# სამხედრო-პოლიტიკური რეალობა

**თემურ დიღმელაშვილი**

კავკასიის საერთაშორისო უნივერსიტეტის სოციალურ და ჰუმანიტარულ მეცნიერებათა ფაკულტეტის პოლიტიკის მეცნიერების დოქტორანტი

temur.digmelashvili@ciu.edu.ge

ORCID iD: https://orcid.org/ 0009-0000-6081-0134

**გიორგი ჯინჭარაძე**

საქართველოს ტექნიკური უნივერსიტეტის სამშენებლო ფაკულტეტის სამხედრო ინჟინერიის დოქტორანტი

jincharadze.giorgi24@gtu.ge

ORCID iD: https://orcid.org/ 0009-0007-7693-6103

DOI: 10.52340/splogos.2025.03.09

## აბსტრაქტი

კვლევა ეხება კიბერსივრცეს თანამედროვე საერთაშორისო ურთიერთობებში, რომელიც იქცა ძალაუფლების ახალი არენად, სადაც სამხედრო და პოლიტიკური ინტერესები გადაჯაჭვულია. ციფრული ტექნოლოგიების სწრაფმა განვითარებამ მნიშვნელოვნად შეცვალა გლობალური უსაფრთხოების არქიტექტურა და წარმოშვა ისეთი ასიმეტრიული საფრთხეები, რომელთა მასშტაბები და ზემოქმედება ტრადიციული სამხედრო გამოწვევებისგან რადიკალურად განსხვავდება. კიბერუსაფრთხოება დღეს აღარ წარმოადგენს მხოლოდ ტექნიკურ საკითხს; ის არის სამხედრო-პოლიტიკური პროცესების ერთ-ერთი უმნიშვნელოვანესი განმსაზღვრელი, რომელიც გავლენას ახდენს როგორც სახელმწიფოების სტრატეგიულ გადაწყვეტილებებზე, ისე საერთაშორისო სისტემის სტაბილურობაზე. სტატია მიმოიხილავს კიბერუსაფრთხოების კონცეფციის ევოლუციას, ასიმეტრიული საფრთხეების სახეებსა და მათი გამოვლინების გზებს, ასევე ავლენს კიბერომის სამხედრო-პოლიტიკურ განზომილებებს. განსაკუთრებული ყურადღება გამახვილებულია იმაზე, თუ როგორ იქცა კიბერშეტევები თანამედროვე ომების განუყოფელ ელემენტად და რა გამოწვევებს უქმნის ეს საერთაშორისო უსაფრთხოების ინსტიტუტებს. ანალიზი ეფუძნება ისტორიულ-თეორიულ საფუძვლებს, საერთაშორისო პრაქტიკასა და თანამედროვე კონფლიქტების მაგალითებს, რაც შესაძლებლობას იძლევა, გამოიკვეთოს კიბერუსაფრთხოების როლი XXI საუკუნის სამხედრო-პოლიტიკურ რეალობაში.

**საკვანძო სიტყვები:** კიბერუსაფრთხოება, ასიმეტრიული საფრთხეები, კიბერომი, საერთაშორისო უსაფრთხოება, სამხედრო-პოლიტიკური რეალობა

## Cybersecurity, Asymmetric Threats, and Modern Military-Political Reality

**Temur Digmelashvili**

PhD Student in Political Science, Faculty of Social and Human Sciences, Caucasus International University

temur.digmelashvili@ciu.edu.ge

https://orcid.org/0009-0000-6081-0134

**Giorgi Jincharadze**

PhD Student in Military Engineering, Faculty of Civil Engineering, Georgian Technical University

jincharadze.giorgi24@gtu.ge

https://orcid.org/0009-0007-7693-6103

### Abstract

Cyberspace has become a new arena of power in modern international relations, where military and political interests are intertwined. The rapid development of digital technologies has significantly altered the architecture of global security, giving rise to asymmetric threats that are radically different in scale and impact from traditional military challenges. Cybersecurity today is no longer just a technical issue; it is one of the most significant determinants of military and political processes, which affects both the strategic decisions of states and the stability of the international system. The article reviews the evolution of the concept of cybersecurity, the types of asymmetric threats and how they manifest themselves, and also reveals the military-political dimensions of cyberwar. Special attention is paid to how cyberattacks have become an integral element of modern wars and what challenges this poses to international security institutions. The analysis is based on historical-theoretical foundations, international practice, and examples of modern conflicts, which makes it possible to outline the role of cybersecurity in the military-political reality of the 21st century.

**Keywords:** cybersecurity, asymmetric threats, cyberwar, international security, military-political reality

## კვლევის მეთოდები

სტატიის მეთოდოლოგია ეფუძნება შედარებით ანალიზს, ქეის-სტადის მეთოდს (2008 წლის რუსეთ–საქართველოს ომი, 2022–2025 წლების რუსეთ–უკრაინის ომი) და თეორიულ-კონცეპტუალურ მიდგომას, რომელიც მოიცავს საერთაშორისო ურთიერთობების რეალიზმისა და უსაფრთხოების სექტორული თეორიების (ბუზანის უსაფრთხოების თეორია) გამოყენებას.

**თეორიული ჩარჩო**:

- რეალიზმი საერთაშორისო ურთიერთობებში (ძალაუფლების გადანაწილება და ასიმეტრიული უპირატესობები);
- უსაფრთხოების სექტორული მიდგომა (პოლიტიკური, სამხედრო და ტექნოლოგიური განზომილებები);
- ჰიბრიდული ომის თეორია, სადაც კიბერშეტევები განიხილება როგორც არატრადიციული საბრძოლო საშუალება.

**სამეცნიერო სიახლე** ნაშრომის სიახლე მდგომარეობს იმაში, რომ ის აერთიანებს კიბერუსაფრთხოების, ასიმეტრიული საფრთხეების და სამხედრო-პოლიტიკური რეალობის ანალიზს ერთიან ჩარჩოში, რაც საშუალებას იძლევა, ფართო სურათში დავინახოთ როგორ გარდაქმნის კიბერშეტევები საერთაშორისო პოლიტიკის არსს და სამხედრო ძალის ფუნქციას.

