ინფორმაციული ომები და საქართველოს კიბერსივრცე

პეტრი კუპრაშვილი

საქართველოს ტექნიკური უნივერსიტეტი

ჰენრი კუპრაშვილი

ინფორმაციული ომები და საერთაშორისო კიბერსივრცე

დამტკიცებულია სახელმძღვანელოდ
საქართველოს ტექნიკური
უნივერსიტეტის სარედაქციო-
საგამომცემლო საბჭოს
მიერ. 26.03.2026, ოქმი №1

თბილისი
2026

უაკ 3; 004; 327; 351.746

ნაშრომში განხილულია ინფორმაციული ომებისა და კიბერსივრცის როლი თანამედროვე საერთაშორისო ურთიერთობებში. მასში გაანალიზებულია ომის ევოლუცია ოთხი თაობის ჭრილში, ინფორმაციული რევოლუციის გავლენა სახელმწიფო ინსტიტუტებზე და „რბილი ძალის“ მნიშვნელობა. განსაკუთრებული ყურადღება ეთმობა კიბერუშიშროების სტრატეგიებს, კრიტიკული ინფრასტრუქ-ტურის დაცვასა და საქართველოს ეროვნულ ინტერესებს ციფრულ ეპოქაში.

განკუთვნილია პოლიტიკის მეცნიერებების, საერთაშორისო ურთიერთობებისა და სამართლის სპეციალობის სტუდენტებისთვის, აგრეთვე პრაქტიკოსი პოლიტიკოსებისა და ეროვნული უშიშროების საკითხებით დაინტერესებული პირებისთვის.

Henri Kuprashvili

INFORMATION WARS AND INTERNATIONAL CYBERSPACE

The paper explores the role of information warfare and cyberspace in modern international relations. It analyzes the evolution of warfare thro-ugh the lens of four generations, the impact of the information revolu-tion on state institutions, and the significance of 'soft power.' Special emphasis is placed on cybersecurity strategies, the protection of critical infrastructure, and Georgia's national interests in the digital age. This work is intended for students of political science, international relations, and law, as well as those interested in national security issues.

სამეცნიერო რედაქტორი პოლიტიკის მეცნიერებათა დოქტორი,
პროფესორი **ვახტანგ მაისაია**

რეცენზენტები: საქართველოს ტექნიკური უნივერსიტეტის
ინფორმატიკისა და მართვის სისტემების
ფაკულტეტის ასისტენტ-პროფესორი **ლუკა შონია,**

კავკასიის უნივერსიტეტის აფილირებული
პროფესორი, „სამეცნიერო კიბერუსაფრთხოების
ასოციაციის“ ვიცე-პრეზიდენტი, საჯარო
მმართველობის დოქტორი **ვლადიმერ სვანაძე**

ISBN 978-9941-528-12-5

http://www.gtu.ge

სარჩევი

რედაქტორის წინასიტყვაობა

თანამედროვე სამყაროში ტექნოლოგიური პროგრესი აღარ არის მხოლოდ განვითარების ინსტრუმენტი, იგი გეოპოლიტიკური დაპირისპირების მთავარ არენად გადაიქცა. ჰენრი კუპრაშვილის ეს ნაშრომი დროული და სიღრმისეული კვლევაა იმისა, თუ როგორ შეცვალა ინფორმაციულმა ნაკადებმა ომის წარმოების ტრადიციული გაგება. უნდა აღინიშნოს, რომ ჯერ კიდევ 24 წლის წინ საქართველოდან ავტორს პირველს მოუწია ამ პრობლემასთან შეხება და მოხსენებით გამოსვლა მიუნხენში, ჯ. მარშალის უშიშროებისა და საერთაშორისო ურთიერთობების შემსწავლელი ევროპული ცენტრის სემინარზე „კიბერგანზომილება, როგორც ეროვნული უშიშროებისათვის მუქარების ჩანასახი“ (2-5.12.2002).

ავტორი კვალიფიციურად აკავშირებს თეორიულ ასპექტებს პრაქტიკულ გამოწვევებთან — დაწყებული ქსელური ომებიდან, დამთავრებული კიბერტერორიზმის საფრთხეებით. წიგნი არა მხოლოდ აკადემიური სახელმძღვანელოა, არამედ სტრატეგიული გზამკვლევი მათთვის, ვისაც სურს გაიგოს 21-ე საუკუნის კონფლიქტების ბუნება. რედაქტორის სახით, მჯერა, რომ ეს ნაშრომი მნიშვნელოვან წვლილს შეიტანს ქართული სამხედრო-პოლიტიკური აზროვნების განვითარებაში.

