდივნის მიერ წარმოდგენილი კრიტერიუმები ადეკვატურია ცნობილი კეროლაინის ინციდენტით დადგენილი წინაპირობებისა.[181] ე.წ. „ბუშის დოქტრინა“ ასეთ მკაცრ შეზღუდვებს არ ცნობს.[182] იაპონიის ხელისუფლების განცხადება იმის თაობაზე, რომ ჩრდილოეთ კორეის წინააღმდეგ განახორციელებს უპირატეს თავდაცვას, თუ ეს უკანასკნელი განიზრახავს სარაკეტო თავდასხმას, დაცილებულია კეროლაინის კრიტერიუმებისგან. 2012 წელს ანალოგიური მოსაზრება გამოითქვა რუსეთის ფედერაციის წარმომადგენელთა მიერ, პოლონეთში განთავსებული ნატოს სარაკეტო კომპლექტთან დაკავშირებით.[183] თუმცა, შესაძლოა, ვივარაუდოთ, რომ უპირატესი თავდაცვის დოქტრინა წარმატებით იქნება იმპლემენტირებული სწორედ კიბერთავდაცვის კუთხით. მაგალითად, დიდი ბრიტანეთის გაერთიანებული სამეფო კიბერტერორიზმს ჩვეულებრივი ტერორიზმიდან მომდინარე საფრთხის ნაწილად განიხილავს.[184] 2012 წლის ნოემბერში ისრაელმა ჩაატარა საზღვაო სამხედრო ოპერაცია და ბლოკადაში მოაქცია ღაზას სექტორი, რათა თავიდან აეცილებინა ჰამასიდან მომდინარე კიბერშეტევის საფრთხე.[185]

6. დასკვნა

წარმოდგენილი ანალიზი შესაძლებელია, შეჯამდეს შემდეგი სახით:

კიბერშეტევები შეიძლება, მოვიაზროთ გაეროს ქარტიის 2(4)-ე მუხლით აკრძალული ძალის გამოყენების ფარგლებში, რადგან: ა) ქმედების ძალის გამოყენებად შეფასება ხორციელდება შედეგობრივი მაჩვენებლების მიხედვით. იმ შემთხვევაში, თუ

[181] *Greenwood, C.,* The Caroline, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009.

[182] *Simma, B., et al (eds.),* The Charter of the United Nations: A Commentary, Volume I (3rd ed.), Oxford University Press, 2012, 1422.

[183] *Weller, M. (ed.).,* The Oxford Handbook of the Use of Force in International Law. Oxford University Press, 2015, 666-668.

[184] *Ohlin, J. D., et al.*, Cyber War: Law and Ethics for Virtual Conflicts, Oxford University Press, 2015, 58-59.

[185] *იქვე,* 167.

კიბერშეტევები გამოიწვევს ისეთივე შედეგებს, რასაც გამოიწვევდა შეიარაღებული თავდასხმები, მაშინ, კიბერეკვივალენტურობის მიდგომის თანახმად, არაფერი უშლის ხელს, რომ ასეთი კიბერშეტევა ჩაითვალოს ძალის გამოყენებად; ბ) ძალის გამოყენების კონცეფცია არ არის მკაცრად შეზღუდული „შეიარაღებულის“ კრიტერიუმით, როგორც, მაგალითად, გაეროს ქარტიის 51-ე მუხლში მოხსენიებული „შეიარაღებული თავდასხმა“; გ) 2(4)-ე მუხლი წარმოადგენს სახელშეკრულებო ნორმას, რომელზეც თავისუფლად შეიძლება, გავრცელდეს ხელშეკრულების ევოლუციური ინტერპრეტაცია. ამ მუხლის მიზანი იყო, აეკრძალა იძულების ელემენტის მომცველი 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 თვითმიზნის შესრულების თვალსაზრისით, ევოლუციური ინტერპრეტაცია წარმოადგენს სამართლებრივად რელევანტურ მექანიზმს. შესაბამისად, დღეის მდგომარეობით, კიბერშეტევები, გარკვეული წინაპირობების არსებობისას (სიმძიმე, მასშტაბურობა, ინტენსივობა და ა.შ.) შეიძლება, ჩაითვალოს გაეროს ქარტიის 2(4)-ე მუხლით აკრძალულ ქმედებად. თუ კიბერშეტევა ვერ მიაღწევს იმ სტანდარტს, რაც საჭიროა მის ძალის გამოყენებად შესაფასებისთვის, საერთაშორისო სამართალი სამართლებრივი დაცვის გარეშე არ ტოვებს დაზარალებულ სახელმწიფოს, რადგან, ამ შემთხვევაში, ამოქმედდება შიდა საქმეებში ჩაურევლობის პრინციპი. ამ პრინციპით გათვალისწინებული დაცვით სარგებლობისთვის კი საჭიროა: ა) ჩარევის მიზანს წარმოადგენდეს სამიზნე სახელმწიფოს იძულება, შეცვალოს პოლიტიკა; ბ) იძულების/ძალადობრივი მეთოდის გამოყენება უნდა ეხებოდეს იმ საკითხებს, რომლებიც სახელმწიფოს შეუძლია თავისუფლად გადაწყვიტოს. აქედან გამომდინარე, შეიძლება ითქვას, რომ ესტონეთის მიმართ განხორციელებული კიბერშეტევები წარმოადგენდა ესტონეთის სუვერენიტეტისა და შიდა საქმეებში ჩაურევლობის პრინციპის დარღვევას.

სასამართლოს პოზიციის მიხედვით, ხელშეკრულების ნორმის გაგებამ, დროთა განმავლობაში, შეიძლება განიცადოს ევოლუცია, რაც იძლევა საშუალებას, რომ კიბერშეტევებზე გავრცელდეს უკვე არსებული ნორმები. ეს მიდგომა, თავის მხრივ,

მიანიშნებს საერთაშორისო სამართლის ახლებურ გააზრებაზე კიბერშეტევების მიმართ.

საბოლოო შეჯამების სახითა 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 რეგულირების ფარგლებს. ახლებური გააზრება საჭიროა მხოლოდ იმ ფარგლებში, რაც აუცილებელია, ერთი მხრივ, კიბერშეტევების უკვე არსებულ საერთაშორისო სამართლებრივ ჩარჩოში ინკორპორაციისთვის.

III. კიბეროპერაციების ზღვარი და *jus contra bellum*: კიბერძალის გამოყენებიდან შეიარაღებულ კიბერშეტევამდე

1. შესავალი

ომის წარმოების უფლება, საუკუნეების განმავლობაში, სახელმწიფოთა შეუზღუდავ და მოუწესრიგებელ სუვერენულ უფლებას წარმოადგენდა.[186] დროდადრო აღნიშნული პრაქტიკა შეიცვალა. სახელმწიფოთა მიერ ომის წარმოების უფლების პირველი შეზღუდვა „სამართლიანი ომისა“ (*bellum justum*) და „უსამართლო ომის“ (*bellum injustum*) ცნებებს შორის განსხვავების დადგენა იყო. აღნიშნული სათავეს ჯერ კიდევ ძველი რომიდან იღებს.[187] ეს თეორია კიდევ უფრო განვითარდა შუა საუკუნეებში და, ქრისტიანული თეოლოგიის წყალობით, კონკრეტულ ფაქტებსაც ემყარებოდა. სამართლიანი ომის თეორიის მიხედვით, ომი არ არის დანაშაული *per se,* მაგრამ ომის მიზეზებიდან გამომდინარე, შეგვიძლია, მივიჩნიოთ სამართლიანად ან უსამართლოდ.[188] შესაბამისად, არასამართლიანი მიზეზით წარმოებული ომი შეგვიძლია, წარმოვიდგინოთ უსამართლოდ, ხოლო სამართლიანი მიზეზით წარმოებული კი - სამართლიანად. სახელმწიფოებს კვლავ შეუძლიათ, იმსჯელონ სამართლიან ომზე, რიტორიკულ განზომილებაში, მაგრამ ომის წარმოება აღარ წარმოშობს სამართლებრივ ვალდებულებებს. სამართლიანი ომის თეორიამ ვეღარ პოვა განვითარება პოზიტიურ საერთაშორისო სამართალში[189] და, შესაბამისად, მისი შემდგომი განხილვა აზრსმოკლებულია. თუმცა, საერთაშორისო სამართლით ომის თანამედროვე რეგულაციას ღრმა ფესვები გააჩნია და ნაწილობრივ დაკავშირებულია სამართლიანი ომის დოქტრინასთან.[190] გარდამტეხი და მნიშვნელოვანი მომენტი სახელმწიფოების მიერ ძალის გამოყენების რეგულირების საკითხში ერთა ლიგის

[186] *Sur, S.,* The Evolving Legal Aspects of War, The Oxford Handbook of War*, Lindley-French J., Boyer Y. (eds.),* Oxford University Press, 2012, 116.
[187] *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 65.
[188] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 273.
[189] *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 69.
[190] *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds),* Edward Elgar Publishing, 2013, 89–90.

შექმნა იყო. ერთა ლიგის პაქტის მე-11 მუხლი აცხადებდა, რომ *„ნებისმიერი ომი ან ომის მუქარა წარმოადგენს მთლიანი ლიგის საერთო საკითხს და ლიგამ უნდა განახორციელოს ნებისმიერი ქმედება, რომელიც შეიძლება, ჩაითვალოს გონივრულად და ეფექტიანად, რათა დაცულ იქნეს ერების მშვიდობა“.*[191]

ისტორიამ გვიჩვენა, რომ ერთა ლიგის პაქტმა ვერ აღკვეთა მეორე მსოფლიო ომი. ამის ძირითადი მიზეზი იყო პაქტის მიერ დაწესებული ზომები, გარდა ომთან დაკავშირებით დაწესებული ზომებისა.[192] ზომები ძალის გამოყენების ინტენსივობის შესახებ არ იყო მკაფიო და რთული იყო მიჯნის დადგენა, როდის აღწევდა ძალის გამოყენება საომარი მოქმედებების ზღვარს.[193] ძალის გამოყენების კანონიერებისა და უკანონობის შეფასება ერთა ლიგის პაქტის ან ბრიან-კელოგის პაქტის[194] მიხედვით, ფაქტობრივად, შეუძლებელი იყო, რადგან არ არსებობდა სახელმწიფოთა მხრიდან კონსენსუსი დოქტრინის თაობაზე. მკვლევარების ნაწილი აღნიშნულ ზომებს მანამდე მიიჩნევდა კანონიერად, სანამ არ მიიღებდა შენიღბული ომის ფორმას.[195] სახელმწიფოთა პრაქტიკაც მხარს უჭერდა აღნიშნულ პოზიციას.[196]

1945 წელს გაეროს ქარტიის მიღება და სახელმწიფოებისთვის კარგად ნაცნობი, ძალის გამოყენების ან მისი მუქარის აკრძალვის დამდგენი 2(4) მუხლი იყო მნიშვნელოვანი ეტაპი ძალის გამოყენების რეგულირებაში. მის ძირითად მიზანს წარმოადგენდა ერთა ლიგის წესდებაში არსებული ნაკლოვანებების გამოსწორება.[197] ვიწრო ტერმინი - „ომი“ ჩაანაცვლა ბევრად ფართო ტერმინმა - „ძალის გამოყენება“.[198] აღნიშნული ტრანსფორმაციის გათვალისწინებით, *jus ad bellum,* შეუზღუდავი და დაურეგულირებელი ომის უფლება, თანდათან შეიცვალა *jus contra bellum*-ით (სამართალი ომის წინააღმდეგ; ძალის გამოყენების აკრძალვის სამართალი) და

---

[191] ერთა ლიგის პაქტი (მიღებულია 1919 წლის 28 ივნისს, ძალაში შევიდა 1920 წლის 10 იანვარს), მუხლი 11.

[192] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 274.

[193] *იქვე.*

[194] Treaty between the United States and Other Powers Providing for the Renunciation of War as an Instrument of National Policy (ხელმოწერის თარიღი: 27 August 1928, ძალაში შესვლის თარიღი: 27 July 1929), 94 LNTS, 57 (შემდგომში მოხსენიებული, როგორც ბრიან-კელოგის პაქტი).

[195] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 274.

[196] *იქვე.*

[197] *Franck, T. M.,* Recourse to Force: State Action against Threats and Armed Attacks, Cambridge University Press, 2009, 1–2.

[198] *Gray, C.,* International Law and the Use of Force, Oxford University Press, 2004, 6–7.

ზოგადი, როგორც საერთაშორისო ურთიერთობების წარმოების მეთოდის, ომის აკრძალვით.[199]

გაეროს ქარტია აწესებს კოლექტიური თავდაცვის სისტემას და კრძალავს სახელმწიფოს მიერ ძალის ინდივიდუალური მიმართვის შესაძლებლობას (მუხლი 2, ნაწილი 4). ქარტია უშვებს დღესდღეობით მხოლოდ ორ გამონაკლისს: პირველი, ძალის მიმართვა უნდა იყოს ავტორიზებული, გაეროს უშიშროების საბჭოს მიერ, ქარტიის VII თავის საფუძველზე და, მეორე, თავდაცვის უფლება (ქარტიის 51-ე მუხლი).[200] აღნიშნულ გამონაკლისებთან მიმართებით საერთაშორისო სამართლის მკვლევარებს განსხვავებული პოზიციები გააჩნიათ. „ფართო მიდგომის" მიხედვით ძალის გამოყენების აკრძალვა აღიარებს მეტ გამონაკლისს, ისეთებს, როგორებიცაა - პრევენციული თავდაცვა, ჰუმანიტარული ინტერვენცია ან თუნდაც უშიშროების საბჭოს სავალდებულო ავტორიზაცია. „შეზღუდული მიდგომა" კი ემხრობა აკრძალვის ბევრად მკაცრ განმარტებას.[201] „შეზღუდული მიდგომა" პოპულარულია სახელმწიფოებს შორის, რასაც ადასტურებს მათი სამართლებრივი პრაქტიკა.[202] ამ უკანასკნელ პოზიციას იზიარებს სასამართლოც. კერძოდ, *ნიკარაგუა კოლუმბიის* წინააღმდეგ საქმეში.[203] სამი ერთმანეთთან დაკავშირებული ზღვარი არსებობს: 1) მუქარა ან ძალის გამოყენება; 2) შეიარაღებული თავდასხმა: 3) მუქარა მშვიდობას, მშვიდობის დარღვევა და აგრესიის აქტი.[204] ზოგადად, აღიარებულია, რომ სახელმწიფოთა შორის ურთიერთობები მიმდინარეობს აღნიშნული პირობების ფარგლებში.[205] ტერმინი „შეიარაღებული თავდასხმა" უფრო ვიწრო ტერმინია და წარმოადგენს აგრესიის ქვეკატეგორიას, თავად აგრესია კი „ძალის" ქვეკატეგორიაა.[206] თუმცა, არც ერთი ზემოთჩამოთვლილი ტერმინი არ არის განმარტებული გაეროს ქარტიით.

---

[199] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 275; *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012.

[200] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 275.

[201] *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013, 247.

[202] *Corten, O.,* The Controversies over the Customary Prohibition on the Use of Force: A Methodological Debate, European Journal of International Law, 2005, 810–814.

[203] *Territorial and Maritime Dispute* (Nicaragua v. Colombia) ICJ, Judgment, 2012, § 186.

[204] *Okimoto, K.,* The Distinction and Relationship between Jus Ad Bellum and Jus in Bello, Hart, 2011.

[205] *Ruys, T.*, Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 137.

[206] იხ. ქვემოთ, თავი VII.

ზემოაღნიშნული სამი ზღვარი შესაძლებელია, შეჯამდეს შემდეგნაირად: ქარტიის 2(4) მუხლი კრძალავს სახელმწიფოების მიერ მუქარას ან ძალის გამოყენებას. პირველი ზღვარი არის ყველაზე ფართო და დაბალი, რომელსაც აწესებს გაეროს ქარტია. კიბეროპერაციების მიერ ამ ზღვარის მიღწევა, ფაქტობრივად, ნიშნავს კიბერომის გაჩაღებას, *jus contra bellum*-ის ფარგლებში. მეორე ზღვარი გამომდინარეობს გაეროს ქარტიის 51-ე მუხლიდან: შეიარაღებული თავდასხმა ააქტიურებს მსხვერპლი სახელმწიფოს თავდაცვის უფლებას. განსჯის საგანს წარმოადგენს განსხვავება შეიარაღებული თავდასხმისა და ძალის გამოყენების ცნებებს შორის. მეცნიერთა და სახელმწიფოთა ნაწილისთვის აღნიშნული ორივე გაგება ეკვივალენტურია. შედეგის მხრივ, ყველა ძალის გამოყენების შემთხვევა ააქტიურებს სახელმწიფოს თავდაცვის უფლებას.[207] თითქმის ყველა ემხრობა მოსაზრებას, რომ მხოლოდ ყველაზე მძიმე ფორმის ძალის გამოყენება წარმოადგენს შეიარაღებულ თავდასხმას. *ნიკარაგუის საქმეში* სასამართლომ აირჩია მეორე მიდგომა და დაადგინა, რომ ძალის გამოყენების ყველაზე მძიმე ფორმები შეიძლება, დაკვალიფიცირდეს, როგორც შეიარაღებული თავდასხმა.[208] მესამე ზღვარი ეფუძნება გაეროს ქარტიის 39-ე მუხლს, რომლის თანახმადაც, გაეროს უშიშროების საბჭო „განსაზღვრავს მშვიდობისთვის ნებისმიერ დამუქრებას, მშვიდობის ნებისმიერ დარღვევას ან აგრესიის აქტის არსებობას“. გაეროს უშიშროების საბჭოს მთავარი პასუხისმგებლობა საერთაშორისო მშვიდობისა და უსაფრთხოების უზრუნველყოფაა.[209] უშიშროების საბჭო პოლიტიკური და არა სასამართლო ან სამართალდამცავი ორგანოა. აგრესიის განმარტება განისაზღვრა, როგორც ძალის გამოყენების ყველაზე სერიოზული და საფრთხის შემცველი, უკანონო ფორმა.[210] მშვიდობის დარღვევის ან მუქარის გაგება კი პირიქით, არ განიმარტა სამართლებრივად და დარჩა უშიშროების საბჭოს დისკრეციისა და პრაქტიკის იმედად.[211] საბოლოოდ, კიბერომის ზღვარი, რომელსაც აწესებს გაეროს ქარტია,

---

[207] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 47, § 7.

[208] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 191.

[209] გაერთიანებული ერების ქარტია, მუხლი 24, ნაწილი 1.

[210] Definition of Aggression, UNGA Res 3314 (XXIX) (14 December 1974).

[211] *Wood, M.,* Breach of Peace, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009; *de Wet, E.,* Threat to Peace, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009.

მუქარაა ან ძალის გამოყენების ზღვარი, რომელსაც ითვალისწინებს 2(4) მუხლი. მხოლოდ კიბეროპერაციები, რომლებიც აღწევენ ამ ზღვარს, თუ შეიძლება, ასე ითქვას, დაკვალიფიცირდა როგორც მუქარა ან ძალის გამოყენება, როგორც კიბერომი - *jus contra bellum*-ის ფარგლებში.

ვიდრე კიბეროპერაციებსა და *jus contra bellum*-ის უფრო ღრმად გავაანალიზებთ, საჭიროა, წინასწარ დაისვას შეკითხვა: გამოიყენება თუ არა *jus contra bellum* კიბერომის დროს? პასუხი ერთმნიშვნელოვნად დადებითია - დიახ! - თუ კიბერშეტევა თავისი „შედეგებითა და მასშტაბით" გაუტოლდება ძალის გამოყენებას.[212] გაეროს ქარტია მიიღეს დაახლოებით ნახევარი საუკუნით ადრე, ვიდრე საერთოდ განხორციელდებოდა რომელიმე კიბეროპერაცია. შესაბამისად, ქარტიაში არ მოიხსენიება და ვერც აისახა კონკრეტული დებულება კიბეროპერაციების შესახებ. მხოლოდ ქარტიის 41-ე მუხლი არის ზოგადად დაკავშირებული კიბეროპერაციებთან: „...სატელეგრაფო, რადიო ან კავშირგაბმულობის სხვა საშუალებები"... აღნიშნული დებულება საინტერესოა წინამდებარე ნაშრომისთვის, რადგან ის ზუსტად ასახავს იმ დროისთვის კავშირგაბმულობის ქსელების ერთადერთ დანიშნულებას - კომუნიკაციას. 1945 წელს, გაეროს ქარტიის შედგენისას, წინასწარ ვერ გათვლიდნენ კავშირგაბმულობის ქსელების სამხედრო კიბეროპერაციების განსახორციელებლად გამოყენების შესაძლებლობას. კიბეროპერაციებზე კონკრეტული მითითებების ან დებულებების არარსებობა არ ნიშნავს იმას, რომ გაეროს ქარტია არ გამოიყენება კიბეროპერაციებთან დაკავშირებით. გაეროს ქარტიის მუხლები გაწერილია იმგვარად, რომ ტოვებს განმარტების საშუალებას და მოქნილია იმდენად, რომ ადაპტირდეს საერთაშორისო უსაფრთხოების სფეროში გამოვლენილ ახალ განვითარებებთან, მათ შორის, კიბეროპერაციების ევოლუციასთან.[213] ნათელია, რომ ყველა კიბეროპერაცია ვერ დაკვალიფიცირდება, ვერ დააკმაყოფილებს „ძალის" მოთხოვნებსა და სხვა

[212] ამ პოზიციას მხარს უჭერს საერთაშორისო ექსპერტთა უმრავლესობა, რაც აისახა მათ მიერ შემუშავებული „ტალინის პრინციპების" მე-10, მე-11 და მე-12 წესებში. იხ., *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 42-68.

[213] *Waxman, M. C.,* Regulating Resort to Force: Form and Substance of the UN Charter Regime, European Journal of International Law, 24, 2013, 24; *Radziwill Y.,* Cyber-Attacks and the Exploitable Imperfection of International Law, Brill & Martinus Nijhoff Publishers, 2015, 125–126.

ზღვრებს, რომლებსაც ადგენს *jus contra bellum*. აუცილებელია, გაანალიზდეს თითოეული ცალ-ცალკე, რაც წარმოადგენს კიდეც მომდევნო თავის მიზანს.[214]

2. კიბეროპერაციები და ძალის გამოყენების აკრძალვა

მუქარის ან ძალის გამოყენების ზოგადი აკრძალვა ასახულია გაეროს ქარტიის 2(4) მუხლში:

> *„გაერთიანებული ერების ორგანიზაციის ყველა წევრი საერთაშორისო ურთიერთობებში თავს იკავებს ძალის, მუქარის ან მისი გამოყენებისგან, როგორც ნებისმიერი სახელმწიფოს ტერიტორიული ხელშეუხებლობის ან პოლიტიკური დამოუკიდებლობის წინააღმდეგ, ისე გაერთიანებული ერების მიზნებისთვის შეუფერებელი სხვა ნებისმიერი სახით.“*

აღნიშნულ თავში ყურადღება გამახვილდება მხოლოდ ძალის გამოყენების აკრძალვაზე. განხილული მუხლით დაწესებული მეორე აკრძალვა, ძალის გამოყენების მუქარა და გაეროს ქარტიის 2(4) მუხლის მხოლოდ პირველი ნაწილი წარმოდგენილი იქნება შემდეგ თავში.[215] დიდი ხნის განმავლობაში, მკვლევარები დავობდნენ, 2(4) მუხლი ადგენს ზოგად აკრძალვას თუ მისი მეორე ნაწილი ზღუდავს მისი მოქმედების სფეროს.[216] დღეს უკვე არსებობს აკადემიური კონსენსუსი და პრაქტიკაც ამტკიცებს, რომ დაწესებული აკრძალვა მოქმედებს ყველა სახის მუქარაზე ან ძალის გამოყენებაზე სახელმწიფოებს შორის.[217] წინამდებარე ნაშრომშიც ქარტიის 2(4) მუხლი აღქმულია იმგვარად, რომ აწესებს ზოგად აკრძალვას მუქარაზეც და ძალის გამოყენებაზეც.

---

[214] *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002, 84–85.

[215] იხ. ქვემოთ, თავი VI.

[216] *Gray, C.,* International Law and the Use of Force, Oxford University Press, 2004, 30–33.

[217] *Crawford, J.,* Brownlie's Principles of Public International Law, Oxford University Press, 2012, 747. *Randelzhofer A., Dörr O.,* Article 2 (4), The Charter of the United Nations: A Commentary, *Simma B et al (eds),* Oxford University Press, 2012, 208.

2.1. ძალის გამოყენების აკრძალვა

გაეროს ქარტიის 2(4) მუხლი დღესდღეობით უთანაბრდება საერთაშორისო სამართლის პრინციპს ძალის გამოყენების აკრძალვის შესახებ და მისი მნიშვნელობა სცდება გაეროს ქარტიას. არ არის გასაკვირი, რომ აკრძალვა გვხვდება არაერთ ხელშეკრულებაში, მათ შორის ქარტიამდელ, 1928 წელს გაფორმებულ, ბრიან-კელოგის პაქტშიც.[218]

2.1.1. ძალის გამოყენების აკრძალვა და მართლმსაჯულების საერთაშორისო სასამართლო

სასამართლომ საქმეში - *კონგო უგანდის წინააღმდეგ* - ძალის გამოყენების აკრძალვა მოიხსენია, როგორც გაეროს ქარტიის ქვაკუთხედი.[219]

კორფუს არხის საქმე - სასამართლოს მიერ განხილული პირველი საქმე ეხებოდა ძალის გამოყენების საკითხს.[220] მას შემდეგ სასამართლოს პრაქტიკაში იყო რამდენიმე საქმე, რომელიც პირდაპირ ან ირიბად ეხებოდა ძალის გამოყენებას.[221] თუმცა, სასამართლოს მიერ განვითარებული მსჯელობა, ძალის გამოყენების შესახებ, ძირითადად, ეფუძნება სადავო იურისდიქციის ფარგლებში განხილულ ოთხ საქმესა (*კორფუს არხი, ნიკარაგუა, ნავთობის პლატფორმები, კონგო უგანდის წინააღმდეგ*[222]) და ორ საკონსულტაციო დასკვნას (*ბირთვული იარაღისა და კედლის* შესახებ[223]). სასამართლომ ჩამოაყალიბა თანმიმდევრული მიდგომა ძალის გამოყენების

---

[218] *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 101–104.

[219] *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005, § 148.

[220] იხ. *Bannelier K., Christakis T. and Heathcote S. (eds),* The ICJ and the Development of International Law: The Enduring Impact of the Corfu Channel Case, Routledge, 2011.

[221] იხ., ზოგადად *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013.

[222] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* ICJ, Judgment, 1949. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986; *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003; *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005.

[223] *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* ICJ, Advisory Opinion, 2004.

აკრძალვასთან მიმართებით. სახელმწიფოთა პრაქტიკებიც, როგორც წესი, მიჰყვება სასამართლოს მიდგომას.[224] რა თქმა უნდა, არსებობს გამონაკლისები. ზოგ სახელმწიფოს გააჩნია უნიკალური მიდგომა საკითხისადმი, მაგალითად, ამერიკის შეერთებულ შტატებს.[225] წინამდებარე ნაშრომი, მისი მიზნებიდან გამომდინარე, იზიარებს სასამართლოს მიდგომას.

2.1.2. ძალის გამოყენების აკრძალვა და შიდა საქმეებში ჩაურევლობის პრინციპი

ძალის გამოყენების აკრძალვას აძლიერებს მასთან მჭიდროდ დაკავშირებული შიდა საქმეებში ჩაურევლობის პრინციპი, რომლის მიმართ სასამართლოს ჩამოყალიბებული აქვს თანმიმდევრული და მკაცრი მიდგომა.[226] კერძოდ, *ნიკარაგუის* საქმეზე მსჯელობისას სასამართლომ, შესაბამისი სახელმწიფოთა პრაქტიკისა და *opinion juris*-ის გამოკვლევის შედეგად,[227] დაადგინა შიდა საქმეებში ჩაურევლობის პრინციპის ჩვეულებითი ხასიათი.[228]

ნიკარაგუის საქმეში სასამართლომ უარყო შიდა საქმეებში ჩაურევლობის პრინციპის გამონაკლისები, რასაც მანამდე სახელმწიფოები საკუთარი იურისდიქციის ფარგლებს მიაკუთვნებდნენ, მათ შორის, ჰუმანიტარულ ინტერვენციასა[229] და პრო-დემოკრატიულ ან იდეოლოგიურ ინტერვენციას.[230] შიდა საქმეებში ჩაურევლობის პრინციპი განმეორებით განმტკიცდა სხვადასხვა ხელშეკრულებაში[231] და გაეროს

---

[224] *Gray, C.,* International Law and the Use of Force, Oxford University Press, 2004, 31; *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013, 247.

[225] იხ. ზოგადად *Henderson, C.,* The Persistent Advocate and the Use of Force: The Impact of the United States upon the Jus Ad Bellum in the Post-Cold War Era, Ashgate, 2013.

[226] *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013, 248.

[227] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 202–209.

[228] *იქვე* § 202.

[229] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 267–268.

[230] *იქვე* § 263-267.

[231] არაბულ სახელმწიფოთა ლიგის პაქტი (22 მარტი, 1945) 70 UNTS 237, მუხლი 8; ამერიკის სახელმწიფოს ორგანიზაციის ქარტია (ხელმოწერის თარიღი: 30 აპრილი, 1948, ძალაში შესვლის თარიღი - 13 დეკემბერი, 1951), მუხლი 15; აფრიკული გაერთიანების ორგანიზაციის ქარტია (ხელმოწერის თარიღი - 25 მაისი, 1963, ძალაში შესვლის თარიღი - 13 სექტემბერი, 1963) 479 UNTS 70, მუხლი 3; აფრიკული კავშირის საკონსტიტუციო აქტი (11 ივლისი, 2000) 2158 UNTS 3, მუხლი 4(g).

გენერალური ასამბლეის რეზოლუციებში, ისეთებში, როგორებიცაა: სახელმწიფოთა უფლებებისა და მოვალეობების შესახებ დეკლარაციის პროექტი,[232] სახელმწიფოთა შიდა საქმეებში ჩარევის დაუშვებლობის, მათი დამოუკიდებლობისა და სუვერენიტეტის დაცვის შესახებ დეკლარაცია[233], საერთაშორისო სამართლის პრინციპების შესახებ დეკლარაცია, გაეროს წესდების შესაბამისად, სახელმწიფოებს შორის მეგობრული ურთიერთობებისა და თანამშრომლობის შესახებ.[234]

სამხედრო ინტერვენცია, იგივე ინტერვენცია, ძალის გამოყენებით აკრძალულია გაეროს ქარტიის 2(4) მუხლით. ეს ინტერვენციის ერთადერთი ფორმაა, რომელიც აკრძალულია აღნიშნული პრინციპით. ინტერვენციის სხვა ფორმები, ისეთები, როგორებიცაა - დიპლომატიური, პოლიტიკური და ეკონომიკური ინტერვენციები, აკრძალულია შიდა საქმეებში ჩაურევლობის პრინციპით, მაგრამ არა გაეროს ქარტიის 2(4) მუხლით, გამომდინარე იქიდან, რომ არ იგულისხმება ძალის გამოყენება.[235]

2.1.3. ძალის გამოყენების აკრძალვა საერთაშორისო ჩვეულებითი სამართლისა და *jus cogens*-ის ფარგლებში

გაეროს ქარტიის 2(4) მუხლით რეგულირებულ ძალის გამოყენების აკრძალვას გააჩნია ჩვეულებითი სამართლის სტატუსი.[236] ნორმის ეს ორმაგი გამოხატულება სახელშეკრულებო სამართალსა და ჩვეულებით სამართალში გვიბიძგებს შეკითხვისკენ - არის თუ არა იდენტური აღნიშნული ნორმის გაგება ორივე მიმართულებით. *ნიკარაგუის* საქმეში სასამართლომ დაადგინა პარალელები და ურთიერთმიმართება გაეროს ქარტიის 2(4) მუხლით გაწერილი ძალის გამოყენების

[232] სახელმწიფოთა უფლებებისა და მოვალეობების შესახებ დეკლარაციის პროექტი, UNGA Res 375 (IV) (6 დეკემბერი, 1949).
[233] Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UNGA Res 2131 (XX) (21 December 1965).
[234] Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, UNGA Res 2625 (XXV) (24 October 1970).
[235] *Kunig P.,* Intervention, Prohibition of, Max Planck Encyclopedia of Public International Law (MPEPIL), Oxford University Press, 2008, § 22–27; ასევე იხ. *Waxman M. C.,* Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 36, 2011, 428–429.
[236] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 187; ასევე იხ. *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013, 244.

აკრძალვის პრინციპსა და ჩვეულებით საერთაშორისო სამართალს შორის. ორივე წესს გააჩნია მსგავსი შინაარსი. თუმცა, აღნიშნული პარალელი არ ვრცელდება ისეთ გამონაკლისზე, როგორიცაა, მაგალითად, თავდაცვა.[237] ამგვარად, შესაძლებელია ანალოგიური საკითხის მარეგულირებელი ჩვეულებითი და წერილობითი ნორმების თანაარსებობა. მიუხედავად იმისა, რომ ჩვეულებითი და სახელშეკრულებო ნორმა, ფაქტობრივად, იდენტურია, ისინი შესაძლოა, განსხვავებულად განვითარდეს და მათი დატვირთვა და შინაარსიც დროსთან ერთად შეიცვალოს.[238] ძალის გამოყენების აკრძალვა იყო ერთ-ერთი პირველი ნორმა, რომელიც მოხსენიებულ იქნა, როგორც *jus cogens* ნორმა, საერთაშორისო სამართლის კომისიის მიერ, 1966 წელს.[239] დღესდღეობით აღიარებულია, რომ ძალის გამოყენების აკრძალვას აქვს *jus cogens* ხასიათი.[240] მეცნიერთა ნაწილის აზრით, მხოლოდ აგრესიის აკრძალვა შეიძლება აღქმულ იყოს *jus cogens* ნორმად.[241] წინამდებარე ნაშრომის მიზნებიდან გამომდინარე, ძალის გამოყენების აკრძალვა მიჩნეული იქნება, ზოგადად, საერთაშორისო სამართლის იმპერატიულ ნორმად.

როგორც იმპერატიული ნორმა, ძალის გამოყენების აკრძალვა საერთაშორისო სამართლებრივი ნორმების იერარქიაში მაღალ საფეხურზე დგას, ვიდრე სახელშეკრულებო სამართალი ან თუნდაც ჩვეულებითი სამართლის წესები.[242]

---

[237] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 178.

[238] *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 100; ასევე იხ. *D'Amato A.,* Trashing Customary International Law, American Journal of International Law, 101, 1987, 104.

[239] 'Draft Articles on the Law of Treaties with Commentaries' (1966) II Yearbook of the International Law Commission 177, 247, („ძალის გამოყენების შესახებ ქარტიის სამართალი თავისთავად წარმოადგენს საერთაშირისო სამართლის ისეთი წესის თვალშისაცემ მაგალითს, რომელსაც აქვს jus cogens ხასიათი". ICJ-მ მიუთითა ამ ეპიზოდზე *ნიკარაგუის* საქმეში. იხ., *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, §190. სასამართლოს მიერ აღნიშნული ნორმის განმარტების შესახებ იხილეთ *Green J. A.,* Questioning the Peremptory Status of the Prohibition of the Use of Force, Michigan Journal of International Law, 32, 2010, 223–224.

[240] იხ., *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 200–213; *Green J. A.,* Questioning the Peremptory Status of the Prohibition of the Use of Force, Michigan Journal of International Law, 32, 2010, 255; *Gray, C.,* International Law and the Use of Force, Oxford University Press, 2008, 29; *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 105–109; *Crawford, J.,* Brownlie's Principles of Public International Law, Oxford University Press, 2012, 747;

[241] *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 200–201.

[242] *Prosecutor v. Furundžija*, ICTY, Judgment, 1998, Trial Chamber IT-95-17/1-T, 58, § 153.

სახელშეკრულებო ან ჩვეულებითი სამართლის ნორმისთვის დასაშვები გამონაკლისები ვერ იქნება მისაღები იმპერატიული ნორმისთვის.[243]

ძალის გამოყენების აკრძალვა ერთ-ერთი ყველაზე ხელშეუხებელი ნორმაა საერთაშორისო სამართალში და განპირობებულია მისი ორმაგი ბუნების, ჩვეულებითი და *jus cogens* ხასიათის გამო. მნიშვნელოვანია, აღნიშნოს, რომ არ არსებობს საერთაშორისო ხელშეკრულება, რომელიც მკაცრად აკრძალავდა სახელმწიფოების მიერ „კიბერძალის“ გამოყენებას.[244] თუმცა, შეიძლება ითქვას, რომ კიბერძალის გამოყენება აკრძალულია ზოგადი ძალის გამოყენების აკრძალვით, როგორც გაეროს ქარტიის, ისე ჩვეულებითი სამართლის საფუძველზე. რეალურად სახელმწიფოებსა და სამეცნიერო წრეებს პასუხი აქვთ გასაცემი შეკითხვაზე: საჭიროა თუ არა ცალკე ხელშეკრულების შემუშავება კიბერომის თაობაზე? არსებული ვითარება ცხადყოფს, რომ მუქარისა და ძალის გამოყენების აკრძალვის მიზნებისთვის საკმარისია ზოგადი აკრძალვის არსებობა, ისეთის, როგორიც გაწერილია ჩვეულებითი სამართლითა და გაეროს ქარტიის 2(4) მუხლით.[245] ეს ყველაფერი არის შედეგი იმისა, რომ წესი თავის დროზე მიღებულ იქნა ზოგადი და მოქნილი ფორმულირებით, რაც აძლევს საშუალებას, განიცადოს ევოლუცია, თავი გაართვას უსაფრთხოების ახალ გამოწვევებს.[246] ჩვეულებითი სამართლის ნორმის შინაარსი დღემდე არ შეცვლილა ისევე, როგორც - სახელმწიფოთა პრაქტიკა გაეროს ქარტიის მიღების შემდეგ.[247]

---

[243] Commentary to the Draft articles on Responsibility of States for Internationally Wrongful Acts, 2001, 84-85; დეტალური კვლევა იხ. *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 198–248.

[244] იხ,. *Barkham J.,* Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, 34, 2001, 96–97; *Hoisington M.,* Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, International & Comparative Law Review, 32, 2009, 444–446.

[245] ტალინის სახელმძღვანელო პრინციპების შემმუშავებელ ექსპერტთა საერთაშორისო ჯგუფი მხარს უჭერს ანალოგიურ განმარტებას და გაეროს ქარტიის 2(4) მუხლის მოქმედებას ავრცელებს კიბერ სამყაროზე. იხ., *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 42-43.

[246] *Green J. A.,* Questioning the Peremptory Status of the Prohibition of the Use of Force, Michigan Journal of International Law, 32, 2010, 237.

[247] *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013, 245; *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 100.

2.2. კიბეროპერაციები - როგორც აკრძალული ძალის გამოყენების შემთხვევები

ტერმინი - „ძალა“ არ არის განმარტებული გაეროს ქარტიაში, ტერმინი - „ომი“ კი, რომლიც წარმოადგენს კიბეროომის ერთ-ერთ შემადგენელ ელემენტს, ერთადერთი ფორმაა, რომელიც განსაზღვრავს „ძალას“.[248] „ძალის“ გაგება უფრო ფართოა.[249] როგორც იორამ დინშტაინი შენიშნავს, გაეროს ქარტიის 2(4) მუხლში ტერმინს - „ძალა“ - წინ არ უძღვის ზედსართავი „შეიარაღებული“, მაშინ, როდესაც ტერმინი - „შეიარაღებული ძალა“ - გამოყენებულია ქარტიის სხვა ნაწილებში, პრეამბულაში, მუხლებში 41, 46.[250]

ზუსტი განმარტების არარსებობა რეალურ პრობლემად შეიძლება იქნეს მიჩნეული. ცნება რომ შეიქმნას, აუცილებელია მისი ინტერპრეტირება. 1969 წლის ვენის კონვენცია, სახელშეკრულებო სამართლის შესახებ, იძლევა ზოგადი ინტერპრეტაციის წესს, რომელიც გამოყენებულია წინამდებარე ნაშრომშიც. აქედან გამომდინარე, მუქარის ან ძალის გამოყენების აკრძალვა უნდა განიმარტოს კეთილსინდისიერად, ჩვეულებითი მნიშვნელობის, ხელშეკრულების ობიექტისა და მიზნების შესაბამისად.[251] კიბეროპერაციები ახალი ტიპის საფრთხეა საერთაშორისო მშვიდობისთვის, რომელიც ცვლის აკრძალვის კონტექსტს. გაეროს ქარტიის 2(4) მუხლში გამოყენებული ტერმინი - „ძალა“ - საკმაოდ ფართო და მოქნილია საიმისოდ, რომ განმარტებაში მოიცვას კიბეროპერაციებიც.[252]

2.3. აკრძალული ძალა არ შემოიფარგლება „შეიარაღებული ძალით“

ძალის გამოყენება აკრძალულია გაეროს ქარტიით. არ არსებობს კონსენსუსი, აკრძალული ძალის დეფინიციასთან დაკავშირებით. აღნიშნული ტერმინი ჯერ კიდევ განსჯის საგანს წარმოადგენს ლიტერატურაში.[253] მეცნიერთა ერთი ნაწილი მიიჩნევს,

---

[248] Salmon (n 52) 595; *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 51.

[249] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 283.

[250] *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 88.

[251] ვენის კონვენცია სახელშეკრულებო სამართლის შესახებ (ხელმოწერის თარიღი: 23 მაისი, 1969, ძალაში შესვლის თარიღი: 27 იანვარი, 1980) 1155 UNTS 331.

[252] *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002, 84.

[253] *Crawford, J.,* Brownlie's Principles of Public International Law, Oxford University Press, 2012, 747.

რომ აკრძალულ ძალაში უნდა იგულისხმებოდეს შეიარაღებული ძალა,[254] მეორე ნაწილი კი, უპირატესობას ანიჭებს ცნების ფართო შინაარსს და თვლის, რომ ტერმინი სცდება შეიარაღებული ძალის ფარგლებს.[255] სასამართლომ *ბირთვული იარაღის შესახებ* საკონსულტაციო დასკვნაში აღნიშნა, რომ აკრძალვა ეხება ნებისმიერი სახის ძალის გამოყენებას, მიუხედავად იმისა, იქნა თუ არა გამოყენებული იარაღი.[256] აქედან გამომდინარე, შეგვიძლია მივიჩნიოთ, რომ სასამართლო მხარს უჭერს ცნების ფართო გაგებას და არ ზღუდავს მას მხოლოდ შეიარაღებული ძალის ფარგლებით.