## შესავალი

ციფრული ეპოქის განვითარებასთან ერთად, კიბერსივრცე იქცა საერთაშორისო ურთიერთობებისა და სამხედრო-პოლიტიკური დინამიკის ერთ-ერთ უმთავრეს კომპონენტად. თანამედროვე უსაფრთხოების გარემო აღარაა დამოკიდებული მხოლოდ ტრადიციულ სამხედრო ძალასა და ეკონომიკურ რესურსებზე; გადამწყვეტ როლს ასრულებს ინფორმაციული ტექნოლოგიები, ციფრული ინფრასტრუქტურები და მათზე განხორციელებული კიბერშეტევები. სწორედ ამიტომ, კიბერუსაფრთხოების საკითხი გახდა როგორც ინდივიდუალური სახელმწიფოების, ისე საერთაშორისო ორგანიზაციების მთავარი სტრატეგიული პრიორიტეტი.

ნაშრომის აქტუალობა განპირობებულია იმით, რომ XXI საუკუნეში კიბერსაფრთხეები კლასიკური სამხედრო საფრთხეებთან ერთად იქცა გლობალური უსაფრთხოების ერთ-ერთ ყველაზე რთულ და **ნაკლებად პროგნოზირებად გამოწვევად. მათ შორის განსაკუთრებით საგულისხმოა ასიმეტრიული საფრთხეები,** რომელთა ბუნება მოიცავს ისეთ თავდასხმებს, რომლებსაც მცირე რესურსების მქონე აქტორები ახორციელებენ ძლიერ სახელმწიფოებზე, რაც არსებითად ცვლის ძალთა ბალანსის ტრადიციულ აღქმას.

კიბერუსაფრთხოების მნიშვნელობა თანამედროვე სახელმწიფოებრივ პრაქტიკაში განპირობებულია იმ რეალობით, რომ ციფრული ინფრასტრუქტურები და მათი მოწყვლადობები გადამწყვეტად განსაზღვრავენ ეკონომიკურ, სოციალურ და სამხედრო მიმართულებებს[94]. აქედან გამომდინარე, კიბერუსაფრთხოება უნდა განვიხილოთ არა მხოლოდ ტექნიკურ საქმედ, არამედ კომპლექსურ სამხედრო-პოლიტიკურ ინსტრუმენტად, რომელიც ეხმარება აქტორს პირდაპირ ან ირიბად მიაღწიოს სასურველ პოლიტიკურ შედეგს. ამ თვალსაზრისით მნიშვნელოვანია ხაზი გავუსვათ ასიმეტრიული საფრთხეების სპეციფიკას: მათი განხორციელება პრინციპულად ეყრდნობა იაფად მოდელირებადი, ტექნოლოგიური შესაძლებლობების ეფექტურ გამოყენებას და ცდილობს მიაღწიოს არაპროპორციულ შედეგს – მცირე რესურსების ხარჯზე ფართო სტრუქტურული ზიანის მიყენებას.

ასიმეტრიულობის ტექნიკურ და ოპერაციულ საფუძველს წარმოადგენს რამდენიმე მახასიათებელი: თავდამსხმელი ხშირად სარგებლობს ანონიმურობით და ურთიერთგამომრიცხავი მეთოდებით (პროქსი სერვერები, საკონტრაქტო ჯგუფები, კრიმინალური ქსელი), შეუძლია სწრაფად შეცვალოს ტაქტიკა და მიზანი და უპირატესად იყენებს არაპირდაპირ მეთოდებს - ინფორმაციული ოპერაციები, დეზინფორმაცია, და საინფორმაციო მანიპულაციები და ეს ყველაფერი ერთად გამანადგურებელ შედეგამდე მიდის[95]. მოწყობილობების მასიური ჩართვა ქსელში და ინტერნეტში (IoT), ღრუბლოვანი სერვისების ფართო დანერგვა, და გლობალური მიწოდების ჯაჭვების შეფერხებულობა ქმნის არაერთ მოწყვლად წერტილს, სადაც პატარა შეტევამაც კი შეიძლება გამოიწვიოს სწრაფად გავრცელებადი კრიზისი.

ოპერაციულად, კიბერსივრცეში შეტევები ხშირად იყოფა რამოდენიმე ფაზად: დაკვირვება (reconnaissance), პრივილეგირებული წვდომის მოპოვება (initial access), გვერდითი გადაადგილება და პოზიციონირება (lateral movement), ფუნქციური ზიანის მიყენება (disruption/degradation) ან მონაცემთა მოპოვება/ექსტრაქცია (exfiltration), და საჭიროებისამებრ დესტრუქციული ფაზა (wiping, sabotage). სტრატეგიული თვალთახედვით კიბერშეტევები ემსახურებიან არაერთ მიზანს: მზადყოფნის დასუსტებას, სამთავრობო კომუნიკაციების

[94] ზედელაშვილი, თ. 2023. "კიბერშესაძლებლობები და გლობალური უსაფრთხოების ახალი გამოწვევები."https://dspace.nplg.gov.ge/bitstream/1234/482400/1/KibershesadzleblobebiDaGlobaluriUsafrtxoebisAxaliGamowvevebi.pdf?utm.

[95] Almalawi, A., Hassan, S., Fahad, A., Iqbal, A. and Khan, I. A. 2025. "Hybrid Cybersecurity for Asymmetric Threats: Intrusion Detection and SCADA System Protection Innovations." *Symmetry* 17 (4): 616–16. https://doi.org/10.3390/sym17040616.

პარალიზებას, გადაწყვეტილების მიმღების როლის მოპოვებას, თავდაცვის სუსტი წერტილების გამოსაჩენად და საერთაშორისო იმიჯის შელახვისთვის. განსაკუთრებით ეფექტურია კიბერი და ინფორმაციული ოპერაციები, როცა ისინი სინქრონიზებულია კონვენციურ სამხედრო მოქმედებებთან - ამგვარი ჰიბრიდული კომბინაცია ზრდის ოპერაციული ეფექტურობის შესაძლებლობას და რთულს ხდის მოწინააღმდეგისთვის თავდაცვითი სტრატეგიების დროულ შემუშავებას იმისათვის, რომ ვერ მოხერხდეს შეტევის სწრაფი შეფასება და მათზე რეაგირება.

2008 წლის რუსეთ–საქართველოს ომი მსოფლიოში ხშირად ნახსენებია, როგორც პირველი ფაქტობრივი მაგალითი, სადაც ვიხილეთ ძირითადად პოლიტიკური და საომარი მოქმედებების პარალელურად განხორციელებული მასობრივი კიბერშეტევების გამოყენება. კონფლიქტის დროს მოხდა მთავრობისა და მედიის ვებ-რესურსების ზრდადი DDoS-შეტევები, ვებგვერდების სახეცვლილება (defacement) და კომუნიკაციის შეფერხება, რაც გამიჯნულია კონვენციური სამხედრო ოპერაციების დროში. ამას მოსდევდა მოსახლეობის ინფორმაციის ვაკუუმი და ფინანსური ოპერაციების მოშლა - თვისებები, რომლებიც აჩვენებდა, რომ კიბეროპერაციები წინ უძღოდა სამხედრო მოქმედებებს და ზრდიდნენ არსებულ არეულობას. საქართველოს შემთხვევაში განსაკუთრებით თვალსაჩინო იყო, რომ სამოქალაქო კრიტიკული ინფრასტრუქტურის დაცვა ადრეული ეტაპიდან არ იყო ადეკვატურად მომზადებული კოორდინირებული კიბერინციდენტების შესაჩერებლად.

2022–2024 წლების რუსეთ–უკრაინის ომი უფრო რთული და მასშტაბური გამოცდილებაა - აქ კიბერშეტევებმა მიიღეს მრავალთქმედითი ფორმა. უკრაინის წინააღმდეგ განხორციელებული კამპანიების დროს დაფიქსირდა როგორც მიზნობრივი განადგურება (wiper ტიპის პროგრამები), ასევე ინტენსიური DDoS-აქტივობები და მიზნობრივი შეტევები ენერგეტიკულ და სატელეკომუნიკაციო სისტემებზე. ამავე დროს, უკრაინამ მიიღო ძლიერი მხარდაჭერა ტექნიკურ და ინფორმაციულ სფეროში - კერძო კომპანიების, სატელიტური მომსახურების პროვაიდერების, საერთაშორისო მხარდამჭერების მხრიდან, რაც წარმოადგენდა თანამედროვე კონფლიქტის ერთ-ერთ უაღრესად მნიშვნელოვანი შტრიხს: ციფრულ ბრძოლაში გამარჯვება ხშირად იმაზეა დამოკიდებული, არა მხოლოდ თავდაპირველ შესაძლებლობებზე, არამედ საერთაშორისო ტექნოლოგიურ ეკოსისტემასთან წვდომასა და დახმარებაზე.

ზემოთ აღწერილი გამოცდილებიდან გამომდინარეობს რამდენიმე მნიშვნელოვანი დასკვნა სამხედრო-პოლიტიკური პრაქტიკისთვის: პირველი, თანამედროვე ქვეყნის უსაფრთხოება მოითხოვს «ყველა სახელმწიფო ინსტიტუტის» მიდგომას - სამხედრო, დაზვერვა, ეროვნული უსაფრთხოება და სამოქალაქო სექტორი უნდა მონაწილეობდნენ კიბერუსაფრთხოების საერთო

არქიტექტურის შექმნაში[96]; მეორე, კრიტიკული ინფრასტრუქტურის დაცვა უფრო მყარია, როდესაც ინფორმაციის მიწოდების ჯაჭვი მრავალფეროვანია და ყველა მხრიდან ხდება პრობლემის დაფიქსირება, მესამე, ავტორობისა და სამართლებრივი რეაგირების საკითხებმა შეაფერხეს ადეკვატური საერთაშორისო რეაქცია, რაც უსვამს ხაზს გლობალური ნორმატიული ჩარჩოს საჭიროებაზე და კონფლიქტების დეესკალირების მექანიზმების შექმნაზე.

ასიმეტრიული საფრთხეების გათვალისწინებით სამხედრო სტრატეგიებში საჭიროა არა მხოლოდ თავდაცვის ტექნიკური გაძლიერება, არამედ ნეირო-პოლიტიკური და საზოგადოებრივი მდგრადობის ამაღლება: საჯარო კომუნიკაციის გამჭვირვალობა, ინფორმაციის სწრაფი გადამოწმების მექანიზმები, და საზოგადოებრივი სიმართლის უზრუნველყოფა ისეთ გარემოში, სადაც დეზინფორმაცია ერთადერთი-ყოველდღიური იარაღია.

## ტექნიკური ტაქტიკა და პროტოკოლები - ოპერაციული ანატომია

კიბეროპერაციების ოპერაციული არქიტექტურა თანმიმდევრული, ფაზურ სტრუქტურაზეა აგებული და წარმოადგენს სისტემურ პროცესს, რომლის თითოეული ეტაპი განსაზღვრავს თავდამსხმელის შესაძლებლობასა და დაცვის საჭირო ღონისძიებებს. აღნიშნული ფაზები იწყება კიბერდაზვერვით - საჯარო წყაროების (OSINT) გამოყენებით ინფორმაციის შეგროვებით, ქსელური სკანირებითა და სისტემური fingerprinting–ით, დღესდღეობით კვლავაც გამოიყენება ღრმა ქსელური მეთოდები და მავნე აქტივობის ანალიზი[97]. მეორე ეტაპი, პირველადი წვდომა, აღენიშნება ისეთ ტაქტიკებს, როგორიცაა ფიშინგი, მიზანმიმართული მატყუარა შეტყობინებები, მოწყვლადობის ექსპლოიტაცია და ე.წ. supply-chain შეტევები ხიდების უგულებელყოფით. აღნიშნული ფაზა ხშირად იყენებს სერვისებსა და არხებს (RDP, VPN), რომლებიც ადვილად ხდება სამიზნე მოძველებული განახლებების ან არასათანადო კონფიგურაციის გამო. შემდეგი ეტაპი მოიცავს პოზიციონირებას და ლატერალურ გადაადგილებას (lateral movement)[98]: თავდამსხმელი ერიდება მხოლოდ ერთ სისტემაზე შეჩერებას და ახდენს თვისობრივ ბინარულ წმენდას - უკანა კარს (backdoor) ამუშავებს, იყენებს SMB/LDAP ტიპის კომუნიკაციას და მიმართავს პრივილეგიების ესკალაციას, ხშირად Mimikatz–ს ან მსგავსი ხელსაწყოების მეშვეობით. ოპერაციული გავლენის

[96] Aos, M., Qolomany, B., Gyorick, K., Abdo, B. J., Aledhari, M., Qadir, J., Carley, K., and Al-Fuqaha, A. 2025. "A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects." *Computers in Human Behavior Reports* 18 (100668): https://doi.org/10.1016/j.chbr.2025.100668

[97] James, K., Ahmad, A., and Scheepers, R. 2022. "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation." *European Journal of Information Systems* 32 (1): 1–17. https://doi.org/10.1080/0960085x.2022.2088414.