ზემოაღნიშნულის მიუხედავად, ნათელია, რომ ძალის გაგება არ მოიცავს „ნებისმიერი სახის ძალას".[257] სან-ფრანცისკოს კონფერენციაზე, გაეროს ქარტიის ტექსტზე მუშაობის დროს, მხარეებმა უარყვეს ძალის გარკვეული ფორმების ტექსტში ასახვა. გაეროს ქარტიის მიღების წინაპირობები ცხადყოფს, რომ 2(4) მუხლით გათვალისწინებული ძალის გამოყენების აკრძალვა არ მოიცავს ეკონომიკურ, პოლიტიკურ და არაპირდაპირ ძალას.[258] გამომდინარე აქედან, ეკონომიკური ან პოლიტიკური ძალის გამოყენება არ არღვევს ქარტიის 2(4) მუხლს. თუმცა, შესაძლოა, არღვევდეს საერთაშორისო სამართლის სხვა პრინციპებს, მაგალითად, შიდა საქმეებში

---

[254] *Ruys T.,* The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, American Journal of International Law, 108, 2014, 163; *Brunnée J.,* The Meaning of Armed Conflict and the Jus ad Bellum, Martinus Nijhoff Publishers, 2012, 32; *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge University Press, 2012, 40–49.

[255] *Crawford, J.,* Brownlie's Principles of Public International Law, Oxford University Press, 2012, 747; *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 52; *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 88.

[256] *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, § 39 („აღნიშნული დებულებები არ ეხება კონკრეტულ იარაღს. ითვალისწინებს ძალის გამოყენებას, მიუხედავად იმისა, რა ტიპის იარაღი იქნა გამოყენებული. გაეროს ქარტია ხაზგასმით არ კრძალავს და არც ნებას რთავს ნებისმიერი სახის იარაღის გამოყენებას, მათ შორის, არც ბირთვული იარაღის. იარაღი, რომელიც უკანონოა, კონკრეტული ხელშეკრულებისა თუ ჩვეულების თანახმად, ვერ გახდება კანონიერი, თუნდაც ემსახურებოდეს, გაეროს ქარტის შესაბამის, კანონიერ მიზანს.").

[257] *Kelsen H.,* Collective Security under International Law, International Law Studies, Naval War College and The Lawbook Exchange, 2001, 57.

[258] ბრაზილიამ მხარეებს შესთავაზა, მე-2 მუხლის მე-4 ნაწილის აკრძალვა დაეწესებინა ორგანიზაციის წევრ-სახელმწიფოს ნებისმიერ საშინაო და საგარეო საქმეში ჩარევაზე, იხ., Brazilian Comment on Dumbarton Oaks Proposals: Memorandum of Brazilian Acting Minister for Foreign Affairs to American Charge d'Affaires, November 4, 1944, (1945) 3 Documents of the United Nations Conference on International Organization 232, 237. ბრაზილიამ მხარეებს ასევე შესთავაზა, გათვალისწინებული ყოფილიყო ეკონომიკური ზომების გამოყენება ან მუქარა, *იქვე,* 558–559. თუმცა, საბოლოოდ, ეკონომიკური, პოლიტიკური და სხვა არაპირდაპირი ძალის აკრძალვა არ მოექცა 2(4) მუხლის ფარგლებში. იხ., *Randelzhofer A., Dörr O.,* Article 2 (4), The Charter of the United Nations: A Commentar, *Simma B et al (eds),* Oxford University Press, 2012, 208–212.

ჩაურევლობის პრინციპს ან ეკონომიკურ უფლებებს.[259] არაპირდაპირი ძალა - მათ შორის სახელმწიფოს ჩართულობა სხვა სახელმწიფოს მიერ ძალის გამოყენების აქტში ან სახელმწიფოს მხარდაჭერა და არასახელმწიფო აქტორების კონტროლი, როგორც ჩანს, მოცულია ძალის გამოყენების აკრძალვაში.[260]

ცალკე საკითხია, მოიცავს თუ არა ძალის გამოყენების აკრძალვა იძულებას, ყველა თანმდევი გამოვლინებით? განვითარებული და განვითარებადი სახელმწიფოების ხელისუფალთა აზრი აღნიშნულ საკითხთან მიმართებით იყოფა. ეს უკანასკნელნი მხარს უჭერენ ფართო ინტერპრეტაციის გამოყენებას.[261] რეალურად საკითხი დგას შემდეგნაირად, სად გადის ზღვარი ძალის გამოყენების აკრძალვის მიერ მოცულ იძულების ფორმებზე, ანუ რომელ ფორმას მოიცავს ცნება და რომელს - არა. აშკარაა, რომ ყველა ფორმის იძულებას ცნება არ ფარავს, მაგალითად, ეკონომიკური ან დიპლომატიური იძულება აღნიშნული ცნების მიღმა რჩება.

ახალი ტექნოლოგიების განვითარება ბევრად ართულებს იმის განსაზღვრას, რა წარმოადგენს „იარაღს“. ისეთი ტიპის იარაღის შექმნა, რომელსაც არ ახლავს „აფეთქების ეფექტი“, თუნდაც ისეთი, როგორებიცაა: ქიმიური, ბაქტერიოლოგიური, ბიოლოგიური იარაღი, კითხვის ნიშნის ქვეშ აყენებდა ტრადიციული განმარტების სრულყოფილებას. კიბეროპერაციები მოქცეულია შეიარაღებული ძალის კატეგორიაში და, აქედან გამომდინარე, მათი, როგორც იარაღის გამოყენება, გამოწვევას წარმოადგენს ცნების ტრადიციული გაგების მიმართ.[262]

იან ბრაუნლიმ შეიმუშავა ჩარჩო იმის დასადგენად, არღვევს თუ არა აღნიშნული იარაღის გამოყენება ძალის გამოყენების აკრძალვას:

„შეიძლება ითქვას, რომ აღნიშნული იარაღის გამოყენება შესაძლებელია, გაიგივდეს ძალის გამოყენებასთან ორი საფუძვლით.

---

[259] მაგ., Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations, UNGA Res 2625 (XXV) (24 October 1970). იხ., ზოგადად, *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds)*, Edward Elgar Publishing, 2013, 101.

[260] *Randelzhofer A., Dörr O.,* Article 2 (4), The Charter of the United Nations: A Commentar, *Simma B et al (eds),* Oxford University Press, 2012, 211–212.

[261] *Waxman M. C.,* Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 36, 2011, 428–429; *Gray, C.,* International Law and the Use of Force, Oxford University Press, 2004, 30.

[262] *Randelzhofer A., Dörr O.,* Article 2 (4), The Charter of the United Nations: A Commentar, *Simma B et al (eds),* Oxford University Press, 2012, 210.

პირველ რიგში, იარაღის მსხვერპლი მათ მოიხსენიებს, როგორც „იარაღს“ და „ომის“ წარმოების მეთოდს. უფრო ყურადსაღები მეორე საფუძველია, მიზანი, თუ რისთვის იყენებენ ამ იარაღს, ეს არის სიცოცხლისა და საკუთრების მოსპობა. მათ ხშირად მოიხსენიებენ „მასობრივი განადგურების იარაღად“.[263]

იან ბრაუნლის მიერ შემოთავაზებული განმარტების ორივე ნაწილი შეიძლება, მიესადაგოს კიბეროპერაციებს: პირველი, მათი გამოყენება, უმეტეს შემთხვევაში, მოხსენიებულია, როგორც „კიბერომი“ ან „საინფორმაციო ომი“; და მეორე, მათი გამოყენება შესაძლებელია, სიცოცხლისა და საკუთრების მოსპობის მიზნით.[264] თუ ბრაუნლის დეფინიციას მოვარგებთ კიბეროპერაციებს, მაშინ დავინახავთ, რომ აღნიშნული განმარტება ხაზს უსვამს ძალის „შეიარაღებულად“ ან „მილიტარიზებულად“ კვალიფიცირების კრიტერიუმთა შეუსაბამობას, განსაკუთრებით იმის გათვალისწინებით, რომ დღესდღეობით არსებული „ძალის“ რამდენიმე ფორმა არ ექცევა იარაღის ტრადიციული მახასიათებლების განმარტებაში.

შეჯამების სახით შეიძლება ითქვას, რომ დღეს აღარ იქნება მართებული ძალის გამოყენების ან მუქარის აკრძალვა შეიარაღებული თავდასხმით. უფრო მეტიც, კიბეროპერაციები შესაძლებელია, წარმოადგენდეს შეიარაღებული ოპერაციების ერთ-ერთ სახეობას და ამაზე დამატებითი დავა საჭიროებას მოკლებულია. შესაბამისად, კიბეროპერაციები შესაძლებელია, განხილულ იქნეს გაეროს ქარტიის 2(4) მუხლით დადგენილი ძალის გამოყენების აკრძალვის კონტექსტში.

3. კიბერძალასთან დაკავშირებული მიდგომები

როდესაც საქმე ეხება კიბეროპერაციების ძალის გამოყენებად დაკვალიფიცირებას, არ გვაქვს სახელმწიფოთა შეჯერებული პრაქტიკა. სახელმწიფოთა პოზიციები მუდმივად იცვლება და გამოაქვთ განსხვავებული დასკვნები. წინამდებარე ქვეთავში

[263] *Brownlie I.,* International Law and the Use of Force by States, Oxford University Press, 1963, 362.

[264] *Roscini M.,* World Wide Warfare - Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, 14, 2010, 106; *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge University Press, 2012, 58.

განხილული იქნება ამჟამად არსებული სხვადასხვა მიდგომა, რათა განისაზღვროს კიბერძალის დახასიათებისთვის ყველაზე შესაფერისი და ზუსტი გზები.

ფაქტობრივად, ყველა, ვინც საკუთარ პოზიციას გამოთქვამს, ამყარებს ამჟამად ძალის გამოყენების მიმართ არსებული სამართლებრივი ჩარჩოთი. აღნიშნული მიდგომებიდან შესაძლებელია სამის გამოყოფა: მიზნობრივი, ინსტრუმენტული, შედეგობრივი.[265] როგორც ირკვევა, მიზნობრივ და ინსტრუმენტულ მიდგომებთან შედარებით, შედეგობრივი მიდგომა სარგებლობს ყველაზე მეტი პოპულარობით.

3.1. მიზნობრივი მიდგომა

მიზნობრივი მიდგომა ფოკუსირებულია კიბეროპერაციის მიზანზე და ამ უკანასკნელს ძალის გამოყენებად აკვალიფიცირებს, ეროვნულ კრიტიკული ინფრასტრუქტურის სისტემებში შეღწევის შემთხვევაში. აღნიშნული მიდგომა ძირითად განვითარებას პოულობს თავდაცვის პირობებში. მისი ამოსავალია მოსაზრება, რომ ძალის გამოყენების აკრძალვის სამართლებრივი ჩარჩო საკმარისად არ იცავს სამიზნე სახელმწიფოს. აღნიშნული მიდგომის მომხრეთა აზრით, კრიტიკულ ინფრასტრუქტურაზე თავდასხმის შემთხვევაში, სახელმწიფოს მოუწევს ძალის გამოყენება, როგორც საკუთარი თავის დახმარების ზომა. შესაბამისად, მსგავსი მიდგომა ინკლუზიურია და კიბეროპერაციებს აკვალიფიცირებს მხოლოდ მისი მიზნის გათვალისწინებით, განურჩევლად ინტენსივობისა თუ მახასიათებლებისა.[266] ზემოაღნიშნულიდან გამომდინარე, არ იქნება გამართლებული, მიზნობრივი მიდგომის გამოყენება კიბეროპერაციის ძალის გამოყენებად დაკვალიფიცირებისას. თუმცა, რელევანტურია, ვინაიდან სამიზნე ინფრასტრუქტურა ყოველთვის გასათვალისწინებელია კიბეროპერაციების სიმძიმისა და შედეგების შეფასებისას.

---

[265] იხ. ზოგადად: *Nguyen R.,* Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, 2013, 1117–1129; *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002, 86–92.

[266] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 54; *Radziwill Y.,* Cyber-Attacks and the Exploitable Imperfection of International Law, Brill & Martinus Nijhoff Publishers, 2015, 138.

3.2. ინსტრუმენტზე დაფუძნებული მიდგომა

ინსტრუმენტზე დაფუძნებული ანუ ინსტრუმენტული მიდგომა ფოკუსირებულია თავდასხმის ვექტორზე. ამ მიდგომის თანახმად, კიბეროპერაციების უმრავლესობა არ დაკვალიფიცირდება ძალის გამოყენებად. მათი დახასიათება, როგორც შეიარაღებული ან იარაღით აღჭურვილი შეტევა, ფაქტობრივად, შეუძლებელია. აღნიშნულ მიდგომას კიდევ უფრო პრობლემატურს ქმნის კიბერშეტევებისა და ტრადიციულ იარაღს შორის მსგავსების აღმოჩენის აუცილებლობა, რომლის გამოძებნაც რთული და, უმეტესწილად, შეუძლებელიც კია.[267]

ინსტრუმენტული მიდგომა გაცილებით ეფექტიანი იყო წარსულში. თუმცა, ახალი ტექნოლოგიებისა და ომის წარმოების საშუალებათა განვითარებასთან ერთად, დაკარგა ეფექტიანობა. უფრო მეტიც, კიბეროპერაციების შემთხვევაში, ფაქტობრივად, შეუძლებელია კლასიფიცირება, რომელი პროგრამა წარმოადგენს იარაღს და რომელს გააჩნია რამდენიმე სახის დატვირთვა, რაც, საბოლოო ჯამში, ინსტრუმენტზე დაფუძნებულ მიდგომას მოძველებულად განიხილავს.

3.3. შედეგზე დაფუძნებული მიდგომა

შედეგზე დაფუძნებული ანუ შედეგობრივი მიდგომა ფოკუსირებულია კიბეროპერაციების საბოლოო შედეგზე (ვირტუალური შედეგი, ფიზიკური განადგურება ან სიკვდილი). კიბეროპერაციები, რომლებსაც შედეგად მოჰყვება ფიზიკური განადგურება ან სიცოცხლის მოსპობა, ფაქტობრივად, ყოველთვის დაკვალიფიცირდება, როგორც ძალის გამოყენება. თუმცა, არაფიზიკური შედეგების არსებობისას საბოლოო კვალიფიკაციის მინიჭება რთულია. აღნიშნულ მიდგომას იყენებს ამერიკის შეერთებული შტატები, მასვე ემხრობა მეცნიერთა უმრავლესობა.[268] მართლაც, შედეგობრივი მიდგომა ყველა დანარჩენზე უკეთ იძლევა შეფასების

[267] *Hathaway O. A., et al*, The Law of Cyber-Attack, California Law Review, 2012, 846; *Nguyen R.,* Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, 2013, 1117–1119.

[268] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 54.

საშუალებას - აკმაყოფილებს თუ არა კიბეროპერაციები გაეროს ქარტიის 2(4) მუხლის მოთხოვნებს.

მარკო როსინიმ წარმოადგინა განსხვავებული ხედვა, რომელიც გულისხმობს ინსტრუმენტზე დაფუძნებული და შედეგობრივი მიდგომების ინტეგრირებას.[269] როსინის აზრით, შედეგის უპირობო მნიშვნელობის მიუხედავად, შეუძლებელია გამოყენებული ინსტრუმენტის უგულებელყოფა. მარტივად რომ ითქვას, ეს არის მიზნობრივისა და ინსტრუმენტულის ელემენტებით გაძლიერებული შედეგობრივი მიდგომა.

ნებისმიერი მიდგომა დაფუძნებულია ამჟამად არსებულ სამართლებრივ ჩარჩოზე, რომელიც არეგულირებს ძალის გამოყენების აკრძალვას. არსებობს მოსაზრება, რომ არსებული სამართლებრივი რეგულაციების მორგების ნაცვლად, უმჯობესი იქნება, თუ სპეციალურად კიბეროპერაციებზე მორგებული სამართლებრივი დოკუმენტები შემუშავდება.[270] შესაძლოა, ახალი სამართლებრივი რეგულაციების შექმნა გაეროს ქარტიის გაუთვალისწინებლად მიმზიდველად ჩანდეს. თუმცა, არსებობს დამარწმუნებელი მიზეზები არსებული სამართლებრივი ბაზის განვითარებისთვის. პირველი, გაეროს ქარტია გვთავაზობს საკმაოდ მოქნილ სამართლებრივ ბაზას. უკიდურესად გართულდება სახელმწიფოების მხრივ ახალი ბაზის შემუშავებისას კონსენსუსის მიღწევა, კონკრეტულ ნორმებთან დაკავშირებით. მეორეც, გაეროს ქარტიის ფარგლებში, შედეგობრივი მიდგომის გამოყენებით, რომელსაც ავსებს დანარჩენი ორი მიდგომის ელემენტები, წარმოადგენს ყველაზე შესაბამის მიდგომას. განსხვავებული ბუნებისა და გამოწვეული ეფექტების გამო, თითოეული კიბეროპერაცია უნდა განიხილოს ცალ-ცალკე.[271]

4. იძულებითი კიბერაქტივობის სიმძიმე ან სიმწვავე

ძალიან რთულია ზღვრის გავლება კიბეროპერაციების ძალის გამოყენებად დაკვალიფიცირებისას. ზღვარი უნდა დადგინდეს ყოველ კონკრეტულ შემთხვევაში,

[269] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 50.
[270] *Hollis D. B.,* New Tools, New Rules: International Law and Information Operations, 2008, 8.
[271] *Radziwill Y.,* Cyber-Attacks and the Exploitable Imperfection of International Law, Brill & Martinus Nijhoff Publishers, 2015, 139.

თითოეულისთვის დამახასიათებელ სხვადასხვა კრიტერიუმსა და მტკიცებულებაზე დაყრდნობით. დღემდე არც ერთი კიბეროპერაციის გამოვლენა არ დაკვალიფიცირებულა ძალის გამოყენებად. სახელმწიფოთა ძალიან მწირი პრაქტიკის გამო, წინამდებარე ნაშრომი ეფუძნება საერთაშორისო სამართლებრივ რეგულაციებს და სახელმწიფოთა პრაქტიკას.[272] ჯერ ისევ არ არსებობს საერთაშორისო კონსენსუსი კიბერძალის გამოყენების განმარტებასა და კვალიფიკაციაზე. მნიშვნელოვანია, კარგად იქნეს გააზრებული ის მოცემულობა, რომ კიბეროპერაციებისთვის დამახასიათებელ სპეციფიკურ მახასიათებელთა გამო, ნებისმიერი მცდელობა *jus contra bellum*-ის ფარგლებში მოქცევისა, იქნება მწვავე დებატების საბაბი.[273]

სიმძიმისა და სიმწვავის ზღვარი ცნობილია შეიარაღებული თავდასხმისა და აგრესიისთვის. ერთი მხრივ, სასამართლო შეიარაღებულ თავდასხმას მიიჩნევს თავდასხმის უმძიმეს ფორმად,[274] მეორე მხრივ, გაეროს გენერალური ასამბლეის რეზოლუცია 3314 აკვალიფიცირებს აგრესიად, უკანონო ძალის გამოყენების ყველაზე სერიოზულ და საშიშ ფორმად.[275]

არც გაეროს ქარტია და არც სასამართლო არ ადგენს ზღვარს აკრძალული ძალის სიმძიმისთვის. თუმცა, ეს ფაქტი არ გამორიცხავს ამ ზღვრის არსებობას. წინამდებარე ქვეთავის მიზანია, სახელმწიფოთა პრაქტიკის ანალიზის მეშვეობით განისაზღვროს ძალის გამოყენების სიმძიმის ზღვარი და გააანალიზდეს, მოერგება თუ არა აღნიშნული კიბეროპერაციებსაც.

4.1. აკრძალული ძალის გამოყენების სიმძიმის ზღვარი

გაეროს ქარტიის მიღების შემდეგ მეცნიერთა ნაწილმა აღიარა, რომ სახელმწიფოთა პრაქტიკაში რეალურად არსებობს სიმძიმის ზღვარი.[276] ამგვარი ზღვრის არსებობას

---

[272] *Schmitt M.N.,* Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, 2011, 575.

[273] *Waxman M. C.,* Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 36, 2011, 443.

[274] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US),* Merits, ICJ, Judgment, 27 June 1986, § 191.

[275] Definition of Aggression, UNGA Res 3314 (XXIX) (14 დეკემბერი1974).

[276] ოლივერ კორტენის აზრით, სახელმწიფოების მიერ განხორციელებული ყველა ტრანსნაციონალური იძულებითი აქტი არ მოექცევა ძალის გამოყენების აკრძალვის ფარგლებში. აქედან გამომდინარე, შემოიტანა ორი კრიტერიუმი 2(4) - მუხლის ზღვრის დასადგენად. პირველი, „ძალისმიერი აქტის

ადასტურებს რამდენიმე მაგალითი, რომელთა მიხედვით, დაბალი ინტენსივობის ძალის გამოყენება არ დაკვალიფიცირებულა სახელმწიფოს მიერ ძალის გამოყენებად. დოქტრინალური არგუმენტი იქნა შემოთავაზებული საქართველოსთვის, კონფლიქტის ფაქტების მომძიებელი საერთაშორისო კომისიის მიერ, რომელმაც განაცხადა, რომ ძალის გამოყენების აკრძალვა ფარავს ყველა სახის ფიზიკურ ძალას, რომელიც სცდება ინტენსივობის მინიმალურ ზღვარს.[277] მკვლევართა ნაწილი საწინააღმდეგო პოზიციას გამოთქვამს და აცხადებს, რომ არ არსებობს ე.წ. კონკრეტული ზღვარი, ასევე გამორიცხავს „მინიმალური ძალის გამოყენების“ ცნების არსებობას გაეროს ქარტიის 2(4) მუხლის ფარგლებში.[278] ესკალაციის თავიდან აცილების, სახელმწიფოებს შორის მეგობრულ ურთიერთობათა განვითარების სურვილი შეიძლება იყოს ახსნა იმისა, დაბალი ინტენსივობის ძალა რატომ არ კვალიფიცირდება ძალის გამოყენების აკრძალვად.[279]

მცირე მასშტაბის ძალის გამოყენება მოიცავს ისეთ ინციდენტებს, როგორებიცაა - კონკრეტულ პირთა მიზანმიმართული მკვლელობები, საზღვარგარეთ საკუთარი მოქალაქეების გადარჩენის ოპერაციები, ასევე საზღვარგარეთ განხორციელებული მცირე მასშტაბის კონტრტერორისტული ოპერაციები, საპოლიციო ოპერაციები, ცხელ კვალზე დევნის ოპერაციები და სასაზღვრო შეტაკებები.[280]

სასამართლოს პირდაპირ არასდროს დაუწესებია სიმძიმის ზღვარი ქარტიის 2(4) მუხლისთვის. მიუხედავად ამისა, მტკიცება იმისა, რომ მინიმალური სიმძიმის ზღვარი რეალურად არსებობს, შეგვიძლია დავასკვნათ რამდენიმე საქმიდან გამომდინარე. *კორფუს არხის* საქმეში სასამართლომ დაადგინა, რომ, მართალია, ბრიტანეთის სამხედრო ხომალდებმა ალბანეთის წყლებში დაარღვიეს ალბანეთის სუვერენიტეტი, მაგრამ ამ ფაქტს არ ჰქონია მუქარის ან ძალის გამოყენების აკრძალვის

სიმძიმეა“, მეორე - „სახელმწიფოს განზრახვა გამოიყენოს ძალა მეორე სახელმწიფოს წინააღმდეგ“. იხ., *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 52–92.

[277] Report of the International Fact-Finding Commission on the Conflict in Georgia, vol II, 2009, 242.

[278] მაგალითად იხ., *Ruys T.,* The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, American Journal of International Law, 108, 2014; ასევე იხ. *de Hoogh A.,* Georgia's Short-Lived Military Excursion into South Ossetia: The Use of Armed Force and Self-Defence EJIL: Talk!, 9 დეკემბერი 2009 <https://www.ejiltalk.org/georgia%E2%80%99s-short-lived-military-excursion-into-south-ossetia-the-use-of-armed-force-and-self-defence/> [30.05.2020].

[279] *Ruys T.,* The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, American Journal of International Law 159, 2014, 169–170.

[280] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 292.

დარღვევის ხასიათი.[281] ზოგი მკვლევარი სასამართლოს ამ მიდგომას იყენებს არგუმენტად, როდესაც ამტკიცებს სიმძიმის ზღვრის არსებობას.[282]

სასამართლოს წინაშე წარდგენილ სხვა საქმეებშიც იქნებოდა მტკიცებულებები ამგვარი ზღვრის არსებობის შესახებ, თუმცა, როგორც ზემოთ აღინიშნა, ამგვარი საქმეების უმეტესობა კონცენტრირებულია თავდაცვის უფლებაზე (ქარტიის 51-ე მუხლი), რაც, თავის მხრივ, ართულებს აღნიშნულ საქმეებზე სიმძიმის ზღვრის გაეროს ქარტიის 2(4) მუხლზე გავრცელებას.[283] საზღვაო სამართლის არსებული საქმეები მეტ-ნაკლებად უჭერს მხარს ამგვარ ზღვარს. ამ საქმეებში უცხოური ხომალდების წინააღმდეგ მინიმალური ძალის გამოყენების შემთხვევები სასამართლოს მიერ არ დაკვალიფიცირებულა ძალის გამოყენებად.[284]

თუ ყველა საქმეს განვიხილავთ ინდივიდუალურად, მაშინ კიდევ უფრო გართულდება სიმძიმის ზღვრის არსებობის დადგენა, მაგრამ, თუ მათ განვიხილავთ ერთიანობაში, გვექნება საკმარისი საფუძველი პოზიციის გასამყარებლად. მკვლევართა ნაწილის აზრით, სიმძიმის ზღვრის არსებობის დამადასტურებელი არგუმენტების მოძიება შესაძლებელია სასამართლოს იურისდიქციის მიღმა.[285]

---

[281] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* ICJ, Judgment, 1949, 35.

[282] *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 69–70; *Ruys T.,* The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, American Journal of International Law, 108, 2014, 166–167.

[283] კომენტატორები ძირითადად ეყრდნობიან შემდეგ საქმეებს: *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986; *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003; *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* ICJ, Advisory Opinion, 2004; *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005. მაგალითად იხ. *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds),* Edward Elgar Publishing, 2013, 102–105.

[284] იხ., *Fisheries Jurisdiction* (United Kingdom of Great Britain and Northern Ireland v. Iceland), ICJ, Judgment on the Merits, 1974, ICJ; *Fisheries Jurisdiction (Federal Republic of Germany v. Iceland)* (Judgment on the Merits) [1974] ICJ. *თევზჭერის იურისდიქციის* (Fisheries Jurisdiction) საქმე ეხებოდა კანადის დროშის ქვეშ მცურავი ხომალდის მიერ ესპანეთის დროშის ქვეშ მცურავი ხომალდის მიმართ მინიმალური ძალის გამოყენებას. ესპანეთის მხარე ითხოვდა აღნიშნული ქმედების ძალის გამოყენებად დაკვალიფიცირებას, თუმცა, სასამართლომ თავი არაკომპეტენტურად გამოაცხადა და თავი აარიდა საქმის განხილვას: *Fisheries Jurisdiction (Spain v. Canada) (Judgment on the jurisdiction of the Court)* [1998] ICJ, 467, § 87.

[285] ზოგადად იხ., *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 52–92; *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds),* Edward Elgar Publishing, 2013, 102–107.

მერი ელენ ოკონელი, რომელიც მხარს უჭერს სიმძიმის მინიმალური ზღვრის არსებობას, ძალის გამოყენების აკრძალვისთვის, მიიჩნევს, რომ კიბერსივრცე კიდევ ერთი სფეროა, სადაც მეცნიერები ცდილობენ, ერთმანეთს გაუთანაბრონ დანაშაული და შეიარაღებული თავდასხმა, თავდაცვის უფლების გააქტიურების მიზნით და გაეროს ქარტიის 51-ე მუხლით მოქმედებისთვის. ინტერნეტი წარმოადგენს კომუნიკაციებისა და კომერციის სფეროს. კიბერუსაფრთხოების გაძლიერებამ შესაძლოა დახმარება გაუწიოს პოლიციას, მაგრამ არა სამხედროებს.[286]

სახელმწიფოების მიერ დაფინანსებული კიბეროპერაციები უნდა განცალკევდეს არასახელმწიფო დაფინანსებით განხორციელებულთაგან. მხოლოდ სახელმწიფოს მიერ დაფინანსებული კიბერშეტევები ექცევა 2(4) მუხლის მოქმედების სფეროში, სხვა დანარჩენი - სისხლის სამართლის იურისდიქციაში. თუმცა, სახელმწიფოთა მიერ ან მათი ეფექტური კონტროლით განხორციელებული კიბეროპერაციების მხოლოდ ის ნაწილი დაკვალიფიცირდება ძალის გამოყენებად, რომელიც გადალახავს 2(4) მუხლით დადგენილ ზღვარს.

4.2. კიბეროპერაციები და სიმძიმის ზღვარი

კიბეროპერაციები მრავალფეროვანი კატეგორიაა განსხვავებული შეფასების შკალითა და სავარაუდო შედეგებით, რომლებიც, შესაძლოა, მოიცავდეს მონაცემთა განადგურებას, ზიანს, სიცოცხლის მოსპობას. ზოგიერთი ავტორი სიმძიმის ზღვარს აფასებს სიმწვავის კრიტერიუმით. უფრო ზუსტად კი, ერთი სახელმწიფოს მიერ მეორის წინააღმდეგ დაწყებულმა კიბეროპერაციამ უნდა მიაღწიოს გარკვეულ ზღვარს, რათა დაკვალიფიცირდეს ძალის გამოყენებად.

სიმწვავის კრიტერიუმი ერთ-ერთია რვა ნორმატიული ჩარჩოს კრიტერიუმიდან, რომელიც 1999 წელს იქნა შემოთავაზებული, მაიკლ შმიტის მიერ.[287] აღნიშნული

[286] *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds),* Edward Elgar Publishing, 2013, 107.

[287] აღნიშნულ სტატიაში მაიკლ შმიტი გვთავაზობს ტრადიციულ ინსტრუმენტს, შედეგზე დაფუძნებულ მიდგომებსა და „ნორმატიულ ჩარჩოს", რომელიც განსაზღვრავს, კიბეროპერაცია აკმაყოფილებს თუ არა შეიარაღებული ძალის პოლიტიკური და ეკონომიკური ძალისგან განსხვავების კრიტერიუმებს. მკაფიო ზღვრის არარსებობის გამო აღნიშნული „სამართლებრივი ჩარჩო" ემყარება ექვს კრიტერიუმს: 1)

კრიტერიუმები განიხილა და შეისწავლა ტალინის პრინციპების შემმუშავებელმა ექსპერტთა ჯგუფმა, შმიტის ხელმძღვანელობით.[288] აღნიშნული ნორმატიული ჩარჩო მრავალჯერ იქნა კომენტირებული და გაკრიტიკებული.[289]

შმიტის მიერ შემუშავებული სიმწვავის კრიტერიუმი ძირითადად დაფუძნებულია კიბეროპერაციის შედეგებისა და შეიარაღებული იძულებით გამოწვეული შედეგების შედარებაზე. ამ გადმოსახედიდან, ტალინის პრინციპები 2.0 ადგენს, რომ *de minimis* წესის საგანია შედეგები, რომლებიც მოიცავს ფიზიკურ ზიანს ფიზიკური პირების ან საკუთრების მიმართ და აქტს აკვალიფიცირებს ძალის გამოყენებად.[290]

„სიმწვავე", 2) „იმწუთიერობა", 3) „პირდაპირობა", 4) „შემტევი ხასიათი", 5) „გაზომვადობა", 6) „კანონიერების პრეზუმფცია". იხ., *Schmitt M. N.,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1999, 914–915.

[288] *Schmitt M. N., Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 333–337. შმიტის მიერ შემუშავებული „ნორმატიული ჩარჩოს" იერარქია ჩამოყალიბდა შემდეგნაირად: 1) „სიმწვავე" - პირველი კრიტერიუმი ფოკუსირებულია შედეგებზე და აფასებს დაზიანების ან ტრავმის ხარისხს; ყველაზე მწვავე კიბეროპერაციები, რომელთაც შედეგად მოჰყვება დაზიანება, განადგურება, ტრავმა ან სიცოცხლის მოსპობა, დიდი ალბათობით დაკვალიფიცირდება ძალის გამოყენებად; 2) „იმწუთიერობა" - ხანგრძლივობა კიბეროპერაციების განხორციელებასა და მათი შედეგების დადგომას შორის. რაც უფრო მცირეა დრო კიბეროპერაციასა და მის შედეგს შორის, მით მეტია შესაძლებლობა, დაკვალიფიცირდეს ძალის გამოყენებად. 3) „პირდაპირობა" - ეს კრიტერიუმი აფასებს მიზეზობრივ კავშირს კიბეროპერაციასა და დამდგარ შედეგს შორის. რაც უფრო მკაფიოა კავშირი, მით მეტია შესაძლებლობა, კიბეროპერაციას მიენიჭოს ძალის გამოყენების კვალიფიკაცია; 4) „შემტევი ხასიათი" - აღნიშნული კრიტერიუმი აფასებს სამიზნე სახელმწიფოს სუვერენიტეტის დარღვევას ან შეჭრის ხარისხს. რაც უფრო შემტევი ხასიათი გააჩნია კიბეროპერაციას, მით მარტივია მისი დაკვალიფიცირება ძალის გამოყენებად; 5) „შედეგების გაზომვადობა" - გამოიყენება კიბეროპერაციის შედეგების გაზომვისთვის, რამდენად განჭვრეტადია კიბეროპერაციის შედეგები. მეტი განჭვრედატობა ნიშნავს მეტ შესაძლებლობას ძალის გამოყენებად დაკვალიფიცირებისთვის; 6) „სამხედრო ხასიათი" - აღნიშნული კრიტერიუმი იყენებს კავშირს კიბეროპერაციებსა და სამხედრო ოპერაციებს შორის, რათა აამაღლოს კიბეროპერაციის ძალის გამოყენების კვალიფიკაციის ალბათობა; 7) „სახელმწიფოს ჩართულობა" - აღნიშნული კრიტერიუმი აფასებს კავშირს კიბეროპერაციასა და სახელმწიფოს შორის. სახელმწიფო შესაძლოა, ჩართული იყოს თავად ან სხვა აქტორების მეშვეობით. რაც ზუსტია კავშირი, მით მეტია ალბათობა, კიბეროპერაციას მიენიჭოს ძალის გამოყენების კვალიფიკაცია; 8) „კანონიერების პრეზუმფცია" - აღნიშნული კრიტერიუმი იკვლევს, შესაძლოა თუ არა, კიბეროპერაცია ეკუთვნოდეს საერთაშორისო სამართლით მოწესრიგებულ სხვა კატეგორიას. მაგალითად, ეკონომიკური ან პოლიტიკური იძულება არ წარმოადგენს ძალის გამოყენების აკრძალვის დარღვევას.

[289] *Barkham J.,* Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, 34, 2001, 85–86; *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002, 89–92; *Antolin-Jenkins V. M.,* Defining the parameters of Cyberwar Operations: Looking for Law in All the Wrong Places, Naval Law Review, 51, 2005, 168–172; *Schmitt M.N.,* Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, 2011, 575–578; *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge University Press, 2012, 63-65;

[290] *Schmitt M. N., Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 334, წესი 69-ის კომენტარი, § 9(a).

ზემოაღნიშნული მიდგომა საკმაოდ საინტერესოა და შესაძლებელია, გავრცელდეს სხვა სიტუაციებზეც. მცირედი ცვლილების შემთხვევაში, შესაძლოა, სიმწვავის ზღვრის ელემენტის დამატება ისეთ კიბეროპერაციებზე, რომლებსაც ახლავს ფიზიკური პირების ან საკუთრების ფიზიკური ზიანი.

4.3. განსხვავება კიბეროპერაციებს შორის, რომლებიც იწვევს რეალურ და კიბერ შედეგებს

ერთმანეთისგან უნდა იქნეს განსხვავებული კიბეროპერაციები, რომელთა შედეგად გამოწვეულია ფიზიკური შედეგები (ფიზიკური ზიანი, ტრავმა, სიცოცხლის მოსპობა) და კიბეროპერაციები, რომლებიც წარმოშობენ, მხოლოდ არაფიზიკურ შედეგებს (მონაცემთა განადგურება, კომპიუტერული პროგრამების დაზიანება ან თუნდაც DDoS შეტევა). კომენტატორთა უმეტესობა მიიჩნევს, რომ კიბეროპერაციები, რომლებსაც შედეგად ფიზიკური ზიანი მოსდევს, კვალიფიცირდება ძალის გამოყენებად.[291] ამის საწინააღმდეგოდ, ისეთი კიბეროპერაციების გამოვლენა, რომლებსაც არ ახლავს თანმდევი შედეგები, რეალურ სამყაროში ბევრად რთულია.[292]

ნებისმიერი ფიზიკური შედეგი, იქნება ეს ფიზიკური ზიანი, ტრავმა[293] თუ სიცოცხლის მოსპობა - გამოწვეული კიბეროპერაციის შედეგად, დაკვალიფიცირდება ძალის გამოყენებად. ძალის გამოყენებად შეიძლება დაკვალიფიცირდეს ასევე შედარებით ნაკლები ზიანის მქონე კიბერშეტევაც, თუნდაც ერთი კომპიუტერის დაზიანება. ასეთ შემთხვევაში, კვალიფიკაციის მინიჭება მსხვერპლი სახელმწიფოს პრეროგატივაა. ჰიპოთეტური მაგალითის საფუძველზე თუ ვიმსჯელებთ, შეგვიძლია განვიხილოთ ერთი სახელმწიფოს თავდასხმა მეორეზე, რომლის შედეგადაც ფიზიკურად დაზიანდა მსხვერპლი სახელმწიფოს მთავრობის წარმომადგენელთა

---

[291] მაგალითად იხ., *Schmitt M.N.,* Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, 2011, 573. ასევე იხ. *Schmitt M. N.,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1999, 17; *Joyner C. C. and Lotrionte C.,* Information Warfare as International Coercion: Elements of a Legal Framework, European Journal of International Law, 12, 2001, 850; *Radziwill Y.,* Cyber-Attacks and the Exploitable Imperfection of International Law, Brill & Martinus Nijhoff Publishers, 2015, 131.

[292] *Barkham J.,* Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, 34, 2001, 84–85.

[293] ტრავმა გულისხმობს ადამიანისთვის მიყენებულ ფიზიკურ თუ ფსიქოლოგიურ დაზიანებას.

მობილური ტელეფონები. თუმცა, ნაკლებ სავარაუდოა, თავად მსხვერპლმა სახელმწიფომ მოინდომოს მსგავსი თავდასხმის ძალის გამოყენებად დაკვალიფიცირება, გამომდინარე მცირე მასშტაბის ზიანიდან. აღნიშნულის მაგალითად გამოდგება Stuxnet-ის შემთხვევა. 2010 წელს ირანის ბირთვული პროგრამის კუთვნილი ცენტრიფუგები დაზიანდა ვირუსის გამოყენებით. კიბეროპერაციას სამეცნიერო წრეების მიერ მიენიჭა ძალის გამოყენების კვალიფიკაცია. თუმცა, არც ირანულ მხარეს და არც თავდასხმის განმახორციელებელს მსგავსი კვალიფიკაცია არ მიუცია შემთხვევისთვის.[294] მკვლევართა განმარტებით, ამის მიზეზი იყო ზიანის ოდენობა - დაზიანდა მხოლოდ რამდენიმე ცენტრიფუგა და არა, მაგალითად, მთლიანი ბირთვული სადგური. არსებობს განსხვავებული მოსაზრებებიც, რომელთა თანახმად, ირანს ან არ სურდა ვითარების ესკალაცია, ან ცდილობდა, სხვა გზებითა და ფორმატით გაეცა პასუხი თავდამსხმელებისთვის.[295] აღნიშნულ შემთხვევაში, ყველაზე მნიშვნელოვანია ის, რომ რეალურად შესაძლებელია, ირანის ბირთვულ სადგურზე კიბერშეტევა სამართლებრივად დაკვალიფიცირებულიყო ძალის გამოყენებად. სხვა საკითხია, რამდენად გამართლებული იყო ამგვარი გადაწყვეტილება, სახელმწიფოს პოლიტიკური თუ სტრატეგიული მიზნებიდან გამომდინარე. თუმცა, საერთაშორისო სამართლისთვის მთავარი მაინც ისაა, რომ ირანს ჰქონდა ძალის გამოყენების კვალიფიკაციის მინიჭების შესაძლებლობა.

გაცილებით რთულადაა საქმე ისეთი კიბეროპერაციების კვალიფიკაციისას, რომელიც არ იწვევს შედეგებს რეალურ სამყაროში. ასეთი კიბეროპერაციები, მკვლევართა აზრით, საერთოდ არ უნდა დაკვალიფიცირდეს ძალის გამოყენებად. თუმცა, სამეცნიერო წრის ნაწილის შეხედულებით კი, ძალის გამოყენებად კვალიფიცირება შესაძლებელია, მხოლოდ გარკვეული პირობების შემთხვევაში.[296]

---

[294] *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge University Press, 2012, 37–75; Stuxnet-ის შესახებ ზოგადად იხ., *Zetter K.,* Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown, 2014.

[295] სიმწვავის ზღვართან დაკავშირებით, ვრცლად იხ. *Ruys T.,* The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, American Journal of International Law, 108, 2014.

[296] იხ., *Hoisington M.,* Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, International & Comparative Law Review, 32, 2009, 447; ასევე იხ., *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002, 85; *Schmitt M. N.,*

აღნიშნული პოზიციები წარმოქმნის ორ შეკითხვას: პირველი - ფიზიკური შედეგის არსებობა, თავის მხრივ, წარმოადგენს თუ არა ზღვარს? და მეორე - ნებისმიერ შემთხვევაში, ფიზიკური შედეგები მიიჩნევა თუ არა უფრო მძიმედ, ვიდრე არაფიზიკური? ორივე ამ შეკითხვაზე შესაძლებელია უარყოფითი პასუხის გაცემა. მართალია, ის ფაქტი, რომ ფიზიკური შედეგები უფრო ადვილად დასანახი და ხელშესახებია და, შესაბამისად, მარტივია მათთვის კვალიფიკაციის მორგება, მაგრამ არ უნდა დაგვავიწყდეს ისიც, რომ არაფიზიკური შედეგის მქონე კიბეროპერაციებმაც შესაძლებელია, გამოიწვიოს ფართომასშტაბიანი შედეგები.[297] ლოგიკას მოკლებულია კიბეროპერაციებისთვის ძალის გამოყენების კვალიფიკაციის მინიჭება მხოლოდ მათი შედეგის ტიპიდან გამომდინარე, მიუხედავად იმისა, იქნება ეს ფიზიკური თუ არაფიზიკური შედეგები.

5. კიბეროპერაციები, რომელთა სამიზნეს წარმოადგენს კრიტიკული ინფრასტრუქტურა

უტოლდება თუ არა კონკრეტული კიბეროპერაცია ძალის გამოყენებას, აუცილებლად შესაფასებელია, სამიზნე წარმოადგენდა თუ არა კრიტიკულ ინფრასტრუქტურას. თუ სამიზნე წარმოადგენს კრიტიკულ ინფრასტრუქტურას, დამამძიმებელი ფაქტორია, რომელმაც შეიძლება გადაძალოს შემთხვევის ძალის გამოყენებად დაკვალიფიცირების ალბათობა. წინამდებარე ქვეთავი მოიცავს კრიტიკული ინფრასტრუქტურის ცნების განმარტებას, ინფორმაციას მის შესახებ და აანალიზებს, თუ როგორ გავლენას ახდენს კიბერძალის კვალიფიკაციაზე.

უნდა აღინიშნოს, რომ კრიტიკული ინფრასტრუქტურის ცნება, რომელიც გამოყენებულია წინამდებარე ნაშრომში, გამომდინარეობს კიბერუსაფრთხოებისა და ძალის გამოყენების კონტექსტის აღქმიდან და შესაძლებელია, განსხვავდებოდეს არაერთ რომელიმე სფეროში არსებული კრიტიკული ინფრასტრუქტურის ცნებისგან. შესაბამისად, კრიტიკული ინფრასტრუქტურის ცნება განხილული იქნება უფრო

Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1999, 913.

[297] *Lin H. S.,* Offensive Cyber Operations and the Use of Force, Cybersecurity Symposium: National Leadership, Individual Responsibility, Journal of National Security Law & Policy, 2010, 74.

ფართო მნიშვნელობით, ვიდრე მხოლოდ ძალის გამოყენების აკრძალვაა. მაგალითად, კრიტიკული ინფრასტრუქტურის ცნება შესაძლოა, მოიცავდეს განსაზღვრულ მნიშვნელობას ჯეროვანი გულისხმიერების პრინციპის იმპლემენტაციისას, კიბერ კონტექსტში.[298]

5.1. კრიტიკული ინფრასტრუქტურის ცნება

ზოგადი ტერმინი - კრიტიკული ინფრასტრუქტურა - მოიცავს ინფრასტრუქტურებს, აქტივებს ან სისტემებს, რომელთაც სახელმწიფო მიიჩნევს აუცილებლად, საზოგადოების სასიცოცხლო ფუნქციების შენარჩუნებისთვის ან წარმოადგენს სერიოზულ რისკს მოსახლეობისთვის. რეალურად მათი დაზიანება, განადგურება ან შეჩერება შესაძლოა, იყოს სერიოზული რისკის შემცველი მოსახლეობისთვის ან უარყოფით გავლენას ახდენდეს სახელმწიფო უსაფრთხოებაზე. კრიტიკული ინფრასტრუქტურის კიბერსაფრთხეები სერიოზული გამოწვევაა ეროვნული და საერთაშორისო უსაფრთხოებისთვის.[299] დაკვირვება ნათელყოფს, რომ კრიტიკული ინფრასტრუქტურის არაერთი განმარტება მოიცავს სამთავრობო და საჯარო სერვისების, უსაფრთხოების, საკვების, წყლის, ტრანსპორტის, ენერგეტიკის, ჯანდაცვის, საფინანსო და საბანკო სექტორებს.[300] ამის მიუხედავად, ჯერჯერობით არ არსებობს უნივერსალური ჩამონათვალი, რისგან შედგება კრიტიკული სექტორი.[301]

სახელმწიფოთა უმეტესობა შეიმუშავებს საკუთარ დეფინიციას, რას წარმოადგენს კრიტიკული ინფრასტრუქტურა და კრიტიკული სექტორი. მათი მიზანია, შეძლონ იმ დაწესებულებებისა და აქტივების იდენტიფიცირება, რომლებიც წარმოადგენენ კრიტიკულ ინფრასტრუქტურას მათთვის და გააანალიზონ, როგორ დაიცვან ადამიანური საფრთხისგან, მათ შორის კიბერსაფრთხისა და ბუნებრივი

[298] *Kulesza J.,* Due Diligence in International Law, Brill & Martinus Nijhoff Publishers, 2016, 292–299.

[299] *Myjer E.,* Some Thoughts on Cyber Deterrence and Public International Law, Research Handbook on International Law and Cyberspace, *Tsagourias N., Buchan R. (eds),* Edward Elgar Publishing, 2015, 287–290.

[300] Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, UNGA Res 58/199 (23 December 2003); ასევე იხ. *Tsagourias N.,* Cyber Attacks, Self-Defence and the Problem of Attribution, Journal of Conflict and Security Law 17, 2012, 231.

[301] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 56; *Focarelli C.,* Self-Defence in Cyberspace in *Tsagourias N. and Buchan R.* (eds), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 268.

კატაკლიზმებისგან. ზოგადად, სახელმწიფოები ადგენენ კრიტიკული სექტორების ჩამონათვალს და, შემდეგ, თითოეულ სექტორში ცალ-ცალკე გამოყოფენ კრიტიკულ ინფრასტრუქტურას.

საერთაშორისო დონეზე გაეროს გენერალურმა ასამბლეამ 2003 წელს მიიღო რეზოლუცია კიბერუსაფრთხოების გლობალური კულტურის შექმნისა და კრიტიკული ინფრასტრუქტურის დაცვის შესახებ, რომელიც ადგენს, რომ კრიტიკული ინფრასტრუქტურა ზოგადად დაკავშირებულია ენერგიის, ჰაერისა და საწყლოსნო ტრანსპორტის წარმოქმნასთან, გადაცემასა და მიწოდებაზე, საბანკო და საფინანსო მომსახურებებთან, ელექტრონულ კომერციასთან, წყლის მარაგთან, საკვების დისტრიბუციასა და საზოგადოებრივ ჯანდაცვასთან. როგორც ირკვევა, ეს არ არის სრულყოფილი ნუსხა. რეზოლუცია მიუთითებს სახელმწიფოებს, თავად განსაზღვრონ საკუთარი კრიტიკული ინფრასტრუქტურა.[302]

ევროკავშირმა მიიღო ევროპული პროგრამა კრიტიკული ინფრასტრუქტურის დაცვისთვის (EPCIP)[303], 2008 წლის ევროპული დირექტივის საფუძველზე, რომელიც ეხებოდა კრიტიკულ ინფრასტრუქტურას და მისი დაცვის ჩარჩოს.[304] ევროკავშირი ერთმანეთისგან განასხვავებს ეროვნულ კრიტიკულ ინფრასტრუქტურასა და ევროპულ კრიტიკულ ინფრასტრუქტურას. ეს უკანასკნელი გულისხმობს ევროკავშირის წევრ-სახელმწიფოებში განთავსებულ კრიტიკულ ინფრასტრუქტურას, რომელთა დაზიანება ან განადგურება იქონიებს არსებით გავლენას სულ ცოტა, ორ წევრ სახელმწიფოზე. გავლენის მნიშვნელობა ფასდება მკვეთი კრიტერიუმებით. აღნიშნული მოიცავს მომიჯნავე სექტორების დამოკიდებულებას სხვა ტიპის ინფრასტრუქტურაზე.[305] დირექტივა გამოჰყოფს ევროკავშირის ორ კრიტიკულ ინფრასტრუქტურის სექტორს, რომლებიც მოიცავს რამდენიმე ქვესექტორს, მათ შორის, პირველ რიგში, ენერგეტიკას (ელექტროენერგია, ნავთობი, გაზი) და მეორე, ტრანსპორტს (გზა, რკინიგზა, ჰაერი, შიდა საწყლოსნო ტრანსპორტი, ასევე ოკეანე,

[302] Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, UNGA Res 58/199 (23 December 2003).

[303] European Union, Communication from the Commission on a European Programme for Critical Infrastructure Protection (2006) COM(2006) 786 final.

[304] European Union, Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (2008) Council Directive 2008/114/EC.

[305] European Union, Communication from the Commission on a European Programme for Critical Infrastructure Protection (2006) COM(2006) 786 final,4.

პორტები).[306] აღნიშნული სია არა სრულყოფილი დოკუმენტია, ვინაიდან წარმოადგენს მხოლოდ იმ კრიტიკულ ინფრასტრუქტურას, რაზეც ყურადღებას ამახვილებს ევროკავშირი.

2004 წელს ევროპულმა კომისიამ მიიღო დოკუმენტი - კრიტიკული ინფრასტრუქტურის დაცვა ტერორიზმთან ბრძოლაში, რომელიც მოიცავდა კრიტიკული ინფრასტრუქტურების სიას.[307] აღნიშნული ნუსხის მიხედვით, სექტორები, რომლებიც მოიცავენ კრიტიკულ ინფრასტრუქტურას, წარმოდგენილია შემდეგი სახით: 1) ენერგეტიკული ნაგებობები და ქსელები; 2) კომუნიკაციები და ინფორმაციული ტექნოლოგია (მაგალითად ტელეკომუნიკაციები, სამაუწყებლო სისტემები, ინტერნეტი და სხვ.); 3) ფინანსები; 4) ჯანდაცვა; 5) საკვები; 6) წყალი (კაშხლები, ქსელი, წყალსაცავები და სხვ.); 7) ტრანსპორტი; 8) საშიში მასალების წარმოება, შენახვა, და გადაზიდვა; 9) მთავრობა.[308]

ამერიკის შეერთებულმა შტატებმა, დროთა განმავლობაში, გამოცადა სხვადასხვა მიდგომა და დაადგინა, რომ კრიტიკული ინფრასტრუქტურა შესაძლოა, დაკავშირებული იყოს წარმოდგენილ თექვსმეტ მიმართულებასთან:[309]

1) ქიმიური; 2) კომერციული დაწესებულებები; 3) კომუნიკაციები; 4) კრიტიკული წარმოება; 5) კაშხლები; 6) თავდაცვის სამრეწველო ბაზა; 7) გადაუდებელი საჭიროების სამსახურები; 8) ენერგეტიკა; 9) საფინანსო მომსახურებები; 10) საკვები და სოფლის მეურნეობა; 11) სამთავრობო დაწესებულებები; 12) ჯანდაცვა და საჯარო ჯანმრთელობა; 13) ინფორმაციული ტექნოლოგიები; 14) ბირთვული რეაქტორები, მასალები და ნარჩენები; 15) ტრანსპორტირების სისტემები; 16) წყალი და წყლის მარაგის სისტემები.[310]

საფრანგეთმა, კრიტიკული ინფრასტრუქტურის იდენტიფიცირების მიზნით,[311] თორმეტი სექტორი დაყო სამ კატეგორიად: 1) მთავრობა (სახელმწიფოს სამოქალაქო აქტივობები, სახელმწიფოს სამხედრო აქტივობები, სასამართლო აქტივობები,

[306] European Union, Council Directive 2008/114/EC (n 121), Annex I 'List of ECI sectors'.
[307] European Union, Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the Fight against Terrorism (2004) COM(2004) 702 final.
[308] *იქვე* 4.
[309] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 56.
[310] US White House, Critical Infrastructure Security and Resilience, 2013, Presidential Policy Directive/PPD-21.
[311] ფრანგულად, 'critical infrastructure' ითარგმნება, როგორც 'opérateur d'importance vitale' (OIV) და 'critical sectors', როგორც 'secteurs d'activités d'importance vitale' (SAIV).

კოსმოსი და კვლევა); 2) მოსახლეობის დაცვა (ჯანდაცვა, წყლის მარაგი, საკვების მარაგი); 3) ეკონომიკური და სოციალური სექტორები (ენერგეტიკა, ინფორმაცია, აუდიო-ვიზუალური და ელექტრონული კომუნიკაციები, ტრანსპორტი, ფინანსები, ინდუსტრია).[312]

თუ გადავხედავთ ზემოთ განხილულ სამ მაგალითს, შეგვიძლია დავასკვნათ, რომ სახელმწიფოები იყენებენ განსხვავებულ მიდგომებს კრიტიკულ ინფრასტრუქტურებთან დაკავშირებით. განსხვავებების მიუხედავად, წარმოდგენილ ნუსხებს ძირითადი მიმართებები მაინც საერთო აქვთ: კომუნიკაციები, ინფორმაციული ტექნოლოგიები, ენერგეტიკა, წყალი, ტრანსპორტი, მთავრობა, ჯანდაცვა, ფინანსები და ა.შ. აღნიშნული მსგავსება მიუთითებს იმ გარემოებაზე, რომ თანამედროვე სამყაროში წამყვან სახელმწიფოებს, მეტწილად, მსგავსი ინფრასტრუქტურული სისტემები გააჩნიათ.

თანამედროვე კრიტიკული ინფრასტრუქტურები სასიცოცხლოდაა დამოკიდებული კომპიუტერულ სისტემებსა და ქსელებზე. ამიტომაც არის მოწყვლადი კიბეროპერაციების წინაშე.[313] Stuxnet-მა აჩვენა ბირთვული სადგური, რომელიც წარმოადგენს კრიტიკულ ინფრასტრუქტურას, როგორ შეიძლება დაზიანდეს კიბეროპერაციების შედეგად.[314] ანალოგიურად, კიბეროპერაციამ 2014 წელს ფიზიკური ზიანი მიაყენა ფოლადის ქარხანას, გერმანიაში, რის შესახებაც განაცხადა კიდეც გერმანიის ინფორმაციის უსაფრთხოების ფედერალურმა ოფისმა.[315] აღნიშნული შემთხვევა ააშკარავებს კრიტიკული ინფრასტრუქტურისა და კიბერსაფრთხეებისადმი მოწყვლადობის ფაქტებს.

საზოგადოდ, მოწყვლადობა მნიშვნელოვანი საკითხია სახელმწიფოებისა და საერთაშორისო ორგანიზაციებისთვის. კრიტიკული ინფრასტრუქტურის წინააღმდეგ მიმართულ კიბეროპერაციებს შესაძლებელია, დამანგრეველი შედეგები მოჰყვეს.

---

[312] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 301.

[313] *Shackelford S.,* From Nuclear War to Net War: Analogizing Cyber Attacks in International, Berkley Journal of International Law, 27, 2009, 199.

[314] *McConnell B. W. and Austin G.,* A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets, EastWest Institute, 2014, Policy Paper 1/2014 10–11.

[315] იხ., გერმანულად, Die Lage der ITSicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik, 2014, 31.

შესაბამისად,[316] კრიტიკული ინფრასტრუქტურის კიბეროპერაციებისგან დაცვა მნიშვნელოვან კიბერუსაფრთხოების გამოწვევას წარმოადგენს, რომელსაც შეუძლია ახსნას, რატომ კონცენტრირდება კიბერთავდაცვის სფეროზე კრიტიკული ინფრასტრუქტურის წინააღმდეგ მიმართული უსაფრთხოების სხვადასხვა სცენარი.[317]

5.2. კრიტიკული ინფორმაციული ინფრასტრუქტურები

კრიტიკული ინფორმაციული ინფრასტრუქტურა წარმოადგენს კრიტიკული ინფრასტრუქტურის ქვეკატეგორიას, რომელიც ეხება კომპიუტერულ ქსელებსა და სისტემებს (CII). კრიტიკული ინფორმაციული ინფრასტრუქტურა ისეთი კომპიუტერული ქსელები და სისტემებია, რომელთა დაზიანება ან განადგურება სერიოზულ ზეგავლენას ახდენს მოსახლეობის ჯანმრთელობაზე, უსაფრთხოებაზე ან ეკონომიკურ კეთილდღეობაზე ან მთავრობის ან ეკონომიკის ეფექტიანად ფუნქციონირებაზე.[318]

კრიტიკული ინფორმაციული ინფრასტრუქტურა წარმოადგენს ილუსტრაციას, თუ როგორ არის დამოკიდებული ჩვენი საზოგადოება და ეკონომიკა კომპიუტერულ ქსელებსა და სისტემებზე.[319]

თანამედროვე საზოგადოება და ეკონომიკა სრულად აგებულია კომპიუტერულ სისტემებზე. აქედან გამომდინარე, არსებითი რაოდენობის კომპიუტერული ქსელები და სისტემები შესაძლებელია, მიჩნეულ იქნეს კრიტიკულ ინფორმაციულ ინფრასტრუქტურად. 2007 წელს ესტონეთზე განხორციელებულმა კიბერთავდასხმამ

---

[316] *Jensen E. T.,* Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense, Stanford Journal of International Law, 38, 2002, 207; European Union, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience' (2009) COM(2009) 149 final.

[317] *Radziwill Y.,* Cyber-Attacks and the Exploitable Imperfection of International Law, Brill & Martinus Nijhoff Publishers, 2015, 44.

[318] OECD Recommendation of the Council on the Protection of Critical Information Infrastructures (2008) C(2008)35; European Union, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience' (2009) COM(2009) 149 final).

[319] Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, UNGA Res 58/199 (23 December 2003).

აჩვენა, რამდენად მძიმე შედეგები შეიძლება მოჰყვეს კომპიუტერული ქსელებისა და სისტემების დაზიანებას.[320]

კიბეროპერაციების მიმართ კრიტიკული ინფრასტრუქტურის მოწყვლადობას გააჩნია ორმაგი დატვირთვა: კომპიუტერული ქსელებისა და სისტემების მოწყვლადობა, რომელზეც დამოკიდებულია კრიტიკული ინფრასტრუქტურა და კომპიუტერული ქსელებისა და სისტემების მოწყვლადობა, რომლებიც თავად წარმოადგენენ კრიტიკულ ინფრასტრუქტურას.

ამ თვალსაზრისით მნიშვნელოვანია 2016 წლის აგვისტოში ძალაში შესული ევროკავშირის დირექტივა, საინფორმაციო სისტემებისა და ქსელების უსაფრთხოების შესახებ (NIS Directive).[321] ევროკავშირის წევრ სახელმწიფოებს 2018 წლის მაისამდე ჰქონდათ ვადა აღნიშნული დირექტივის შიდასაკანონმდებლო სისტემაში იმპლემენტაციისთვის.[322] დირექტივა ითვალისწინებს კონკრეტულ ვალდებულებებს არსებითი სერვისების, ოპერატორთა ქსელებისა და ინფორმაციული სისტემების უსაფრთხოების თაობაზე.

5.3. კიბერძალა და კრიტიკული ინფრასტრუქტურა

განსაზღვრა იმისა, წარმოადგენს თუ არა კიბეროპერაცია ძალის გამოყენებას, უმთავრესად დამოკიდებულია მის მიერ წარმოქნილ შედეგებზე. კიბეროპერაციები, რომლებსაც შედეგად მოჰყვება სიცოცხლის მოსპობა, ტრავმა, საკუთრების ზიანი ან განადგურება, დიდი ალბათობით დაკვალიფიცირდება ძალის გამოყენებად. თუმცა, აღნიშნული კვალიფიკაცია საეჭვო და ნაკლებ სავარაუდოა ისეთი კიბეროპერაციების მიმართ, რომლებსაც მხოლოდ კიბერ შედეგები ახლავს, როგორიცაა, მაგალითად, მონაცემთა დაზიანება ან განადგურება.

---

[320] European Union, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience' (2009) COM(2009) 149 final 5.

[321] European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016.

[322] *იქვე,* მუხლი 25

გარდა წარმოქმნილი შედეგების რეალურობისა, კიბეროპერაციის ძალის გამოყენებად დაკვალიფიცირებაზე შესაძლოა, გავლენა იქონიოს ოპერაციის სამიზნემ. მუნიციპალური ბიბლიოთეკის კომპიუტერული ქსელის ნაწილობრივი დაზიანება არ დაკვალიფიცირდება ძალის გამოყენებად. თუმცა, თუ დაზიანებული ქსელი წარმოადგენს კრიტიკულ ინფორმაციულ ინფრასტრუქტურას ან კრიტიკული ინფრასტრუქტურის ფუნქციონირებისთვის არსებით პირობას, შესაძლებელია, კიბეროპერაციამ მიიღოს ძალის გამოყენების კვალიფიკაცია. მიუხედავად იმისა, რომ შედეგებს წარმოშობს მხოლოდ ციფრულ სამყაროში.[323] გარკვეული თვალსაზრისით, ეს არ ნიშნავს, რომ კრიტიკული ინფრასტრუქტურის მიმართ განხორციელებული ნებისმიერი კიბეროპერაცია ძალის გამოყენებას წარმოადგენს.[324] კიბეროპერაციების შეფასებისას, თუ შეიძლება, ასე ითქვას, „უშედეგო“ შემთხვევები, რომლებსაც არ მოჰყვება ფიზიკური ზიანი, ფაქტობრივად, ვერ აკმაყოფილებს ძალის გამოყენების მოთხოვნებს. ამდენად, კრიტიკული ინფრასტრუქტურის სამიზნე შეიძლება, გახდეს კიბეროპერაციების კვალიფიკაციის შეცვლის გადამწვეტი ელემენტი. რაც შეგვიძლია დანამდვილებით დავასკვნათ, არის ის, რომ კიბეროპერაციამ, რომელიც სამიზნედ არ ისახავს კრიტიკულ ინფრასტრუქტურას და არ წარმოშობს ფიზიკურ შედეგებს, ნაკლებ სავარაუდოა, მოახერხოს და მიიღოს ძალის გამოყენების კვალიფიკაცია.[325]

კრიტიკული ინფრასტრუქტურისა და კიბეროპერაციების თანაკვეთა მხოლოდ ძალის გამოყენების კონტექსტში არ გვხვდება. შეიარაღებული შეტევისას ასევე დგება ზღვრის საკითხი.[326]

6. დასკვნა

ნაშრომში ამ ეტაპამდე განვითარებული მსჯელობის შედეგად თამამად შეიძლება ითქვას, რომ კიბეროპერაციებზე ზოგადად ვრცელდება ძალის გამოყენების

[323] *Roscini M.,* Cyber Operations as a Use of Force in *Tsagourias N. and Buchan R. (eds),* Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015, 245.
[324] *Jensen E. T.,* Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense, Stanford Journal of International Law, 38, 2002.
[325] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 58.
[326] იხ., ნაშრომის VI თავი.

აკრძალვის სამართალი. დღესდღეობით კიბერძალასთან დაკავშირებით, მეცნიერულ დონეზე განვითარებული მიდგომების გაანალიზებით, ნათლად ჩანს, რომ ყველაზე ეფექტიანი და რეალობის შესაბამისია შედეგზე დაფუძნებული მიდგომა. თუმცა, ეს მიდგომა არ ასახავს სურათს სრულყოფილად. როდესაც აშკარაა შედეგზე დაფუძნებული მიდგომა, თავისი არსითა და მასთან სინთეზში გამოიყენება მიზნობრივი და ინსტრუმენტული მიდგომის ელემენტები, მაშინ ვიღებთ ყველაზე სრულფასოვან, ერთიან შეფასების სისტემას. ამასთანავე, დიდი მნიშვნელობა ენიჭება იმ ფაქტს, რომ კიბეროპერაცია შედეგებს წარმოშობს რეალურ თუ ვირტუალურ სამყაროში. არაფიზიკური სახის შედეგების პირობებში, შესაძლოა, დაბალი სტატუსის მქონე კიბეროპერაციამ მიიღოს ძალის გამოყენების კვალიფიკაცია. სხვა მსგავს შემთხვევებში, მიზნობრივი და ინსტრუმენტული მიდგომების ელემენტები ერთგვარად ეხმარება შედეგზე დაფუძნებულ მიდგომას, გახდეს უფრო მეტად მრავალფეროვანი და მოიცვას ყველა შესაძლო შედეგი. მაგალითად, თუ კიბეროპერაციას აქვს არაფიზიკური ზიანი, მაგრამ სამიზნეს წარმოადგენს კრიტიკული ინფრასტრუქტურა ან კრიტიკული ინფორმაციული ინფრასტრუქტურა, ამან შესაძლოა, შეცვალოს კიბეროპერაციის სამართლებრივი კვალიფიკაციის საკითხი და გადაიხაროს ამ უკანასკნელის ძალის გამოყენებად დაკვალიფიცირების სასარგებლოდ. შესაბამისად, იმის განსასაზღვრად, კიბეროპერაცია წარმოადგენს თუ არა ძალის გამოყენებას, ჯერჯერობით საუკეთესო გამოსავალი არსებული მიდგომების გაერთიანება, მიზნობრივი და ინსტრუმენტული მიდგომების ელემენტების დამატებაა.

IV. სახელმწიფოს მიერ იძულებითი ხასიათის კიბერაქტივობის გამოყენება და მისი განზრახვა

1. შესავალი

კიბეროპერაციების სტატუსი და მათდამი გამოსაყენებელი სამართლებრივი ჩარჩო დამოკიდებულია მათივე განვითარების კონტექსტზე. ამ მხრივ, მხედველობაში მისაღებია კიბეროპერაციის განმახორციელებელი სახელმწიფოს განზრახვა და თავდამსხმელ და მსხვერპლ სახელმწიფოებს შორის არსებული პოლიტიკური ურთიერთობა. ზოგჯერ სახელმწიფოების მიერ დასპონსორებული[327] კიბეროპერაციები ხორციელდება არასახელმწიფო აქტორების მიერ, რაც ხელს უწყობს ამგვარი აქტების სამომავლოდ მომრავლებას და ზრდის მიმზიდველობას თავდამსხმელი სახელმწიფოსთვის. რა თქმა უნდა, კვლავ რჩება ადგილი შეცდომისა და უნებლიეთ განხორციელებული უკანონო აქტებისთვის, რომლებიც შეიძლება დაკვალიფიცირდეს ძალის გამოყენებად, მაგრამ, უნდა ითქვას, რომ მათი რიცხვი უკიდურესად მცირეა.[328]

2. პროქსების მიერ განხორციელებული იძულებითი კიბერაქტივობების შერაცხვა

სახელმწიფოსთვის მოქმედების შერაცხვა საერთაშორისო სამართლის მნიშვნელოვან საკითხს წარმოადგენს.[329] სახელმწიფო აბსტრაქტული ერთობაა, რომელსაც შეუძლია, იმოქმედოს ერთი ან რამდენიმე პირის საშუალებით, რომელთა

---

[327] კიბეროპერაციების კონტექსტში ტერმინი - „სახელმწიფოს მიერ დასპონსორებული“ - წარმოადგენს ერთგვარ მარტივ გამოსავალს იმ რთული პრობლემიდან, რომელიც რჩება ერთ-ერთ უდიდეს გამოწვევად თანამედრო კიბერუსაფრთხოების ლანდშაფტისთვის: ობიექტური მტკიცებულებებითა და გადამოწმებული ინფორმაციის საფუძველზე დამტკიცდა სახელმწიფოს მონაწილეობა კონკრეტულ ოპერაციაში. აქედან გამომდინარე, ტერმინი გამოიყენება მაშინ, როდესაც არსებობს მეტ-ნაკლებად დასაბუთებული ვარაუდი, რომ კონკრეტული კიბეროპერაცია ემსახურება სახელმწიფოს ინტერესებს და მის განხორციელებაში სახელმწიფო ჩართულია ნებისმიერი ფორმით. იხ., *Maurer, T.*, Cyber Mercenaries: the State, Hackers, and Power, Cambridge University Press, 2018, 22-23.

[328] *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 79–84.

[329] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 305.

ქმედებებიც მას შეერაცხება.[330] მარტივად, რომ ვთქვათ, შერაცხვის მიზნისთვის სახელმწიფოს მოქმედება წარმოადგენს სხვას არაფერს, გარდა კონკრეტულ ინდივიდთა მოქმედებებისა, რომელიც შემდეგ შეერაცხება სახელმწიფოს.[331]

ძალის გამოყენების აკრძალვა ვრცელდება მხოლოდ სახელმწიფოებზე. თუმცა, შესაძლოა, სახელმწიფომ დაარღვიოს ძალის გამოყენების აკრძალვა არასახელმწიფო აქტორებისთვის ხელის შეწყობით ან მათთვის მითითებების მიცემით. პროქსების მიერ წარმოებული ომი, რომელიც განვითარდა ცივი ომის პერიოდში, ქმნის გაურკვევლობას და რთულდება მეომარი მხარის იდენტიფიცირება და მის წინააღმდეგ მოქმედება.[332] რიგი კიბეროპერაციებისა, რომელთა განხორციელება ბრალად ედებათ კონკრეტულ სახელმწიფოებს, რეალურად ჩადენილი იყო არასახელმწიფო აქტორების მიერ.[333] მაგალითად, 2007 წელს ესტონეთზე განხორციელებული კიბერთავდასხმის შემდეგ, ესტონეთმა დაადანაშაულა რუსეთის ფედერაცია, თუმცა, აღიარა ისიც, რომ არ გააჩნდა შესაბამისი სამხილები ბრალდების გასამყარებლად.[334] სამაგიეროდ, რუსულმა ახალგაზრდულმა დაჯგუფებამ - „ნაში“ - (Наши)[335] აღიარა ჩართულობა ესტონეთში მომხდარ ამბებში[336]. ასევე რუსეთის ფედერაციის პარლამენტის წევრმაც დაადასტურა, რომ მისმა ასისტენტმა განახორციელა კიბეროპერაციები ესტონეთის წინააღმდეგ.[337] ამას გარდა, სხვადასხვა ჯგუფი, მათ შორის, „ანონიმუსი“ (Anonymous), „რუსეთის ბიზნეს ქსელი“ (Russian Business Network - RBN) ასევე ეჭვმიტანილები იყვნენ სახელმწიფოს სახელით კიბეროპერაციების განხორციელებაში. ცნობილია, „რუსეთის ბიზნეს ქსელი“

---

[330] *Condorelli L. and Kreß C.,* The Rules of Attribution: General Considerations in *Crawford J. et al (eds),* The Law of International Responsibility, Oxford University, Press, 2010, 221.

[331] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 305.

[332] *Waxman M. C.,* Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 36, 2011, 446.

[333] კიბერსამყაროში მეტწილად რთულ ამოცანად რჩება კიბეროპერაციის განმახორციელებელთან დაკავშირება. იხ. *Rid T.,* Cyber War Will Not Take Place, Oxford University Press, 2013, 140.

[334] 'Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks', RIA Novosti, 9 June 2007, <http://en.ria.ru/world/20070906/76959190.html> [15.07.2020].

[335] Nashi („Наши“) იგულისხმება რუსული ახალგაზრდული დემოკრატიული ანტიფაშისტური მოძრაობა, რუსეთის „გრუ-ს“ მართული ორგანიზაცია.

[336] *Clover C.,* 'Kremlin-Backed Group behind Estonia Cyber Blitz', Financial Times, 11 March 2009, <www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz2TBcey8a5> [26.05.2020].

[337] *Leyden J.,* 'Russian Politician: "My Assistant Started Estonian Cyberwar" – Dubious DDoS Lols', The Register, 10 March 2009, <www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/> [15.07.2020]; 'Behind The Estonia Cyberattacks', Radio Free Europe/Radio Liberty, 6 March 2009, <www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html> [15.07.2020].

ახორციელებდა კიბეროპერაციებს საქართველო-რუსეთის 2008 წლის კონფლიქტის დროს.[338] ამგვარი კიბეროპერაციები, რომლებიც განხორციელებულია პროქსების მეშვეობით, ძალზე ართულებს და, ფაქტობრივად, შეუძლებელს ხდის კიბეროპერაციების შერაცხვას სახელმწიფოსთვის და საერთაშორისო სამართლის ამოქმედებას.

კიბეროპერაციები შესაძლოა, განხორციელდეს შიდასახელმწიფოებრივი სამართლით ავტორიზებული იურიდიული პირების მიერ, რომლებსაც გააჩნიათ სახელმწიფოს სახელით მოქმედების სამართლებრივი უფლება ისევე, როგორც სახელმწიფოს ორგანოებს ან სხვა ავტორიზებულ დაწესებულებებს, რომლებიც მოქმედებენ განსაზღვრულ სამთავრობო სფეროებში. ამგვარი იურიდიული პირების მიერ განხორციელებული ნებისმიერი ქმედება შესაძლოა, შეერაცხოს სახელმწიფოს, იმ შემთხვევაშიც კი, თუ დაწესებულება მოქმედებს მათი ავტორიზაციის ფარგლებს მიღმა. გარდა იმ შემთხვევისა, თუ დაწესებულების წარმომადგენელი კონკრეტული პირი არ მოქმედებს პირადი ინტერესების კარნახით. კიბეროპერაციები, შესაძლოა, განხორციელდეს იურიდიული პირების მიერაც, რომლებიც პირდაპირ ავტორიზებულნი არ არიან სახელმწიფოს შიდა სამართლით, მაგრამ მათი ქმედებების ნაწილი შესაძლოა, შეერაცხოს სახელმწიფოს.[339]

3. შეცნობის გარეშე განხორციელებული იძულებითი სახის კიბერმოქმედებები

სახელმწიფოს განზრახვის კრიტერიუმი იმოქმედოს სხვა სახელმწიფოს წინააღმდეგ, ნათელს ხდის, რომ შეცდომით ან უნებლიეთ განხორციელებული აქტი შესაძლოა, დაკვალიფიცირდეს ძალის გამოყენებად. აღნიშნული მტკიცება უფრო პრაქტიკული ხასიათისაა, ვიდრე სამართლებრივი, რომელსაც მკვლევართა ნაწილი განიხილავს სახელმწიფოთა პრაქტიკაზე დაკვირვების საფუძველზე.[340]

---

[338] *Roscini M.,* World Wide Warfare – Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, 14, 2010, 100–101; *Woltag J. C.,* Cyber Warfare: Military Cross-Border Computer Network Operations under International Law, Intersentia, 2014, 90–93.

[339] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 307.

[340] *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 78–84.

კრიტერიუმი ყველაზე რელევანტურია ბოტნეტით განხორციელებული კიბეროპერაციისას. ბოტნეტი, როგორც უკვე აღინიშნა, გულისხმობს კომპიუტერებისა და ქსელების დავირუსებას და მათ დისტანციურად გამოყენებას. ესტონეთზე 2007 წელს განხორციელებულ კიბერთავდასხმისას, ბოტნეტის მეშვეობით, გამოიყენეს კომპიუტერები მთელი მსოფლიოს მასშტაბით. ვითარების შეფასება, თავდასხმა წარმოადგენდა თუ არა ძალის გამოყენებას, მნიშვნელოვანია იმ შემთხვევაშიც კი, თუ სახელმწიფო ფლობს დაინფიცირებულ კომპიუტერებს, ამ სახელმწიფოს არ უნდა დაეკისროს პასუხისმგებლობა კიბერძალის გამოყენებაზე, რადგან მისი კომპიუტერებიდან შეტევა მსხვერპლ სახელმწიფოზე განხორციელდა მისი ნების საწინააღმდეგოდ და შეცნობის გარეშე.

4. სათანადო გარემოებითი მტკიცებულებები იძულებითი კიბერაქტივობის ძალის გამოყენებად დაკვალიფიცირებისთვის

ყურადღება უნდა მიექცეს გარემოებითი მტკიცებულებების ან კონტექსტუალური ფაქტორების ორ შემთხვევას: კიბეროპერაციის კონტექსტს და იძულებითი კიბერაქტივობის საჯაროობას.

4.1. იძულებითი კიბერაქტივობის გარემოებები

კიბეროპერაციის განხორციელების გარემოებებმა შესაძლოა, დიდი დახმარება გაუწიოს იმის განსაზღვრას, აკმაყოფილებს თუ არა მოქმედება ძალის გამოყენების აკრძალვის კრიტერიუმებს. კიბეროპერაციები, როგორც წესი, ექცევა დაბალი ინტენსივობის ძალის გამოყენების კატეგორიაში, რაც ართულებს მათ ძალის გამოყენებად დაკვალიფიცირებას. როზალინ ჰიგინსმა გამოთქვა მოსაზრება, „ძალის ხარისხის“ შესახებ: „მიუხედავად, იმისა, რომ გამოყენებული ძალის ხარისხი, თავის მხრივ, წარმოადგენს რელევანტურ ფაქტორს, თუ გაეროს ქარტია მტკიცების ტვირთს ადებს სახელმწიფოს, რომელიც იყენებს ძალას, დაამტკიცოს მისი მოქმედების სამართლიანობა, მაშინ ნებისმიერი ფართო მასშტაბის მქონე ზომა წამოწევს უკანონობის პრეზუმფციას. ნაკლები ინტენსივობის ძალადობა შესაძლოა,

გამოყენებულ იქნეს შესაბამის დამამტკიცებელ ფაქტორად, მხოლოდ სხვა გარემოებასთან ერთად.[341] ჯერჯერობით არ ყოფილა შემთხვევა, როდესაც კიბეროპერაცია პირდაპირ და ერთხმად შერაცხულიყო მუქარად ან ძალის გამოყენებად, რომელიმე სახელმწიფოს ან საერთაშორისო ორგანიზაციის მიერ. აღნიშნულის მიზეზად შეიძლება, მივიჩნიოთ ის ფაქტი, რომ ჯერჯერობით განხორციელებული კიბეროპერაციების უმეტესობა დაბალი ინტენსივობის ხასიათისაა. კიბეროპერაციის კვალიფიკაციაზე კი გავლენას ახდენს სხვადასხვა კონტექსტუალური ფაქტორი. მაგალითად, მონაწილე მხარეებს შორის ურთიერთობა. მათ შორის მშვიდობიანი ურთიერთობების არსებობის შემთხვევაში კიბეროპერაციის ძალის გამოყენებად კვალიფიკაციის ზღვარი უფრო მაღალი იქნება. შესაბამისად, დაძაბული ურთიერთობების არსებობისას შესაძლებელია კიბეროპერაცია უფრო მარტივად იქნეს მიჩნეული ძალის გამოყენებად.

კიდევ ერთი მნიშვნელოვანი კონტექსტუალური ფაქტორი - წარმოადგენს თუ არა კიბეროპერაცია განყენებულ აქტს,[342] თუ ის ბევრად რთული ვითარების ნაწილია. ცალკე მდგომი აქტი ნაკლებ სავარაუდოა, დაკვალიფიცირდეს ძალის გამოყენებად.[343] მაგალითად, სხვა მოქმედებების პარალელურად, ან მიმდინარე კონფლიქტის ფარგლებში, განხორციელებული კიბეროპერაცია უფრო მარტივად იქნება მიჩნეული ძალის გამოყენებად.

აქამდე განხორციელებული კიბეროპერაციების ძირითადი ნაწილი წარმოადგენს ცალკეულად მდგომ განყენებულ აქტს, რაც, თავის მხრივ, არის კიდევ ერთი ხელშემწყობი ფაქტორი იმისა, თუ რატომ არ გვაქვს დღემდე ძალის გამოყენებად დაკვალიფიცირებული კიბეროპერაცია, მიუხედავად იმისა, რომ, რიგ შემთხვევაში, გაეროს ქარტიის 2(4) მუხლის მოთხოვნები აშკარად დაკმაყოფილებული იყო.

[341] *Higgins R.,* The Development of International Law by the Political Organs of the United Nations, Oxford University Press, 1963 181.

[342]იხ., ნაშრომის VI თავის მე-3 ქვეთავი.

[343] *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 67–76.

4.2. იძულებითი კიბერაქტივობის საჯაროობა

გარემოებითი მტკიცებულებების მეორე მაგალითია კიბეროპერაციებისა და მათ მიერ გამოწვეული შედეგების საჯაროობა. საჯაროობა შესაძლოა, დაკავშირებული იყოს „სიმძიმისა“ და „სიმწვავის“ კრიტერიუმებთან და გავლენა მოახდინოს საზოგადოების აღქმაზე. იძულებითი კიბეროპერაციისა და მისი შედეგების საჯაროობა უნდა განისაზღვროს სახელმწიფოს ზოგადი პოლიტიკური და სტრატეგიული ინტერესებიდან გამომდინარე.

აშკარაა, დღესდღეობით საერთაშორისო სამართალში დგას კიბეროპერაციების სამართლებრივი კვალიფიკაციის პრობლემა, რასაც ხელს უწყობს ის ფაქტორიც, რომ სახელმწიფოები ხშირად თავს იკავებენ კიბეროპერაციებზე საჯაროდ საუბრისა და მისთვის კვალიფიკაციის მინიჭებისგან, რათა არ მოხდეს დაბალი ან საშუალო ინტენსივობის აქტრის ძალის გამოყენებად კვალიფიცირება. ამისთვის სახელმწიფოებს გააჩნიათ სამი ძირითადი მიზეზი: პირველი - სახელმწიფოების დიდ ნაწილს არ სურს, საჯაროდ აღიაროს სისუსტე და გააცხადოს, რომ მოწყვლადია კიბერთავდასხმის წინაშე. შესაბამისად, როდესაც განხორციელებული კიბეროპერაცია არ საჯაროვდება, როგორც წესი, ცდილობენ, საკუთარი სამხედრო სამსახურების ფარგლებში თავადვე გაუმკლავდნენ მას; მეორე - გამომდინარე იქიდან, რომ ჯერ კიდევ არ არსებობს განსაზღვრული ნორმები კიბეროპერაციების მოსაწესრიგებლად, ზოგიერთ სახელმწიფოს ურჩევნია, გამოიჩინოს ინიციატივა და თავად გადაწყვიტოს, როგორ იმოქმედოს კანონით დატოვებულ რუხ სივრცეში; მესამე - ძალის გამოყენების კვალიფიკაციის მინიჭებამ შესაძლოა, გამოიწვიოს ვითარების ესკალაცია მონაწილე მხარეებს შორის და კიბეროპერაცია გადაიზარდოს სხვა ტიპის ძალის გამოყენებაში, მაგალითად, შეიარაღებულ თავდასხმაში.

ხოლო თუ აშკარაა ფართომასშტაბიანი კიბეროპერაცია, თანმდევი სერიოზული ზიანითა და მძიმე შედეგებით, სახელმწიფოებს შესაძლოა, უღირდეთ კიდეც ასეთი შემთხვევების გასაჯაროვება, რათა მოხდეს მათი ძალის გამოყენებად დაკვალიფიცირება. მაგალითად, თუ სახელმწიფოს კიბერთავდაცვა გახდება ობიექტი ისეთი მასშტაბის კიბერთავდასხმის, რომელიც გამოიწვევს მისი ფუნქციონირების შეზღუდვას ან კითხვის ნიშნის ქვეშ დააყენებს მისი გადარჩენის საკითხს, მაშინ

სახელმწიფო, სავარაუდოდ, გაასაჯაროვებს ინფორმაციას კიბერთავდასხმის შესახებ, საერთაშორისო მხარდაჭერის მოპოვების მიზნით.