[98] Lex, C. 2024. "Technical Deep Dive: Understanding the Anatomy of a Cyber Intrusion | MITRE-Engenuity." Medium. MITRE-Engenuity. https://medium.com/mitre-engenuity/technical-deep-dive-understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3.

ფაზა გულისხმობს სისტემური ფუნქციის დარღვევას: მონაცემთა ექსტრაქციას (exfiltration), ინფრასტრუქტურულ დეზორგანიზაციას (disruption) და ინფორმაციის მანიპულაციას, რაც შეიძლება გადაიზარდოს ფიზიკურ დესტრუქციაში (firmware-ის დაზიანება, wiper ტიპის კოდები). საბოლოო ეტაპები მოიცავს persistence მექანიზმებს, ლოგების დამალვას და ღია კვალის მოხსნას, რათა შეტევა გარდამავალი ან შენიღბული დარჩეს.

ტექნიკური ინსტრუმენტების და ტაქტიკების სპექტრი ფართოა: DDoS და ტრაფიკის ამპლიფიკაცია (NTP, DNS amplification) უზრუნველყოფს სისტემების დროებით გათიშვას; botnet–ების გამოყენება მატებს შეტევებს მასშტაბურობას; supply-chain შეტევები კი საქართველოსა და უკრაინის გამოცდილებებიდან ჩანს, როგორც მაღალეფექტური და რთულად გამოსაკვლევი მეთოდი, როცა შეტევა ხორციელდება მესამე მხარის კომპონენტის დაინფიცირებით. Wiper ტიპის მავნე კოდი, რომლის მიზანია მონაცემების და სისტემური რესურსების ფიზიკური ან ლოგიკური წაშლა, წარმოადგენს იშვიათად გამოყენებულ, თუმცა უკიდურესად მძიმე შედეგებს მომცემ ძალადობრივ ინსტრუმენტს. ამავე კონტექსტში განსაკუთრებით საშიშია Living-off-the-Land (LotL) მიდგომა, როდესაც თავდამსხმელები იყენებენ ლეგიტიმურ სისტემურ ინსტრუმენტებს (PowerShell, WMI, certutil) ხელოვნურად თავიანთი მოქმედებების დაფარვისთვის. ქსელური პროტოკოლების დონეზე, HTTP/HTTPS ხშირად წარმოადგენს C2 (command-and-control) არხს, RDP/SSH – პირდაპირი კონტროლის საშუალებებს, ხოლო SMB და NetBIOS - ლატერალური მოძრაობის და ფაილური რესურსების მოპოვების გზებს.

თავდაცვისთვის საყოველთაო და პრაქტიკული ნაბიჯები მოიცავს: სისტემატურ და პრიორიტეტულ პაჩ-მენეჯმენტს, ქსელური სეგმენტაციას და OT–სა და IT–ს მკაცრ იზოლაციას, EDR/XDR და SIEM სისტემების იმპლემენტაციას ოპერატიული ალერტინგით, immutable და air-gapped ბექაპების გამოყენებით აღდგენის უზრუნველყოფასა და tabletop ვარჯიშების მოწყობას. ასევე მნიშვნელოვანი არის threat-intelligence–ის ინტეგრირება - IoC-ების (Indicator of Compromise) სწრაფი განახლებითა და მოკავშირეებისა თუ სექტორის მასშტაბით სათანადო ინფორმაციის გაზიარებით. აღნიშნული ტექნიკური ღონისძიებები, თუ ისინი შემუშავებულია და რეალიზირებული იქნება თანმიმდევრულად, მნიშვნელოვნად ამცირებს კიბეროპერაციების ეფექტიანობას და ზრდის სახელმწიფოებრივი და პირადი სქემების მდგრადობას.

**სამართლებრივი ასპექტები და ნორმატიული წინადადებები**

კიბერუსაფრთხოების სამართლებრივი ასპექტები წარმოადგენს ერთ-ერთ რთულ და ჯერ კიდევ არასტაბილურ მხარეს საერთაშორისო სამართლის სექტორში. უპირველესად, ატრიბუციის პრობლემა - თავდასხმის ავტორობის განსაზღვრა - ნამდვილად ერთ-ერთი ყველაზე მნიშვნელოვანი სამართლებრივი გამოწვევაა. დროსა და რესურსის უქონლობის პირობებში მიღებული მტკიცებულებები ხშირად არ არის საკმარისი საერთაშორისო სამართლებრივი მოთხოვნების დასაკმაყოფილებლად, რის გამოც სახელმწიფოები ერიდებიან

საჯარო ბრალდებებს ან სამართლებრივი დევნის ინიციატივებს[99]. ეს იწვევს ისედაც რეგლამენტირებულ ველთან დაკავშირებულ პოლიტიკურ და იურიდიული მყიფეობას და ზრდის ესკალაციის რისკს, თუ ხელთ არსებული მტკიცებულებების საფუძველზე განიხილება სამხედრო პასუხი. მეორე მნიშვნელოვანი საკითხი არის რა სახის ხასიათი ექნება ინტენსიურ კიბეროპერაციებს - არის თუ არა ისინი ძალის გამოყენებისა ან შეიარაღებული კონფლიქტის მოვლენების მსგავსად. ამ საკითხზე საერთაშორისო იურიდიული დებულებები განსხვავებულადვე ინტერპრეტირებადია; ზოგიერთი შემთხვევა შეიძლება მკვეთრად მიეკუთვნოს ძალის გამოყენების დეფინიციას (მაგ., მნიშვნელოვანი ინფრასტრუქტურის სისტემური დესტრუქცია, რომელმაც გამოიწვია ფიზიკური ზიანი ან სიცოცხლის დანაკარგი), ხოლო სხვა - უფრო რთულ სამართლებრივ კლასიფიკაციას საჭიროებს. ამასთანავე, საზღვარგარეშე სახელმწიფოებთან დაკავშირებული არასახელმწიფო აქტორების ზრდასთან ერთად რთულდება პასუხისმგებლობის განსაზღვრა - სახელმწიფოს როლი შეიძლება იყოს პირდაპირი, არასრული ან საკონტრაქტო ურთიერთობის სახით, რაც ქმნის სამართლებრივ არეულობას.