ამდენად, ესტონეთზე 2007 წელს და ირანის ბირთვულ სადგურზე 2010 წელს განხორციელებული თავდასხმისას სახელმწიფოებს მიადგათ არსებითი ზიანი, რის შემდეგაც გაასაჯაროვეს კიბეროპერაციები და მისი შედეგები. განსხვავებული იყო 2008 წელს საქართველოს წინააღმდეგ განხორციელებული კიბერშეტევები, რომლებიც წარმოადგენდა „აგვისტოს ომის“ ნაწილს და გასაჯაროვება/არგასაჯაროვების საკითხი საქართველოსთვის აზრსმოკლებული იყო. კვლავ რომ დავუბრუნდეთ ესტონეთისა და ირანის შემთხვევებს, საქართველოსგან განსხვავებით, მართალია, კიბეროპერაციები არ დაკვალიფიცირებულა ძალის გამოყენებად, მაგრამ იქცა, სახელმწიფოთა მხრივ ფართო განხილვის თემად[344]. საერთაშორისო საზოგადოება ხმამაღლა ალაპარაკდა კიბეროპერაციებსა და მათ ადგილზე საერთაშორისო სამართლის სისტემაში. სავარაუდოდ, ირანის ბირთვულ სადგურზე განხორციელებული Stuxnet ტიპის შეტევა დაკვალიფიცირდება ძალის გამოყენებად, რადგან შედეგად მოჰყვა ხელშესახები ფიზიკური ზიანი. ზოგი კომენტატორის მიერ ირანის ბირთვულ სადგურზე განხორციელებული შეტევა შედარებულ იქნა ისრაელის საჰაერო ძალების მიერ 1981-2007 წლებში ბაღდადსა და სირიაში რეაქტორებზე მიტანილ იერიშებთან.[345] თუმცა, აღნიშნულ შეტევას ნაკლები ზიანი რომ მიეყენებინა ირანისთვის, ამ უკანასკნელს ერჩია მისი საიდუმლოდ დატოვება და თავად ემოქმედა შეტევის განმახორციელებელი საუდის არაბეთში რეგისტრირებული კომპანიის

[344] მაგალითად, მკვლევრები მიიჩნევენ, რომ Stuxnet შესაძლოა, გათანაბრებოდა ძალის გამოყენებას. იხ.: *Hollis D. B.,* 'Could Deploying Stuxnet Be a War Crime?', Opinio Juris, 25 January 2011, <http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/> [15.07.2020]; *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 45; ესტონეთის მაგალითზე, ეს უკანასკნელი თავიდან იკვლევდა ჩრდილო ატლანტიკური ხელშეკრულების მე-5 მუხლის ამოქმედების შესაძლებლობას და, შესაბამისად, აღნიშნულ კიბეროპერაციებს განიხილავდა, როგორც „შეიარაღებულ თავდასხმას“, რაც გამოიწვევდა ინდივიდუალური ან კოლექტიური თავდაცვის უფლების გააქტიურებას. თუმცა, საკითხის ამგვარი გადაწყვეტა არ მოხერხდა. კონკრეტულად იხ.: *Davis J.,* 'Hackers Take Down the Most Wired Country in Europe', WIRED, 21 August 2007, <http://archive.wired.com/politics/security/magazine/15-09/ff_estonia> [15.07.2020]; *Tikk E., Kaska K. and Vihul L.,* International Cyber Incidents: Legal Considerations, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010, 25 *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds),* Edward Elgar Publishing, 2013, 192–193.

[345] *Nguyen R.,* Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, 2013, 1082–1083.

წინააღმდეგ.[346] ამ შემთხვევაშიც, ბევრი მიიჩნევს, რომ საკამათოა Stuxnet-ის ძალის გამოყენებად დაკვალიფიცირების საკითხი, ვინაიდან, დამდგარი ფიზიკური ზიანის მიუხედავად, გაეროს ქარტიის 2(4) მუხლით დადგენილი ინტენსივობის ზღვარი არ ყოფილა მიღწეული. ირანის ბირთვული სადგურის ინციდენტი გვიჩვენებს, რომ, ზოგიერთ შემთხვევაში, სახელმწიფოთა მოლოდინი ძალის გამოყენების კვალიფიკაციასთან დაკავშირებით, ბევრად მაღალია, მიუხედავად კიბეროპერაციით გამოწვეული სიმძიმისა.

5. დასკვნა

კიბეროპერაციები, რომლებიც წარმოშობს ფიზიკურ შედეგებს, როგორებიცაა - საკუთრების დაზიანება, სიცოცხლის მოსპობა ან ჯანმრთელობის დაზიანება, შედარებით მარტივად დაკვალიფიცირდება ძალის გამოყენების აკრძალვის დარღვევად. ამ თვალსაზრისით, ირანის ბირთვულ სადგურზე განხორციელებული კიბერშეტევა ერთ-ერთი იშვიათია, რომელმაც გამოიწვია ფიზიკური ზიანი,[347] და, შესაძლოა, დაკვალიფიცირდეს ძალის გამოყენებად. სამეცნიერო წრეების წარმომადგენელთა უმრავლესობა ირანის ბირთვულ სადგურზე თავდასხმას მიიჩნევს კიდეც ძალის გამოყენებად. თუმცა, ჯერჯერობით არც ერთ სახელმწიფოს ამის თაობაზე საჯაროდ არ განუცხადებია.

ესტონეთზე თავდასხმამ მნიშვნელოვანი გავლენა მოახდინა სახელმწიფოს ყოველდღიურ ყოფაზე, მაგრამ არ დამდგარა ქვეყნის არსებობა/არარსებობის საკითხი. ესტონეთის შემთხვევა თავდაპირველად მიიჩნეოდა ძალის გამოყენების აკრძალვის დარღვევად, მაგრამ, დროთა განმავლობაში, ეს მოსაზრება მიივიწყეს.

---

[346] *Perlroth N.,* 'Cyberattack on Saudi Oil Firm Disquiets U.S.', The New York Times, 23 October 2012, <www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html> [15.07.2020].

[347] გერმანიის ინფორმაციის უსაფრთხოების ფედერალურმა ოფისმა 2014 წელს განაცხადა კიბეროპერაციის შესახებ, რომელსაც შედეგად მოჰყვა ფოლადის ქარხნის ფიზიკური ზიანი. იხ. გერმანულად, Die Lage der ITSicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik, 2014, 31.

სხვა არსებული შემთხვევებიდან ვერც ერთმა დააკმაყოფილა ძალის გამოყენების ზღვარი. აღნიშნული იდეალურად ავლენს, რამდენად ცოტა კიბეროპერაცია კვალიფიცირდება ძალის გამოყენებად.

V. კიბერსაფრთხე და კიბერძალის საფრთხე

1. შესავალი

გაეროს ქარტიის 2(4) მუხლი იყო რევოლუციური ჩანაწერი. ძალის გამოყენების აკრძალვასთან ერთად, მოიცავდა ძალის გამოყენების მუქარის აკრძალვას.[348] კიბეროპერაციების მიმართ *jus contra bellum*-ის გამოყენება განმარტავს კიბერძალის კონცეფციას და ასახავს სურათს, რამდენად რთულია რეალობაში სახელმწიფოების მიერ განხორციელებული კიბეროპერაციების ძალის გამოყენებად დაკვალიფიცირება. ძალის გამოყენების საქმეების მსგავსად, სახელმწიფოების ან საერთაშორისო ორგანიზაციების მიერ კიბეროპერაციის დაკვალიფიცირება ძალის გამოყენების მუქარად ჯერ არ გამოცხადებულა.

მიუხედავად იმისა, რომ მუქარა და ძალის გამოყენება რეგულირდება ქარტიის 2(4) მუხლით, თითოეული ცალ-ცალკეა განსახილველი.[349] დღესდღეობით არსებული სამეცნიერო ლიტერატურა, გაეროს ქარტიის 2(4) მუხლის განხილვისას, კიბეროპერაციების კონტექსტში, მიმოიხილავს ძალის გამოყენებას, მუქარის ნაწილი კი უარყოფილი და შეუსწავლელი რჩება.[350] წინამდებარე თავი მიზნად ისახავს, ანალიზის საფუძველზე შეავსოს ძალის გამოყენების მუქარასთან დაკავშირებული სახელმწიფოთაშორისი კიბეროპერაციების ფენომენი. უმეტესობა სახელმწიფოთაშორისი კიბეროპერაციების კვალიფიკაცია ძალის გამოყენების მუქარად უფრო შეესაბამება რეალობას, ვიდრე მათი ძალის გამოყენებად

---

[348] იხ. ზოგადად: *Brownlie I.,* International Law and the Use of Force by States, Oxford University Press, 1963, 364; *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 19–25; *Roscini M.,* Threats of Armed Force and Contemporary International Law, Netherlands International Law Review, 54, 2007, 233; *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 92.

[349] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 44; *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 92–125; *Roscini M.,* Threats of Armed Force and Contemporary International Law, Netherlands International Law Review, 54, 2007, 233.

[350] *Schmitt M. N.,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1999, 17; *Nguyen R.,* Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, 2013, 1079-1130; *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002, 84–85.

კვალიფიცირება. ძალის გამოყენების მუქარის ორი ტიპი ხელს შეუწყობს წარმოდგენილი მოსაზრების არგუმენტებით გამყარებას. ერთი მხრივ, არსებობს ღია ძალის გამოყენების მუქარა, გარკვეულ დათმობებზე წასვლის მიზნით. მუქარის პირველი ფორმა უშუალოდ გამომდინარეობს გაეროს ქარტიის მიერ შემუშავებული ფორმულირებიდან. სახელმწიფო, რომელიც მეორე სახელმწიფოს ემუქრება ძალის გამოყენებით, რათა ეს უკანასკნელი წავიდეს გარკვეულ დათმობებზე, წარმოადგენს ქარტიის 2(4) მუხლის დარღვევას. მეორე მხრივ, არსებობს ძალის დემონსტრირების ელემენტი, რათა დამმუქრებული სახელმწიფო წავიდეს დათმობებზე.

2. ძალის გამოყენების მუქარის აკრძალვა

გაეროს ქარტიის 2(4) მუხლი კრძალავს მუქარასა და ძალის გამოყენებას, თუმცა არც გაეროს ქარტია და არც მოსამზადებელი სამუშაოები არ გვაძლევს ძალის მუქარის განმარტებას.[351] მიუხედავად ამისა, შეგვიძლია, მივიჩნიოთ, რომ აღნიშნული ტერმინი არ მოიცავს სახელმწიფოებს შორის არსებულ ყველა ტიპის მუქარას.[352] წინამდებარე ქვეთავი, ნაშრომის მიზნებიდან გამომდინარე, განიხილავს და შეაჯამებს ძალის გამოყენების მუქარის აკრძალვის მახასიათებლებს.

უნდა აღინიშნოს, რომ ტერმინი - „მუქარა“ - გაეროს ქარტიაში გვხვდება ორ ადგილას: 2(4) მუხლი, რომელიც კრძალავს ძალის გამოყენების მუქარას და 39-ე მუხლი - მშვიდობისთვის დამუქრებას. წინამდებარე ნაშრომში განხილული იქნება ქარტიის 2(4) მუხლში არსებული მუქარის აკრძალვა.

მუქარის აკრძალვასა და ძალის გამოყენების აკრძალვას რამდენიმე საერთო მახასიათებელი გააჩნია. პირველ რიგში, უნდა აღინიშნოს ის ფაქტი, რომ მუქარა ან ძალის გამოყენება შეიძლება, ჩაითვალოს კანონიერად ორ შემთხვევაში, თუ საქმე გვაქვს ინდივიდუალურ ან კოლექტიურ თავდაცვასთან (გაეროს ქარტიის მუხლი 51),[353] ან ავტორიზებულია გაეროს უშიშროების საბჭოს მიერ ქარტიის VII თავის საფუძველზე. მეორეც, მუქარის ან ძალის გამოყენების აკრძალვა წარმოადგენს

[351] *Roscini M.,* Threats of Armed Force and Contemporary International Law, Netherlands International Law Review, 54, 2007, 234.
[352] *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 88.
[353] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 218–252.

საერთაშორისო ჩვეულებითი სამართლის ნორმას, რომელიც წერილობით ასახულია გაეროს ქარტიის 2(4) მუხლში, განმტკიცებულია არსებული პრაქტიკით და *opinion juris*-ით.[354]

ძალის გამოყენების მუქარის აკრძალვა, როგორც ტერმინი, რთული განსამარტია. ჯეიმს კროუფორდი აღნიშნავს, რომ ტერმინი - „გამოყენება“ - შეიარაღებული ძალის კონტექსტში, სრულად ნათელია, ტერმინი - „მუქარა“ კი - ბუნდოვანი და დაუზუსტებელი.[355]

დღესდღეობით არსებობს მხოლოდ სამი პრეცედენტი, როცა სასამართლო ყურადღებას ამახვილებს ძალის გამოყენების მუქარაზე.[356] პირველი - *კორფუს არხის* საქმეში სასამართლომ დაადგინა, რომ საზღვაო ფლოტის ძალების დემონსტრირება, პოლიტიკური დათმობების მოპოვების მიზნით, შესაძლოა, დაკვალიფიცირდეს ძალის გამოყენების მუქარად.[357] მეორე - *ნიკარაგუის* საქმეში სასამართლომ ამერიკის შეერთებული შტატების მიერ ნიკარაგუის საზღვრებთან განხორციელებული სამხედრო მანევრები[358] და ნიკარაგუის მილიტარიზაცია არ დააკვალიფიცირა ძალის გამოყენების მუქარად.[359] ბოლოს კი, სასამართლომ დაადგინა, რომ საერთაშორისო სამართალში არ არსებობს ზოგადი წესი, რომელიც შეზღუდავს სახელმწიფოთა შეიარაღების დონეს. მესამე საქმეში - *ბირთვული იარაღის გამოყენების ან გამოყენების მუქარის კანონიერების* საკონსულტაციო დასკვნაში, სასამართლო აცხადებს, რომ მუქარა შესაძლოა, გადაიზარდოს ძალის გამოყენებაში[360] და ბირთვული იარაღის ფლობა, *per se,* არ წარმოადგენს მუქარას.[361]

---

[354] *Roscini M.,* Threats of Armed Force and Contemporary International Law, Netherlands International Law Review, 54, 2007, 252 *et seq*.

[355] *Crawford, J.,* Brownlie's Principles of Public International Law, Oxford University Press, 2012, 747; for a comprehensive study on the different possible interpretations, see, notably, *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 37–64; *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012, 92–93.

[356] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* ICJ, Judgment; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 191; *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996. აღნიშნული საქმეების საფუძვლიანი ანალიზი იხ. *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 65–91.

[357] *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* ICJ, Judgment, 35.

[358] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 227.

[359] *იქვე.* § 269.

[360] *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, § 47.

[361] *იქვე.* § 48.

სამართლიანობისთვის უნდა აღინიშნოს, რომ სასამართლოს მიდგომა ბუნდოვანია და ასახავს არსებით შეუსაბამობებს სხვადასხვა პრეცედენტის მაგალითზე.[362] მესამე საქმეში, *ბირთვული იარაღის გამოყენების ან გამოყენების მუქარის კანონიერების* საკონსულტაციო დასკვნა ერთადერთი პრეცედენტია, რომელიც იძლევა ნათელ განმარტებას.

გაეროს ქარტიის მიღების შემდეგ, ძალის გამოყენების საკითხისგან განსხვავებით, მეცნიერთა წრეებისთვის მუქარის ფენომენი ნაკლებად წარმოადგენდა საკვლევ თემას.[363] შედეგად, არ არსებობს კონსენსუსი ძალის გამოყენების მუქარის განმარტებასთან დაკავშირებით. კომენტატორების ერთი ნაწილი იზიარებს სასამართლოს პოზიციას, აღიარებს უფრო მკაცრ მიდგომას და მუქარის ცნებას შემოფარგლავს ძალის გამოყენების ცნებით, მეორე ნაწილი კი, ემხრობა უფრო ფართო მიდგომას და მიიჩნევს, რომ ძალის გამოყენების მუქარა ბევრად ფართო ცნებაა.

2.1. ძალის გამოყენების კიბერმუქარა

პირველი საკითხი, რომელიც ამ შემთხვევაში წამოიჭრება, არის შემდეგი - წარმოადგენს თუ არა ძალის გამოყენების კიბერმუქარა გაეროს ქარტიის 2(4) მუხლის დარღვევას და აქვს თუ არა, რაიმე მნიშვნელობა ერთი სახელმწიფოს მიერ მეორის დამუქრებისთვის გამოყენებულ ფორმას? პასუხი ერთმნიშვნელოვანია - არა. ქარტიის 2(4) მუხლის დარღვევისთვის, ერთმა სახელმწიფოს უნდა აცნობოს მეორეს მზაობის შესახებ, გამოიყენოს ძალა, განურჩევლად მის მიერ განხორციელებული კომუნიკაციის ფორმისა.[364] მუქარა შესაძლოა, იყოს ზეპირი ან წერილობითი სახის, რომელიც გამოხატავს სახელმწიფოს მზაობას, გამოიყენოს ძალა ან მოახდინოს ძალის გამოყენების მზაობის დემონსტრირება. კიბერმუქარა წარმოადგენს ძალის გამოყენების მუქარას, რომელიც განხორციელდა კიბერსივრცეში. თავად კიბერსივრცე, ამ შემთხვევაში, წარმოადგენს მხოლოდ კომუნიკაციის საშუალებას და კავშირი არ აქვს ძალის ან მუქარის სახეობასთან. შესაბამისად, საბოლოო ჯამში,

[362] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 90.
[363] *იქვე,* James Crawford, 'Foreword', .
[364] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 273.

განხორციელებული მუქარის კანონიერებაზე მსჯელობისას, სავსებით არარელევანტურია იმის თაობაზე დავა, რა საშუალებით განხორციელდა კიბერსივრცეში მუქარა.[365]

ძალის გამოყენების ზეპირი თუ წერილობით მუქარა სახელმწიფოს შესაძლოა, მიეწოდოს ელექტრონული ფოსტის, ტელეფონის, ასევე პრესის მეშვეობითაც, რაც თავისთავად გულისხმობს ინტერნეტგამოცემებსაც. მაგალითად, 2013 წელს ისრაელის პრემიერმინისტრთან, ბენიამინ ნეთანიაჰუსთან, შეხვედრისას ამერიკის შეერთებული შტატების სახელმწიფო მდივანმა, ჯონ კერიმ, გამოხატა ამერიკის მზადყოფნა, განეხორციელებინა მოქმედებები სირიის წინააღმდეგ და განაცხადა, რომ ძალის გამოყენების მუქარა იყო რეალური.[366] მიუხედავად იმისა, რომ აღნიშნულ განცხადებაში არ იგულისხმებოდა სირიის რომელიმე ოფიციალური წარმომადგენელი, სირიისათვის ეს ფაქტი ნაწილობრივ იყო ძალის გამოყენების კიბერმუქარა. სირიის მთავრობა ძალის გამოყენების მუქარას გაეცნო პრესის მეშვეობით. შეხვედრის ოფიციალური ტრანსკრიპტი განთავსდა ამერიკის სახელმწიფო დეპარტამენტის ოფიციალურ საიტზეც.

ზემოაღნიშნულიდან გამომდინარე, ნათლად ჩანს, რომ საერთაშორისო სამართალში სამართლებრივი მნიშვნელობა არ გააჩნია, რა გზით განხორციელდება ძალის გამოყენების მუქარა. თუმცა, საინტერესოა, რას წარმოადგენს არა ძალის გამოყენების კიბერმუქარა, არამედ კიბერძალის გამოყენების მუქარა.

2.2. აკრძალული ძალის გამოყენების მუქარის აკრძალვა

ძალის გამოყენების ღია მუქარა, დათმობების მიღების მიზნით, წარმოადგენს ძალის გამოყენების მუქარის პირველ ფორმას, რომელიც პირდაპირ, სიტყვასიტყვით არის გაწერილი გაეროს ქარტიის 2(4) მუხლში. ვინაიდან ქარტიის 2(4) მუხლით აკრძალულია მუქარა ან ძალის გამოყენება, პირველ ზომას წარმოადგენს იმის

[365] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 67–68.

[366] 'Remarks with Israeli Prime Minister Benjamin Netanyahu after Their Meeting', US Department of State, 15 September 2013, <www.state.gov/secretary/remarks/2013/09/214257.htm> [28.05.2020].

განსაზღვრა, უტოლდება თუ არა ძალის გამოყენების მუქარა აკრძალული ძალის რეალურ მუქარას.

2.3. მართლმსაჯულების საერთაშორისო სასამართლოს ფორმულა

სასამართლო *ბირთვული იარაღის* საქმეში მუქარის აკრძალვაზე საუბრისას შემოიფარგლა აკრძალული ძალის მუქარის აკრძალვით. სხვა სიტყვებით, რომ გადმოვცეთ, უკანონო მუქარა წარმოადგენს ძალის გამოყენების დაპირებას ისეთ გარემოებებში, სადაც თავად ძალის გამოყენება იქნებოდა უკანონო. აღნიშნული მიდგომა ასახულია საკონსულტაციო დასკვნის 47-ე პარაგრაფში:

> *„უკანონო თავდასხმის რიცხვის შემცირების ან გაქრობის მიზნით, სახელმწიფოები ზოგჯერ სხვა სახელმწიფოებს ანიშნებენ, რომ ფლობენ კონკრეტულ იარაღს, რომელსაც გამოიყენებენ თავდაცვისთვის იმის წინააღმდეგ, ვინც დაარღვევს ტერიტორიულ მთლიანობას ან ხელყოფს პოლიტიკურ დამოუკიდებლობას. ძალის გამოყენების განზრახვის ჩვენება, კონკრეტულ შემთხვევებში, წარმოადგენს თუ არა მუქარას, ქარტიის 2(4) მუხლის შესაბამისად, დამოკიდებულია სხვადასხვა ფაქტორზე. თუ განსაზღვრული ძალის გამოყენება, თავის მხრივ უკანონოა, მისი გამოყენების მზაობის გაცხადება იქნება 2(4) მუხლით აკრძალული მუქარა. ამასთან, უკანონო იქნება, თუ სახელმწიფო სხვა სახელმწიფოს დაემუქრება ძალის გამოყენებით მისი ტერიტორიის დაცვის მიზნით, ან გამოიწვევს, რომ კონკრეტული სახელმწიფო გაჰყვეს ან არ გაჰყვეს კონკრეტულ ეკონომიკურ თუ პოლიტიკურ გზას. გაეროს ქარტიის 2(4) მუხლში მოცემული „მუქარისა“ და „გამოყენების“ ცნებები ერთად განიხილება იმ კონტექსტში, რომ თუ რაიმე მიზეზით ძალის გამოყენება იქნება უკანონო, მაშინ ასეთი ძალის გამოყენების მუქარაც უკანონოა. სახელმწიფოს მიერ გამოხატული ძალის გამოყენების მზაობა,*

რომ ჩაითვალოს კანონიერად, მაშინ ეს ძალის გამოყენება შესაბამისი უნდა იყოს გაეროს ქარტიისა."[367]

იან ბრაუნლის მიერ 1963 წელს ჩამოყალიბებული მიდგომა, ძალის გამოყენების მუქარასთან დაკავშირებით, მხარდაჭერილია.[368] *ბირთვული იარაღის* საკონსულტაციო დასკვნა და მოსამართლეთა გამოთქმული მოსაზრებები, არც ერთი ხსნის, რატომ მოხდა შემოთავაზებული ფორმულის არჩევა.[369]

აღნიშნული ფორმულის საილუსტრაციო და ძალის გამოყენების მუქარის საუკეთესო მაგალითია, მუქარა ულტიმატუმის სახით. ულტიმატუმი, როგორც ძალის გამოყენების მუქარა, შეიძლება იყოს შემთხვევა, როდესაც ერთი სახელმწიფო მეორეს უყენებს მოთხოვნას, რომლის უარყოფას ან არშესრულებას, დროის გარკვეულ მონაკვეთში, შედეგად მოჰყვება პირველი სახელმწიფოს მხრივ მეორის მიმართ ძალის გამოყენება. მაგალითისთვის ასევე გამოდგება 2003 წლის 17 მარტს პრეზიდენტ ჯორჯ ბუშ უმცროსის მიერ ერაყისადმი ტელევიზიით გავრცელებული მიმართვა:

„ჩემო თანამოქალაქეებო, ერაყში მიმდინარე მოვლენებმა მიაღწია უკანასკნელ დღეებს. დეკადაზე მეტია, ამერიკის შეერთებული შტატები და სხვა სახელმწიფოები მიმართავდნენ დამთმობ და საყოველთაო პატივისცემაზე დაფუძნებულ მცდელობებს, განეიარაღებინათ ერაყის რეჟიმი ომის გარეშე. [...] გაერთიანებული ერების უშიშროების საბჭომ ვერ შეასრულა მის მიერ ნაკისრი ვალდებულებები, ამიტომ ჩვენ შევასრულებთ ჩვენსას. [...] ბოროტების დეკადები დასასრულს მიუახლოვდა. სადამ ჰუსეინმა და მისმა ვაჟებმა 48 საათის განმავლობაში უნდა დატოვონ ერაყი. მათი უარი შედეგად გამოიღებს სამხედრო კონფლიქტს, რომლის დაწყების დროსაც შევარჩევთ. ყველა უცხო ქვეყნის მოქალაქემ, მათ შორის, ჟურნალისტებმა და ინსპექტორებმა, უსაფრთხოების მიზნით, დაუყოვნებლივ უნდა დატოვონ ერაყი."[370]

ულტიმატუმის ვადის ამოწურვის შემდეგ, პრეზიდენტმა ბუშმა გამოაცხადა ერაყის გამათავისუფლებელი ოპერაციის დაწყება.[371] აღნიშნული შემთხვევა

---

[367] *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, § 47.
[368] *Brownlie I.,* International Law and the Use of Force by States, Oxford University Press, 1963, 364.
[369] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 40.
[370] 'Address to the Nation on Iraq', 2003, 39(12) Weekly Compilation of Presidential Documents 338, 338–341.
[371] *იქვე.* 342, 342–343.

წარმოადგენს ზეპირი მუქარის მაგალითს, რომლის მიზანიც იყო დათმობებზე წასვლა. მისი შეუსრულებლობის შემთხვევაში გამოიყენებოდა ძალა.

2.4. კიბერძალის გამოყენების ღია მუქარა

კიბეროპერაციებში კიბერძალის მუქარა არღვევს 2(4) მუხლით დადგენილ აკრძალვას, მხოლოდ იმ შემთხვევაში, თუ კიბერძალა გაუთანაბრდება ძალის უკანონო გამოყენებას, იმავე გარემოებებში. ამ თანამედროვე მიდგომას აღიარებს მკვლევართა დიდი ნაწილი და იზიარებს ტალინის პრინციპების 2.0 წესი 70: *„კიბეროპერაცია ან კიბეროპერაციის მუქარა წარმოადგენს უკანონო ძალის გამოყენების მუქარას. მუქარის განხორციელება იქნება უკანონო ძალის გამოყენება.“*[372]

ისმის შეკითხვა, საკმარისია თუ არა ძალის გამოყენების ზოგადი მუქარა გაეროს ქარტიის 2(4) მუხლის დარღვევის დადგენისთვის? პასუხი დადებითია. წერილობითი თუ ზეპირი მუქარის უმეტესობა ზოგადია და არ აკონკრეტებს, რა ძალა იქნება გამოყენებული. მაგალითად, ზემოთ განხილულ მაგალითებში, პრეზიდენტ ბუშის ულტიმატუმი ერაყსა და ჯონ კერის გაფრთხილება სირიას, ორივე შემთხვევაში არც მუქარა დაკონკრეტებულა და არც ძალის გამოყენების შესაძლებლობა. კიბერძალა დამმუქრებელი სახელმწიფოს ერთ-ერთი გამოსაყენებელი არჩევანია.

კიბერძალის მუქარა დამოკიდებულია კონკრეტული შემთხვევის სპეციფიკაზე. საფრთხის ნამდვილობას და სამიზნე სახელმწიფოს აღქმას ენიჭება განსაკუთრებული მნიშვნელობა. მართლაც, არსებითად მნიშვნელოვანია, როგორ და რამდენად სერიოზულად აღიქვამს სამიზნე სახელმწიფო ძალის გამოყენების მუქარას. ძალის გამოყენების მუქარა არსებითი საფრთხეა, თუ საკმარის საფრთხედ იქნა მიჩნეული სამიზნე სახელმწიფოს მიერ.

ამ თვალსაზრისით, შესაძლებელია მსჯელობა ალბათობის რისკზე. მაგალითად, თუ რუსეთის ფედერაცია კიბერძალის გამოყენებით ემუქრება პოსტსაბჭოთა სივრცის რომელიმე სახელმწიფოს, მაშინ მაღალია ალბათობა იმის, რომ ამგვარი მუქარა ჩაითვალოს გაეროს ქარტიის 2(4) მუხლის დარღვევად. არსებობს ფაქტობრივი

[372] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 338.

მაგალითებიც მსგავსი შემთხვევებისა საქართველოსა[373] და ესტონეთის[374] მიმართ. შესაბამისად, ზემოაღნიშნული მუქარა რეალური და საფრთხის შემცველია. რუსეთისა და რიგი პოსტსაბჭოთა ქვეყნის დაძაბული ურთიერთობის გათვალისწინებით ბევრი მიიჩნევს, რომ მუდმივად არსებობს რეალური საფრთხე, რუსეთმა გამოიყენოს ძალა ამ სახელმწიფოების მიმართ, მათ შორის კიბერძალაც.

მეორეც, სხვა გარემოებებში, კიბერძალის მუქარა შეიძლება, რეალური არც იყოს. კიბერძალის მუქარა ისეთი ქვეყნის მიმართ, რომელსაც დაბალ დონეზე აქვს განვითარებული ინტერნეტ ინფრასტრუქტურა, შესაძლებელია, არ იქნეს მიჩნეული სერიოზულ საფრთხედ. მართლაც, მსგავს შემთხვევებში, დაპირებულმა კიბერშეტევამ შესაძლოა, არ გამოიღოს მწვავე შედეგები და დიდად არ დააზიანოს მსხვერპლი სახელმწიფო. უნდა აღინიშნოს, რომ საწინააღმდეგო მტკიცება არ იქნება მართებული. სახელმწიფო მძლავრი კიბერშესაძლებლობების გარეშე შესაძლოა, გახდეს კიბეროპერაციის მსხვერპლი. აქედან გამომდინარე, მის წინააღმდეგ გამოთქმული კიბერძალის მუქარა უნდა იქნეს აღქმული რეალურად. დღესდღეობით, შედარებით მარტივი და იაფიცაა ზიანის მომტანი კიბეროპერაციის განხორციელება.

ზემოთ მოყვანილი ჰიპოთეტური მაგალითები ასახავს რეალურობის კრიტერიუმის მნიშვნელობას და ასევე წარმოაჩენს, რა განუზომელი გავლენა აქვს გაეროს ქარტიით განსაზღვრული ძალის გამოყენების აკრძალვას, კიბერძალის მუქარის კვალიფიკაციაზე.

კიბერძალის მუქარა უმეტესწილად, სავარაუდოა, წარმოიშვას სპეციფიკური ხასიათის კიბეროპერაციის შედეგად. კიბეროპერაციის ეფექტიანობა უმთავრესად წარმოადგენს კიბერ სისუსტეების გამოყენებასა და სიურპრიზის ელემენტთა ნაზავს. კონკრეტული ინფრასტრუქტურის მიმართ გამოთქმული მუქარა სამიზნე სახელმწიფოს მისცემს საშუალებას, აღმოფხვრას ინფრასტრუქტურული სისუსტეები. სახელმწიფოსთვის კიბეროპერაციის მუქარის წინასწარ გაცხადება ამ უკანასკნელს უქმნის შესაძლებლობას, მოემზადოს და დაიცვას საკუთარი ინფრასტრუქტურა,

---

373 *Markoff J.,* 'Before the Gunfire, Cyberattacks', The New York Times, 13 August 2008 <www.nytimes.com/2008/08/13/technology/13cyber.html> [17.05.2020].

374 'Estonian Links Moscow to Internet Attack', The New York Times, 18 May 2007, <www.nytimes.com/2007/05/18/world/europe/18estonia.html> [15.07.2020].

შეიმუშაოს ტექნიკური კონტრზომები[375] და განახორციელოს დამუქრებული კიბერძალის შედეგების პრევენცია.

3. კიბერძალის, როგორც აკრძალული ძალის გამოყენების მუქარის დემონსტრირება

კიბერძალის დემონსტრირება წარმოადგენს ძალის გამოყენების მუქარის მეორე ფორმას. კიბერძალის მუქარის შესახებ არსებულ სამეცნიერო ლიტერატურაში ძალის დემონსტრირება აქა-იქ ნახსენებია, მაგრამ ძირითადად მაინც გამოუკვლეველი და შეუსწავლელია.[376]

რას წარმოადგენს ძალის დემონსტრირება, რომელიც არღვევს ძალის გამოყენების მუქარის აკრძალვას? ძალის გამოყენების ღია მუქარისგან განსხვავებით, ძალის დემონსტრირება შედგება სახელმწიფოს მიერ განხორციელებული აქტებისგან. შესაბამისად, ძალის დემონსტრირებას აქვს მრავალი ფორმა, სამხედრო მოქმედებებიდან შეიძლება გამოიყოს ჯარების განლაგება, მანევრები, ბირთვული იარაღის გამოცდა, ჩვენება იმისა, რომ სახელმწიფო მზადაა, მიმართოს ძალის გამოყენებას.[377]

როდესაც საქმე ეხება კიბეროპერაციებს, მათი უმეტესობა ექცევა ფაქტობრივი ძალის გამოყენების კვალიფიკაციაში, მაგრამ შესაძლოა, წარმოადგენდეს ძალის დემონსტრირებას იმ ფორმით, რომ მოხდეს მისი აკრძალული ძალის გამოყენების მუქარად კვალიფიკაცია. აღნიშნული საკითხის ანალიზისთვის განხილული იქნება ორი ტიპის კიბეროპერაცია, შესაბამისი მაგალითებით: პირველი - DDoS ტიპის შეტევა ესტონეთსა და საქართველოზე და მეორე - კომპიუტერული ვირუსი, რომლის სამიზნე იყო ირანის ბირთვული სადგური.

---

[375] კონტრზომები გულისხმობს კიბერუსაფრთხოების კონტრზომებს, როგორებიცაა - რაიმე სახის მოქმედება, მოწყობილობა, პროცედურა, ტექნიკა საფრთხის შემცირებისთვის ან თავდასხმის აღმოფხვრისა და თავიდან აცილებისთვის. ინტერნეტ უსაფრთხოების ლექსიკონი, RFC 2828, <http://tools.ietf.org/html/rfc2828> [15.07.2020].

[376] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 67–69; *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 52–53.

[377] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 172–217.

3.1. ფართომასშტაბიანი DDoS შეტევები, როგორც ძალის დემონსტრირება

DDoS ტიპის შეტევა, როგორც წინა თავებში უკვე განიმარტა, არის კიბეროპერაცია, რომლის მიზანია, მიუწვდომელი გახადოს მანქანა ან ქსელი, მისთვის ინფორმაციის მოთხოვნის აუარებელი ნაკადის მიწოდებით. შესაძლებელია, ფართომასშტაბიანი DDoS შეტევა წარმოადგენდეს ძალის დემონსტრირებას? - პასუხი დადებითია, თუმცა გარემოებების გათვალისწინებით. ფართომასშტაბიანი DDoS შეტევები, რომლებიც განხორციელდა საქართველოსა და ესტონეთის წინააღმდეგ, შეგვიძლია მივიჩნიოთ ძალის დემონსტრირების საილუსტრაციო მაგალითად.

2008 წლის რუსეთ-საქართველოს ომამდე,[378] საქართველოს წინააღმდეგ განხორციელდა კიბეროპერაციები, რომლებიც გაგრძელდა კონფლიქტის დროსაც[379] და როგორც აღმოჩნდა, დასპონსორებული ან განხორციელებული იყო რუსული მხარის მიერ.[380] საქართველოს წინააღმდეგ განხორციელებული კიბეროპერაციები ძირითადად ორი ტიპის იყო: ვებსაიტების ინტერფეისის დაზიანება, შეცვლა და DDoS შეტევები.[381] საქართველოში კიბეროპერაციები განხორციელდა შეიარაღებული კონფლიქტის დაწყებამდე.

საქართველოს მთავრობამ აღნიშნულ კიბეროპერაციებს არ მიანიჭა ძალის გამოყენების მუქარის კვალიფიკაცია.[382] თუმცა, საქართველოსა და რუსეთს შორის არსებული დაძაბული ურთიერთობების ფონზე, კიბეროპერაციების ძალის გამოყენების მუქარად დაკვალიფიცირება სავსებით რეალური უნდა ყოფილიყო. საქართველოს მაგალითზე საუბრისას შეგვიძლია აღვნიშნოთ, რომ საქართველოში ინტერნეტის ინფრასტრუქტურა არ იყო საკმაოდ განვითარებული 2008 წელს და, შესაბამისად, ქვეყანაც არსებითად არ იყო ინტერნეტზე დამოკიდებული. ამ ფაქტორის „დამსახურებით“ კიბერშეტევას არ მოჰყოლია დამანგრეველი შედეგები. მხოლოდ საქართველოს მთავრობას შეეზღუდა წვდომა საკუთარ ვებსაიტებზე და შეექმნა

---

[378] Draft Declaration on Rights and Duties of States, UNGA Res 375 (IV) (6 December 1949).

[379] Report of the International Fact-Finding Commission on the Conflict in Georgia, September 2009, vol II, 217–219.

[380] *Markoff J.,* 'Before the Gunfire, Cyberattacks', The New York Times, 13 August 2008 <www.nytimes.com/2008/08/13/technology/13cyber.html> [17.05.2020].

[381] *Tikk E.,* et al, Cyber Attacks against Georgia: Legal Lessons Identified, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2008, 7–12.

[382] Report of the International Fact-Finding Commission on the Conflict in Georgia, September 2009, vol III.

კომუნიკაციის პრობლემა. აქედან გამომდინარე, რუსეთის მიერ განხორციელებული კიბეროპერაციების ძალის გამოყენების მუქარად დაკვალიფიცირება სადავო იყო. კიბეროპერაციის მიჩქმალვა გამოიწვია იმ ფაქტმაც, რომ ამ ყველაფერს შედეგად მოჰყვა შეიარაღებული კონფლიქტი.[383]

მეორე მაგალითი ეხება 2007 წლის ესტონეთის კიბერკრიზისს. 2007 წლის აპრილში ესტონეთის ქუჩები მოიცვა ძალადობრივი ჯგუფების პროტესტმა. პროტესტანტები იყვნენ რუსული წარმომავლობის, უმცირესობის ჯგუფის წევრები. პროტესტი წარმოშვა საბჭოთა ჯარისკაცის ქანდაკებისთვის ადგილის შეცვლამ. პროტესტის პარალელურად სახელმწიფო გახდა მრავალი კიბეროპერაციის სამიზნე, მათ შორის DDoS შეტევები განხორციელდა კერძო და საჯარო დაწესებულებების ვებსაიტებზე და სერვერებზე.[384] ესტონეთის მთავრობა ბრალს სდებდა რუსეთის ფედერაციას. თუმცა, ეს უკანასკნელი უარყოფდა კიბერშეტევებთან კავშირს.[385] საქართველოსგან განსხვავებით, ესტონეთი ძლიერ იყო დამოკიდებული ინტერნეტ სტრუქტურებზე. კიბეროპერაციების შედეგად ესტონეთის ეკონომიკამ, მედიამ და მთავრობამ განიცადა პარალიზება.

მიუხედავად იმისა, რომ არც ესტონეთმა და არც სხვა სახელმწიფოებმა აღნიშნული კიბეროპერაციები არ მიიჩნიეს მუქარად ან ძალის გამოყენებად, თამამად შეიძლება დავა იმის თაობაზე, რომ ეს კიბეროპერაციები წარმოადგენდა ძალის გამოყენების რეალურ მუქარას. კიბერშეტევებმა გამოიწვია ქვეყნის ნაწილობრივი პარალიზება და შეზღუდა ქვეყნის რეაგირების შესაძლებლობები, სამხედრო მოქმედებების საჭიროების შემთხვევაში. საქართველოს მსგავსად, ესტონეთსა და ეჭვმიტანილ სახელმწიფოს დაძაბული ურთიერთობა ჰქონდათ. ესტონეთის მაგალითი განსაკუთრებით ნათლად აჩვენებს, რამდენად დიდი ზიანი შეიძლება, მიადგეს ინტერნეტზე დამოკიდებულ სახელმწიფოს, კიბეროპერაციების მეშვეობით. ესტონეთის მიმართ განხორციელებული კიბერშეტევები შეიძლება,

---

[383] The Report of the International Fact-Finding Commission on the Conflict in Georgia, vol I, 20, § 13, 25 § 24.

[384] *Landler M. and Markoff J.,* Digital Fears Emerge after Data Siege in Estonia, The New York Times, 29 May 2007, <www.nytimes.com/2007/05/29/technology/29estonia.html> [15.07.2020]; *Tikk, E., Kasha, K., Vihul, L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010, 18–22.

[385] *Tikk, E., Kasha, K., Vihul, L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010, 23–24.

დაკვალიფიცირდეს გაეროს ქარტიის 2(4) მუხლით აკრძალული ძალის გამოყენების მუქარად.

3.2. კომპიუტერული ვირუსი, რომელმაც გამოიწვია არაფიზიკური ზიანი, როგორც ძალის დემონსტრირება.

მართალია, კიბეროპერაციის შედეგად არაფიზიკური ზიანი მიადგა სამიზნე სისტემებს, მაგრამ თავდასხმის ხარისხი არ ყოფილა საკმარისი ძალის გამოყენებად დაკვალიფიცირებისთვის. თუმცა, შეიძლება მსჯელობა, რომ გარკვეულ გარემოებებში აღნიშნული კიბეროპერაცია შესაძლოა, დაკვალიფიცირდეს ძალის გამოყენების მუქარად.

საუბარია Stuxnet ტიპის ვირუსზე, რომელმაც ფიზიკური ზიანი მიაყენა რამდენიმე ცენტრიფუგას, ირანის ბირთვულ სადგურზე.[386] სრულიად სხვა შედეგი შეიძლება დამდგარიყო, თუ ვირუსის ზიანი იქნებოდა შეუმჩნეველი. სადგურის მართვის კომპიუტერული სისტემის დაზიანებას ან დაანგარიშების მონაცემთა ცვლილებას შესაძლოა, კატასტროფული შედეგები გამოეღო, მაგრამ თავდასხმის მიზანი იყო, ბირთვული სადგურისა და, შესაბამისად, სახელმწიფოსთვის ეჩვენებინა თავდამსხმელის ძალა და მზაობაც ბევრად სერიოზული შეტევების განხორციელებისთვის. ამიტომ, სავსებით ლოგიკური იქნება, თუ ვიმსჯელებთ, რომ ირანის ბირთვული სადგურის შემთხვევაში საქმე გვაქვს ძალის დემონსტრირებასთან, რომლის მიზანიც, სავარაუდოდ, ძალის გამოყენების მუქარა იყო.

ხაზი უნდა გაესვას იმ გარემოებასაც, რომ კიბეროპერაციების შემთხვევაში ძალის გამოყენების მუქარა ან ძალის დემონსტრირება წარმოადგენს ფაქტის შედეგს. წინასწარ გაცხადებული კიბეროპერაცია ვერ იქნება იმდენად ეფექტიანი, რადგან სამიზნე სახელმწიფო თუ დაწესებულება შეძლებს მომზადებული შეხვდეს მას.

---

[386] *Shearer J.,* 'W32.Stuxnet', Symantec, 2013, <www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99> [15.07.2020]; ასევე იხ., 'Cracking Stuxnet, a 21st-Century Cyber Weapon', 2011, <www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon> [15.07.2020].

3.3. კომპიუტერული ვირუსი, რომელიც იწვევს ფიზიკურ ზიანს, როგორც ძალის დემონსტრირება

კიბეროპერაცია, რომელიც წარმოქმნის ფიზიკურ ზიანს და კვალიფიცირდება ძალის გამოყენებად, შესაძლოა, ასევე დაკვალიფიცირდეს ძალის გამოყენების მუქარად. საკამათოა, მაგრამ Stuxnet შეტევა, შესაძლოა, წარმოადგენდეს ძალის გამოყენებასა და ძალის დემონსტრირებას ერთდროულად, რომელიც ავლენს თავდამსხმელი სახელმწიფოს მიზანმიმართულობასა და მზაობას, განახორციელოს შემდგომი შეტევები.[387]

პირველი, რაზეც ყურადღება უნდა გამახვილდეს, არის ფაქტი, რომ Stuxnet-მა წარმოშვა ფიზიკური ზიანი[388] და რეალურად მოქმედებდა სამიზნე სახელმწიფოს ტერიტორიაზე. ძალის გამოყენების მუქარად აქტის კვალიფიკაციას არაფერი უშლის ხელს, მით უფრო, როდესაც აქტი კვეთს სხვა სახელმწიფოს ტერიტორიულ საზღვარს. მაგალითად, 1996 წელს, როდესაც ჩრდილოეთ კორეის წყალქვეშა ნავი სამხრეთ კორეის სანაპიროზე გამოჩნდა, ამ უკანასკნელმა აღნიშნული ფაქტი ომის აქტად გამოაცხადა.[389] აღნიშნული შემთხვევა შეგვიძლია, დავაკვალიფიციროთ ძალის გამოყენების მუქარად.[390]

შესაძლოა, ირანის შემთხვევაში, კიბეროპერაცია ყოფილიყო ძალის დემონსტრირება? - პასუხი დადებითია. პირველ რიგში, ამერიკის შეერთებული შტატები და ისრაელი ამ ვირუსის სავარაუდო შემქმნელები არიან,[391] მეორეც, ვირუსის მიზანი შესაძლოა, იყო ირანის ბირთვული პროგრამის შენელება.[392] შედეგად, კიბერშეტევა შეგვიძლია მივიჩნიოთ ძალის დემონსტრირებად ამერიკის შეერთებული შტატებისა და ისრაელის მხრიდან.

---

[387] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 173.

[388] *Broad W. J., Sanger D. E.,* 'Worm Was Perfect for Sabotaging Centrifuges', The New York Times, 18 November 2010, <www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html> [15.07.2020].

[389] 'Crisis Number: 420 – NORTH KOREAN SUBMARINE', International Crisis Behavior Project, July 2010. <www.cidcm.umd.edu/icb/> [15.07.2020].

[390] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 245–249.

[391] *Sanger D. E.,* 'Obama Ordered Wave of Cyberattacks against Iran', The New York Times, 1 June 2012, <www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave-of-cyberattacks-against-iran.html> [15.07.2020].

[392] *Sanger D. E.*, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, Crown, 2012, 200.

3.4. სამხედრო წვრთნები

ერთმანეთისგან უნდა გაიმიჯნოს ძალის დემონსტრირება და სამხედრო წვრთნები. სახელმწიფოს საზღვრებში ან მის ფარგლებს გარეთ ჩატარებული სამხედრო წვრთნები, როგორც წესი, წინასწარ ანონსდება, რათა არიდებულ იქნეს გაუგებრობა და არ ჩაითვალოს ძალის გამოყენების მუქარად ან ძალის გამოყენების პრელუდიად.[393] თუ სახელმწიფო წინასწარ არ დააანონსებს სამხედრო წვრთნებს, მაშინ მესამე სახელმწიფოს შეუძლია, მიიჩნიოს ძალის გამოყენების მუქარად. მაგალითად, 1983 წელს NATO-მ განახორციელა სამხედრო წვრთნები, რომლის დროსაც გამოცადეს ბირთვული მასალები. ორგანიზაციას არ ჰქონდა წინასწარ დაანონსებული წვრთნები, რის გამოც საბჭოთა კავშირმა ფაქტი მიიჩნია ძალის გამოყენების მუქარად და დაიწყო სამხედრო ძალების მობილიზაცია.[394] მართალია, სიტუაციას მალე მოეფინა ნათელი და ყველაფერი მშვიდობიანად დასრულდა, მაგრამ სამხედრო წვრთნებს შესაძლოა, ჰქონოდა ძალის დემონსტრირების ხასიათიც. მაგალითად, 2008 წელს რუსეთ-საქართველოს ომამდე, ამერიკის შეერთებულმა შტატებმა და რუსეთმა, ორივემ სამხედრო წვრთნები ისე ჩაატარეს, რომ შესაძლებელი ყოფილიყო ძალის დემონსტრირება ან სამხედრო ძალის გამოყენებისთვის მზაობა.[395]

კიბერსამხედრო წვრთნები განსხვავდება სხვა ტიპის სამხედრო წვრთნებისგან. სამხედრო წვრთნებს თან ახლავს ხილულობის ელემენტი - ჯარები, მანევრები, იარაღის გამოცდა, რაც შეიძლება შეცდომით იქნეს აღქმული ძალის დემონსტრირებად. თუმცა, კიბერსამხედრო წვრთნების შემთხვევაში, წვრთნები ხილული შეიძლება იყოს სხვა სახელმწიფოთა მიერ და ასევე შეცდომით იქნეს აღქმული ძალის გამოყენების მუქარად. შესაძლოა, შემჩნეულ იქნეს უჩვეულო მოქმედება სამხედრო ბაზაზე, თუნდაც - ფლოტის განლაგება ან იარაღის გამოცდა. შიგადაშიგ კიბერსამხედრო წვრთნების ძალის გამოყენების მუქარად აღქმის ალბათობა ძალიან მცირეა ან პრაქტიკულად არარსებულია.

---

[393] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 214; *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 68.

[394] მაგალითად იხ., 'Crisis Number: 344 – ABLE ARCHER 83', International Crisis Behavior Project, July 2010, <www.cidcm.umd.edu/icb/> [15.07.2020].

[395] The Report of the International Fact-Finding Commission on the Conflict in Georgia, vol I, 20, § 13, 25 § 24.

უნდა ითქვას, რომ ზოგადი სამხედრო სამზადისი არ წარმოადგენს ძალის გამოყენების მუქარას მანამ, სანამ არ ხორციელდება კონკრეტულად ძალის გამოყენების მიზნით.

4. კიბერშესაძლებლობების განვითარება არ წარმოადგენს აკრძალული ძალის გამოყენების მუქარას

წინა ქვეთავებისგან განსხვავებით, წინამდებარე ქვეთავის მიზანია აჩვენოს, რომ კიბერშესაძლებლობების განვითარება არ წარმოადგენს ძალის გამოყენების მუქარას. მსგავსი საკითხი ადრეც გამხდარა განხილვის საგანი. კომენტატორები და აქტორები ძირითადად მიიჩნევენ, რომ კონკრეტული იარაღის განვითარება და სახელმწიფოების მიერ შეიარაღების გაძლიერება წარმოადგენს ძალის გამოყენების მუქარას ან მშვიდობის საფრთხეს. *ბირთვული იარაღის* საქმე ამის კარგი მაგალითია.[396]

ზოგი სახელმწიფო ბირთვული იარაღის ფლობას მიიჩნევს ძალის გამოყენების უკანონო მუქარად, მეორე ნაწილი არ ეთანხმება ამ მოსაზრებას.[397] სასამართლომ აღნიშნულ საკითხთან დაკავშირებით, პოზიცია გამოხატა, *ბირთვული იარაღის* საქმეში, უარყო შეხედულება, რომ ბირთვული იარაღის ფლობა წარმოადგენს გაეროს ქარტიის 2(4) მუხლით გათვალისწინებულ უკანონო მუქარას *per se*:

> *„იკვეთება თუ არა „მუქარა“, ქარტიის 2(4) მუხლის შესაბამისად, დამოკიდებულია იმაზე, კონკრეტული ძალის გამოყენება მიმართულია თუ არა სახელმწიფოს ტერიტორიული მთლიანობის ან პოლიტიკური დამოუკიდებლობის წინააღმდეგ, ან გაერთიანებული ერების მიზნების წინააღმდეგ. ეს ქმედება თუნდაც ჩაფიქრებული ყოფილიყო, როგორც თავდაცვის საშუალება, აუცილებლად დაარღვევს საჭიროებისა და პროპორციულობის პრინციპებს.“*[398]

[396] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 325.
[397] *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 79 et seq.
[398] *Legality of the Threat or Use of Nuclear Weapons,* ICJ, Advisory Opinion, 8 July 1996, § 48; *Stürchler N.,* The Threat of Force in International Law, Cambridge University Press, 2007, 79.

შედეგად, ბირთვული იარაღის აკუმულირება, თავის მხრივ, არ წარმოადგენს ძალის გამოყენების მუქარას.[399] ირანის ან ჩრდილოეთ კორეის შემთხვევაში, საფრთხე მომდინარეობს არა ბირთვული პროგრამის იმპლემენტაციიდან, არამედ თავად სახელმწიფოებიდან.[400]

ნიკარაგუის საქმეში სასამართლომ დაადგინა უფრო ზოგადი წესი სახელმწიფოთა მიერ სამხედრო კომპონენტის განვითარებაზე: საერთაშორისო სამართალში არ არსებობს კონკრეტული ნორმა, რომელიც ზღუდავს სახელმწიფოს შეიარაღების დონეს.[401]

დასკვნის სახით, შეგვიძლია ვთქვათ, რომ იგივე პირობები ვრცელდება კიბერშესაძლებლობებზეც, რომლებიც, თავის მხრივ, არ არის აუცილებელი, წარმოადგენდეს ძალის გამოყენების მუქარას. მაგალითად, ამერიკის შეერთებულმა შტატებმა დანერგა ე.წ. „ოლიმპიური თამაშების“ პროგრამა, კიბერშესაძლებლობების განვითარების მიზნით.[402] რასაკვირველია, აღნიშნული პროგრამა ვერ ჩაითვლება ძალის გამოყენების მუქარად, მაგრამ, თუ პროგრამა გამოყენებული იქნება სხვა სახელმწიფოების წინააღმდეგ, კიბეროპერაციების განხორციელებისთვის, მაშინ შეიძლება ჩაითვალოს კიბერძალის გამოყენების მუქარად.

5. დასკვნა

წინამდებარე თავში განხილვის შედეგად დადგინდა, რომ ძალის გამოყენების მუქარად დაკვალიფიცირება უფრო მარტივი და, ხშირ შემთხვევაში, შესაფერისიცაა სახელმწიფოთაშორის არსებულ კიბეროპერაციებისთვის, ვიდრე ძალის გამოყენებად დაკვალიფიცირება. ნაჩვენები იქნა, რომ ზოგი კიბეროპერაცია წარმოადგენს კიბერძალის ღია მუქარას, ნაწილი კი ექცევა კიბერძალის დემონსტრირების

[399] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 326.

[400] *იქვე.*

[401] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 269.

[402] *Sanger D. E.,* 'Obama Ordered Wave of Cyberattacks against Iran', The New York Times, 1 June 2012, <www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave-of-cyberattacks-against-iran.html> [15.07.2020]; *Sanger D. E.*, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, Crown, 2012, 200.

კატეგორიაში. დღემდე არსებული ფაქტობრივი მასალებიდან ირკვევა, რომ მათი დაკვალიფიცირება, როგორც კიბერძალის გამოყენება ან კიბერძალის გამოყენების ღია მუქარა, ცოტა არ იყოს და რთულია. შესაძლებელია საპირისპირო მაგალითების დასახელებაც და მათი დაკვალიფიცირება ძალის დემონსტრირებად, რაც, თავის მხრივ, უთანაბრდება აკრძალული ძალის გამოყენების მუქარას. თუმცა, აქვე უნდა ითქვას ისიც, რომ კიბერშესაძლებლობათა განვითარება არ წარმოადგენს კიბერძალის გამოყენების მუქარას.

VI. კიბერ შეიარაღებული თავდასხმა და კიბერაგრესია

1. შესავალი

მხოლოდ ისეთი კიბეროპერაცია ააქტიურებს სახელმწიფოს თავდაცვის უფლებას, რომელიც აღწევს შეიარაღებული თავდასხმის დონეს. ჩვეულებით სამართალში არსებული თავდაცვის უფლება გაწერილია გაეროს ქარტიის 51-ე მუხლში და მრავალჯერ არის მოხსენიებული სასამართლოს მიერ განხილულ სხვადასხვა საქმესა თუ საკონსულტაციო დასკვნაში. გაეროს ქარტია არ გვთავაზობს შეიარაღებული თავდასხმის განმარტებას. წინამდებარე თავის მიზანია, განმარტოს, რას წარმოადგენს კიბერ შეირაღებული თავდასხმა. ამისთვის გაანალიზდება, თუ რა პირობებში აღწევს კიბეროპერაცია შეიარაღებულ თავდასხმად კვალიფიცირების სტანდარტებს.

ძალის გამოყენების სხვადასხვა ტიპზე საუბრისას გაეროს ქარტია იყენებს სამ ტერმინს: „ძალა“, „აგრესია“, „შეიარაღებული თავდასხმა“. ქარტიის 2(4) მუხლი კრძალავს მუქარას ან ძალის გამოყენებას. ქარტიის 39-ე მუხლი განსაზღვრავს უშიშროების საბჭოს კომპეტენციას, დაადგინოს მშვიდობისთვის საფრთხის არსებობა, მშვიდობის დარღვევა ან აგრესიის აქტის არსებობა, რაც შესაძლოა, მოითხოვდეს ისეთი მოქმედებების განხორციელებას, რომლებიც მოიცავს ძალის გამოყენებას. და ბოლოს, ქარტიის 51-ე მუხლი ადგენს თავდაცვის უფლებას შეიარაღებული თავდასხმის დროს. შეკითხვა კი მდგომარეობს შემდეგში, რა ურთიერთმიმართება აქვს ერთმანეთთან ძალის გამოყენების ამ სამ ფორმას.

ცნობილია, რომ მათ შორის არსებობს ე.წ. „კასკადური ურთიერთობა“.[403] შეიარაღებული თავდასხმა - შედარებით ვიწრო ტერმინია და წარმოადგენს აგრესიის ქვეკატეგორიას, ხოლო აგრესია, თავის მხრივ, არის ძალის ქვეკატეგორია. არც ერთი ამ ტერმინთაგან არ არის განმარტებული გაეროს ქარტიით. მეტიც, გაეროს ქარტიის სხვადასხვა თარგმანში აღნიშნული ტერმინების გამოყენება, გარკვეულწილად, ბუნდოვანებას ქმნის. მაგალითად, თავდაცვის უფლების *ratione materiae* მდგომარეობა

[403] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 137.

ინგლისურში გვხვდება შეიარაღებული თავდასხმის სახით, ხოლო ფრანგულში, როგორც - *„aggression armee“.* ამ უკანასკნელი ტერმინის გამოყენებამ კი დაბნეულობა გამოიწვია შეიარაღებული თავდასხმისა და აგრესიის ტერმინებს შორის.[404]

სასამართლომ *ნიკარაგუის საქმეში* განაცხადა, რომ შეიარაღებული თავდასხმა განმარტებული არ არის არც გაეროს ქარტიაში, არც სახელშეკრულებო სამართალში.[405] *ბირთვული იარაღის* შესახებ საკონსულტაციო დასკვნაში კი, სასამართლომ დაადგინა, რომ გაეროს ქარტიით დარეგულირებული ძალის გამოყენება ეხება ყველანაირი სახის ძალის გამოყენებას, მიუხედავად გამოყენებული იარაღისა.[406] პოტენციურად არ არსებობს დაბრკოლება, რომელიც კიბეროპერაციას არ მისცემდა შეიარაღებულ თავდასხმად დაკვალიფიცირების საშუალებას. ეჭვგარეშეა, რომ კიბეროპერაცია შესაძლებელია, მოიცავდეს უკანონო ძალის გამოყენებას, აგრესიის აქტს ან თუნდაც შეიარაღებულ თავდასხმას. აღნიშნულ პოზიციას იზიარებენ სახელმწიფოები, რაც ასახულია სამეცნიერო ლიტერატურაშიც.[407] ამის მიუხედავად, დღემდე არც ერთ სახელმწიფოს ან საერთაშორისო საზოგადოებას არ განუცხადებია, რომ რომელიმე კიბეროპერაციამ მიაღწია შეიარაღებული თავდასხმის ზღვარს.[408]

ნიკარაგუისა და *უგანდა vs. კონგოს დემოკრატიული რესპუბლიკის* საქმეებში სასამართლომ გამოიყენა გაეროს გენერალური ასამბლეის მიერ მიღებული „აგრესიის დეფინიციის“ მე-3 მუხლის g ნაწილი შეიარაღებული თავდასხმის განსაზღვრისთვის.[409] 1974 წლის 14 დეკემბერს გაეროს გენერალურმა ასამბლეამ მიიღო რეზოლუცია 3314 აგრესიის დეფინიციაზე.[410] აღნიშნული რეზოლუცია არ წარმოადგენს სახელმძღვანელოს უშიშროების საბჭოსთვის აგრესიის არსებობის

---

[404] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020, 328.

[405] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 176.

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

[407] *Koh H. H.,* International Law in Cyberspace, USCYBERCOM Inter-Agency Legal Conference, 2012, <www.state.gov/s/l/releases/remarks/197924.htm> [15.07.2020]. *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 70–71; *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 54.

[408] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 57-58.

[409] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 195; *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005, § 146.

[410] Definition of Aggression, UNGA Res 3314 (XXIX) (14 December 1974).

განსაზღვრისთვის, გაეროს ქარტიის 39-ე მუხლის ფარგლებში.[411] აგრესიის დეფინიციის პრეამბულა ადგენს, რომ აგრესია წარმოადგენს უკანონო ძალის გამოყენების ყველაზე სერიოზულ და საშიშ ფორმას. აგრესიის დეფინიციის პირველი მუხლის თანახმად, აგრესია არის სახელმწიფოს მიერ შეიარაღებული ძალის გამოყენება სხვა სახელმწიფოს სუვერენიტეტის, ტერიტორიული მთლიანობის ან პოლიტიკური დამოუკიდებლობის წინააღმდეგ, ან ნებისმიერი სხვა ფორმა, რომელიც არ შეესაბამება გაეროს ქარტიას. გარდა ამისა, მე-3 მუხლი გვთავაზობს აგრესიის აქტების სიას. მიჩნეულია, რომ აღნიშნული მუხლის a(ა), b(ბ), d(დ) და g(ზ) ნაწილები, აგრესიის აქტთან ერთად, წარმოადგენს შეიარაღებულ თავდასხმასაც. აღნიშნული ნაწილები:

> *„(ა) სახელმწიფოს შეჭრა ან შეიარაღებული ძალებით თავდასხმა სხვა სახელმწიფოს ტერიტორიაზე, ან ნებისმიერი სახის სამხედრო ოკუპაცია, რომლებსაც შედეგად მოჰყვება მეორე სახელმწიფოს ან მისი ნაწილის ანექსია, ძალის გამოყენებით;*
>
> *(ბ) სახელმწიფოს მიერ მეორე სახელმწიფოს ტერიტორიის დაბომბვა შეიარაღებული ძალების მიერ ან რაიმე სახის იარაღის გამოყენება;*
>
> *[...]*
>
> *(დ) სახელმწიფოს მიერ შეიარაღებული ძალების მეშვეობით განხორციელებული შეტევა მეორე სახელმწიფოს მიწაზე, ზღვაზე ან საჰაერო და საზღვაო ძალებსა და საჰაერო ხომალდებზე;*
>
> *[...]*
>
> *(ზ) სახელმწიფოს სახელით ან დავალებით მოქმედი შეიარაღებული განდების, დაჯგუფებების ან დაქირავებული მებრძოლების მიერ მეორე სახელმწიფოს წინააღმდეგ შეიარაღებული ძალის გამოყენება იმ სიმძიმით, რომელიც უტოლდება ზემოთ ჩამოთვლილ აქტებს და არსებითი მონაწილეობა.“*[412]

აგრესიის დეფინიციაში ნათლად წერია, რომ ჩამოთვლილი აქტები არ არის ამომწურავი და უშიშროების საბჭოს შეუძლია, სხვაც განსაზღვროს აგრესიის აქტებად,

---

[411] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 136.

[412] Definition of Aggression, UNGA Res 3314 (XXIX) (14 December 1974), Article 3.

ქარტიის დებულებათა საფუძველზე.[413] ჩამოთვლილი აქტები ასევე მიჩნეულია შეიარაღებული თავდასხმის ფორმებად და არ არის ყოვლისმომცველი. სხვა აქტებიც შეიძლება გულისხმობდეს შეირაღებულ თავდასხმას.[414]

კასკადური ურთიერთობები ძალის, აგრესიისა და შეიარაღებული თავდასხმის ცნებებს შორის წარმოშობს შეკითხვას, არსებობს თუ არა ნაპრალი ამ სამ ცნებას შორის? უფრო კონკრეტულად, არსებობს თუ არა სხვა ძალის გამოყენების უკანონო ფორმები, რომლებიც არ წარმოადგენს შეიარაღებულ თავდასხმას? სასამართლომ ამგვარი ნაპრალის არსებობა დაადასტურა *ნიკარაგუის საქმეში* და განსაზღვრა ძალის გამოყენების ყველაზე მძიმე ფორმები (შეიარაღებული თავდასხმა).[415] უნდა ითქვას, რომ აღნიშნული ნაპრალის არსებობა სადავო საკითხია საერთაშორისო სამართალში. ზოგი სახელმწიფო, განსაკუთრებით ამერიკის შეერთებული შტატები, შეიარაღებულ თავდასხმას უთანაბრებს ძალის გამოყენებას და, შესაბამისად, მიიჩნევს, რომ ნებისმიერი ძალის გამოყენება ააქტიურებს თავდაცვის უფლებას. ამის მსგავსად, ტალინის სახელმძღვანელო პრინციპების 2.0 შემუშავებაში მონაწილე ექსპერტების უმეტესობა აცნობიერებს ზემოაღნიშნული ნაპრალის არსებობას.[416] მოსაზრების მომხრეები აღნიშნავენ, რომ სადავოა მხოლოდ თავად ამ ნაპრალის მოცულობა.[417]

წინამდებარე ნაშრომი ემხრობა მკვლევართა უმეტესობის მიდგომას და აღიარებს ნაპრალის არსებობას. კიბერძალის გამოყენების მხოლოდ უმძიმესი ფორმები შეიძლება დაკვალიფიცირდეს კიბერ შეიარაღებულ თავდასხმად. მაგალითად, ნებისმიერი ფიზიკური განადგურება, რომელიც მომდინარეობს კიბეროპერაციის შედეგად, დაკვალიფიცირდება კიბერძალის გამოყენებად.[418] დაბალი ინტენსივობის კიბეროპერაციები არ დაკვალიფიცირდება კიბერ შეიარაღებულ თავდასხმად, მაგალითად, ერთი სმარტფონის განადგურება ან სხვა მსგავსი შემთხვევები. ამგვარ

---

[413] Definition of Aggression, UNGA Res 3314 (XXIX) (14 December 1974), Article 4.

[414] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 139.

[415] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 191; ასევე იხ., *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013, 250.

[416] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 341. ასევე იხ., *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 55.

[417] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 72–73.

[418] იხ., ნაშრომის III თავის მე-4 ქვეთავი.

შემთხვევებში, სახელმწიფოს შეუძლიამ მიმართოს მხოლოდ მართლსაწინააღმდეგო ზომებს, მაგრამ ვერ გააქტიურებს თავდაცვის უფლებას. თუ ძალის გამოყენება და შეიარაღებული თავდასხმა ერთმანეთს გაუთანაბრდება, სავარაუდოდ, ორივე შემთხვევაში, გამოყენებულ უნდა იქნეს შეიარაღებული თავდასხმის უფრო მაღალი ზღვარი.

კიბეროპერაციების მასშტაბი და შედეგები განსაზღვრავს, აღწევს თუ არა შეიარაღებული თავდასხმის დონეს.[419] აღნიშნული სტანდარტი შედგება ორი კუმულაციური კრიტერიუმისგან: პირველი „მასშტაბი“, რაც გულისხმობს კიბეროპერაციის მაგნიტუდასა და ინტენსივობას (გამოყენებული ძალის ოდენობა, მისი ადგილმდებარეობა და ხანგრძლივობა); და მეორე, „შედეგები“, რაც გულისხმობს კიბეროპერაციის შედეგებს (ზიანი და დანაკარგი).[420] კიბეროპერაციების შემთხვევაში, იშვიათად შეიძლება დაკმაყოფილდეს ორივე კრიტერიუმი კუმულატიურად. მაგალითად, DDoS შეტევები, რომლებიც განხორციელდა ესტონეთის წინააღმდეგ 2007 წელს, სავარაუდოდ, აკმაყოფილებდა მასშტაბის კრიტერიუმს, თუმცა, საეჭვოა, დაეკმაყოფილებინა შედეგების კრიტერიუმი.[421]

2. კიბეროპერაციების შედეგები

შედეგების მიხედვით შესაძლებელია, გამოიყოს ორი ტიპის კიბეროპერაცია: პირველი, რომელსაც მოსდევს ფიზიკური შედეგები (ტრავმა, სიცოცხლის მოსპობა, საკუთრების ზიანი ან განადგურება) და მეორე, რომელსაც არ მოსდევს ფიზიკური შედეგები (მონაცემების განადგურება, შეცვლა ან დაზიანება). სხვადასხვა შედეგის დეტალურად განხილვამდე აუცილებლად უნდა განისაზღვროს, რომელი უნდა იქნეს გათვალისწინებული.

---

[419] „მასშტაბისა და შედეგების“ სტანდარტი სასამართლოს მიერ გამოყენებულ იქნა *ნიკარაგუის საქმეში: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 195. საზოგადოდ, აღიარებულია, რომ აღნიშნული სტანდარტი გამოიყენება შეიარაღებული თავდასხმის არსებობის დასადგენად.

[420] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 139; *Constantinou A.,* The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter, Sakkoulas & Bruylant, 2000, 63.

[421] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 73.

2.1. გასათვალისწინებელი შედეგები

კომპიუტერული ქსელების ურთიერთკავშირის გამო, კიბეროპერაციებმა შესაძლოა, მარტივად გამოიწვიოს მნიშვნელოვანი გვერდითი ეფექტები და ირიბი ზიანი. მაგალითად, 2003 წლის 25 იანვარს Slammer Worm-მა[422] გამოიყენა მაიკროსოფტის sql სერვერის სუსტი წერტილები და მსოფლიოს მასშტაბით თხუთმეტ წუთზე ნაკლებ დროში დააზიანა ათასობით სერვერი. ქმედების მიზანი იყო, სისტემური მეხსიერებისა და სხვა მიმღებების დაზიანება. მას არ გაუნადგურებია მყარ დისკზე შენახული ინფორმაცია. თუმცაღა, Slammer-მა გამოიწვია სერიოზული დამაზიანებელი შედეგები - რამდენიმე ქვეყანაში ინტერნეტის შენელება, ან საერთოდ შეწყვეტა; ფუნქციონირება შეაჩერა ამერიკის ბანკის ათასობით ბანკომატმა, დაიბლოკა ბილეთების გაცემის სისტემა კონტინენტალურ ავიახაზებში, რამაც კომპანია აიძულა, გაეუქმებინა რამდენიმე რეისი. ვირუსმა ასევე დააზიანა ამერიკაში მდებარე დევის-ბესეს ბირთვული სადგურის კომპიუტერული სისტემა, მოიშალა სადგურის უსაფრთხოების პარამეტრების მონიტორინგის სისტემა. საბედნიეროდ, ბირთვული სადგურისთვის სერიოზული ზიანის მიყენება ვერ მოხერხდა. აღნიშნული შემთხვევის მაგალითზე ნათლად გამოჩნდა, რომ კომპიუტერულმა ვირუსმა გაცილებით ფართო მასშტაბები მოიცვა, ვიდრე მისი რეალური მიზანი იყო.

ტალინის სახელმძღვანელო პრინციპების 2.0 თანახმად, კიბეროპერაციების ყველა გონივრულად განჭვრეტადი შედეგი კვალიფიცირდება.[423] მაგალითად, ქალაქის ელექტროსისტემის დაზიანების პოტენციური შედეგი შეიძლება იყოს ზარალი, ტრავმა, სიცოცხლის მოსპობა და სხვ. აღნიშნული შედეგები უნდა იქნეს მიჩნეული განჭვრეტადად. ამავე ლოგიკით, საჰაერო ტრაფიკის კონტროლის სისტემის

---

[422] Slammer-ის ვირუსი არ წარმოადგენს სახელმწიფოს მიერ განხორციელებულ კიბეროპერაციას და გამოყენებულია, მხოლოდ როგორც მაგალითი. Slammer-ზე, ზოგადად იხ., *Ray E.,* 'Malware FAQ: MS-SQL Slammer' (SANS) <www.sans.org/security-resources/malwarefaq/ms-sqlexploit.php> [25.06.2020]; 'WORM:W32/SLAMMER' (F-Secure) <www.f-secure.com/v-descs/mssqlm.shtml> [25.06.2020]; *Boutin P.,* 'Slammed!', WIRED, 1 July 2003, <www.wired.com/2003/07/slammer/> [25.06.2020]; *Kesler B.,* 'The Vulnerability of Nuclear Facilities to Cyber Attack', Strategic Insights, 10, 2010, 19–20.

[423] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 343. ასევე იხ., *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 57.

დაზიანებისას განჭვრეტად შედეგად შეგვიძლია, მივიჩნიოთ საჰაერო ხომალდის ჩამოვარდნა.

2.2. კიბეროპერაციები, რომლებიც წარმოშობს ფიზიკურ შედეგებს

კიბეროპერაციები, რომლებიც წარმოშობს ფიზიკურ შედეგებს (ტრავმა, სიცოცხლის მოსპობა, საკუთრების დაზიანება ან განადგურება) ძირითადად მიიჩნევა ძალის გამოყენებად. მათგან ყველაზე მძიმემ შესაძლოა, შეიარაღებული თავდასხმის დონესაც კი მიაღწიოს.[424]

მსჯელობის საგანს წარმოადგენს სიმძიმის ზღვრის არსებობა.[425] მარტივად რომ ვთქვათ, საკმარის საფუძველს შეუქმნის თუ არა კიბეროპერაციის შედეგად გამოწვეული საკუთრების ზიანი ან განადგურება, ტრავმა ან სიცოცხლის მოსპობა, რათა მოხდეს მისი კიბერ შეიარაღებულ თავდასხმად დაკვალიფიცირება. აღნიშნულ შეკითხვას მივყავართ კიბერძალის გამოყენებასა და კიბერ შეიარაღებულ თავდასხმას შორის არსებული ნაპრალის მოცულობამდე. როგორც ზემოთ აღინიშნა, კიბეროპერაცია, რომელსაც შედეგად მოჰყვება სიცოცხლის მოსპობა ან დაზიანება, ეჭვგარეშე წარმოადგენს ძალის გამოყენებას.[426] აღნიშული საკითხი განხილვის თემას წარმოადგენს კიბერსამყაროს ფარგლებს გარეთაც. სასამართლომ შეიარაღებული თავდასხმა მიაკუთვნა ძალის გამოყენების ყველაზე მძიმე ფორმას, მაგრამ მიიჩნია, რომ ერთი სამხედრო ხომალდის განადგურება შეიძლება საკმარისი იყოს თავდაცვის თანდაყოლილი უფლების გააქტიურებისთვის.[427]

კიბეროპერაციები, რომლებიც იწვევს განადგურებას, ზიანს, სიცოცხლის მოსპობას ან ტრავმას შესაძლოა, დაკვალიფიცირდეს შეიარაღებულ თავდასხმად, მაგრამ მხოლოდ იმ შემთხვევაში, თუ შედეგები კონკრეტული ინტენსივობის შესაბამისია.

---

[424] *Joyner C. C. and Lotrionte C.,* Information Warfare as International Coercion: Elements of a Legal Framework, European Journal of International Law, 12, 2001, 855; *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 55; *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 73–74.

[425] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 341. ასევე იხ. *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 56.

[426] იხ., ნაშრომის III თავის მე-2 ქვეთავი.

[427] *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, § 72.

როგორც ირკვევა, კიბეროპერაციების ფიზიკური შედეგები უნდა აღწევდეს ინტენსივობის გარკვეულ ზღვარს.[428] მაგალითად, Stuxnet-ის შემთხვევაში, შესაძლოა მსჯელობა ორივე მიმართებით - მიაღწია ან არა ინტენსივობის ზღვარს.[429] ამ მხრივ, შეიძლება ვარაუდი, რომ Stuxnet-ის შედეგები დაკვალიფიცირდება ძალის გამოყენებად, მაგრამ არა შეიარაღებულ თავდასხმად. თუმცა, ის გარემოება, რომ სამიზნე იყო ბირთვული სადგური, შედარებით ამძიმებს სურათს და სწორედ ამიტომ მიიჩნევს კომენტატორთა ნაწილი, რომ აშკარა იყო შეიარაღებული თავდასხმა. ტალინის სახელმძღვანელო პრინციპები 2.0 განმარტავს, შეიძლება თუ არა აღნიშნული შემთხვევა მივიჩნიოთ შეიარაღებულ თავდასხმად, ვინაიდან შედეგად დადგა რამდენიმე ცენტრიფუგის განადგურება. სწორედ ეს პოზიცია გაიზიარა ექსპერტთა საერთაშორისო ჯგუფის ნაწილმა.[430] აღნიშნული კიბეროპერაცია ერთ-ერთია დღემდე, რომელმაც წარმოშვა მძიმე შედეგები. ამ მაგალითით კარგად ჩანს, რომ შეიარაღებულ თავდასხმად კიბეროპერაციების მხოლოდ ძალიან მცირე ნაწილი ჩაითვლება და ამისთვის აუცილებელი იქნება მძიმე შედეგების არსებობა.

2.3. კიბეროპერაციები, რომლებიც არ წარმოქმნის ფიზიკურ შედეგებს

შესაძლებელია თუ არა კიბეროპერაციებმა, რომლებსაც შედეგად არ მოჰყვება ფიზიკური ზიანი (მონაცემთა დაზიანება, შეცვლა ან განადგურება) მიაღწიოს შეიარაღებული თავდასხმის ზღვარს? ეს შეკითხვა რთული და სადავოა.[431] სახელმწიფოთა ნაწილმა გადაწყვიტა, ეს საკითხი გაეთვალისწინებინა საკუთარ კიბერსტრატეგიაში, კერძოდ, გარკვეული გარემოებების არსებობის შემთხვევაში,

[428] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 75.
[429] *O'Connell, M. E.*, The Prohibition of the Use of Force in *Henderson C. and White N. (eds)*, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, Edward Elgar Publishing, 2013, 201–202; ; *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 76.
[430] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 342. ასევე იხ. *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 58.
[431] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 56.

კიბეროპერაციები, რომლებიც არ წარმოქმნის ფიზიკურ შედეგებს, გათანაბრებოდა შეიარაღებულ თავდასხმას.

ინფორმაციის, თუნდაც სენსიტიური სამხედრო მასალის მოპარვა არ უთანაბრდება შეიარაღებულ თავდასხმას. ამასთანავე, მსგავსი კიბეროპერაციის შედეგი არ არის იმწამიერი ტრავმა, სიცოცხლის მოსპობა, საკუთრების დაზიანება ან განადგურება. ქურდობა, თავის მხრივ, არ არის საკმარისი შედეგი, რომ მიესადაგოს „შედეგების“ ზოგად კრიტერიუმს. აღნიშნულ პოზიციას იზიარებს კომენტატორთა უმეტესობა,[432] მიუხედავად იმისა, რომ არსებობს ისეთი ნაწილიც, რომელიც მიიჩნევს, რომ ინფორმაციის მოპარვა სასიცოცხლო მნიშვნელობისაა სახელმწიფო უსაფრთხოებისთვის და შესაძლოა, დაკვალიფიცირდეს შეიარაღებულ თავდასხმად.[433] კიბეროპერაციები, რომლებიც წარმოქმნის უმძიმეს არაფიზიკურ შედეგებს, მართალია, დასაშვებია თეორიულად, მაგრამ მხოლოდ იშვიათ შემთხვევაშია შესაძლებელი, მისი გათანაბრება შეიარაღებულ თავდასხმასთან.

3. კიბეროპერაციების შეკრებითობა, შეიარაღებული თავდასხმის გარდა

რიგ შემთხვევაში, სახელმწიფო შეიძლება გახდეს მსხვერპლი კიბეროპერაციებისა, რომლებიც კვეთს ძალის გამოყენების ზღვარს, თუმცა, ცალ-ცალკე აქტი ვერ აკმაყოფილებს შეიარაღებული თავდასხმის სტანდარტს.[434]

შემთხვევების შეკრებითობის თეორიას ასევე მოიხსენიებენ ქინძისთავის ნაჩხვლეტის (pin-prick) სახელით. აღნიშნული თეორიის თანახმად, ცალკეული კიბეროპერაციის შემთხვევა ვერ დაკვალიფიცირდება შეიარაღებულ თავდასხმად, მაგრამ კუმულატიურად ყველა ერთად მიიღებს ამგვარ კვალიფიკაციას. ამ თეორიას გზა გაუკვალა სასამართლომ, რომელმაც *ნიკარაგუის საქმეზე* დასვა შეკითხვა - სახელმწიფოს ტერიტორიაზე შეჭრა, სამართლებრივი თვალსაზრისით,

[432] *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 55; *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 71.

[433] *Joyner C. C. and Lotrionte C.,* Information Warfare as International Coercion: Elements of a Legal Framework, European Journal of International Law, 12, 2001, 855.

[434] *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2012, 93–95.

დამოუკიდებლად ან ერთობლივად შეიძლება თუ არა მიჩნეულ იქნეს შეიარაღებული თავდასხმის ტოლფასად.[435] მსგავსი მიდგომა გათვალისწინდა *ნავთობის პლატფორმებისა* და *კონგო უგანდას წინააღმდეგ* საქმეებში.[436] მცირე მასშტაბის მოვლენების გაანალიზება, შემთხვევათა შეკრებითობის თეორიის მიხედვით, დამხმარე საშუალებაა შეიარაღებული თავდასხმის იდენტიფიცირებისთვის, რაც, როგორც ჩანს, ფართოდ გამოიყენება თავდაცვის უფლების გააქტიურების მიზნით.[437]

სამეცნიერო ლიტერატურა კიბეროპერაციებისა და თავდაცვის თემებზე ძირითადად ემხრობა ზემოაღნიშნული თეორიას, რადგან ეს უკანასკნელი იძლევა საშუალებას, რამდენიმე კიბეროპერაცია ინტერგრირდეს ერთდროულად.[438] ზოგ შემთხვევაში, კიბეროპერაციების სამიზნე შესაძლოა, იყოს სხვადასხვა სექტორი, რათა მიიღწეს მაქსიმალური შედეგი. მაგალითად, 2007 წელს ესტონეთის წინააღმდეგ განხორციელებული კიბეროპერაციები, ერთდროულად მიმართული იყო სამთავრობო და კერძო სექტორის დაწესებულებათა წინააღმდეგ.[439] ასეთ დროს, შემთხვევების შეკრებითობის თეორია საშუალებას იძლევა, რამდენიმე კიბეროპერაციისგან შემდგარი თავდასხმა იქნეს გათვალისწინებული, რაც წარმოადგენს კიდეც არსებული რეალობიდან გამომდინარე ყველაზე შესაბამის პასუხს. როგორც ზემოთ აღინიშნა, კიბეროპერაციები, რომლებიც აღწევს ძალის გამოყენების ზღვარს, შესაძლოა არ დაკვალიფიცირდეს შეიარაღებულ თავდასხმად. თუმცა, მათი კუმულატიურად გაანალიზება, შესაძლოა, წარმოადგენდეს თავდაცვის უფლების გააქტიურების ერთადერთ გზას. მიუხედავად ამისა, სიტუაციები, როდესაც

---

[435] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 231.

[436] *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, § 64; *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005, § 147.

[437] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 174; *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 206, § 547; *Randelzhofer A., Nolte G.,* 'Article 51' in *Simma B. et al (eds),* The Charter of the United Nations: A Commentary, Oxford University Press, 2012, 1409; *Tams C. J.,* The Use of Force Against Terrorists, European Journal of International Law, 2009, 388.

[438] *Sklerov M. J.,* Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, Military Law Review, 201, 2009, 76; *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2012, 93–95; *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 108–110.

[439] *Sklerov M. J.,* Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, Military Law Review, 201, 2009, 76.