ეროვნული სამართლის დონეზე აუცილებელია მკაფიო კიბერდანაშაულის და კრიტიკული ინფრასტრუქტურის დაცვის ნორმების ჩამოყალიბება[100]. სახელმწიფოებმა უნდა განსაზღვრონ, რა წარმოადგენს კრიტიკულ ინფრასტრუქტურას, როგორია სახელმწიფო და კერძო სუბიექტების პასუხისმგებლობები და რამდენად უნდა ჰქონდეთ სადაზვერვო უწყებებს უფლებამოსილებები ეპიდემიის, ინფორმაციის მოპოვების და პრევენციის მიზნით - ყოველთვის გათვალისწინებული მოქალაქეთა ძირითადი თავისუფლებების დაცვა. მონაცემთა დაცვის სტანდარტების (მაგ., GDPR-ის მსგავს სტრუქტურათა) შესაბამისობა და ჰარმონიზირება წარმოადგენს დამატებით გამოწვევას - სახელმწიფომ უნდა შეძლოს ინფორმაციის დაცვა ისე, რომ არ ზღუდავდეს უსაფრთხოების მნიშვნელოვანი ღონისძიებების განხორციელებას.

საერთაშორისო ნორმების საკითხი მოითხოვს ახალ, მიზანმიმართულ მიდგომებს. საჭიროა წესების ერთობლივი შეთანხმება, რომელიც შინაარსობრივად განისაზღვრება როგორც „არაესკალაციური პრინციპები“ - მაგალითად, შეთანხმება, რომ მიზნად არ უნდა იქნეს დასმული სამოქალაქო კრიტიკული ინფრასტრუქტურა ან მოსახლეობის წინააღმდეგ მიმართული ოპერაციები[101]. ამ ტიპის ნორმები

[99] Anna-Maria, O. and Rõigas, H. 2016. “International Cyber Norms Legal, Policy & Industry Perspectives.” https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf.

[100] Chitadze, N. 2023. “IRMA-International.org: Cyber Security Policies and Strategies of the World’s Leading States (9781668488461)(1668488469)(9781668488478): Nika Chitadze: Books.” Irma-International.org. https://www.irma-international.org/book/cyber-security-policies-strategies-world/316140/?utm_source=chatgpt.com.

[101] Sevis K. N., and Seker, E. 2016. "Cyber warfare: terms, issues, laws and controversies," 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, UK, doi: 10.1109/CyberSecPODS.2016.7502348

თავიდან უნდა იქნას აცილებული არაეთიკური შეტევების გამოყენებით, მაგრამ მათი ფორმალიზება და განმტკიცება რთულია, თუ არ არსებობს ეფექტური ატრიბუციის მექანიზმები და გამჭვირვალე საერთაშორისო გამოძიების პლატფორმები.

ნორმატიული წინადადებების შემოთავაზება არ უნდა შემოიფარგლოს მხოლოდ ფრაზებით; აუცილებელია პრაქტიკული ინსტრუმენტების ჩამოყალიბებაც. უპირველესად, რეკომენდებულია საერთაშორისო ფორუმზე binding და non-binding შეთანხმებების კომბინაციის მიღება - პირველი განსაზღვრავს კრიტიკულ ზღვარსა და პრინციპებს, მეორე კი მოქნილ დიპლომატიურ მექანიზმებს უზრუნველყოფს. უნდა შეიქმნან დამოუკიდებელი, ექსპერტული საერთაშორისო საგამოძიებო დაწესებულებები, რომლებიც შეგროვებული ტექნიკურ მტკიცებულებას შეაფასებენ და ატრიბუციის უმაღლეს სტანდარტს უზრუნველჰყოფენ. ასევე სასარგებლოა 24/7 მობილური ტექნიკური დახმარების ჰაბების ჩამოყალიბება, რომელიც შეძლებს მკაცრი და დროული მხარდაჭერის გაწევას დაზარალებული სახელმწიფოსა და კერძო სექტორის მიმართ.

ასევე მნიშვნელოვანია კერძო და საჯარო სექტორების პარტნიორობის მოდელების შემუშავება - მონაცემთა ცენტრები, ღრუბლოვანი პროვაიდერები და კრიტიკული ტექნოლოგიური კომპანიები უნდა იყვნენ აქტიური წევრები ეროვნული და საერთაშორისო უსაფრთხოების არქიტექტურაში. მათი ინფორმაციის სწრაფი და უსაფრთხო გაზიარება, პასუხისმგებლობის ამხელა განაწილება და რეგულირების მკაფიო ჩარჩო საშუალებას მისცემს სახელმწიფოს და ბაზარს სწრაფ და კოორდინირებულ რეაგირებაზე.

შეჯამების სახით, სამართლებრივი რეფორმების გზავნილი არის შემდეგი: საერთაშორისო თანამეგობრობამ ერთად უნდა იმუშაოს ატრიბუციისა და პასუხისმგებლობისა დაანონსებისთვის, შეიმუშაოს მკაფიო ნორმები „წითელი ხაზებისთვის“ და შექმნას სწრაფი რეაგირებისა და მხარდაჭერის მექანიზმები. ასეთი მიდგომა შეამცირებს გაუგებრობისა და არათავისუფალი რეაგირების შემთხვევებს და გაზრდის დეესკალაციისა და სამართლებრივი მიმართულების მნიშვნელობას კონფლიქტურ სიტუაციებში.

## მოვლენათა ქრონოლოგია - 2008 წლისა და 2022–2024 წლების შემთხვევები

2008 წლის რუსეთ–საქართველოს ომი წარმოადგენს ერთერთ პირველ ცნობილ შემთხვევას, სადაც გამოკვეთილად გამოჩნდა კონვენციურ სამხედრო ოპერაციებთან სინქრონულად განხორციელებული მასიური კიბეროპერაციების გამოყენება. აგვისტოში მომხდარმა კონფლიქტმა აჩვენა, რომ DDoS შეტევებმა და ვებგვერდების დეფეისმენტმა (defacement) შეიძლება კონფლიქტის უცნაურ და ურთიერთგამომრიცხავ ინფორმაციულ გარემოს შექმნაში მნიშვნელოვანი როლი ითამაშონ. კრიტიკული ინფრასტრუქტურის დაცვის რეჟიმი მრავალ ქვეყნებში არ იყო საკმარისად განვითარებული იმგვარად, რომ ეფექტურად აეცილებინა კოორდინირებული კიბერთავდასხმები[102]. საერთაშორისო რეაქცია ტექნიკური

[102] Lomidze, N. 2022. “Cyber Security Challenges in Georgia”. *Georgian Scientists* 4 (3):120-33. https://doi.org/10.52340/gs.2022.04.03.15.

შინაარსის ჰქონდა შეზღუდულად - ძირითადად პოლიტიკურ და დიპლომატიურ დონეზე - რადგან ატრიბუციის საკითხი და მტკიცებულებათა დეფიციტი ართულებდა საინიციატივო, სამართლებრივ ან სამხედრო პასუხს.