შესაძლებელია შეკრებითობის თეორიის გამოყენება, შეზღუდულია, გამომდინარე იქიდან, რომ ცალკეული შემთხვევა უნდა უთანაბრდებოდეს ძალის გამოყენებას.[440]

4. შეიარაღებული თავდასხმის ავტორი

სახელმწიფოს ქმედება, რომელიც წარმოშობს გარკვეულ მასშტაბურ შედეგებს, შესაძლოა, ეჭვგარეშედ ჩაითვალოს შეიარაღებულ თავდასხმად. ტრადიციული შეხედულებით, შეიარაღებული თავდასხმა წარმოადგენს ერთი სახელმწიფოს მიერ მეორის მიმართ გარკვეული სიმძიმის ძალის გამოყენებას. შეიარაღებული თავდასხმის განმარტებაში მის განმახორციელებელ პირზე მიუთითებლობა გამოწვეული იყო იმ ფაქტით, რომ 1945 წელს ქარტიის შედგენისას ნათელი იყო, რომ მხოლოდ სახელმწიფოს შეეძლო ამგვარი სიმძიმის ძალის გამოყენება მეორე სახელმწიფოს წინააღმდეგ.[441] თუმცა განვლილ ნახევარ საუკუნეში არაერთი არასახელმწიფო აქტორი გამოჩნდა სცენაზე, რომელმაც შეძლო სათანადო მასშტაბებისა და სიმძიმის მიღწევა შეიარაღებული თავდასხმისას, ძირითადად, დეკოლონიზაციის პროცესის მიმდინარეობისა და საერთაშორისო ტერორიზმის სფეროებში. აღნიშნული ევოლუცია გახდა მიზეზი, შეკითხვისა, თუ რას წარმოადგენს შეიარაღებული თავდასხმა და როდის შეიძლება იქცეს არასახელმწიფო აქტორების ქმედება შეიარაღებულ თავდასხმად, გაეროს ქარტიის მიხედვით.[442] აღნიშნული შეფასებისას აუცილებლად უნდა გათვალისწინდეს, არასახელმწიფო აქტორი მოქმედებს თუ არა სახელმწიფოს სახელით. ანუ არასახელმწიფო აქტორის ქმედებები შესაძლებელია თუ არა, შეერაცხებოდეს სახელმწიფოს. მრავალწლიანი დებატებისა და ყოყმანის შემდეგ,[443] გვაქვს მოცემულობა, რომ არასახელმწიფო აქტორის ქმედებები, რომლებიც შეიძლება, შეერაცხებოდეს სახელმწიფოს, შეგვიძლია მივიჩნიოთ სახელმწიფოს მიერ

[440] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 110.
[441] *Moir L.,* Reappraising the Resort to Force: International Law, 'Jus Ad Bellum' and the War on Terror, Hart. 2010, 22.
[442] *Brownlie I.,* International Law and the Activities of Armed Bands, International and Comparative Law Quarterly, 7, 1958; *Gray, C.,* International Law and the Use of Force, 3rd edn, Oxford University Press, 2008, 132.
[443] *Moir L.,* Reappraising the Resort to Force: International Law, 'Jus Ad Bellum' and the War on Terror, Hart. 2010, 22 et seq.

დასპონსორებულ შეიარაღებულ თავდასხმად.[444] არასახელმწიფო აქტორების ქმედება, რომელიც შესაძლოა, შეერაცხოს სახელმწიფოს და აკმაყოფილებს შეიარაღებული თავდასხმის ზღვარს, წარმოადგენს შეიარაღებულ თავდასხმას, მხარდამჭერი სახელმწიფოს სახელით. შესაბამისად, მსხვერპლ სახელმწიფოს შეუძლია, გააქტიუროს თავდაცვის უფლება მხარდამჭერი სახელმწიფოს წინააღმდეგ. საბოლოოდ, სახელმწიფოს ან არასახელმწიფო აქტორის მიერ, რომლის ქმედებები შეიძლება, შეერაცხოს სახელმწიფოს, დაკვალიფიცირდება შეიარაღებულ თავდასხმად, რომელსაც ახორციელებს თავდამსხმელი ან მასპონსორებელი სახელმწიფო.

ზოგადი მიდგომაა, რომ შეიარაღებული თავდასხმა უნდა განხორციელდეს სახელმწიფოს მიერ ან სახელმწიფოს სახელით. მეორე უპასუხოდ დარჩენილი შეკითხვაა: უტოლდება თუ არა შეიარაღებულ თავდასხმას არასახელმწიფო აქტორის ისეთი ქმედება, რომელიც არ შეერაცხება სახელმწიფოს? თუ არასახელმწიფო აქტორი განახორციელებს შეიარაღებულ თავდასხმას სახელმწიფოს მიმართ, შეუძლია თუ არა ამ უკანასკნელს გააქტიუროს თავდაცვის უფლება?

გაეროს ქარტიის 2(4) მუხლი ადგენს, რომ სახელმწიფოებმა თავი უნდა შეიკავონ ძალის გამოყენებისგან. ქარტიის მიხედვით, მხოლოდ სახელმწიფოს ქმედება ან ქმედება, რომელიც შეიძლება, შეერაცხოს სახელმწიფოს, წარმოადგენს ძალის გამოყენებას. ქარტიის 51-ე მუხლი არ შეიცავს მინიშნებას შეიარაღებული თავდასხმის ავტორზე. ბოლოდროინდელი ტენდენციის თანახმად, შეიარაღებული თავდასხმა არ გულისხმობს, მხოლოდ სახელმწიფოს მიერ განხორციელებულ მოქმედებებს, აქ მოიაზრება არასახელმწიფო აქტორების მოქმედებებიც, რომლებიც შეიძლება არც შეერაცხოს სახელმწიფოს.[445] შესაბამისად, შეიარაღებული თავდასხმის ამ ფართო

---

[444] *ნიკარაგუის და კონგო უგანდას წინააღმდეგ* საქმეებში სასამართლომ დაადგინა, რომ სახელმწიფოსთვის შერაცხვადი არასახელმწიფო აქტორების ქმედებები შესაძლოა, მიჩნეულ იქნეს შეიარაღებულ თვდასხმად: *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 195 (ასევე იხ. §§ 160, 231); *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005, §§ 106–147.

[445] ზოგადად იხ.,: *Murphy S. D.,* Terrorism and the Concept of Armed Attack in Article 51 of the U.N. Charter, Harvard International Law Journal, 43, 2002, 50; *Murphy S. D.,* Self-Defense and the Israeli Wall Advisory Opinion: An IPSE Dixit from the ICJ?, American Journal of International Law, 2005, 64 et seq; *Tams C. J.,* Light Treatment of a Complex Problem: The Law of Self-Defence in the Wall Case, European Journal of International Law, 2005, 963; *Ruys T., Verhoeven S.,* Attacks by Private Actors and the Right of Self-Defence, Journal of Conflict & Security Law, 2005, 289 et seq; *Moir L.,* Reappraising the Resort to Force: International Law, 'Jus Ad Bellum' and the War on Terror, Hart. 2010, 22–31; *Lubell N.,* Extraterritorial Use of Force against Non-state

გაგებაში, სახელმწიფო შეიძლება იყოს ძალის გამოყენების მსხვერპლი და თავდაცვის უფლება გამოიყენოს, როგორც სახელმწიფოების, ასევე არასახელმწიფო აქტორების მიმართაც. გაეროს ქარტიის 51-ე მუხლი სანქციებს არ აწესებს და არ კრძალავს თავდაცვის უფლებას არასახელმწიფო აქტორთა წინააღმდეგ.[446] აღნიშნული თეორიის მხარდამჭერი გამოდგა ამერიკის შეერთებული შტატების პრაქტიკა 2001 წლის 9/11 ტერორისტულ თავდასხმებზე საპასუხოდ.[447] თუმცა, 2001 წლის შემდეგ არსებულ საქმეებში, კერძოდ, *კედლის საქმის საკონსულტაციო დასკვნასა* და *კონგო უგანდის წინააღმდეგ საქმეში*, სასამართლომ არ გაავრცელა შეიარაღებული თავდასხმის ცნება არასახელმწიფო აქტორებზე, რომლებიც არ მოქმედებენ სახელმწიფოს სახელით.[448] სახელმწიფოთა პრაქტიკა ისევე, როგორც გაეროს უშიშროების საბჭოს პრაქტიკა, როგორც ჩანს, მიმართულია შეიარაღებული თავდასხმის ცნების გაფართოებისკენ, რათა მოიცვას არასახელმწიფო აქტორების მიერ ჩადენილი ისეთი ქმედებები, როდესაც ეს უკანასკნელნი არ მოქმედებდნენ სახელმწიფოს სახელით. 2015 წელს, საფრანგეთი გახდა ტერორისტული თავდასხმების სამიზნე, რამაც გაამართლა საფრანგეთის შემდგომი სამხედრო ოპერაციები სირიისა და ისლამური სახელმწიფოს წინააღმდეგ, როგორც ტერორისტული თავდასხმების საპასუხო თავდაცვა.[449]

ჯერჯერობით გადაჭრით ვერ ვიტყვით, რომ თავდაცვის უფლების ცნება გაფართოვდა და მოიცვა არასახელმწიფო აქტორების თავდასხმები, რომლებიც არ

Actors, Oxford University Press, 2010, 31–32; *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012, 224–230.

[446] ეხება სახელმწიფოებს, როგორც შეიარაღებული თავდასხმის მსხვერპლს, მაგრამ არა როგორც თავდამსხმელს. შესაბამისად, მკვლევართა ნაწილი მიიჩნევს, რომ აღნიშნული გარემოება ღია კარს ტოვებს არასახელმწიფო აქტორების მიერ განხორციელებული შეიარაღებული თავდასხმისთვის, როგორც მსხვერპლი სახელმწიფოს თავდაცვის უფლების საფუძვლისთვის. მაგალითად იხ., *Murphy S. D.,* Terrorism and the Concept of Armed Attack in Article 51 of the U.N. Charter, Harvard International Law Journal, 43, 2002, 50.

[447] *Lubell N.,* Extraterritorial Use of Force against Non-state Actors, Oxford University Press, 2010, 34; *Randelzhofer A., Nolte G.,* 'Article 51' in *Simma B. et al (eds),* The Charter of the United Nations: A Commentary, Oxford University Press, 2012, 1416, § 35.

[448] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* ICJ, Advisory Opinion, 2004, § 139; *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005, § 146. თუმცა, ზოგმა მოსამართლემ განსხვავებული აზრი გამოთქვა და მხარი დაუჭირა თავდაცვის უფლების არასახელმწიფო აქტორებისგან თავდაცვაზე გავრცელებას. ზოგადად იხ., *Gray, C.,* International Law and the Use of Force (3rd ed.), Oxford University Press, 2008, 128–136; *Randelzhofer A., Nolte G.,* 'Article 51' in *Simma B. et al (eds),* The Charter of the United Nations: A Commentary, Oxford University Press, 2012, 1416–1419, §§ 35–41.

[449] France, 'International Law Applied to Operations in Cyberspace', Mministère des Armées, 2019, 9.

შეერაცხება სახელმწიფოს.[450] პოზიტიურ საერთაშორისო სამართალში შეიარაღებული თავდასხმა უნდა განხორციელდეს სახელმწიფოს მიერ ან მისი სახელით. თუმცა, როგორც ჩანს, საერთაშორისო სამართალი ვითარდება და შეიძლება, მალე ყველა შეთანხმდეს, რომ არასახელმწიფო აქტორების მოქმედებებიც დაკვალიფიცირდეს შეიარაღებულ თავდასხმად, განსაკუთრებით მაშინ, როდესაც საქმე ეხება ფართომასშტაბიან ტერორისტულ შეტევებს.[451]

კიბეროპერაციების შემთხვევაში ცოტა რთულია თავდამსხმელ არასახელმწიფო აქტორებსა და სავარაუდო სპონსორ სახელმწიფოს შორის კავშირის დადგენა. თავდაცვის უფლების არასახელმწიფო აქტორებზე გავრცელება ძალიან მიმზიდველია კიბერ კონტექსტში. ტალინის სახელმძღვანელო პრინციპების 2.0 შემუშავებაში ჩართული ექსპერტების აზრი გაიყო აღნიშნულ საკითხთან დაკავშირებით, მაგრამ უმეტესობის მოსაზრებით, თავდაცვის უფლება ასევე ვრცელდება არასახელმწიფო აქტორებზე.[452]

დასკვნის სახით შეიძლება ითქვას, რომ სახელმწიფოების ან სახელმწიფოების სახელით არასახელმწიფო აქტორების მიერ განხორციელებული კიბეროპერაციები შეიძლება, წარმოადგენდეს სახელმწიფოს მიერ განხორციელებულ შეიარაღებულ თავდასხმას. არასახელმწიფო აქტორების მიერ სახელმწიფოთა სპონსორობის გარეშე განხორციელებული კიბეროპერაციები ამ ეტაპზე ვერ გაუტოლდება შეიარაღებულ თავდასხმას საერთაშორისო სამართალში. თუმცა, სავსებით რეალური და ალბათ მოსალოდნელიცაა, მომავალში განვითარდეს და გაფართოვდეს შეიარაღებული თავდასხმის ცნება და მოიცვას არასახელმწიფო აქტორთა მოქმედებები, რომლებიც არ მოქმედებენ სახელმწიფოთა სახელით.

---

[450] *Moir L.,* Reappraising the Resort to Force: International Law, 'Jus Ad Bellum' and the War on Terror, Hart. 2010, 30–31; *Randelzhofer A., Nolte G.,* Article 51, The Charter of the United Nations: A Commentary, *Simma B. et al (eds),* Oxford University Press, 2012, 1417.

[451] *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 338.

[452] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 58–59, §§ 16–17. ასევე იხ., *Schmitt M. N.,* Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, 2011, 598–602; *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2012, 95–99; *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 80–89.

5. შეიარაღებული თავდასხმის მიზანი

შეიარაღებული თავდასხმა ტრადიციულად ხასიათდება ერთი სახელმწიფოს მიერ მეორის ტერიტორიაზე სამხედრო შეჭრით.[453] შესაძლებელია, თუ არა შეიარაღებული თავდასხმა განხორციელდეს სახელმწიფოს ფარგლებს გარეთ? მაგალითად, შეიარაღებულ შეტევად შეიძლება ჩაითვალოს თუ არა სახელმწიფოს ინტერესებზე ან მის ფარგლებს გარეთ მყოფ მოქალაქეებზე თავდასხმა? პასუხი დამოკიდებულია სამიზნეს ბუნებაზე. წარმოადგენს თუ არა „სახელმწიფოს გარეგან გამოვლინებას" თავდაცვის უფლების მიზნისთვის.[454] პირველი რიგში, ერთმანეთისგან უნდა განსხვავდეს სახელმწიფოს ორგანოები, იურიდიული და ფიზიკური პირები.

სახელმწიფოს საზღვრებს გარეთ მდებარე მისი დაწესებულების/ორგანოს წინააღმდეგ განხორციელებული კიბეროპერაცია, შესაძლოა, გაუთანაბრდეს შეიარაღებულ თავდასხმას. საყოველთაოდ აღიარებულია, რომ თავდაცვის უფლების მიზნებისთვის სახელმწიფოს ორგანოები წარმოადგენს სახელმწიფოს გარეგან გამოვლინებას.[455] არსებობს აზრთა სხვადასხვაობა, მიმართულია თუ არა აღნიშნული გაგება სახელმწიფო ორგანოებისკენ, თუ საჭიროა რაიმე დამატებითი განსაზღვრება. სადავო არ არის მდგომარეობა საზღვრებს გარეთ არსებულ სამხედრო დანაყოფებსა და სამხედრო ნაგებობებზე, რომ ისინი წარმოადგენენ სახელმწიფოს გარეგან გამოვლინებას გაეროს ქარტიის 51-ე მუხლის მიზნებისთვის.[456] ასეთ დანაყოფებსა და დანადგარებზე თავდასხმა წარმოადგენს სახელმწიფოს ტერიტორიის გარეთ თავდასხმის ყველაზე გავრცელებულ ფორმას. შესაბამისად, მათ მიმართ განხორციელებული ნებისმიერ თავდასხმა, რომელიც მიაღწევს შესაბამის მასშტაბებსა და შედეგებს ჩაითვლება შეიარაღებულ თავდასხმად სამიზნე სახელმწიფოს წინააღმდეგ და ამ უკანასკნელს ექნება თავდაცვის უფლების გააქტიურების

---

[453] *Gray, C.,* International Law and the Use of Force (3rd ed.), Oxford University Press, 2008, 128; *Greenwood, C.*, Self-Defence, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011, § 20.

[454] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 200; უფრო ვრცლად იხ., 199–249.

[455] *Greenwood, C.*, Self-Defence, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011, § 21; *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 60.

[456] *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 199–200.

სამართლებრივი უფლება. აღნიშნულიდან გამომდინარე, ნებისმიერი კიბეროპერაცია, რომლის სამიზნეა სახელმწიფოს ტერიტორიის გარეთ მდებარე სამხედრო დანაყოფების ან დანადგარების კომპიუტერული სისტემა ან ქსელი ასევე შესაძლოა, დაკვალიფიცირდეს შეიარაღებულ თავდასხმად. მაგალითად, კიბეროპერაცია, რომლის სამიზნეა სახელმწიფოს საჰაერო სივრცის გარეთ მფრინავი სამხედრო ხომალდის კომპიუტერული სისტემა და შედეგად მოჰყვება ხომალდის ჩამოვარდნა, შესაძლოა, წარმოადგენდეს შეიარაღებულ თავდასხმას.

საელჩოებისა და დიპლომატიური მისიების შემთხვევა უფრო საკამათოა, მიუხედავად იმისა, რომ ზოგადად მიღებულია, მათ წინააღმდეგ განხორციელებული მტრული აქტი, გარკვეულ შემთხვევებში, შესაძლოა გაუთანაბრდეს შეიარაღებულ თავდასხმას.[457] საელჩოები, როგორც წესი, აღიქმება სახელმწიფოს გარეგან გამოვლინებად თავდაცვის უფლების მიზნებისთვის. შესაბამისად, თუ მივიჩნევთ, რომ საელჩოზე განხორციელებული თავდასხმა სათანადო მასშტაბისა და შედეგების ზღვრის მიღწევის შემთხვევაში წარმოადგენს შეიარაღებულ თავდასხმას, მაშინ იმავე ლოგიკით აღნიშნული საელჩოების კომპიუტერული სისტემის ან ქსელის მიმართ განხორციელებული კიბეროპერაციაც შეიძლება, წარმოადგენდეს შეიარაღებულ თავდასხმას. მეტიც, საზღვარგარეთ მყოფ დიპლომატიურ დესპანებზე განხორციელებული თავდასხმაც შეიძლება, დაკვალიფიცირდეს შეიარაღებულ თავდასხმად. თუმცა, რეალობაში ამგვარი თავდასხმის პოტენციურად შეზღუდულმა ინტენსივობამ შეიძლება, ხელი შეუშალოს მის შეიარაღებულ თავდასხმად დაკვალიფიცირებას.[458]

შემდეგი შეკითხვა, აღნიშნულ თემასთან დაკავშირებით, წარმოადგენს: შეიძლება თუ არა, სახელმწიფოს საზღვრებს გარეთ არსებული ფინანსური ინტერესების ან მისი მოქალაქეების[459] ფინანსური ინტერესების მიმართ განხორციელებული

---

[457] *იქვე.* 201–204.

[458] *იქვე.* 204.

[459] ზოგიერთი სამხედრო ინტერვენცია დასაბუთდა საზღვარგარეთ მყოფი საკუთარი მოქალაქეების დაცვის მოტივით. ეს ფრიად საკამათო საფუძველი აღარ იქნება დეტალურად განხილული წინამდებარე ნაშრომში, ვინაიდან კიბეროპერაციების კონტექსტში ინტერესმოკლებულია. ზოგადად იხ., *Brownlie I.,* International Law and the Use of Force by States, Oxford University Press, 1963, 298–301; *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 213 et seq; *Greenwood, C.*, Self-Defence, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011, § 24.

კიბეროპერაცია წარმოადგენდეს შეიარაღებულ თავდასხმას? აღნიშნული მიდგომა ცნობილია, თუმცა, საკითხი მაინც სადავოა. მოქალაქეების, საზღვაო ან საჰაერო ხომალდების მიმართ განხორციელებული შეტევა რამდენად წარმოადგენს ისეთ შეიარაღებულ თავდასხმას, რომელიც მსხვერპლ სახელმწიფოს ანიჭებს საპასუხოდ თავდაცვის უფლების გააქტიურების შესაძლებლობას.[460] აქედან გამომდინარე, კიბეროპერაცია, რომლის მიზანია სამოქალაქო საჰაერო ხომალდის ნავიგაციის სისტემის დაზიანება და შედეგად მისი ჩამოვარდნა, გარკვეული გარემოებების ფარგლებში, შესაძლოა, წარმოადგენდეს შეიარაღებულ თავდასხმას ხომალდის რეგისტრაციის სახელმწიფოს მიმართ.

ინტერნეტისა და კომპიუტერული ქსელების განვითარება ქმნის ახალ პოტენციურ სამიზნეს: სერვერების კლასტერს. მაგალითად, შესაძლებელია თუ არა A სახელმწიფოს ან მისი კომპანიის B სახელმწიფოში განლაგებულ სერვერებზე C სახელმწიფოს მიერ განხორციელებული კიბეროპერაცია, შესაბამისი სიმძიმის გათვალისწინებით, წარმოადგენდეს შეიარაღებულ თავდასხმას A სახელმწიფოს წინააღმდეგ? დღესდღეობით პასუხი ალბათ იქნება უარყოფითი.[461] თუმცა, აღნიშნული ქმედება შესაძლოა, წარმოადგენდეს შეიარაღებულ თავდასხმას B სახელმწიფოს მიმართ, რადგან სერვერები მის ტერიტორიაზეა განთავსებული და, აქედან გამომდინარე, კიბეროპერაციას შესაძლოა, მიენიჭოს ამ უკანაკნელის მიმართ განხორციელებული ძალის გამოყენების სტატუსი.

თანამედროვე მსოფლიოში მრავალი სახელმწიფო აქტიურად მიმართავს კიბერ ჯაშუშობას სხვა სახელმწიფოს სამხედრო დანაყოფებისა და დანადგარების, საელჩოებისა და დიპლომატიური წარმომადგენლების მიმართ. კიბეროპერაციები, რომელთა მიზანია მხოლოდ მეთვალყურეობა და მონაცემთა შეგროვება, ვერ მიაღწევს შეიარაღებული თავდასხმისთვის საჭირო ინტენსივობის ზღვარს.

---

[460] *Brownlie I.,* International Law and the Use of Force by States, Oxford University Press, 1963, 305 et seq; *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010, 209; *Greenwood, C.*, Self-Defence, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011, § 22–23. *ნავთობის პლატფორმების საქმეში* სასამართლომ დაადგინა, რომ სახელმწიფოს დროშის ქვეშ მცურავ ხომალდზე თავდასხმა შესაძლოა, გაუთანაბრდეს სახელმწიფოზე განხორციელებულ შეიარაღებულ თავდასხმას. *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003, § 64.

[461] აღნიშნულ საკითხზე ტალინის სახელმძღვანელო პრინციპების შემუშავებისას, ექსპერტთა აზრი გაიყო. იხ., *Schmitt, M. N.,* Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013, 60.

6. კიბეროპერაციები, რომელთა სამიზნეს წარმოადგენს კრიტიკული ინფრასტრუქტურა

როგორც უკვე განვიხილეთ, კრიტიკული ინფრასტრუქტურის აქტივები ან სისტემები სახელმწიფოს მიერ განსაზღვრულია არსებითად სოციალური ფუნქციების შენარჩუნების ან მოსახლეობისთვის სერიოზული რისკის შემცველად.[462] ძალის გამოყენებაზე მსჯელობისას განვსაზღვრეთ, რომ კრიტიკულ ინფრასტრუქტურაზე კიბერთავდასხმა ავტომატურად არ ნიშნავს მისი ძალის გამოყენებად დაკვალიფიცირებას, მაგრამ შეიძლება, წარმოადგენდეს გადამწყვეტ ფაქტორს კიბეროპერაციის კვალიფიკაციისთვის.

Stuxnet-ი, რომელმაც დააზიანა ცენტრიფუგები ირანის ბირთვულ სადგურზე, წარმოადგენდა ძალის გამოყენებას, მაგრამ სადავოა მისი მასშტაბი და შედეგები - აკმაყოფილებდა თუ არა შეიარაღებული თავდასხმის ზღვარს. თუ აღნიშნულ მოცემულობას კვალიფიკაციის განსაზღვრისას დავუმატებთ იმ გარემოებას, რომ კიბეროპერაციის შედეგად დაზიანდა და ფუნქციონირება შეეზღუდა ბირთვულ სადგურს, რაც, თავის მხრივ, წარმოადგენს კრიტიკულ ინფრასტრუქტურას, მაშინ, სავარაუდოდ, აღნიშნული ელემენტი კვალიფიკაციისას არსებულ ბალანსს მცირედით გადახრის შეიარაღებული თავდასხმის მხარეს.

ზოგადად რომ ვისაუბროთ, კიბეროპერაციები, რომლებიც წარმოადგენს ძალის გამოყენებას, მაგრამ მასშტაბისა და შედეგების გამო ვერ აკმაყოფილებს შეიარაღებული თავდასხმის ზღვარს, ასეთ დროს, თუ მათი სამიზნეა კრიტიკული ინფრასტრუქტურა, შეგვიძლია მივიჩნიოთ, რომ გაუთანაბრდება შეიარაღებულ თავდასხმას. რა თქმა უნდა, ეს არ წარმოადგენს ავტომატური კვალიფიკაციის მექანიზმს და კრიტიკული ინფრასტრუქტურის მიმართ განხორციელებული ყველა კიბეროპერაციაც არ წარმოადგენს შეიარაღებულ თავდასხმას.

ცოტა უფრო რთულადაა საქმე ისეთი კიბეროპერაციების შემთხვევაში, რომელიც წარმოშობს მხოლოდ არაფიზიკურ შედეგებს, როგორებიცაა - მონაცემთა დაზიანება ან განადგურება. ნაკლებ სავარაუდოა არაფიზიკური ზიანის მქონე კიბეროპერაციებმა დააკმაყოფილონ ძალის გამოყენების ზღვარი და, ფაქტობრივად, გამორიცხულია

[462] იხ., ნაშრომის III თავის მე-5 ქვეთავი.

დააკმაყოფილონ შეიარაღებული თავდასხმის ზღვარი. თუმცა, ძალის გამოყენების შემთხვევაში, შეგვიძლია ვთქვათ, რომ თუ კიბეროპერაციის სამიზნეს წარმოადგენს კრიტიკული ინფრასტრუქტურა, სურათი შეიძლება შეიცვალოს. აქედან გამომდინარე, ძალის გამოყენებად დაკვალიფიცირებისას გადამწყვეტი მნიშვნელობა ენიჭება ოპერაციის სამიზნის ბუნებას. თუმცა, საბოლოოდ, აღნიშნული მიდგომებიც დროის ცვალებადობასთან ერთად, შეიძლება ტრანსფორმირდეს. ეს ყოველივე დამოკიდებულია საკითხისადმი სახელმწიფოთა მიდგომაზე. უნდა აღინიშნოს ის ფაქტი, რომ კრიტიკული ინფრასტრუქტურის წინააღმდეგ განხორციელებულ კიბეროპერაციას, როგორც წესი, შედეგად მოჰყვება ფიზიკური ზიანი.[463] მაგალითად, სახელმწიფოს საჰაერო ტრაფიკის კონტროლის სისტემის დაზიანება კიბეროპერაციის მეშვეობით, სავარაუდოდ, გამოიწვევს სიცოცხლის მოსპობას, დაზიანებასა და განადგურებას.

შეჯამების სახით შეიძლება ითქვას, რომ სამიზნის ბუნება, უფრო სწორად, წარმოადგენს თუ არა კრიტიკული ინფრასტრუქტურა კიბეროპერაციის სამიზნეს, აუცილებლად უნდა იქნეს გათვალისწინებული კონკრეტული კიბეროპერაციის მასშტაბისა და შედეგების შეფასებისას. ზოგიერთ შემთხვევაში კი, ფაქტი, რომ კიბეროპერაციის სამიზნეს წარმოადგენს კრიტიკული ინფრასტრუქტურა, შესაძლოა გახდეს გადამწყვეტი ფაქტორი კვალიფიკაციისას, უთანაბრდება თუ არა კიბეროპერაცია კიბერ შეიარაღებულ თავდასხმას.

7. დასკვნა

ნაკლებ სავარაუდოა, კიბეროპერაციის უმეტესობა გაუთანაბრდეს ძალის გამოყენებას, გაეროს ქარტიის შესაბამისად, შეიარაღებულ თავდასხმას. თუმცა, საწინააღმდეგო ალბათობა მაინც არსებობს. წინამდებარე თავში განიხილება პირობები, კიბეროპერაცია რა დროს შეიძლება, გაუთანაბრდეს შეიარაღებულ თავდასხმას, რისთვისაც აუცილებელია საკმაოდ მაღალი ზღვრის დაძლევა, რაც კიბეროპერაციათა უმრავლესობისთვის, ფაქტობრივად, შეუსრულებელი ამოცანაა.

[463] *Roscini, M.,* Cyber Operations and the Use of Force in International Law, Oxford University Press, 2014, 59.

კიდევ ერთხელ გაესვა ხაზი იმ გარემოებას, რომ კიბეროპერაციის დაკვალიფიცირებისას მთავარი აქცენტი მაინც მის მიერ წარმოშობილ შედეგებზე კეთდება. თუმცა, დამხმარე გარემოებად აუცილებლად უნდა იქნეს გათვალისწინებული კიბეროპერაციის სამიზნე, როგორც ეს კრიტიკული ინფრასტრუქტურის მაგალითზეა აღნიშნული. კვალიფიკაციის საკითხისთვის კიდევ ერთი მნიშვნელოვანი დეტალია - ფიზიკური ზიანის არსებობა/არარსებობის საკითხი.

საერთაშორისო სამართლისთვის საგულისხმოა, ვინ დგას კიბეროპერაციის უკან, ანუ ვინ არის მისი ავტორი. თუ ეს არის სახელმწიფო ან არასახელმწიფო აქტორი, რომელთა ქმედებებიც შეერაცხება სახელმწიფოს, მაშინ საკითხი მარტივადაა. ხოლო თუ საქმე გვაქვს არასახელმწიფო აქტორებთან, რომელთა ქმედებების შერაცხვა სახელმწიფოსთვის ვერ ხერხდება, მაშინ საკითხი უფრო რთულადაა, ვინაიდან ჯერჯერობით საერთაშორისო სამართალში არ არსებობს მკაფიო პოზიცია, რომ ამგვარი კიბეროპერაციის ავტორის მიმართ სამიზნე სახელმწიფოს შეეძლოს თავდაცვის უფლების ამოქმედება. თუმცა, ეს მდგომარეობაც ცვალებადია და, სავარაუდოდ, უახლოეს მომავალში გვექნება ამ კითხვაზე მკაფიო პასუხი, რასაც ამტკიცებს სახელმწიფოთა მზარდი რიცხვი, რომლებიც მხარს უჭერენ თავდაცვის უფლების არეალის გაფართოებას და ისეთ არასახელმწიფო აქტორებზე გავრცელებას, რომელთა მოქმედებებიც არ შეერაცხება სახელმწიფოს.

VII. სახელმწიფოთა მიდგომები ძალის გამოყენებისა და კიბეროპერაციების ურთიერთმიმართების შესახებ - შედარებითი მიმოხილვა

1. შესავალი

საერთაშორისო სამართალში საკითხის შესწავლისა და განსაკუთრებით იმის გასაგებად, რეალურად რა მნიშვნელობა ენიჭება მას, აუცილებელია სახელმწიფოთა პრაქტიკის ანალიზი, რაც მოგვცემს საშუალებას, გავიგოთ სახელმწიფოთა მიდგომა საკითხისადმი და მივიღოთ სრული სურათი.

2. სახელმწიფოთა საერთაშორისო სამართლებრივი ვალდებულებები კიბერსივრცესთან მიმართებით

კიბეროპერაციების კონტექსტში, სახელმწიფოთა პრაქტიკისა და მიდგომების ანალიზის მეშვეობით, შეგვიძლია, თამამად განვაცხადოთ, რომ არსებობს რამდენიმე განსაზღვრული წესი, რომელსაც სახელმწიფოები იყენებენ კიბეროპერაციებთან მიმართებით. ესენია: სხვა სახელმწიფოს სუვერენიტეტის პატივისცემის ვალდებულება, სხვა სახელმწიფოს შიდა საქმეებში ჩაურევლობის ვალდებულება, ძალის გამოყენების აკრძალვა.[464] შესაბამისად, სახელმწიფოთა პრაქტიკისა და მიდგომების ანალიზი ამ მიმართებებით არის ყველაზე საინტერესო.

3. სუვერენიტეტი

კიბერსივრცეში ერთ-ერთი ყველაზე სადავო საკითხი, რომელიც ეხება სახელმწიფოს სუვერენიტეტს, არის შემდეგი: არღვევს თუ არა სახელმწიფოს სუვერენიტეტს კიბეროპერაციის შედეგად მის ტერიტორიაზე მდებარე ქსელების

[464] *Roguski P.,* Application of International Law to Cyber Operations: A Comparative Analyses of States' Views, The Hague Program for Cyber Norms Policy Brief, 2020, 4.

დაზიანება? აღნიშნულ საკითხზე სახელმწიფოთა მიდგომა იყოფა ორ ძირითად ჯგუფად:

1) მიდგომა - სუვერენიტეტი, როგორც პრინციპი - ადგენს, რომ იგი არის საერთაშორისო სამართლის პრინციპი, რომელსაც გააჩნია გარკვეული ამკრძალავი წესები (შიდა საქმეებში ჩაურევლობა, ძალის გამოყენების აკრძალვა), მაგრამ თავად არ წარმოადგენს წესს;

2) მიდგომა - სუვერენიტეტი, როგორც წესი - ადგენს, რომ საერთაშორისო სამართლის უპირველესი წესი მოითხოვს, სახელმწიფოებმა პატივი სცენ სხვა სახელმწიფოს (ტერიტორიულ) სუვერენიტეტს, რაც ასევე ვრცელდება სახელწმიფოს ქმედებებზე კიბერსივრცეში.[465]

მიდგომა - სუვერენიტეტი, როგორც წესის ფარგლებში, სახელმწიფოთა აზრი იყოფა ორ ნაწილად:

ა) *de minimis* მიდგომა, გულისხმობს, რომ კიბეროპერაციის განხორციელებისას პატივი უნდა ვცეთ სხვა სახელმწიფოს სუვერენიტეტს. თუმცა, არსებობს *de minimis* ზღვარი, რომელიც სახელმწიფოებმა უნდა გადაკვეთონ, რათა დადგინდეს სხვა სახელმწიფოს სუვერენიტეტის უფლების დარღვევა.

ბ) შეღწევაზე დაფუძნებული მიდგომა გულისხმობს, რომ სახელმწიფოს ტერიტორიაზე განთავსებულ კომპიუტერულ ქსელში ნებისმიერი შეღწევა წარმოადგენს სახელმწიფოს სუვერენიტეტის დარღვევას.[466]

ევროპის სახელმწიფოების ნაწილი (საფრანგეთი, გერმანია, ნიდერლანდები) ემხრობიან სუვერენიტეტს, როგორც წესის მიდგომას. თუმცა, ამ საკითხთან დაკავშირებით, ჯერჯერობით უცნობია ამერიკის შეერთებული შტატების პოზიცია. უფრო კონკრეტულად, ნიდერლანდები იყენებს *de minimis* მიდგომას, საფრანგეთი კი - შეღწევაზე დაფუძნებულ მიდგომას.[467] გერმანიის პოზიციას რაც შეეხება, ვიცით მხოლოდ ის, რომ ამ უკანასკნელის განცხადებით კიბერშესაძლებლობათა გამოყენებამ

[465] *იქვე.*
[466] *იქვე.*
[467] *Roguski P.,* Application of International Law to Cyber Operations: A Comparative Analyses of States' Views, The Hague Program for Cyber Norms Policy Brief, 2020, 5.

შესაძლოა, გამოიწვიოს სხვა სახელმწიფოს სუვერენიტეტის დარღვევა.[468] ნიდერლანდების ხელისუფლების განცხადებით, სხვა სახელმწიფოების სუვერენიტეტის პატივისცემის ვალდებულება ვალდებულებაა, რომლის დარღვევამ შესაძლოა, გამოიწვიოს საერთაშორისო უკანონო აქტი.[469] აღნიშნული პოზიციის გასამყარებლად ნიდერლანდები იყენებს სასამართლოს პრაქტიკას, კერძოდ კი, *ნიკარაგუის საქმეს,* რომლის თანახმად, სასამართლომ ნიკარაგუის მიმართ განხორციელებული ამერიკის შეერთებული შტატების ქმედებები მიიჩნია საერთაშორისო ჩვეულებითი სამართლით ნაკისრი ვალდებულების დარღვევად.[470] დარღვევის კონკრეტულ ზღვარზე საუბრისას ნიდერლანდები იხრება საერთაშორისო ექსპერტთა ჯგუფის პოზიციისკენ, რომელმაც ტალინის სახელმძღვანელო პრინციპების 2.0 მე-4 წესში ჩამოაყალიბა, თუ როდის დგება სუვერენიტეტის დარღვევა:

1) როდესაც აშკარაა სამიზნე სახელმწიფოს ტერიტორიული მთლიანობის დარღვევის მაღალი ხარისხი.

2) ან ადგილი აქვს სხვა სახელმწიფოს თანდაყოლილ სამთავრობო უფლებებში ჩარევას ან მათ უზურპაციას.[471]

ტალინის სახელმძღვანელო პრინციპები 2.0 განიხილავს, როდისაა სახელმწიფოს მთლიანობის ხარისხი საკმარისად შელახული. ასეთ დროს ყურადღება ექცევა ფიზიკურ ზიანს, სახელმწიფოს ფუნქციონირების დაქვეითებასა და დარღვევებს, რომლებიც ვერ აკმაყოფილებს ფუნქციონირების დაკარგვის ზღვარს.[472]

საფრანგეთის პოზიციის თანახმად, ნებისმიერი კიბერშეტევა, რომელიც მიმართულია საფრანგეთის ციფრული სისტემების წინააღმდეგ ან საფრანგეთის ტერიტორიაზე წარმოშობს ნებისმიერ ეფექტს და განხორციელებულია სხვა

---

[468] "Cyber Security as a Dimension of Security Policy". (2015). Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832> [17.07.2020].

[469] Letter to the parliament on the international legal order in cyberspace. (2019). Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [17.07.2020].

[470] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, §§ 213, 252, 292(5).

[471] *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 20.

[472] *იქვე.*

სახელმწიფოს ორგანოს მიერ, ან სხვაგვარად შეერაცხება სახელმწიფოს, წარმოადგენს სუვერენიტეტის დარღვევას.[473] უნდა აღინიშნოს, რომ საფრანგეთი ყურადღებას აქცევს მისდამი დაქვემდებარებულ სისტემებში შეღწევას და არ აინტერესებს მისი შედეგები. საფრანგეთისთვის შეღწევა მისი სუვერენიტეტის დარღვევას ნიშნავს. შესაბამისად, უარყოფს ნიდერლანდებისა და ტალინის სახელმძღვანელო პრინციპების 2.0 მიერ მხარდაჭერილ *de minimis* მიდგომას. საფრანგეთის კიბერუსაფრთხოების სისტემა იყენებს შეღწევაზე დაფუძნებულ მიდგომას,[474] ეს უკანასკნელი წარმოადგენს კომპიუტერული სისტემის კონფიდენციალურობის, ერთიანობის ან ხელმისაწვდომობის ნებისმიერ დარღვევას, როგორც კიბერუსაფრთხოების ინციდენტი. თავის მხრივ, კიბერუსაფრთხოების ინციდენტი წარმოადგენს ორივე, შიდა და საერთაშორისო სამართლის მიზნების დარღვევას. ინციდენტის სამართლებრივი კვალიფიკაცია დამოკიდებულია მის სიმძიმეზე, რაც შეიძლება მერყეობდეს 0-დან (უმნიშვნელო ზიანი) 5-მდე (ექსტრემალურად მძიმე ზიანი) და რომელიც ფასდება ყოველ კონკრეტულ შემთხვევაზე, ცალ-ცალკე.

საფრანგეთის პოზიციასთან მიმართებით რჩება ორი შეკითხვა. კიბერჯაშუშობის ოპერაციათა უმრავლესობა მოიცავს სამიზნე კომპიუტერულ სისტემებში შეღწევას. საფრანგეთს მიდგომის თანახმად, ამგვარი კიბერჯაშუშობის ოპერაციები ჩაითვლება თუ არა სამიზნე სახელმწიფოს სუვერენიტეტის დარღვევად? და, თუ ეს არის შედეგი, როგორ შეესაბამება სადაზვერვო ინფორმაციის შეგროვების აქამდე არსებულ გზებს, მათ შორის ინფორმაციის შეგროვების კიბერსაშუალებებს? - არ არის *per se* რეგულირებული საერთაშორისო სამართლით?[475]

და ბოლოს, ამერიკის შეერთებული შტატების პოზიცია, კიბერსივრცეში სუვერენიტეტის დარღვევასთან მიმართებით, როგორც ჩანს, ჯერ არ ჩამოყალიბებულა. ამერიკის შეერთებული შტატების სახელმწიფო დეპარტამენტის ორმა სამართლებრივმა მრჩეველმა დაადასტურა, რომ სახელმწიფოებმა, რომლებიც

[473] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.
[474] Secrétariat Général de la Défense et de la Sécurité Nationale, Revue Stratégique de Cyberdéfense, 12 February 2018, 80, <http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/> [17.07.2020].
[475] *Egan B. J.,* "Remarks on International Law and Stability in Cyberspace", 2016, Remarks by, Legal Adviser to the U.S. Department of State, 10 November 2016, 174, <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> [17.07.2020]; *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 168.

ახორციელებენ მოქმედებებს კიბერსივრცეში, უნდა გაითვალისწინონ სხვა სახელმწიფოების სუვერენიტეტი.[476] თუმცა, ყველა დისტანციურად, სხვა სახელმწიფოს ტერიტორიაზე მდებარე კომპიუტერის მეშვეობით განხორციელებულ ოპერაციას ვერ მივიჩნევთ საერთაშორისო სამართლის დარღვევად, მით უმეტეს, თუ არ ახლავს შედეგი ან ახლავს მხოლოდ *de minimis* შედეგები. აღნიშნული განცხადებების საფუძველზე შეგვიძლია დავასკვნათ, რომ აშშ-ის მიდგომის თანახმად კიბეროპერაციებმა შეიძლება დაარღვიოს სახელმწიფოს სუვერენიტეტი, თუმცა, მხოლოდ *de minimis* მიდგომის გათვალისწინებით. აღნიშნულის მიუხედავად, აშშ-ის ბოლოდროინდელი სამხედრო დოქტრინები - „მუდმივი ჩართულობა“[477] და „წინასწარი თავდაცვა“[478] - ურჩევს ამერიკის შეერთებულ შტატებს, საერთაშორისო სამართლის ფარგლებში, დასაშვებად მიიჩნიოს, იყოს აქტიური მესამე სახელმწიფოს ტერიტორიაზე განთავსებულ ქსელებში, თუნდაც პრევენციული ხასიათის ღონისძიებებითა და ყოველგვარი გასამართლებელი საფუძვლის გარეშე, ისეთის, როგორიცაა - კონტრზომების აუცილებლობა. კერძოდ, ამერიკის შეერთებული შტატების თავდაცვის დეპარტამენტის მთავარმა მრჩეველმა განაცხადა, რომ არ არსებობს სათანადოდ გავრცელებული და თანმიმდევრული სახელმწიფო პრაქტიკა, რომელიც სამართლებრივი ვალდებულების ჭრილში, საერთაშორისო ჩვეულებითი სამართლის მეშვეობით ზოგადად აკრძალავდა შეუთანხმებელი კიბეროპერაციების განხორციელებას სხვა სახელმწიფოს ტერიტორიაზე.[479] მიუხედავად იმისა, რომ უცნობია, ზემოაღნიშნული პოზიცია წარმოადგენს აშშ-ის მთავრობის ერთიან პოზიციას თუ მხოლოდ ერთი წარმომადგენლის აზრია, მაინც ნათლად ჩანს, რომ აშშ-ის სამხედროები ინფორმირებულნი არიან აღნიშნული მიდგომის შესახებ.

---

[476] *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, 18 September 2012, 9, < https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. [17.07.2020].

[477] *Lopez C. T.,* Persistent Engagement, Partnerships, Top Cybercom's Priorities, 14 May 2019, <https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/> [17.07.2020].

[478] *Lopez C. T.,* DOD More Assertive, Proactive in Cyber Domain, 28 June 2019, <https://www.defense.gov/Explore/News/Article/Article/1891495/dod-more-assertive-proactive-in-cyber-domain/> [17.07.2020].

[479] *Ney P. C.,* DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 March 2020, <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> [18.07.2020].

3.1. დასკვნები და რეკომენდაციები სუვერენიტეტის საკითხზე

წარმოდგენილ სახელმწიფოთა პრაქტიკის ანალიზი ცხადყოფს, რომ კიბეროპერაციებისა და სახელმწიფოთა სუვერენიტეტის ურთიერთმიმართების საკითხზე ჯერ კიდევ არ არსებობს სახელმწიფოთა შეჯერებული ერთიანი პოზიცია. თუმცა, სავარაუდოდ, სახელმწიფოთა უმრავლესობას არჩეული აქვს მიდგომა, რომელსაც თავად ემხრობა. სახელმწიფოთა უმრავლესობა აღიარებს და ხაზს უსვამს სხვა სახელმწიფოების სუვერენიტეტის პატივისცემის ვალდებულებას. შექმნილ ვითარებაში შესაძლებელია შემდეგი რეკომენდაციების ჩამოყალიბება, რომლებიც დაეხმარება სახელმწიფოების პრაქტიკას, გახდეს ერთგვაროვანი:

1) სახელმწიფოებმა უნდა ჩამოაყალიბონ პოზიცია, სუვერენიტეტთან დაკავშირებით - ეს არის საერთაშორისო სამართლის პრინციპი თუ საერთაშორისო სამართლის წესი, რომელიც სახელმწიფოებს სთხოვს, პატივი სცენ სხვა სახელმწიფოთა სუვერენიტეტს კიბერსივრცეში;

2) აღნიშნულ საკითხზე პოზიციის ჩამოყალიბებისას სახელმწიფოებს შეუძლიათ, გაითვალისწინონ სასამართლოს პოზიციაც, რაც მომდინარეობს *ნიკარაგუის საქმიდან;*[480]

3) თუ სახელმწიფოები ჩათვლიან, რომ სუვერენიტეტი მხოლოდ საერთაშორისო სამართლის პრინციპია, მაშინ აუცილებელია, განისაზღვროს კონკრეტული ზღვარი, რომელსაც უნდა მიაღწიოს კიბეროპერაციამ ძალის გამოყენებად ან ზოგადად ინტერვენციად დაკვალიფიცირებისთვის;

4) თუ სახელმწიფოები ჩათვლიან, რომ სუვერენიტეტი არის საერთაშორისო სამართლით დადგენილი წესი, მაშინ უნდა განსაზღვრონ ზღვარი, თუ როდის დგება სუვერენიტეტის დარღვევა: სახელმწიფოს ტერიტორიაზე განთავსებულ კომპიუტერულ სისტემებში შეღწევისას, თუ ამ სისტემებში შეღწევის შემდეგ *de minimis*-ზე მეტი შედეგის დადგომის შემთხვევაში;

5) თუ სახელმწიფოები აირჩევენ *de minimis* ზიანის მიყენებას, მაშინ უნდა მოხდეს ამ უკანასკნელის ზღვრის დადგენა;

---

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

6) ასევე აუცილებლად უნდა განისაზღვროს, თუ რა ტიპის კომპიუტერული სისტემების დაზიანებაზეა საუბარი. ეს ეხება მხოლოდ სამიზნე სახელმწიფოს ტერიტორიაზე განთავსებულ კომპიუტერულ სისტემებს თუ ნებისმიერ კომპიუტერულ სისტემას, რომელიც ახორციელებს სამთავრობო ფუნქციებს (მაგალითად ე.წ. ციფრული საელჩოები), ასევე სამხედრო თუ სამოქალაქო დანიშნულების საზღვაო და საჰაერო ხომალდებს.

4. შიდა საქმეებში ჩაურევლობა

ფაქტობრივად, ყველა სახელმწიფო, რომლის პრაქტიკაც გააანალიზდა, თანხმდება, რომ შიდა საქმეებში ჩაურევლობის პრინციპი მოქმედებს კიბერსივრცეშიც. სახელმწიფოები ფართოდ იყენებენ სასამართლოს მიერ *ნიკარაგუის საქმის* მიგნებებს, რაც გულისხმობს, რომ ქმედების შიდა საქმეებში შესარაცხად საჭიროა ორი პირობის დადგომა კუმულატიურად:

1) ქმედება წარმოადგენს იძულებით ჩარევას.

2) ხორციელდება სახელმწიფოს დაცულ სფეროში, მაგალითად, ისეთ საკითხებზე რომელთა დამოუკიდებლად გადაწყვეტა წარმოადგენს თითოეული სახელმწიფოს სუვერენულ უფლებას.[481]

შეკითხვაზე, თუ რა წარმოადგენს დაცულ სფეროს კიბერსივრცეში, სახელმწიფოებმა დაადგინეს, რომ ეს ეხება საკითხებს, სადაც სახელმწიფო ნებადართულია, თავისუფლად მიიღოს გადაწყვეტილება, მოიცვას თავისი პოლიტიკური, სოციალური, ეკონომიკური და კულტურული სისტემა,[482] საგარეო პოლიტიკა,[483] ეროვნული არჩევნები, სახელმწიფოთა აღიარება და საერთაშორისო ორგანიზაციების წევრობა.[484] იძულების ელემენტთან მიმართებით სახელმწიფოები

---

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

[482] Speech by Attorney General Wright J. QC MP "Cyber and International Law in the 21st Century", 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [17.07.2020]; French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.

[483] Australia, International Law Supplement, 2019, < https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html> [18.07.2020]; French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.

[484] Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace,

აცნობიერებენ მისი ზუსტი განმარტების სირთულეებს. ავსტრალია იძულებით ზომებს აღწერს, როგორც მექანიზმს, რომელიც ეფექტიანად ართმევს სახელმწიფოს შესაძლებლობას, აკონტროლოს, გადაწყვიტოს ან მართოს თანდაყოლილი სუვერენული ბუნების საკითხები.[485] ნიდერლანდები იძულებას განმარტავენ, როგორც საშუალებას, დააჯეროს სახელმწიფო, განახორციელოს ისეთი მოქმედება (ქმედება ან უმოქმედობა), როგორსაც ეს უკანასკნელი არ განახორციელებდა საკუთარი ნებით.[486] საბოლოოდ, ორივე სახელმწიფოს მიდგომა მაინც დადის სახელმწიფოს სუვერენულ ნებამდე, იქნება ეს არასასურველი ქმედების/უმოქმედობის განხორციელება თუ საკუთარი ნების განხორციელების შეუძლებლობა. ზოგი სახელმწიფო წარმოადგენს კიბეროპერაციების მაგალითებს, რომლებიც არღვევს შიდა საქმეებში ჩაურევლობის პრინციპს. აღნიშნული მაგალითები მოიცავს:

- ოპერაციებს საარჩევნო სისტემის მანიპულაციისთვის, მათ შორის, სხვა სახელმწიფოს შიდა საქმეებში ჩარევას ჩაატაროს არჩევნები;[487]
- სხვა სახელმწიფოს არჩევნების შედეგების შეცვლას;[488]
- პარლამენტის ფუნდამენტურ მოქმედებებში ჩარევას;[489]

3, < https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020].

[485] Australia, International Law Supplement, 2019, < https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html> [18.07.2020].

[486] Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 3, <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020].

[487] Speech by Attorney General Wright J. QC MP "Cyber and International Law in the 21st Century", 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [17.07.2020]; *Egan B. J.,* "Remarks on International Law and Stability in Cyberspace", 2016, Remarks by, Legal Adviser to the U.S. Department of State, 10 November 2016, 175, <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> [17.07.2020].

[488] Australia, International Law Supplement, 2019, <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html> [18.07.2020]; *Egan B. J.,* "Remarks on International Law and Stability in Cyberspace", 2016, Remarks by, Legal Adviser to the U.S. Department of State, 10 November 2016, 175, <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> [17.07.2020].

[489] Australia, International Law Supplement, 2019, <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html> [18.07.2020].

- ჩარევას, რომელიც იწვევს ან შეიძლება გამოიწვიოს სახელმწიფოს პოლიტიკური, ეკონომიკური, სოციალური და კულტურული სისტემის დაზიანება;[490]
- სახელმწიფოს ფინანსური სისტემის სტაბილურობაში ჩარევას.[491]

შიდა საქმეებში ჩაურევლობის პრინციპი ბოლომდე დამუშავებული არ არის. ჯერჯერობით არ განსაზღვრულა, ყველა სახელმწიფო ერთი და იმავე ზღვარს იყენებს თუ არა იძულების დასადგენად. ასევე გასარკვევია, რას ნიშნავს „იძულება“ კიბერსივრცეში, თუნდაც ოპერაციებზე ზეგავლენის მოხდენის კონტექსტში.

4.1. დასკვნები და რეკომენდაციები შიდა საქმეებში ჩაურევლობის პრინციპთან დაკავშირებით

პრეცედენტული ანალიზი გვიჩვენებს, რომ სახელმწიფოების პოზიცია ერთგვაროვანია და მხარს უჭერენ კიბერსივრცეში შიდა საქმეებში ჩაურევლობის პრინციპის არსებობას, მაგრამ პრინციპის ზუსტი კონტურები კვლავ შესამუშავებელია. შესაბამისად, არსებობს რეკომენდაციები, რომელთა გათვალისწინება ხელს შეუწყობს აღნიშნული პრინციპის სრულყოფას:

- სახელმწიფოებმა უნდა გაითვალისწინონ და პრაქტიკაში გამოიყენონ სასამართლოს მიერ *ნიკარაგუის საქმეში* დადგენილი შიდა საქმეებში ჩაურევლობის პრინციპის ელემენტები.[492] ამასთან, *ნიკარაგუის საქმით* დადგენილი ელემენტებიდან პირველი გულისხმობს, რომ იძულებითი ხასიათის ჩარევა შეგვიძლია, არც განვიხილოთ კიბეროპერაციების

[490] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.

[491] Australia, International Law Supplement, 2019, <https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html> [18.07.2020].

[492] სასამართლომ *ნიკარაგუის საქმეში* განმარტა, რომ ქმედება წარმოადგენს შიდა საქმეებში აკრძალულ ჩარევას, თუ იგი აკმაყოფილებს ორ პირობას: 1) ჩარევის განმახორციელებელ ქმედებას უნდა ჰქონდეს იძულების ხასიათი; 2) ჩარევა ხდება ისეთ სფეროში, რომელიც წარმოადგენს სახელმწიფოს დამოუკიდებელი გადაწყვეტილების სფეროს, სახელმწიფოთა სუვერენიტეტის პრინციპის შესაბამისად; *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 205.

კონტექსტში. ამის მიზეზია ის, რომ შიდა საქმეებში ჩარევად კიბეროპერაციებს დაკვალიფიცირებისთვის შედარებით დაბალი ზღვრის დაკმაყოფილებაც ჰყოფნის და აუცილებლობას არ წამოადგენს იძულების ელემენტის არსებობა;

- სახელმწიფოებმა უნდა წარმოადგინონ თავიანთი ინტერპრეტაცია ორივე ზემოაღნიშნულ ელემენტზე, იძულება და დაცული სფერო და რა გავლენას ახდენს მათზე კიბეროპერაციები;
- სახელმწიფოებმა მკაფიოდ უნდა განსაზღვრონ ვალდებულება, პატივი სცენ სახელმწიფოს ტერიტორიულ სუვერენიტეტსა და შიდა საქმეებში ჩაურევლობის პრინციპს.

5. ძალის გამოყენების აკრძალვა

ფაქტობრივად, ყველა სახელმწიფო თანხმდება, რომ კიბეროპერაციებზე ვრცელდება გაეროს ქარტიის 2(4) მუხლით დადგენილი ძალის გამოყენების ან მუქარის აკრძალვა. აღნიშნულ საკითხთან მიმართებით, თუ რა ქმედებები წარმოადგენს ძალის გამოყენებას კიბერსივრცეში, ავსტრალია, გერმანია, საფრანგეთი, ნიდერლანდები, დიდი ბრიტანეთის გაერთიანებული სამეფო და ამერიკის შეერთებული შტატები კონკრეტულად თუ ირიბად მხარს უჭერენ ერთსა და იმავე მიდგომას, რაც გულისხმობს „მასშტაბისა და შედეგების“[493] ტესტს, რომელიც

[493] Commonwealth of Australia, Department of Foreign Affairs and Trade, "Annex A: Australia's position on how international law applies to State conduct in cyberspace", in: Australia's International Cyber Engagement Strategy, 90, <https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf> [18.07.2020]; "Cyber Security as a Dimension of Security Policy". (2015). Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832> [17.07.2020]; French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 8; Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 3-4, < https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020]; UK Ministry of Defence, Cyber Primer, 2nd ed, 2016, 12, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf> [18.07.2020]; *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, on 18 September 2012, 4, < https://2009-

სასამართლომ გამოიყენა *ნიკარაგუის* საქმეში.[494] აღნიშნული ტესტის მიხედვით კიბეროპერაცია წარმოადგენს ძალის გამოყენებას თუ მისი მასშტაბი და შედეგები შედარებითია „ტრადიციული“ კინეტიკური ძალის გამოყენების მასშტაბებსა და შედეგებთან.

სახელმწიფოთა პრაქტიკის ანალიზის შედეგად შესაძლებელია მასშტაბისა და შედეგების შეფასების ფაქტორების გამოყოფა:

- ოპერაციის წარმოშობა და წესრიგის დამრღვევის ბუნება (სამხედროა თუ არა);[495]
- თავდასხმის სერიოზულობის/შეჭრის ხარისხი;[496]
- ოპერაციის რეალური ან განზრახული შედეგები;[497]
- შედეგების იმწუთიერობა;[498]
- კიბერინფრასტრუქტურის შეღწევადობის სიღრმე;[499]
- სამიზნის ბუნება, მაგალითად, სამხედრო ხასიათის სამიზნე ინფრასტრუქტურა.[500]

უფრო მეტიც, კიბერშეტევის მაგალითები, რომლებიც, შესაძლოა, წარმოადგენდეს ძალის გამოყენებას, მოიცავს ოპერაციებს, რომლებსაც, უმეტეს შემთხვევაში, მივყავართ შემდეგ შედეგებამდე:

2017.state.gov/s/l/releases/remarks/197924.htm. [17.07.2020]. ასევე იხ., *Schmitt M. N., Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017, 330-337.

[494] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 195.

[495] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.

[496] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7; Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832> [17.07.2020].

[497] Commonwealth of Australia, Department of Foreign Affairs and Trade, "Annex A: Australia's position on how international law applies to State conduct in cyberspace", in: Australia's International Cyber Engagement Strategy, 90, <https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf> [18.07.2020]; French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.

[498] Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832> [17.07.2020].

[499] *იქვე.*

[500] *იქვე.*

- ფიზიკური პირების დაზიანება ან გარდაცვალება;[501]
- ობიექტების დაზიანება ან განადგურება;[502]
- მნიშვნელოვანი ფინანსური ან ეკონომიკური გავლენა;[503]
- სამხედრო სისტემებში შეღწევა თავდაცვის შესაძლებლობების დაზიანების მიზნით;[504]
- კონკრეტული პირების დაფინანსება ან მომზადება სახელმწიფოების წინააღმდეგ კიბეროპერაციების განხორციელების მიზნით;[505]
- ბირთვული რეაქტორის ფუნქციონირებაში ჩარევა, რასაც შედეგად მოჰყვა სიცოცხლის ფართომასშტაბიანი მოსპობა;[506]
- საჰაერო კონტროლის სისტემის დაზიანება, რასაც შედეგად მოჰყვა საჰაერო ხომალდის ჩამოვარდნა;[507]
- დასახლებული პუნქტის თავზე კაშხლის გახსნა და მიმდებარე სივრცის განადგურება;[508]
- არსებით სამედიცინო სერვისებზე იერიშის მიტანა.[509]

---

[501] Commonwealth of Australia, Department of Foreign Affairs and Trade, "Annex A: Australia's position on how international law applies to State conduct in cyberspace", in: Australia's International Cyber Engagement Strategy, 90, <https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf> [18.07.2020]; *Kaljulaid K.,* "President of the Republic at the opening of CyCon 2019", 29 May 2019, < https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html> [18.07.2020].

[502] *იქვე.*

[503] Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 4, < https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020].

[504] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 7.

[505] *იქვე.*

[506] *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, on 18 September 2012, 4, < https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. [17.07.2020].

[507] *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, on 18 September 2012, 4, < https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. [17.07.2020]; Speech by Attorney General Wright J. QC MP "Cyber and International Law in the 21st Century", 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [17.07.2020].

[508] *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, on 18 September 2012, 4, < https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. [17.07.2020].

[509] Speech by Attorney General Wright J. QC MP "Cyber and International Law in the 21st Century", 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> [17.07.2020].

5.1. დასკვნები და რეკომენდაციები ძალის გამოყენების საკითხთან მიმართებით

ძალის გამოყენების კონტექსტში სახელმწიფოები ერთსულოვნად თანხმდებიან, რომ კიბეროპერაცია შესაძლებელია, წარმოადგენდეს ძალის გამოყენებას ან მუქარას. იმის დასადგენად კი, კონკრეტული კიბეროპერაცია აკმაყოფილებს თუ არა ძალის გამოყენების სტანდარტს, საჭიროა მასშტაბისა და შედეგების ტესტი, რაზეც ასევე თანხმდებიან სახელმწიფოები. ზემოაღნიშნულიდან გამომდინარე შესაძლოა, გათვალისწინდეს შემდეგი რეკომენდაციები:

- სახელმწიფოები რეკომენდაციას უწევენ მასშტაბებისა და შედეგების ტესტის გამოყენებას იმის დასადგენად, კონკრეტული კიბეროპერაცია წარმოადგენს თუ არა ძალის გამოყენებას;
- სახელმწიფოებისთვის მნიშვნელოვანია ფაქტორების ჩამოყალიბება, რომლებიც მიუთითებს კიბეროპერაციისა და კინეტიკური ძალის გამოყენების მსგავს მასშტაბებსა და შედეგებზე;
- კიბერსფეროში მწირი ფაქტობრივი მაგალითების გამო, კარგი იქნება თუ სახელმწიფოები წარმოადგენენ ჰიპოთეტურ მაგალითებს, თუ რა შემთხვევაში იქნება კიბერ საშუალებების გამოყენება ძალის გამოყენების ტოლფასი.

6. თავდაცვა

ყველა სახელმწიფო, რომელთა პრაქტიკაც გაანალიზდა, აცნობიერებს, რომ ნებისმიერ სახელმწიფოს გააჩნია ინდივიდუალური თუ კოლექტიური თავდაცვის უფლება კიბეროპერაციების წინააღმდეგ, რომლებიც უთანაბრდება შეიარაღებულ თავდასხმას, გაეროს ქარტიის 51-ე მუხლის ფარგლებში. სახელმწიფოები თანხმდებიან, რომ ძალის გამოყენების მსგავსად, კიბეროპერაცია შესაძლოა, დაკვალიფიცირდეს, როგორც შეიარაღებული თავდასხმა, თუ მისი მასშტაბი და შედეგები მსგავსია, როგორც კინეტიკური ან ფიზიკური შეიარაღებული თავდასხმის შემთხვევაში, *ნიკარაგუის საქმის* მიერ დადგენილი მასშტაბებისა და შედეგების

ტესტის თანახმად.[510] საფრანგეთი იყენებს ოდნავ განსხვავებული მასშტაბისა და სიმძიმის ტესტს, შეიარაღებული თავდასხმის განსასაზღვრად.[511] უფრო მეტიც, მხოლოდ საფრანგეთი,[512] ნიდერლანდები[513] და ამერიკის შეერთებული შტატები[514] აცხადებენ კონკრეტულად, რომ თავდაცვისას ძალის გამოყენებამ უნდა დააკმაყოფილოს აუცილებლობისა და პროპორციულობის პირობები. შეგვიძლია ვივარაუდოთ, რომ ყველა სახელმწიფო იზიარებს აღნიშნულ პოზიციას, რაც ასახულია საერთაშორისო ჩვეულებით სამართალში.[515] აქვე უნდა აღინიშნოს, რომ ამერიკის შეერთებული შტატების პოზიციის თანახმად, თავდაცვის უფლება წარმოიქმნება ნებისმიერი უკანონო ძალის გამოყენების მიმართ, შესაბამისად, უარყოფენ შეიარაღებული თავდასხმის ძალის გამოყენებისგან განსხვავებული ზღვრის არსებობას.[516] საფრანგეთი და ნიდერლანდები არ იზიარებენ აღნიშნულ მიდგომას და უპირატესობას ანიჭებენ სასამართლოს მიერ *ნიკარაგუის* საქმეში მიღებულ გადაწყვეტილებას.[517]

კიბეროპერაციისთვის აუცილებელ მასშტაბსა და შედეგებთან ერთად ნიდერლანდების მთავრობა შენიშნავს, რომ დღესდღეობით არ არსებობს კონსენსუსი კიბერშეტევის შეიარაღებულ თავდასხმად დაკვალიფიცირებაზე, თუ იგი არ იწვევს სიცოცხლის მოსპობას, ფიზიკურ ზიანს, განადგურებას ან ძალიან სერიოზულ არამატერიალურ შედეგებს.[518] საფრანგეთის პოზიციის თანახმად, სავარაუდოა შეიარაღებული თავდასხმა იმ შემთხვევაში, თუ იგი იწვევს არსებითი სიცოცხლის

---

[510] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 195.

[511] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 8.

[512] *იქვე.* 9.

[513] Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 9, <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020].

[514] *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, on 18 September 2012, 7, < https://2009-2017.state.gov/s/l/releases/remarks/197924.htm. [17.07.2020].

[515] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US)*, ICJ, Judgment, 27 June 1986, § 176.

[516] *იქვე.*

[517] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 8; Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 8, < https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020].

[518] *იქვე.* 9.

მოსპობას, მნიშვნელოვან ფიზიკურ ან ეკონომიკურ ზიანს.[519] აღნიშნული მაგალითები მოიცავს თავდასხმას კრიტიკულ ინფრასტრუქტურაზე, რომელსაც მოჰყვება არსებითი შედეგები, რამაც შესაძლოა, გამოიწვიოს სახელმწიფოთა მოქმედებების პარალიზება, ასევე - ტექნოლოგიური ან ეკოლოგიური კატასტროფები, შეიწიროს უამრავი სიცოცხლე.[520] გერმანიის მიდგომის თანახმად, ფაქტორები, რომლებიც უნდა გაითვალისწინოს სახელმწიფომ, თავდასხმის სერიოზულობა, მისი შედეგების იმწუთიერობა, კიბერ ინფრაქსტუქტურის პენეტრაციის სიღრმე და მისი სამხედრო ხასიათია.[521] დამატებით, საფრანგეთი მხარს უჭერს შედეგების შეკრებითობის თეორიას,[522] რომლის თანახმადაც, კიბერშეტევები, რომლებიც ცალ-ცალკე ვერ აკმაყოფილებს შეიარაღებული თავდასხმის ზღვარს, მაგრამ მათი შედეგები კუმულატიურად აღწევს შეიარაღებული თავდასხმის ზღვარს, უნდა ჩაითვალოს შეიარაღებულ თავდასხმად. ამ შემთხვევაში, გასათვალისწინებელია ისიც, რომ მსგავსი შეტევები განხორციელდა ერთსა და იმავე დაწესებულების ან სხვადასხვა ორგანიზაციათა მიერ, თუმცა, მათი მიზანი ერთი იყო.[523]

გერმანიამ და საფრანგეთმა წამოწიეს თავდაცვის უფლების საკითხი არასახელმწიფო აქტორთა წინააღმდეგ, რომლებიც ახორციელებენ შეიარაღებულ თავდასხმებს კიბერსაშუალებებით. თუმცა, სახელმწიფოებს გააჩნიათ განსხვავებული პოზიციებიც. გერმანია აღიარებს, რომ თავდაცვის ზომები შესაძლოა, განხორციელდეს არასახელმწიფო აქტორების მიმართაც, რომლებსაც შეერაცხება კიბეროპერაცია.[524] საფრანგეთი კი მიიჩნევს, რომ თავდაცვის უფლება არ ვრცელდება არასახელმწიფო აქტორების საწინააღმდეგო ზომებზე, თუ მათი ქმედებები არ შეერაცხება რომელიმე სახელმწიფოს.[525] გამონაკლისს შეიძლება წარმოადგენდნენ ისეთი არასახელმწიფო

---

[519] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 8.

[520] *იქვე.*

[521] Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832> [17.07.2020].

[522] შეკრებითობის თეორიის სამეცნიერო განმარტებისთვის იხ., *Gray C.,* International Law and the Use of Force, Oxford University Press, 2018, 164; *Kretzmer D.,* The Inherent Right to Self-Defense and Proportionality in *Jus ad Bellum*, European Journal of International Law, 24, 2013, 235-282; *Lobo J. F.,* One Piece at a Time: The "Accumulation of Events" Doctrine and the "Bloody Nose" Debate on North Korea, Lawfare, 2018.

[523] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 9.

[524] Deutscher Bundestag, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE", BT-Drs. 18/6989, 2015, 11.

[525] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 8-9.

აქტორები, რომლებსაც გააჩნიათ კვაზისახელმწიფოებრივი მოწყობა, მაგალითად, ისლამური სახელმწიფო. თუმცა, საფრანგეთი მაინც აღიარებს, რომ სახელმწიფოთა პრაქტიკა, დროთა განმავლობაში, შეიძლება გადაიხაროს არასახელმწიფო აქტორებისა და თავდაცვის უფლების გავრცობისკენ.

რაც შეეხება კიბერსივრცეში წინასწარი თავდაცვის საკითხს, ამ მიმართებით ავსტრალიასა და საფრანგეთს გაცხადებული აქვთ თავიანთი პოზიციები. ავსტრალიის პოზიციის თანახმად, სახელმწიფოს შეუძლია, გამოიყენოს წინასწარი თავდაცვა შეიარაღებული თავდასხმის წინააღმდეგ, როდესაც თავდამსხმელს მტკიცედ აქვს გადაწყვეტილი შეიარაღებული თავდასხმის განხორციელება ისე, რომ მსხვერპლმა დაკარგოს ეფექტიანად თავდაცვის ყველანაირი შესაძლებლობა.[526] საფრანგეთი თავს უფლებას აძლევს, გამოიყენოს წინასწარი თავდაცვის უფლება კიბერშეტევის საპასუხოდ, რომელიც ჯერ არ დაწყებულა, მაგრამ დაიწყება უსწრაფესად და, სავარაუდოდ, გამოიწვევს არსებით შედეგებს.[527]

საკმაოდ დიდ გამოწვევად რჩება კიბერშეტევის გარდაუვალობისა და ნამდვილობის შეფასება. ნიდერლანდების მხარის განცხადებით, სახელმწიფოს შეუძლია, გამოიყენოს ძალა, თავდაცვის მიზნით, მხოლოდ იმ შემთხვევაში, თუ თავდასხმასა და მასზე პასუხისმგებელ პირთა ვინაობაში არიან დარწმუნებულნი, რა თქმა უნდა, შესაბამისი დამარწმუნებელი მტკიცებულებებით.[528]

6.1. დასკვნები და რეკომენდაციები თავდაცვის თაობაზე

ნებისმიერი სახელმწიფო აღიარებს ინდივიდუალური ან კოლექტიური თავდაცვის უფლებას ისეთი კიბეროპერაციების წინააღმდეგ, რომელიც უტოლდება შეიარაღებულ თავდასხმას. შეიარაღებული თავდასხმა უნდა დადგინდეს

[526] Australia, International Law Supplement, 2019, < https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html> [18.07.2020].

[527] French Ministry of the Armies, International Law Applied to Operations in Cyberspace, 9.

[528] Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, 9, < https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> [18.07.2020].

კიბეროპერაციის მასშტაბისა და შედეგების შედარებით ფიზიკური ძალით განხორციელებული შეიარაღებული თავდასხმის მასშტაბსა და შედეგებთან. თავდაცვისთვის ნებისმიერი ძალის გამოყენება უნდა იყოს გაეროს ქარტიის 51-ე მუხლის მოთხოვნების შესაბამისი.

თუმცა, არსებული რეალობის გათვალისწინებით, არსებობს სივრცეები, სადაც შესაძლებელია პრაქტიკის დახვეწა:

- სახელმწიფოებმა უნდა წარმოადგინონ საკუთარი პოზიციები კიბეროპერაციისა და კინეტიკური შეიარაღებული თავდასხმის მასშტაბებისა და შედეგების შედარებითობასთან დაკავშირებით;
- სახელმწიფოებმა ასევე უნდა გამოხატონ პოზიცია, უჭერენ თუ არა მხარს შედეგების შეკრებითობის თეორიას;
- ასევე სახელმწიფოებმა უნდა დასვან საკითხი არასახელმწიფო აქტორების წინააღმდეგ, თავდაცვის უფლების გამოყენებაზე, რომლებმაც განახორციელეს შეიარაღებული თავდასხმა კიბერსაშუალებათა გამოყენებით და მათი ქმედებები არ შეერაცხება რომელიმე კონკრეტულ სახელმწიფოს;
- სახელმწიფოებმა უნდა გადაწყვიტონ, დასაშვებია თუ არა წინასწარი ან მოსალოდნელი თავდაცვის უფლების გამოყენება კიბეროპერაციების, როგორც შეიარაღებული თავდასხმის მიმართ და მხოლოდ ასე განისაზღვროს კიბერშეტევის გარდაუვალობა.

დასკვნა

ტექნოლოგიების განვითარების კვალდაკვალ აქტუალურია საერთაშორისო სამართლის კონსერვატიული ხედვის გადაფასების საკითხი. ამ პროცესის დაწყების ერთ-ერთი მნიშვნელოვანი ფაქტორი კი, სწორედ საერთაშორისო სივრცეში მიმდინარე კიბეროპერაციების სამართლებრივი რეგულირების აუცილებლობაა. სახელმწიფოს უსაფრთხოებაში სულ უფრო დიდ ადგილს იკავებს კიბერუსაფრთხოება.

ნაშრომის მიზნებისთვის წარმოებული კვლევიდან გამომდინარე დადგინდა, რომ ჯერჯერობით საერთაშორისო სამართალში არ არსებობს სპეციალიზებული ნორმები, რომლებიც დაარეგულირებს კიბეროპერაციების სფეროს. ამის მიუხედავად, თამამად შეიძლება ითქვას, რომ დღესდღეობით არსებული საერთაშორისო სამართლებრივი რეჟიმი ვრცელდება კიბეროპერაციებზეც. მიუხედავად იმისა, რომ გაეროს ქარტიის მიღების დროს შეუძლებელი იყო ძალის გამოყენებაში კიბერშეტევების მოაზრება, საერთაშორისო ხელშეკრულებათა ევოლუციური განმარტებით, შესაძლებელია უკვე არსებული ნორმების ახლადწარმოქმნილ ფენომენზე გავრცელება. ქარტიის ტექსტი ფორმულირებულია იმგვარად, რომ ფეხი აუწყოს მომავლის ტენდენციებს და ზოგადი ფორმულირებებისა და დებულებების თანამედროვე გააზრების მეშვეობით მოიცვას ახალი რეალობის მიერ წარმოქმნილი ისეთი გამოწვევები, როგორებიცაა - კიბეროპერაციები. ამ ხარვეზის აღმოსაფხვრელად 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.

ამასთან, სასამართლოს პოზიცია, რომ ხელშეკრულების ნორმის გაგებამ დროთა განმავლობაში შეიძლება, განიცადოს ევოლუცია, იძლევა საშუალებას, რომ კიბერშეტევებზე გავრცელდეს უკვე არსებული ნორმები. ეს მიდგომა კი, თავის მხრივ, მიანიშნებს საერთაშორისო სამართლის ახლებურ გააზრებაზე, კიბერშეტევების მიმართ.

უკანასკნელ წლებში ასევე შეინიშნება ტენდენცია იმისა, რომ კიბერშეტევები დარეგულირდეს უფრო სპეციალიზებული ნორმებით, რომლის კარგი მაგალითია ტალინის სახელმძღვანელო პრინციპები, რომლებიც შემუშავდა ისეთი საერთაშორისო ორგანიზაციის ეგიდით, როგორიცაა ნატო, რაც, თავის მხრივ, კიდევ უფრო მეტად ზრდის ამ დოკუმენტის სანდოობას. აღნიშნული დოკუმენტი, რომელიც წარმოადგენს აღიარებულ მეცნიერთა ნაშრომს, ჩამოყალიბებულია ნორმატიული ენით და კიდევ უფრო ამაღლებს მის, როგორც რბილი სამართლის წყაროს, ავტორიტეტს.

ტალინის პრინციპების შემუშავების მიზეზი გახდა 2007 წელს ესტონეთზე განხორციელებული კიბერშეტევა. ეს უკანასკნელი წარმოადგენდა პირველ შემთხვევას, როდესაც კიბეროპერაციის მეშვეობით სახელმწიფოს მიაყენეს არსებითი ზიანი. ესტონეთს მოსდევს საქართველოს 2008 წლის მაგალითიც. რუსეთ-საქართველოს შეიარაღებული კონფლიქტის დროს რუსეთის მიერ განხორციელდა უპრეცედენტო მასშტაბის კიბერშეტევა. აღნიშნული კიბერშეტევა წარმოადგენდა საქართველოსა და რუსეთს შორის მიმდინარე სამხედრო კონფლიქტის ნაწილს, რაც გახდა მიზეზი იმისა, რომ აღნიშნული ფართომასშტაბიანი კიბეროპერაციის ცალკეულ, განყენებულ კონტექსტში განხილვა, ფაქტობრივად, არ ხდება. 2010 წელს განხორციელდა კიბერშეტევა ირანის ბირთვულ სადგურზე, რასაც შედეგად მოჰყვა ფიზიკური ზიანიც. და ბოლოს, 2019 წლის 28 ოქტომბერს კიბერშეტევის მსხვერპლი გახდა ისევ საქართველო, კიბერშეტევის ავტორი კი, ისევ - რუსეთი. ის ფაქტი, რომ დღევანდელ დღემდე განხორციელებული ოთხი ყველაზე ფართომასშტაბიანი კიბერშეტევიდან ორი განხორციელდა საქართველოს წინააღმდეგ, კიდევ ერთხელ მიუთითებს საქართველოს მიერ კიბერუსაფრთხოების სფეროს განვითარების სასიცოცხლო მნიშვნელობაზე. განსაკუთრებით მაშინ, როდესაც ქვეყნის მთავარი საფრთხე, მსოფლიო მასშტაბით, ყველაზე აქტიურად იყენებს კიბეროპერაციების იარაღს საკუთარი მიზნების მისაღწევად.

იმის გათვალისწინებით, რომ გაეროს ქარტიის მე-2(4) მუხლი კრძალავს ძალის გამოყენებას და ფორმულირებაში გამოყენებულია ზოგადი ტერმინი - „ძალა“, შეგვიძლია, თამამად ვამტკიცოთ, რომ აღნიშნული აკრძალვა ვრცელდება ნებისმიერი სახის ძალაზე, მათ შორის, კიბერძალაზე. შესაბამისად, კიბერშეტევები შეიძლება

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

ა) ქმედების ძალის გამოყენებად შეფასება ხორციელდება შედეგობრივი მაჩვენებლების მიხედვით. იმ შემთხვევაში, თუ კიბერშეტევები გამოიწვევს ისეთსავე შედეგებს, რასაც გამოიწვევდა შეიარაღებული თავდასხმები, მაშინ, კიბერეკვივალენტურობის მიდგომიდან გამომდინარე, არაფერი უშლის ხელს, რომ ასეთი კიბერშეტევა ჩაითვალოს ძალის გამოყენებად;

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

გ) 2(4)-ე მუხლი წარმოადგენს სახელშეკრულებო ნორმას, რომელზეც შეიძლება გავრცელდეს ხელშეკრულების ევოლუციური ინტერპრეტაცია - ამ მუხლის მიზანი იყო, აეკრძალა იძულების ელემენტის მომცველი მოქმედებები სახელმწიფოთაშორის ურთიერთობებში.

მეორე მხრივ, თუ კიბერშეტევა ვერ მიაღწევს იმ სტანდარტს, რაც საჭიროა მისი 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:

ა) ჩარევის მიზანს წარმოადგენდეს სამიზნე სახელმწიფოს იძულება, შეცვალოს პოლიტიკა.

ბ) იძულების/ძალადობრივი მეთოდის გამოყენება უნდა ეხებოდეს იმ საკითხებს, რომლებიც სახელმწიფოს შეუძლია, გადაწყვიტოს თავისუფლად, საკუთარი სუვერენიტეტის ფარგლებში.

კიბეროპერაციების მსხვერპლი სახელმწიფოსთვის გადამწყვეტი მნიშვნელობა აქვს, ზუსტად იცოდეს, რასთან აქვს საქმე და იმოქმედოს შესაბამისად. იმისთვის, რომ კიბეროპერაციის საპასუხოდ სახელმწიფომ გააქტიუროს თავდაცვის უფლება, აუცილებელია, კიბეროპერაციამ დააკმაყოფილოს გარკვეული ზღვარი. ამ შემთხვევაში, გვაქვს სამი მიდგომა, რომელთა დახმარებითაც არის შესაძლებელი კიბეროპერაციის „გაზომვა“. როგორც ნაშრომში არაერთხელ აღინიშნა, ესენია:

მიზნობრივი მიდგომა, ინსტრუმენტული მიდგომა და შედეგობრივი მიდგომა. მკვლევრებისა და სახელმწიფოთა პოზიციების უმრავლესობა ემხრობა შედეგობრივ მიდგომას. ეს უკანასკნელი გულისხმობს კიბეროპერაციის „გაზომვას“ მის მიერ გამოწვეული შედეგებით. რამდენად მძიმე იქნება კიბეროპერაციის შედეგები, იმდენად მაღალი იქნება შესაძლებლობა, ეს უკანასკნელი დაკვალიფიცირდეს ძალის გამოყენებად ან „შეიარაღებულ თავდასხმად“. სწორედ შეიარაღებული თავდასხმის ზღვარის დაკმაყოფილების შემთვევაში იქნება შესაძლებელი, რომ მსხვერპლმა სახელმწიფომ გამოიყენოს თავდაცვის უფლება. სახელმწიფოთა უმრავლესობა იზიარებს აღნიშნულ მიდგომას. თუმცა, გამონაკლისია ამერიკის შეერთებული შტატები, რომელიც ძალის გამოყენებისა და შეიარაღებული თავდასხმისთვის აწესებს იდენტურ ზღვრებს. შესაბამისად, ნებისმიერი კიბეროპერაციის შემთხვევაში, რომელიც აკმაყოფილებს თუნდაც ძალის გამოყენების ზღვარს, აშშ-ის მიდგომის თანახმად, სამიზნე სახელმწიფოს შეუძლია, გამოიყენოს თავდაცვის უფლება. თავის მხრივ, თავდაცვის უფლების გააქტიურებისას მსხვერპლი სახელმწიფო არ არის შეუზღუდავი. მას ბოჭავს აუცილებლობისა და პროპორციულობის ტესტი, რაც ნიშნავს, რომ თავდაცვისას ძალა უნდა გამოიყენოს უკიდურეს შემთხვევაში, თუ სხვა თავის დაცვის საშუალებები ამოწურულია და ძალა გამოყენებულ უნდა იქნეს მხოლოდ თავდასხმის აღკვეთის მიზნით.

კიბერძალასთან დაკავშირებით, მეცნიერულ დონეზე განვითარებული თანამედროვე მიდგომების გაანალიზებით, ნათლად ჩანს, რომ ყველაზე ეფექტიანი და რეალურია შედეგზე დაფუძნებული მიდგომა. თუმცა, ეს მიდგომა ბოლომდე ვერ ასახავს სრულ სურათს. შედეგზე დაფუძნებული მიდგომის გარდა, სინთეზურად უნდა იქნეს გამოყენებული მიზნობრივი და ინსტრუმენტული მიდგომის ელემენტები, რადგან ასეთ დროს ვიღებთ ერთიანი შეფასების სისტემას. ამასთან, ძალიან დიდი მნიშვნელობა აქვს, წარმოშობს თუ არა კიბეროპერაცია შედეგებს რეალურ თუ ვირტუალურ სამყაროში. არაფიზიკური სახის შედეგების შემთხვევაში, ძალიან დაბალია შესაძლებლობა იმისა, რომ კიბეროპერაციამ მიიღოს ძალის გამოყენების კვალიფიკაცია. სწორედ ასეთ დროს არის განსაკუთრებულად სასარგებლო მიზნობრივი და ინსტრუმენტული მიდგომების ელემენტების თანმხვედრი გამოყენება, რაც შედეგზე დაფუძნებულ მიდგომას ხდის უფრო

მრავალფეროვანს და პრაქტიკულს. მაგალითად, თუ კიბეროპერაციას აქვს არაფიზიკური ზიანი, მაგრამ სამიზნეს წარმოადგენს კრიტიკული ინფრასტრუქტურა ან კრიტიკული ინფორმაციული ინფრასტრუქტურა, შესაძლოა, შეიცვალოს კიბეროპერაციის სამართლებრივი კვალიფიკაცია და უპირატესობა მიენიჭოს ამ უკანასკნელის ძალის გამოყენებად დაკვალიფიცირებას. შესაბამისად, იმის განსასაზღვრად, კიბეროპერაცია წარმოადგენს თუ არა ძალის გამოყენებას, ჯერჯერობით საუკეთესო გამოსავალია არსებული მიდგომების გაერთიანება და შედეგზე დაფუძნებული მიდგომისთვის მიზნობრივი და ინსტრუმენტული მიდგომების ელემენტების დამატება.