ამ შემთხვევამ დაადასტურა, რომ ციფრული ასიმეტრიულობის ძალა: მცირე კომპლექტითა და დაბალი ხარჯით განხორციელებულმა ციფრულმა აქტივობებმა მნიშვნელოვანი პოლიტიკური და სოციალური შედეგები გამოიღო. ამ მაგალითმა ასევე გამოავლინა სახელმწიფო ინსტიტუტების შორის კოორდინაციის ნაკლები მზადყოფნა და კერძო სექტორის ჩართულობის სუსტი მექანიზმები.

2022–2024 წლების რუსეთ–უკრაინის ომი კი წარმოადგენდა კიბერშეტევების ევოლუციის უფრო სრულ, მრავალფაზიან და მასშტაბურ მაგალითს. აქ მოქმედებამ მოიცვა როგორც დესტრუქციული პროგრამული მოწყობილობები (wiper), ისე ენერგეტიკულ და სატელეკომუნიკაციო ინფრასტრუქტურებზე მიზნობრივი შეტევები, რთული supply-chain ექსპლოიტაციები და მუდმივი საინფორმაციო ომი[103]. მნიშვნელოვანი იყო ისიც, რომ უკრაინას მიეხმარა ფართო საერთაშორისო ტექნოლოგიური და ინტელექტუალური მხარდაჭერა: კერძო კომპანიებმა და საერთაშორისო პარტნიორებმა დახმარების სახით გამოიყენეს ტექნიკური ინსტრუმენტები, threat-intelligence-ის გაცვლის მექანიზმები და დახმარების პლატფორმები, რაც სასიცოცხლოდ მნიშვნელოვანი აღმოჩნდა ქვეყნის მდგრადობისთის.

ამ ომმა აჩვენა, რომ თანამედროვე ციფრულ ბრძოლის ველზე წარმატება არ შემოიფარგლება მხოლოდ თავდასხმის ტოლფასობაზე. მნიშვნელოვანია საერთაშორისო ეკოსისტემის მხარდაჭერა, ხელმისაწვდომი ტექნოლოგიური რესურსები და სწრაფი ტექნიკური რეაგირება. უკრაინის მაგალითმა ასევე ხაზგასმით დაანახა supply-chain შეტევების ეფექტურობა, აგრეთვე ის, რომ ინფორმაციული ოპერაციები ხშირად მოქმედებდნენ კონვენციურ სამხედრო ოპერაციებთან პარალელურად, გაზრდილი ეფექტიანობით.

ორივე შემთხვევა აჩვენებს საერთო ტენდენციას: კიბერშეტევები მნიშვნელოვანად ცვლის საომარ სტრატეგიას და სახელმწიფოებრივი მდგრადობის განზომილებას[104]. აქედან გამომდინარე სახელმწიფოთა სისტემებმა დაუყოვნებლად უნდა გააძლიერონ ეროვნული რეკომენდირებული სადაზვერვო, ტექნიკური და სამართლებრივი მექანიზმები; საერთაშორისო თანამეგობრობამ კი - სწრაფად და მიზანმიმართულად უნდა იმუშაოს ნორმების, ატრიბუციის ხელსაწყოების და თანამშრომლობის მექანიზმების გაძლიერებაზე.

ამ ყველაფრიდან გამომდინარე ვხედავთ, რომ კიბერუსაფრთხოება დღეს წარმოადგენს სამხედრო-პოლიტიკური პროცესების ორგანულ ნაწილს. ასიმეტრიული საფრთხეები არამხოლოდ ცვლის ვიზუალურად საომარ მეთოდებს,

---

[103] Eduard, K. 2023. "A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War." SecurityWeek, https://www.securityweek.com/one-year-of-russia-ukraine-war-cybersecurity-industry-sums-up-impact/.

[104] Yuan, T. L. 2024. "Asymmetry in the Digital Age: Cyber Deterrence Strategies for Small States." *Journal of Strategic Security* 17 (4): 71–88. https://doi.org/10.5038/1944-0472.17.4.2268.

არამედ ცვლის საერთაშორისო სამართლის, საერთაშორისო თანამშრომლობის და ეროვნული პოლიტიკის სტრატეგიულ პრიორიტეტებს. მომავალი გამოწვევები მოითხოვს სისტემურ, ტექნოლოგიურ და ინსტიტუციონალურ ცვლილებებს, რათა სახელმწიფომ შეძლოს როგორც თავდაცვის ხარისხის ამაღლება, ასევე კიბერშეტევების პოლიტიკურ და სამართლებრივ შედეგებზე პასუხის გაცემისუნარიანობის გაძლიერება.

## დასკვნა

კვლევის შედეგად დასტურდება, რომ კიბერსივრცე XXI საუკუნის სამხედრო-პოლიტიკური რეალობის განუყოფელ ელემენტადაა სახეცვლილი და მისი მნიშვნელობა აგრესიული სახელმწიფოებრივი და არასახელმწიფო აქტორების ქმედებების შეფასებასა და თავდაცვის სტრატეგიების ჩამოყალიბებაში წინასწარ განისაზღვრება. ზემოთ მოყვანილი აღნიშნული მაგალითბი (2008 წ. რუსეთ–საქართველოს ომი და 2022–2024 წწ. რუსეთ–უკრაინის ომი) აჩვენებენ, თუ როგორ განვითარდა კიბეროპერაციების ტაქტიკა: პრაიმარული DDoS/defacement–ის ეტაპიდან გადავიდა დახვეწილ wiper-ტიპის დესტრუქციაზე და Living-off-the-Land სტრატეგიებზე, ანუ ეს ნიშნავს რომ კიბერსივრცე არის განზომილება სადაც თავდამსხმელები იყენებენ ლეგიტიმურ სისტემურ ინსტრუმენტებს თავიანთი მოქმედების დაფარვისათვის. შესაბამისად, კიბერუსაფრთხოება აღარ წარმოადგენს მხოლოდ IT-პრობლემას - ის მოითხოვს მთლიანი სახელმწიფო ინსტიტუციების, კერძო სექტორის და საზოგადოებისა და საერთაშორისო პარტნიორების ერთობლივ და კოორდინირებულ მოქმედებებს.