რეალურად, კრიტიკული ინფრასტრუქტურის ელემენტი სახელმწიფოებში არსებობდა უძველესი დროიდან. კრიტიკულ ინფრასტრუქტურას წარმოადგენს აქტივები, სისტემები, დაწესებულებები, რომლებიც აუცილებელია სახელმწიფოსა და მისი საზოგადოების სასიცოცხლო ფუნქციების შენარჩუნებისთვის. აგრესორი სახელმწიფოების მიერ ჰიბრიდული მეთოდების გამოყენებამ წარმოშვა კრიტიკული ინფრასტრუქტურების განსაკუთრებული დაცვის აუცილებლობა. არასათანადო დაცვის შემთხვევაში, კრიტიკული ინფრასტრუქტურა და მით უმეტეს, კრიტიკული ინფორმაციული ინფრასტრუქტურა, შესაძლოა გახდეს კიბეროპერაციების იოლი სამიზნე, განსაკუთრებით, თანამედროვე რეალობის გათვალისწინებით, როდესაც ყველაფერი იმართება კომპიუტერული სისტემების მეშვეობით.

კიბერსამყაროში ადვილია არამართლზომიერი მექანიზმების განხორციელება. ამის ნათელი მაგალითი იყო ესტონეთსა და საქართველოზე მიტანილი კიბერშეტევებისას გამოყენებული DDoS მეთოდი. კიბერაქტივობის დაკვალიფიცირებისას აუცილებლად გასათვალისწინებელია გარემო ფაქტორები, თუ რა ვითარებაში ხორციელდება კიბეროპერაცია, არის იგი რაიმე სხვა მოქმედების ნაწილი, თუ წარმოადგენს განყენებულ აქტს. საქართველოს შემთხვევაში, 2008 წლის კიბერშეტევა წარმოადგენდა შეიარაღებული კონფლიქტის ნაწილს და ამ მიზეზით ვერ მოხერხდა კიბერშეტევისთვის სათანადო საერთაშორისო ყურადღების მიპყრობა.

კიბეროპერაციები, რომლებიც წარმოქმნიან ისეთ ფიზიკურ შედეგებს, როგორებიცაა - საკუთრების დაზიანება, სიცოცხლის მოსპობა ან ჯანმრთელობის დაზიანება, შედარებით მარტივად დაკვალიფიცირდება ძალის გამოყენების

აკრძალვის დარღვევად. ამ მიმართებით, ირანის ბირთვულ სადგურზე განხორციელებული კიბერშეტევა ერთ-ერთი იშვიათთაგანია, რომელმაც გამოიწვია ფიზიკური ზიანი და, შესაბამისად, ყველაზე მეტი შესაძლებლობა გააჩნია, დაკვალიფიცირდეს ძალის გამოყენებად. მიუხედავად იმისა, რომ მეცნიერთა უმრავლესობაც ირანის ბირთვულ სადგურზე თავდასხმას მიიჩნევს ძალის გამოყენებად, ჯერჯერობით არც ერთი სახელმწიფოს ამის შესახებ საჯაროდ არ განუცხადებია.

ესტონეთზე თავდასხმამ მნიშვნელოვანი გავლენა მოახდინა სახელმწიფოს ყოველდღიურ ყოფაზე, მაგრამ არ დამდგარა ქვეყნის არსებობა/არარსებობის საკითხი. ესტონეთის შემთხვევა თავდაპირველად მიიჩნეოდა ძალის გამოყენების აკრძალვის დარღვევად. თუმცა, დროთა განმავლობაში, ამ მოსაზრების მიმართ ინტერესი განელდა.

სხვა არსებული შემთხვევებიდან ვერც ერთმა დააკმაყოფილა ძალის გამოყენების ზღვარი. აღნიშნული ადასტურებს, თუ რამდენად მცირერიცხოვანი კიბეროპერაცია კვალიფიცირდება ძალის გამოყენებად.

ვინაიდან კიბეროპერაციების ძალის გამოყენებად დაკვალიფიცირება საკმაო სირთულეებთანაა დაკავშირებული, გაჩნდა ვარაუდი, რომ კიბეროპერაციები განეხილათ გაეროს ქარტიის 2(4) მუხლის სხვა აკრძალვის, კერძოდ, ძალის გამოყენების მუქარის აკრძალვის ფარგლებში. ნაშრომში განვითარებული მსჯელობიდან გამოჩნდა, რომ ძალის გამოყენების მუქარად დაკვალიფიცირება ბევრად მარტივია, ვიდრე ძალის გამოყენებად დაკვალიფიცირება. ზოგიერთი კიბეროპერაცია შესაძლოა, წარმოადგენდეს კიბერძალის ღია მუქარას. კიბეროპერაციების ნაწილი კი ექცევა კიბერძალის დემონსტრაციის კატეგორიაში. დღემდე არსებული მაგალითებით (ესტონეთი, საქართველო, ირანი) ვლინდება, რომ მათი დაკვალიფიცირება, როგორც კიბერძალის გამოყენება ან კიბერძალის გამოყენების ღია მუქარა, მაინც რთულია. და პირიქით, ზოგიერთი შემთხვევა შეიძლება დაკვალიფიცირდეს, როგორც ძალის დემონსტრირება, რომელიც უთანაბრდება აკრძალული ძალის გამოყენების მუქარას. თუმცა, აქვე უნდა ითქვას ისიც, რომ კიბერშესაძლებლობების განვითარება, თავის მხრივ, არ წარმოადგენს კიბერძალის გამოყენების მუქარას, რადგან ამ უკანასკნელის არსებობისთვის

აუცილებელია მუქარის განმახორციელებელი სახელმწიფოს მიზანმიმართული მოქმედებები.

საერთაშორისო სამართლისთვის მნიშვნელოვანი საკითხია, ვინ დგას კიბეროპერაციის უკან, ანუ ვინ არის მისი ავტორი. თუ გამოვლინდებიან სახელმწიფო ან არასახელმწიფო აქტორები, რომელთა ქმედებებიც შეერაცხება სახელმწიფოს, მაშინ საერთაშორისო სამართლით შედარებით იოლია შესაბამისი ნორმების საფუძველზე მსჯელობა. ხოლო თუ საქმე გვაქვს არასახელმწიფო აქტორებთან, რომელთა ქმედებების შერაცხვა სახელმწიფოსთვის ვერ ხერხდება, მაშინ საკითხი რთულადაა, ვინაიდან ჯერჯერობით საერთაშორისო სამართალში არ არსებობს მკაფიო პოზიცია, რომ არასახელმწიფო აქტორების მიერ განხორციელებული კიბეროპერაციის წინააღმდეგ დაზარალებულ სახელმწიფოს შეუძლია, გააქტიუროს თავდაცვის უფლება. თუმცა, ეს მდგომარეობაც ცვალებადია და, სავარაუდოდ, უახლოეს მომავალში გვექნება ამ კითხვაზე მკაფიო პასუხი. ამ ყველაფერს ამტკიცებს სახელმწიფოთა მზარდი რიცხვი, რომლებიც მხარს უჭერენ თავდაცვის უფლების არეალის გაფართოებას და ისეთ აქტორებზე გავრცელებას, რომელთა მოქმედებებიც არ შეერაცხება სახელმწიფოს.

ჩატარებული სამართლებრივი კვლევის სრულფასოვნების აუცილებელი ელემენტია სახელმწიფოთა პრაქტიკის ანალიზი. ეს უკანასკნელი გვაძლევს საშუალებას, რეალურად აღვიქვათ კიბეროპერაციების ადგილი საერთაშორისო სამართალში. ჩატარებული კვლევის შედეგად გამოვლინდა, რომ მსოფლიოს წამყვანი სახელმწიფოები, როგორებიცაა ამერიკის შეერთებული შტატები, დიდი ბრიტანეთის გაერთიანებული სამეფო, საფრანგეთი, გერმანია, ნიდერლანდები და ავსტრალია, ყველა მათგანი კიბეროპერაციებთან მიმართებით გამოყოფს ოთხ ძირითად მიმართულებას: სუვერენიტეტი, შიდა საქმეებში ჩაურევლობა, ძალის გამოყენების აკრძალვა და თავდაცვა.

ა) სუვერენიტეტთან მიმართებით ჯერჯერობით არ არსებობს სახელმწიფოთა ერთიანი პოზიცია. სუვერენიტეტი წარმოადგენს საერთაშორისო სამართლით დადგენილ წესს თუ მხოლოდ საერთაშორისო სამართლის პრინციპს. ძირითადი ნაწილი მაინც იხრება სუვერენიტეტის, როგორც წესის მიდგომისკენ. ასეთ შემთხვევაში, აუცილებელია სახელმწიფოები შეჯერდნენ კონკრეტულ ზღვარზე, თუ

როდის ხდება აღნიშნული წესის დარღვევა, ანუ როდის არღვევს კიბეროპერაცია სახელმწიფოს სუვერენიტეტს. აქ კი, სახელმწიფოთა პოზიციები ორ ჯგუფად იყოფა. ძირითადი ნაწილი მხარს უჭერს *de minimis* მიდგომას, რაც ნიშნავს, რომ, სახელმწიფოს სისტემებში შეღწევის გარდა, რაიმე სახის ზიანი მაინც უნდა გამოიწვიოს კიბეროპერაციამ. ყველასგან განსხვავებით, მხოლოდ საფრანგეთი მიიჩნევს სუვერენიტეტის დარღვევად სახელმწიფოს სისტემებში შეღწევის ფაქტს. ზემოაღნიშნულიდან გამომდინარე, ცხადია, რომ სუვერენიტეტის ნაწილში სახელმწიფოები თანხმდებიან საკითხის მხოლოდ ძირითად კონტურებზე.

ბ) შიდა საქმეებში ჩაურევლობა განხილულ იქნა და საბოლოოდ დადგინდა, რომ ის კიბეროპერაციები, რომლებიც არღვევს სახელმწიფოთა სუვერენიტეტს, მაგრამ ვერ აკმაყოფილებს ძალის გამოყენების ზღვარს, ექცევა შიდა საქმეებში ჩაურევლობის ფარგლებში. აქ, როგორც მეცნიერულ, ისე პრაქტიკულ დონეზე იკვეთება ორი ძირითადი კომპონენტი: 1) შიდა საქმეებში ჩარევის ქმედება უნდა წარმოადგენდეს იძულებით ჩარევას; 2) ჩარევა უნდა განხორციელდეს დაცულ სფეროში, რომელიც განეკუთვნება სახელმწიფოს დისკრეციას. რეალობაში ჩარევისას იშვიათად შეიძლება შეგვხვდეს იძულების ელემენტი. ძირითადი აქცენტი გადატანილია სახელმწიფოს დაცულ სფეროში ჩარევაზე.

გ) ძალის გამოყენებასთან მიმართებით, სახელმწიფოების პრაქტიკის ანალიზისას, გამოიკვეთა ნაცნობი გარემოება. ყველა სახელმწიფო კიბეროპერაციების ძალის გამოყენებად დაკვალიფიცირებისთვის იყენებს ამ უკანასკნელის მასშტაბებისა და შედეგების ტესტს, რა შედეგებს წარმოშობს კიბეროპერაცია (ფიზიკური, არაფიზიკური) და რამდენად მასშტაბური და ყოვლისმომცველია იგი.

დ) თავდაცვის ნაწილი სახელმწიფოთა პრაქტიკაში განსაკუთრებით საინტერესოა. ყველა სახელმწიფო აღიარებს ინდივიდუალური ან კოლექტიური თავდაცვის უფლების არსებობას, კიბეროპერაციების წინააღმდეგ. ამისთვის კიბეროპერაცია უნდა გაუტოლდეს შეიარაღებულ თავდასხმას. თავის მხრივ, შეიარაღებული თავდასხმის არსებობისთვის სახელმწიფოები მიმართავენ კარგად ნაცნობი მასშტაბისა და შედეგების ტესტს. მხოლოდ, ამ შემთხვევაში, ისინი კიბეროპერაციის შედეგებს ადარებენ ფიზიკური ძალით განხორციელებული შეიარაღებული თავდასხმის შედეგებს და, თუ ამ ორის მსგავსების პირობებში, ეძლევა სახელმწიფოს თავდაცვის

უფლების გააქტიურების შესაძლებლობა. თავდაცვის საკითხის განხილვისას აუცილებლად უნდა გამახვილდეს ყურადღება შედეგების შეკრებითობის თეორიაზე, რომელსაც მხარს ღიად უჭერს საფრანგეთი. აღნიშნული თეორია სამიზნე სახელმწიფოს აძლევს საშუალებას, შეკრიბოს მის წინააღმდეგ განხორციელებული კიბეროპერაციები. თუ რეალობაში ვლინდება რამდენიმე კიბეროპერაცია, რომელიც ცალკე ვერ აკმაყოფილებს, თუნდაც ძალის გამოყენების ზღვარს, მათი მასშტაბი და შედეგები შესაძლოა, საკმარისიც იყოს ერთიანად შეიარაღებულ თავდასხმად დაკვალიფიცირებისთვის.

ბუნებრივია, ყველა სახელმწიფოს მიდგომა ვერ იქნება იდენტური. თუმცა, მნიშვნელოვანია ის გარემოება, რომ ძირითად საკითხებზე თანხმდება ყველა მოწინავე სახელმწიფო, რომლებიც რეალურად ქმნიან საერთაშორისო სამართლებრივ სურათს.

საბოლოო შეჯამების სახით, შეიძლება ითქვას, რომ კიბეროპერაციები წარმოადგენს გამოწვევას ძალის გამოყენების საერთაშორისო სამართლისთვის და საჭიროებს ახლებურ გააზრებას საერთაშორის სამართლის ჭრილში. თუმცა, ეს არ ნიშნავს, რომ იგი ვერ ექცევა დღეს არსებული საერთაშორისო სახელშეკრულებო და ჩვეულებითი სამართლის ჩარჩოში და სცდება მისი რეგულირების ფარგლებს. მიუხედავად ამისა, ნაშრომში გამოკვეთილი ტენდენციების გათვალისწინებით, შეიძლება საფუძვლიანად ვივარაუდოთ, რომ უახლოეს მომავალში ჩამოყალიბდება სამართლის ახალი დარგი, სახელწოდებით, „კიბეროპერაციების საერთაშორისო სამართალი“, რომელიც, სახელმწიფო უსაფრთხოების ინტერესებიდან გამომდინარე, აქცენტს გადაიტანს რეაგირების მექანიზმებისა და სახელმწიფოთა პასუხისმგებლობის საკითხებზე.

ბიბლიოგრაფია

წიგნები, მონოგრაფიები

1. *Bjorge, E.*, The Evolutionary Interpretation of Treaties, Oxford University Press, 2014.
2. *Brownlie I.,* International Law and the Use of Force by States, Oxford University Press, 1963.
3. *Brunnée J.,* The Meaning of Armed Conflict and the Jus ad Bellum, Martinus Nijhoff Publishers, 2012.
4. *Clarke, R. A., Knake, R. K.,* Cyber War: The Next Threat to National Security and What to Do about It, Harper Collins, 2010.
5. *Condorelli L. and Kreß C.,* The Rules of Attribution: General Considerations in *Crawford J. et al (eds),* The Law of International Responsibility, Oxford University, Press, 2010.
6. *Constantinou A.,* The Right of Self-Defence under Customary International Law and Article 51 of the United Nations Charter, Sakkoulas & Bruylant, 2000.
7. *Corten, O.,* The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart, 2012.
8. *Crawford, J.*, Brownlie's Principles of Public International Law (8th Edition), Oxford University Press, 2013.
9. *Delerue, F.,* Cyber Operations and International Law, Cambridge University Press, 2020.
10. *Dinniss H. H.,* Cyber Warfare and the Laws of War, Cambridge University Press, 2012.
11. *Dinstein, Y.*, War, Aggression and Self-Defence (4th ed.), Cambridge University Press, 2005.
12. *Dinstein, Y.,* War, Aggression, and Self-Defence, Cambridge University Press, 2012.
13. *Franck, T. M.,* Recourse to Force: State Action against Threats and Armed Attacks, Cambridge University Press, 2009.
14. *Gray C.,* International Law and the Use of Force, Oxford University Press, 2018.
15. *Gray, C.,* International Law and the Use of Force (3rd ed.), Oxford University Press, 2008.
16. *Gray, C.,* International Law and the Use of Force, Oxford University Press, 2004.

17. *Gray, C.,* The International Court of Justice and the Use of Force, Oxford University Press, 2013.

18. *Higgins R.,* The Development of International Law by the Political Organs of the United Nations, Oxford University Press, 1963.

19. *Jennings, R., Watts, A.,* Oppenheim's International Law (9th Edition): Volume 1 Peace, Oxford University Press, 2008.

20. *Kulesza J.,* Due Diligence in International Law, Brill & Martinus Nijhoff Publishers, 2016.

21. *Langille, B.,* It's 'Instant Custom': How the Bush Doctrine Became Law after the Terrorist Attacks of September 11, 2001, Boston College International & Comparative Law Review, 26(145) 2001.

22. *Lubell N.,* Extraterritorial Use of Force against Non-state Actors, Oxford University Press, 2010.

23. *Maurer, T.*, Cyber Mercenaries: the State, Hackers, and Power, Cambridge University Press, 2018.

24. *Moir L.,* Reappraising the Resort to Force: International Law, 'Jus Ad Bellum' and the War on Terror, Hart. 2010.

25. *Ohlin, J. D., et al.*, Cyber War: Law and Ethics for Virtual Conflicts, Oxford University Press, 2015.

26. *Okimoto, K.,* The Distinction and Relationship between Jus Ad Bellum and Jus in Bello, Hart, 2011.

27. *Radziwill Y.,* Cyber-Attacks and the Exploitable Imperfection of International Law, Brill & Martinus Nijhoff Publishers, 2015.

28. *Rid T.,* Cyber War Will Not Take Place, Oxford University Press, 2013.

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

30. *Ruys, T.*, 'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice, Cambridge University Press, 2010.

31. *Sanger D. E.*, Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power, Crown, 2012.

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

33. *Stürchler N.,* The Threat of Force in International Law, Cambridge Unversity Press, 2007.

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

35. *Woltag J. C.,* Cyber Warfare: Military Cross-Border Computer Network Operations under International Law, Intersentia, 2014.

სტატიები

1. *ალექსიძე, ლ.* საქართველოში კონფლიქტთან დაკავშირებული ფაქტების დამდგენი საერთაშორისო დამოუკიდებელი მისიის მოხსენების საერთაშორისო სამართლებრივი ასპექტები. საერთაშორისო სამართლის ჟურნალი, N2, 2009 - N1, 2010, 2010.

2. *Antolin-Jenkins V. M.,* Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places, Naval Law Review, 51, 2005.

3. *Barkham J.,* Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, 34, 2001.

4. *Corten, O.,* The Controversies over the Customary Prohibition on the Use of Force: A Methodological Debate, European Journal of International Law, 2005.

5. *D'Amato A.,* Trashing Customary International Law, American Journal of International Law 101, 1987.

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

7. *Green J. A.,* 'Questioning the Peremptory Status of the Prohibition of the Use of Force', Michigan Journal of International Law, 32, 2010.

8. *Hathaway O. A.,* et al, The Law of Cyber-Attack, California Law Review, 2012.

9. *Hoisington M.,* Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense, International & Comparative Law Review, 32, 2009.

10. *Hodgson, Q. E.*, Understanding and Countering Cyber Coercion, 10th International Conference on Cyber Conflict, *T. Minárik, R. Jakschis, L. Lindström (eds.)*, NATO CCD COE Publications, 2018.

11. *Jensen E. T.,* Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense, Stanford Journal of International Law, 38, 2002.

12. *Joyner C. C., Lotrionte C.,* Information Warfare as International Coercion: Elements of a Legal Framework, European Journal of International Law, 12, 2001.

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

14. *Kretzmer D.,* The Inherent Right to Self-Defense and Proportionality in *Jus ad Bellum*, European Journal of International Law, 24, 2013.

15. *Lin H. S.,* Offensive Cyber Operations and the Use of Force, Cybersecurity Symposium: National Leadership, Individual Responsibility, Journal of National Security Law & Policy, 2010.

16. *Lobo J. F.,* One Piece at a Time: The "Accumulation of Events" Doctrine and the "Bloody Nose" Debate on North Korea, Lawfare, 2018.

17. *Murphy S. D.,* Self-Defense and the Israeli Wall Advisory Opinion: An IPSE Dixit from the ICJ?, American Journal of International Law, 2005.

18. *Murphy S. D.,* Terrorism and the Concept of Armed Attack in Article 51 of the U.N. Charter, Harvard International Law Journal, 43, 2002.

19. *Nguyen R.,* Navigating Jus Ad Bellum in the Age of Cyber Warfare, California Law Review, 2013.

20. *Roscini M.,* Threats of Armed Force and Contemporary International Law, Netherlands International Law Review, 54, 2007.

21. *Roscini M.,* World Wide Warfare – Jus ad bellum and the Use of Cyber Force, Max Planck Yearbook of United Nations Law, 14, 2010.

22. *Ruys T.,* The Meaning of "Force" and the Boundaries of the Jus Ad Bellum: Are "Minimal" Uses of Force Excluded from UN Charter Article 2(4)?, American Journal of International Law, 108, 2014.

23. *Ruys T., Verhoeven S.,* Attacks by Private Actors and the Right of Self-Defence, Journal of Conflict & Security Law, 2005.

24. *Schmitt M. N.,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 1999.

25. *Schmitt M.N.,* Cyber Operations and the Jus Ad Bellum Revisited, Villanova Law Review, 2011.

26. *Schmitt, M. N., O'Donnell, B. T (eds.),* Computer Network Attack and International Law, US Naval War College, International Law Studies, 76, 2002.

27. *Scmitt, M. N.,* Wired Warfare: Computer Network Attack and Jus in Bello, International Review of the Red Cross, 84, 2002.

28. *Shackelford S.,* From Nuclear War to Net War: Analogizing Cyber Attacks in International, Berkley Journal of International Law, 27, 2009.

29. *Sharp W. G. Sr.*, The Past, Present, and Future of Cybersecurity. Journal of National Security Law & Policy, 2010.

30. *Silver, D. B.,* Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter, International Law Studies, 76, 2002.

31. *Sklerov M. J.,* Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent, Military Law Review, 201, 2009.

32. *Tams C. J.,* Light Treatment of a Complex Problem: The Law of Self-Defence in the Wall Case, European Journal of International Law, 2005.

33. *Tams C. J.,* The Use of Force Against Terrorists, European Journal of International Law, 2009.

34. *Tikk, E., Kasha, K., Vihul, L.,* International Cyber Incidents: Legal Considerations, Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2010.

35. *Waxman M. C.,* Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law, 36, 2011.

36. *Waxman, M. C.,* Regulating Resort to Force: Form and Substance of the UN Charter Regime, European Journal of International Law, 24, 2013.

კრებულები

1. *Beyerlin, U., Stoutenburg, J. G.*, International Protection of Environment, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2015.

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

3. *Cassese, A., (ed.),* The Oxford Companion to International Criminal Justice, Oxford University Press, 2009.

4. *Damrosch, L.,* Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs, American Journal of International Law, 83, 1989.

5. *de Wet, E.,* Threat to Peace, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009.

6. *Focarelli C.,* Self-Defence in Cyberspace, Research Handbook on International Law and Cyberspace, *Tsagourias N., Buchan R. (eds),* Edward Elgar Publishing, 2015.

7. *Greenwood, C.*, Self-Defence, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2011.

8. *Greenwood, C.,* The Caroline, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009.

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

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

11. *Kunig P.,* Intervention, Prohibition of, Max Planck Encyclopedia of Public International Law, Oxford University Press, 2008.

12. *Myjer E.,* Some Thoughts on Cyber Deterrence and Public International Law, Research Handbook on International Law and Cyberspace, *Tsagourias N., Buchan R. (eds),* Edward Elgar Publishing, 2015.

13. *O'Connell, M. E.,* The Prohibition of the Use of Force, Research Handbook on International Conflict and Security Law: Jus ad Bellum, Jus in Bello and Jus post Bellum, *Henderson C., White N. (eds),* Edward Elgar Publishing, 2013.

14. *Randelzhofer A., Dörr O.,* Article 2 (4), The Charter of the United Nations: A Commentary, *Simma B et al (eds),* Oxford University Press, 2012.

15. *Randelzhofer A., Nolte G.,* Article 51, The Charter of the United Nations: A Commentar, *Simma B et al (eds),* Oxford University Press, 2012.

16. *Roscini M.,* Cyber Operations as a Use of Force, Research Handbook on International Law and Cyberspace, *Tsagourias N., Buchan R. (eds),* Edward Elgar Publishing, 2015.

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

18. *Schmitt M. N. and Vihul L. (eds)*, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd edn, Cambridge University Press, 2017.

19. *Schmitt, M. N.,* Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 37, 1999.

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

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

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

23. *Stiennon R.* A Short History of Cyber Warfare, Cyber Warfare: A Multidisciplinary Analysis, Green JA (ed), Routledge, 2015.

24. *Sur, S.,* The Evolving Legal Aspects of War, The Oxford Handbook of War*, Lindley-French J., Boyer Y. (eds.),* Oxford University Press, 2012.

25. *Thurer, D.,* Soft Law. Max Planck Encyclopedia of Public International Law, Oxford University Press, 2009.

26. *Waxman, M. C.,* Regulating Resort to Force: Form and Substance of the UN Charter Regime, European Journal of International Law, 24, 2013.

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

28. *Zemanek, K.*, Armed Attack, Max Planck Encyclopedia of Public International Law. Oxford University Press, 2013.

სასამართლო პრაქტიკა

1. *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda) ICJ, Judgment, 2005.

2. *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.

3. *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* ICJ, Judgment, 1949.

4. *Dispute Regarding Navigational and Related Rights* (*Costa Rica v. Nicaragua*), ICJ, Judgment, 13 July 2009.

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

6. *Guzzardi v Italy*, ECtHR, Judgment, 6 November 1980, Series A, No. 39.

7. *Ireland v United Kingdom*, ECtHR, Judgment, 18 January 1978, Series A, No. 25.

8. *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* ICJ, Advisory Opinion, 2004.

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

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

11. *North Sea Continental Shelf* (Germany v. Denmark/The Netherlands), ICJ, Judgment of 20 February 1969.

12. *Oil Platforms case (Iran v. USA)*, ICJ, Judgment, 6 November 2003.

13. *Rasmussen v Denmark*, ECtHR, Judgment, 28 November 1984, Series A, No. 87.
14. *Rees v the United Kingdom*, ECtHR, Judgment, 17 October 1986, Series A, No. 106.
15. *SS Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A. No. 10.
16. *Territorial and Maritime Dispute* (Nicaragua v. Colombia) ICJ, Judgment, 2012.
17. *The Prosecutor v. Dusko Tadic,* ICTY, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case IT-94-1, 2 October 1995.
18. *The Prosecutor v. Furundžija*, ICTY, Judgment, 1998, Trial Chamber IT-95-17/1-T.

ნორმატიული აქტები

1. ამერიკის სახელმწიფოების ორგანიზაციის ქარტია (ხელმოწერის თარიღი: 30 აპრილი 1948, ძალაში შესვლის თარიღი: 13 დეკემბერი. 1951).
2. არაბულ სახელმწიფოთა ლიგის პაქტი (22 მარტი. 1945) 70 UNTS 237.
3. აფრიკული გაერთიანების ორგანიზაციის ქარტია (ხელმოწერის თარიღი 25 მაისი 1963, ძალაში შესვლის თარიღი: 13 სექტემბერი. 1963) 479 UNTS 70.
4. აფრიკული კავშირის საკონსტიტუციო აქტი (11 ივლისი. 2000) 2158 UNTS 3.
5. გაერთიანებული ერების ორგანიზაციის ქარტია (მიღების თარიღი: 26.06.1945; ძალაში შესვლის თარიღი: 24.10.1945).
6. ერთა ლიგის პაქტი (მიღებულია 1919 წლის 28 ივნისს, ძალაში შევიდა 1920 წლის 10 იანვარს).
7. ვენის კონვენცია სახელშეკრულებო სამართლის შესახებ (ხელმოწერის თარიღი 23 მაისი 1969, ძალაში შესვლის თარიღი: 27 იანვარი. 1980) 1155 UNTS 331.
8. კონვენცია კიბერდანაშაულის შესახებ, ევროპის საბჭო, ETS No. 185, (მიღების თარიღი: 23.11.2001; ძალაში შესვლის თარიღი: 01.07.2004).
9. მართლმსაჯულების საერთაშორისო სასამართლოს სტატუტი.
10. Articles on State Responsibility for Internationally Wrongful Acts, International Law Commission, 2001.
11. Treaty between the United States and Other Powers Providing for the Renunciation of War as an Instrument of National Policy (adopted 27 August 1928, entered into force 27 July 1929).

საერთაშორისო ორგანიზაციების აქტები

1. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, UNGA Res 58/199 (23 December 2003) UN Doc A/RES/58/199.
2. Creation of a global culture of cybersecurity and the protection of critical information infrastructures, UNGA Res 58/199 (23 December 2003).
3. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, UNGA Res 2131 (XX) (21 December 1965).
4. Definition of Aggression, UNGA Res 3314 (XXIX) (14 December 1974).
5. Draft Declaration on Rights and Duties of States, UNGA Res 375 (IV) (6 December 1949).
6. European Union, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience' (2009) COM(2009) 149 final.
7. European Union, Communication from the Commission on a European Programme for Critical Infrastructure Protection (2006) COM(2006) 786 final.
8. European Union, Communication from the Commission to the Council and the European Parliament – Critical Infrastructure Protection in the Fight against Terrorism (2004) COM(2004) 702 final.
9. European Union, Council Directive 2008/114/EC (n 121), Annex I 'List of ECI.
10. European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016.
11. European Union, Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection (2008) Council Directive 2008/114/EC.
12. OECD Recommendation of the Council on the Protection of Critical Information Infrastructures (2008) C(2008)35.
13. United Nations General Assembly 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;
- 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; 55/63 of 4 December 2000;
- 56/121 of 19 December 2001; 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, 2625(XXV) of 24 October 1970;
- 217 A, of 10 December 1948; 3314 (XXIX) of 14 December 1974;
- 2131(XX) of 21 December 1965; A/66/152 of 15 July 2011;
- 66/359 of 14 September 2011; UNGA A/57/166/Add.1, 29 August 2002;
- UNGA A/64/129/Add.1, 9 September 2009; UNGA A/65/154, 20 July 2010.

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

სხვა დოკუმენტები

1. „Address to the Nation on Iraq“, 2003, 39(12) Weekly Compilation of Presidential Documents
2. Australia, International Law Supplement, 2019, < https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html>.
3. Commonwealth of Australia, Department of Foreign Affairs and Trade, “Annex A: Australia’s position on how international law applies to State conduct in cyberspace”, in: Australia’s International Cyber Engagement Strategy, 90, <https://www.dfat.gov.au/sites/default/files/DFAT%20AICES_AccPDF.pdf>.
4. Cyber Security as a Dimension of Security Policy”. (2015). Speech by Ambassador Norbert Riedel, Commissioner for International Cyber Policy, Federal Foreign Office, Berlin, at Chatham House, London, <https://www.auswaertiges-amt.de/en/newsroom/news/150518-ca-b-chatham-house/271832>.

5. *Egan B. J.,* "Remarks on International Law and Stability in Cyberspace", 2016, Remarks by, Legal Adviser to the U.S. Department of State, on 10 November 2016, <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm>.
6. Final Act, Conference on Security and Co-Operation in Europe, 1975.
7. French Ministry of the Armies, International Law Applied to Operations in Cyberspace.
8. *International Humanitarian Law Institute,* Rules of Engagement Handbook. September 2009.
9. *Kaljulaid K.,* "President of the Republic at the opening of CyCon 2019", 29 May 2019, < https://www.president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/index.html>.
10. *Kesler B.,* The Vulnerability of Nuclear Facilities to Cyber Attack, Strategic Insights, 10, 2010.
11. *Koh H. H.,* "International Law in Cyberspace", 2012, Remarks by, Legal Adviser to the US Department of State, on 18 September 2012. < https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>.
12. Letter to the parliament on the international legal order in cyberspace. (2019). Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace, <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>.
13. Letter to the parliament on the international legal order in cyberspace, 5 July 2019, from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace. < https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>.
14. *Lopez C. T.,* DOD More Assertive, Proactive in Cyber Domain, 28 June 2019, <https://www.defense.gov/Explore/News/Article/Article/1891495/dod-more-assertive-proactive-in-cyber-domain/>.
15. *Lopez C. T.,* Persistent Engagement, Partnerships, Top Cybercom's Priorities, 14 May 2019, <https://www.defense.gov/Explore/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/>.
16. *McConnell B. W. and Austin G.,* A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets, EastWest Institute, 2014.

17. *National Research Council's Committee on Offensive Information Warfare's.*, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. The National Academies Press, 2009, 33-34. <http://www.steptoe.com/assets/attachments/3785.pdf>.

18. National Research Council's Committee on Offensive Information Warfare's, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. The National Academies Press, 2009, 259-261. <http://www.steptoe.com/assets/attachments/3785.pdf>.

19. 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>.

20. *Ney P. C.,* DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 March 2020, <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/>.

21. OSCE, Astana Commemorative Declaration — Towards a Security Community, SUM.DOC/ 1/10/Corr.1, 3 December 2010.

22. Remarks with Israeli Prime Minister Benjamin Netanyahu after Their Meeting', US Department of State, 15 September 2013, <www.state.gov/secretary/remarks/2013/09/214257.htm>.

23. Report of the Independent Fact-Finding Mission on the Conflict in Georgia, September 2009, Vol. I-III.

24. *Roguski P.,* Application of International Law to Cyber Operations: A Comparative Analyses of States' Views, The Hague Program for Cyber Norms Policy Brief, 2020.

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

26. Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom at the Newseum, Washington, D.C. (Jan. 21, 2010).

27. Speech by Attorney General Wright J. QC MP "Cyber and International Law in the 21st Century", 23 May 2018, <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

28. The Bush Administration's Doctrine of Preemption (and Prevention): When, How, Where?" *Council on Foreign Relations,* 2004. <http://www.cfr.org/world/bush-administrations-doctrine-preemption-prevention-/p6799>.

29. UK Ministry of Defence, Cyber Primer, 2nd ed, 2016, 12, < https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf>.

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

31. US White House, Critical Infrastructure Security and Resilience, 2013, Presidential Policy Directive/PPD-21.

32. *Waxman, M. C.*, Cyber Attacks as Force under UN Charter Article 2(4), International Law and the Changing Character of War: Part III: The Changing Character of the Battlefield: The Use of Force in Cyberspace, 2011, 45. <http://unstudies.ir/static/fckimages/files/vol-87_III_waxman_cyberattacks.pdf>.

33. Die Lage der ITSicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik, 2014.

34. Deutscher Bundestag, "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE", BT-Drs. 18/6989, 2015, 11.

ინტერნეტ-წყაროები

1. *RFERL,* საქართველოს მთავრობა ადანაშაულებს რუსეთს „ვირტუალური ცეცხლის" წამოწყებაში, 12.08.2008. <http://www.rferl.org/content/Georgian_Government_Accuses_Russia_Of_Cyberwar/1190477.html>.

2. 'Behind The Estonia Cyberattacks', Radio Free Europe/Radio Liberty, 6 March 2009, <www.rferl.org/content/Behind_The_Estonia_Cyberattacks/1505613.html>.

3. 'Cracking Stuxnet, a 21st-Century Cyber Weapon', 2011, .<www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon >.

4. 'WORM:W32/SLAMMER' (F-Secure) <www.f-secure.com/v-descs/mssqlm.shtml>.

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

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

7. *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>.

8. *Boutin P.,* 'Slammed!', WIRED, 1 July 2003, <www.wired.com/2003/07/slammer/>.

9. *Broad W. J., Sanger D. E.,* 'Worm Was Perfect for Sabotaging Centrifuges', The New York Times, 18 November 2010, <www.nytimes.com/2010/11/19/world/middleeast/19stuxnet.html>.

10. *Clover C.,* 'Kremlin-Backed Group behind Estonia Cyber Blitz', Financial Times, 11 March 2009, <www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz2TBcey8a5>.

11. Crisis Number: 420 – NORTH KOREAN SUBMARINE', International Crisis Behavior Project, July 2010. <www.cidcm.umd.edu/icb/>.

12. Cyber Attacks Disable Georgian Websites, Ministry of Foreign Affairs of Georgia <http://georgiamfa.blogspot.com/2008/08/cyber-attacks-disable-georgian-websites.html>.

13. *Davis J.,* 'Hackers Take Down the Most Wired Country in Europe', WIRED, 21 August 2007, <http://archive.wired.com/politics/security/magazine/15-09/ff_estonia>

14. *de Hoogh A.,* Georgia's Short-Lived Military Excursion into South Ossetia: The Use of Armed Force and Self-Defence EJIL: Talk!, 9 December 2009.

15. *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/>.

16. Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks', RIA Novosti, 9 June 2007, <http://en.ria.ru/world/20070906/76959190.html>.

17. *Hollis D. B.,* 'Could Deploying Stuxnet Be a War Crime?', Opinio Juris, 25 January 2011, <http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime/>.

18. *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>.

19. *Leyden J.,* 'Russian Politician: "My Assistant Started Estonian Cyberwar" – Dubious DDoS Lols', The Register, 10 March 2009, <www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/>.

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

21. *Nakashidze G.,* Cyberattack against Georgia and International Response: Emerging Normative Paradigm of 'Responsible State behavior in Cyberspace'?, EJIL: Talk!, 28 February 2020, <https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative§digm-of-responsible-state-behavior-in-cyberspace/>.

22. *Ray E.,* 'Malware FAQ: MS-SQL Slammer' (SANS) <www.sans.org/security-resources/malwarefaq/ms-sqlexploit.php>.

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

24. *Sanger D. E.,* 'Obama Ordered Wave of Cyberattacks against Iran', The New York Times, 1 June 2012, <www.nytimes.com/2012/06/01/world/middleeast/obama-orderedwave-of-cyberattacks-against-iran.html>.

25. *Shearer J.,* 'W32.Stuxnet', Symantec, 2013, <www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>.

26. *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>.

27. *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>;

28. UK condemns Russia's GRU over Georgia cyber-attacks (20 February 2020), <https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks>;

29. Comment by the Information and Press Department on accusations against Russia of carrying out large-scale cyberattacks on Georgian websites <https://www.mid.ru/ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4050783?p_p_id=101_INSTANCE_cKNonkJE02Bw&_101_INSTANCE_cKNonkJE02Bw_languageId=en_GB>;

30. The United States Condemns Russian Cyber Attack Against the Country of Georgia (February 20, 2020), <https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/?fbclid=IwAR0RICJwF5Um_djH3cxZPbPXaoQ8i4Sfy56BARRXgy8eSFYyaS2rwh28dqU>;

31. Attribution of malicious cyber activity in Georgia by Russian Military Intelligence <https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-malicious-cyber-activity-georgia-russian-military-

intelligence?fbclid=IwAR30-b2Ei4r0x3lGOaVM9IWIz1Sj8i_LJKrPMeZAAQPThmv3XdrKvW_h5s8>;

32. The Netherlands considers Russia's GRU responsible for cyber attacks against Georgia (20-02-2020) <https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/diplomatic-statements/2020/02/20/the-netherlands-considers-russia%E2%80%99s-gru-responsible-for-cyber-attacks-against-georgia?fbclid=IwAR0gmhX1vWkbss7KMe6Id7tFjuKTRVBpl4nbt60rZgTyQZ4jILS3A31_PTg>;
33. Statement of the Polish MFA on cyberattacks against Georgia (20.02.2020) <https://www.gov.pl/web/diplomacy/statement-of-the-polish-mfa-on-cyberattacks-against-georgia>;
34. Latvia condemns cyber-attack against Georgia (21.02.2020) <https://www.mfa.gov.lv/en/news/latest-news/65504-latvia-condemns-cyber-attack-against-georgia>;
35. Declaration by the High Representative on behalf of the European Union - call to promote and conduct responsible behaviour in cyberspace (21.02.2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/02/21/declaration-by-the-high-representative-on-behalf-of-the-european-union-call-to-promote-and-conduct-responsible-behaviour-in-cyberspace/?fbclid=IwAR1xbr-X62Nz_xjVpNXaAwFA0k-7h8wXhUCvIKmD51tNmAaTzgKbgnjihSQ>;
36. Statement of the Foreign Minister of the Republic of Estonia Urmas Reinsalu (20 February 2020) <https://vm.ee/en/news/statement-foreign-minister-republic-estonia-urmas-reinsalu>;
37. <http://mae.ro/node/51739?fbclid=IwAR1xakYudOR6D4OU4GVL7Fz6SHTESyKmHvYXGUemRAKez1WDWnygUBHKhmk>;
38. Коментар МЗС України щодо кібератак, вчинених Російською Федерацією проти Грузії <https://mfa.gov.ua/news/komentar-mzs-ukrayini-shchodo-kiberatak-vchinenih-rosijskoyu-federaciyeyu-proti-gruziyi>;
39. <https://twitter.com/MFAgovge/status/1230479514431631363>;
40. <https://twitter.com/MFA_MNE/status/1230534482081525762>;
41. https://twitter.com/MFA_Austria/status/1230880949610721280>;
42. <https://twitter.com/LT_MFA_Stratcom/status/1230485445798219777>;
43. <https://twitter.com/DanishMFA/status/1230483524123320322>;
44. <https://twitter.com/AnnLinde/status/1230496401873887233>;
45. <https://twitter.com/NorwayMFA/status/1230487577502855169>;

46. <https://twitter.com/CzechMFA/status/1230491060150964230>;

47. <https://twitter.com/GudlaugurThor/status/1230527048906682369>;

48. <https://twitter.com/GUAMSecretariat/status/1230542765345398784>.

განცხადება ნაშრომის ავთენტურობის შესახებ

ვადასტურებ, რომ სადისერტაციო ნაშრომი შესრულებულია ჩემ მიერ, წარმოადგენს დამოუკიდებელი კვლევის შედეგს, არ შეიცავს პლაგიატს და ნაშრომში გამოყენებული ყველა წყარო სათანადოდ არის მითითებული. ვაცნობიერებ სიყალბის გამოვლენის შემთხვევაში ჩემი შედეგის ბათილად ცნობისა და შესაბამისი პროგრამიდან აღდგენის უფლების გარეშე გარიცხვის რეალობას.

გურამ ღვინჯილია