კვლევის ერთ-ერთი მნიშვნელოვანი დასკვნა გახლავთ ასიმეტრიული საფრთხეების ბუნების ცვლილება: მცირე რესურსების მქონე აქტორებმა ციფრული ტექნოლოგიების გამოყენებით მოახერხეს არაპროპორციული ზიანის მიყენება, რაც ტრადიციულ ძალთა ბალანსს ცვლის. ამ პროცესში განსაკუთრებით გამოჩნდა ატრიბუციისა და პასუხისმგებლობის სამართლებრივი ნაკლებობებიდან წარმოებული პოლიტიკურ-ტაქტიკური პრობლემები: მტკიცებულებების დეგრადაცია, სამართლებრივი სპექტრის ბუნდოვანება და საერთაშორისო ნორმების არარსებობა ზრდის ესკალაციის რისკს და ამსხვრევს ეფექტური, კანონმდებლური რეაგირების შესაძლებლობას. ამ თვალსაზრისით, 2008 წლის შემთხვევის შეზღუდული სამართლებრივი რეაგირებისა და 2022–2024 წლების ომის დროს ტექნიკურმა მხარდაჭერამ ერთნაირი პერსპექტივით დააფიქსირა ორი არჩევანი - ტექნიკური და დიპლომატიური მექანიზმების გაძლიერება ან ნორმატიული უთანაბრობის შენარჩუნება, რომელსაც მოჰყვება მაღალი არასტაბილურობა.

ამ ყველაფრიდან შეგვიძლია გამოვიტანოთ დასკვნა რომ განხილული საკითხი გვთავაზობს მრავალსაფეხურიან მიდგომას: ტექნიკური ზომები (სისტემატური პაჩ-მენეჯმენტი, ქსელური სეგმენტაცია და OT/IT იზოლაცია, EDR/XDR და SIEM სისტემები) უნდა იყოს ინტეგრირებული ეროვნული კიბერუსაფრთხოების სტრატეგიაში. თუმცა ტექნიკური შესაძლებლობების მხოლოდ განვითარება არასაკმარისია - აუცილებელია ინფორმაციულ, სამართლებრივ და მმართველობით ცვლილებებთან ჰარმონიზაცია: ინციდენტების

სწრაფი გამოძიების პლატფორმების შექმნა, დამოუკიდებელი საერთაშორისო ჯგუფების მხარდაჭერა, და მუდმივი სადაზვერვო ინფორმაციის გაცვლა როგორც საჯარო, ასევე კერძო სექტორის შესრულებით. კვლევამ განსაკუთრებული ყურადღება მოაქცია supply-chain მოწყვლადობებსა და კერძო კომპანიების როლზე: თანამედროვე თავდასხმების დიდი ნაწილი მიმართულია მესამე მხარის უზრუნველყოფაზე, ამიტომ საჯარო-კერძო პარტნიორობის დახვეწა და პროვაიდერებთან რისკების მენეჯმენტი პოლიტიკური და ოპერაციული ცენტრი უნდა გახდეს.

ნორმატიულ და დიპლომატიურ ჭრილში აუცილებელია დიდი ყურადღების მიქცევა ატრიბუციის მექანიზმების დახვეწაზე და საერთაშორისო ნორმების ჩამოყალიბებაზე, რომელიც შეძლებს გამოავლინოს „წითელი ხაზები“ (მაგალითად: სამოქალაქო კრიტიკული ინფრასტრუქტურის მიზნებისაგან დაცვა) და უზრუნველყოს სამართლებრივი საფუძველი პროპორციული და ლეგიტიმური პასუხისთვის. ეს პროცესი უნდა მოიცავდეს როგორც binding, ისე non-binding ინსტრუმენტების კომბინაციას - პირველი უზრუნველყოფს მკაფიო სამართლებრივ შეზღუდვებს და პასუხისმგებლობებს, მეორე კი მოქნილ პლატფორმას დიპლომატიური გადაწყვეტილებებისათვის და ტექნიკური თანამშრომლობისთვის. განხილული იყო ასევე სწრაფი, რეგიონული საერთო მხარდაჭერის მექანიზმების და 24/7 ტექნიკური ჰაბების საჭიროება, რომლებიც დაზარალებულ მხარეში მომენტალურად უზრუნველყოფენ ექსპერტულ და ლოჯისტიკურ დახმარებას.

საზოგადოებრივი და ინფორმაციული მდგრადობა ერთ-ერთი უცვლელი რეკომენდაციაა: დეზინფორმაციისა და პოლიტიკური მანიპულაციის წინააღმდეგ მხოლოდ ტექნიკური საშუალებები არ მუშაობს. სახელმწიფოს დონეზე საჭიროა საზოგადოებრივი კომუნიკაციის გამჭვირვალე პოლიტიკა, მედიასთან შესაბამისი სამუშო პროგრამები, fact-checking ინფრასტრუქტურების გაძლიერება და კრიზისულ სიტუაციებში სწრაფი, ხოლო დამაჯერებელი საჯარო ინფორმაციის მიწოდების მენეჯმენტი. ეს კომპონენტი განსაკუთრებით მნიშვნელოვანია უმნიშვნელო სახელმწიფოებსა და საზოგადოების მაღალი მგრძნობელობის პირობებში, სადაც ინფორმაციის ნაკლებობა ან მცდარი ინფორმაცია ხელს უწყობს პანიკის და პოლიტიკურ დესტაბილიზაციას.

საერთო ჯამში, შედეგები მიუთითებს შემდეგზე: კიბერუსაფრთხოება არის მრავალგანზომილებიანი გამოწვევა, რომელიც მოითხოვს არა მხოლოდ ტექნიკურ, არამედ ინსტიტუციურ, იურიდიულ და საზოგადოებრივ ცვლილებებს. სახელმწიფოს შეუძლია დაიცვას თავისი უსაფრთხოება მხოლოდ მაშინ, როცა კიბერ კრიზისს პასუხობს «მთლიანი საზოგადოების» პრიზმიდან - ადეკვატური ტექნიკური დაცვისგან დაწყებული, სამართლებრივი სტანდარტების დანერგვითა და საერთაშორისო ნორმების ჩამოყალიბებით დასრულებული. ამ მონაპოვრების გარეშე, ასიმეტრიული საფრთხეები გააგრძელებენ გავლენის ზრდას და იქნებიან საფუძველი როგორც სამხედრო, ისე პოლიტიკურ არასტაბილურობათა გაფართოებისა. ამისათვის კი აუცილებელია კოორდინირებული, პრაქტიკული და დროული მოქმედებები. მხოლოდ ასეთი მრავალმხრივი რეფორმა გახდის შესაძლებელს კიბერუსაფრთხოების თანმიმდევრულ და მდგრად განვითარებას თანამედროვე სამხედრო-პოლიტიკურ რეალობაში.

## გამოყენებული ლიტერატურა


1. ზედელაშვილი, თ. 2023. "კიბერშესაძლებლობები და გლობალური უსაფრთხოების ახალი გამოწვევები." https://dspace.nplg.gov.ge/bitstream/1234/482400/1/KibershesadzleblobebiDaGlobaluriUsafrtxoebisAxaliGamowvevebi.pdf?utm.
2. კობა ლიკლიკაძე. 2013. "როგორი წესებით უნდა ვიომოთ კიბერომში?" რადიო თავისუფლება, https://www.radiotavisupleba.ge/a/military-programm/24950058.html.
3. საქართველოს მთავრობა, 2021. „საქართველოს კიბერუსაფრთხოების 2021-2024 წლების ეროვნული სტრატეგია", საქართველო, თბილისი. https://matsne.gov.ge/ka/document/view/5263611?publication=0
4. Almalawi, A., Hassan, S., Fahad, A., Iqbal, A. and Khan, I. A. 2025. "Hybrid Cybersecurity for Asymmetric Threats: Intrusion Detection and SCADA System Protection Innovations." *Symmetry* 17 (4): 616–16. https://doi.org/10.3390/sym17040616.
5. Aos, M., Qolomany, B., Gyorick, K., Abdo, B. J., Aledhari, M., Qadir, J., Carley, K., and Al-Fuqaha, A. 2025. "A Survey of Social Cybersecurity: Techniques for Attack Detection, Evaluations, Challenges, and Future Prospects." *Computers in Human Behavior Reports* 18 (100668): https://doi.org/10.1016/j.chbr.2025.100668.
6. Anna-Maria, O. and Rõigas, H. 2016. "International Cyber Norms Legal, Policy & Industry Perspectives." https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf.
7. Chitadze, N. 2023. "IRMA-International.org: Cyber Security Policies and Strategies of the World's Leading States (9781668488461)(1668488469)(9781668488478): Nika Chitadze: Books." Irma-International.org. https://www.irma-international.org/book/cyber-security-policies-strategies-world/316140/?utm_source=chatgpt.com.
8. Chitadze, N. 2022. "Cyber Warfare – New Threat for National and International Security and Transformation of the Conflicts under the Conditions of the New Geopolitical Order." *Journal of Social Sciences* 7 (2): 70–76. https://doi.org/10.31578/jss.v7i2.120.
9. Eduard, K. 2023. "A Year of Conflict: Cybersecurity Industry Assesses Impact of Russia-Ukraine War." SecurityWeek, https://www.securityweek.com/one-year-of-russia-ukraine-war-cybersecurity-industry-sums-up-impact/.
10. Gesley, J. 2016. "Cyber Warfare: Military Cross-Border Computer Network Operations under International Law. By Johann-Christoph Woltag. Cambridge, Antwerp, Portland: Intersentia Publisher, 314. ISBN: 978-1780682266." *International Journal of Legal Information* 44 (1): 61–62. https://doi.org/10.1017/jli.2016.9.
11. James, K., Ahmad, A., and Scheepers, R. 2022. "Adopting and Integrating Cyber-Threat Intelligence in a Commercial Organisation." *European Journal of Information Systems* 32 (1): 1–17. https://doi.org/10.1080/0960085x.2022.2088414.

12. Lomidze, N. 2022. "Cyber Security Challenges in Georgia". *Georgian Scientists* 4 (3):120-33. https://doi.org/10.52340/gs.2022.04.03.15.
13. Laura S, T., O Sami, S. and Farrell, D. 2024. "Cyberwar Strategy and Tactics: An Analysis of Cyber Goals, Strategies, Tactics, and Techniques." ArXiv.org. 2024. https://arxiv.org/abs/2406.00496.
14. Lex, C. 2024. "Technical Deep Dive: Understanding the Anatomy of a Cyber Intrusion | MITRE-Engenuity." Medium. MITRE-Engenuity. https://medium.com/mitre-engenuity/technical-deep-dive-understanding-the-anatomy-of-a-cyber-intrusion-080bddc679f3.
15. Mostofa, A., Nygard, E. K., Gomes, R., Chowdhury, M. M., Rifat, N. and Connolly, F J. 2022. "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—a Review." *Journal of Cybersecurity and Privacy* 2 (3): 527–55. https://doi.org/10.3390/jcp2030027.
16. Mikael, W., Nilsson, N., Palmertz, B., and Thunholm, P. 2021. Hybrid Warfare: Security and Asymmetric Conflict in International Relations. London: I.B. Tauris,. http://dx.doi.org/10.5040/9781788317795.
17. NATO. 2016. "Cyber Defence Pledge." NATO. https://www.nato.int/cps/en/natohq/official_texts_133177.htm?utm.
18. NATO. 2021. "North Atlantic Treaty Organization Www.nato.int/Factsheets Factsheet NATO Cyber Defence." https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.
19. Shekeladze, A. 2022. "GEORGIAN EXPERIENCE of DEVELOPING CYBER CAPABILITIES in the DEFENCE FIELD." https://jodrm.eu/wp-content/uploads/2025/04/02-Shekeladze.pdf?utm_source=chatgpt.com.
20. Sevis K. N. and Seker, E. 2016. "Cyber warfare: terms, issues, laws and controversies," 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security), London, UK, doi: 10.1109/CyberSecPODS.2016.7502348
21. Vicens, AJ. 2022. "Ukraine Warns of 'Massive Cyberattacks' Coming from Russia on Critical Infrastructure Sites." CyberScoop. September 26, 2022. https://cyberscoop.com/ukrainians-warn-of-massive-cyberattacks/.
22. Weissmann, M., Nilsson, N., 2024. "Russian Warfare and Influence." *Bloomsburycollections.com* 1 (978-1-3503-3524-0). https://doi.org/b-9781350335257.
23. Woltag, J. C. 2014. *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law*. of *International Law*. Intersentia.
24. Yuan, T. L. 2024. "Asymmetry in the Digital Age: Cyber Deterrence Strategies for Small States." *Journal of Strategic Security* 17 (4): 71–88. https://doi.org/10.5038/1944-0472.17.4.2268.
25. Zeeshan, F. 2025. "Cyber Warfare and International Security: A New Geopolitical Frontier." *The Critical Review of Social Sciences Studies* 3 (2): 513–27. https://doi.org/10.59075/k9cbhz04.