ვახტანგ მაისაია

პოლიტიკის მეცნიერებათა დოქტორი, პროფესორი კავკასიის საერთაშორისო უნივერსიტეტის საერთაშორისო ურთიერთობებისა და საერთაშორისო უშიშროების სამაგისტრო პროგრამის ხელმძღვანელი, გლობალური პოლიტიკისა და უშიშროების კვლევების ინგლისურენოვანი სამაგისტრო პროგრამის ხელმძღვანელი, საქართველოს ეროვნული მეცნიერებათა აკადემიის ექსპერტი სამეცნიერო-აკადემიურ საკითხებში, პოლონეთის რესპუბლიკის პოლიტიკური მეცნიერებების ასოციაციის წევრი, ვარშავის უნივერსიტეტის პროფესორი

რ ე ც ე ნ ზ ი ა

ნაშრომი წარმოადგენს აქტუალურ და სიღრმისეულ კვლევას თანამედროვე გეოპოლიტიკის ერთ-ერთ ყველაზე დინამიკურ სფეროში. პროფ. ჰ. კუპრაშვილი წარმატებით ახერხებს ტრადიციული კონფლიქტების თეორიისა და ციფრული ტექნოლოგიების სინთეზს, რაც დღევანდელი საქართველოს ეროვნული უშიშროების გარემოს გათვალისწინებით უაღრესად მნიშვნელოვანია.

ნაშრომის ძირითადი ღირებულებებად შეიძლება ჩაითვალოს:

- **მრავალშრიანი ანალიზი**: ნაშრომში კარგად არის გამიჯნული ინფორმაციული ომის ორი ძირითადი ასპექტი: ტექნიკური (ინფრასტრუქტურაზე თავდასხმა) და ფსიქოლოგიური (საზოგადოებრივი აზრით მანიპულირება);
- **საერთაშორისო სამართლებრივი ასპექტები**: განსაკუთრებით აღსანიშნავია თავი, სადაც განხილულია „ტალინის სახელმძღვანელოს“ (Tallinn Manual) პრინციპები და კიბერსივრცეში საერთაშორისო ჰუმანიტარული სამართლის გამოყენების სირთულეები;
- **ატრიბუციის პრობლემატიკა**: ავტორი სწორად სვამს აქცენტს ატრიბუციის (თავდამსხმელის ვინაობის დადგენის) სირთულეზე, რაც კიბერომებს „ჰიბრიდული ომის“ ყველაზე ეფექტურ იარაღად აქცევს.

ასევე საინტერესოა ნაშრომის სტრუქტურული და შინაარსობრივი მხარე, კერძოდ:

- ნაშრომი ლოგიკურად არის აგებული. ავტორი მიმოიხილავს კიბერსივრცის, როგორც მეხუთე საბრძოლო დომენის (სახმელეთო, საზღვაო, საჰაერო და კოსმოსურ დომენებთან ერთად) ჩამოყალიბების პროცესს;
- გამოყენებული წყაროების მრავალფეროვნება მოწმობს ავტორის მაღალ აკადემიურ მომზადებასა და თემისადმი კომპლექსურ მიდგომას. ნაშრომში განხილული ქეისები (Case Studies) რეალური მაგალითების საფუძველზე აჩვენებს, თუ როგორ შეუძლია კიბერშეტევას მოახდინოს კრიტიკული ინფრასტრუქტურის პარალიზება და გავლენა იქონიოს პოლიტიკურ პროცესებზე.

ნაშრომი სრულად აკმაყოფილებს სამეცნიერო ნაშრომისადმი წაყენებულ მოთხოვნებს და უდავოდ იმსახურებს მაღალ შეფასებას. მასში წარმოდგენილი დასკვნები და რეკომენდაციები, რომლებიც ეხება ეროვნული კიბერმდგრადობის (Cyber Resilience) გაძლიერებას, პრაქტიკული ღირებულების მატარებელია.

ვლადიმერ სვანაძე

საჯარო მმართველობის დოქტორი, კავკასიის უნივერსიტეტის აფილირებული პროფესორი, „სამეცნიერო კიბერუსაფრთხოების ასოციაციის“ ვიცე - პრეზიდენტი

რ ე ც ე ნ ზ ი ა

პროფესორ ჰენრი კუპრაშვილის ნაშრომი წარმოადგენს კომპლექსურ კვლევას, რომელიც ეხება თანამედროვეობის ერთ-ერთ ყველაზე აქტუალურ და დინამიკურ სფეროს — ინფორმაციულ და კიბერუშიშროებას. ნაშრომის სამეცნიერო სიახლე მდგომარეობს იმაში, რომ ავტორი ახდენს ინფორმაციული ომების ევოლუციის სისტემატიზაციას და მას განიხილავს არა მხოლოდ ტექნოლოგიურ, არამედ პოლიტიკურ, სამხედრო და ფსიქოლოგიურ ჭრილში.

რეცენზირებულ ნაშრომში ავტორი წარმატებით ახდენს **„ომის ოთხი თაობის“** კონცეფციის ადაპტირებას თანამედროვე რეალობასთან. განსაკუთრებით აღსანიშნავია თავები, რომლებიც ეხება **„ქსელურ ომებს“ (Netwar)** და **„რბილი ძალის“ (Soft Power)** როლს საერთაშორისო პოლიტიკაში. ავტორი არ შემოიფარგლება მხოლოდ თეორიული მსჯელობით და გვთავაზობს პრაქტიკულ რეკომენდაციებს საქართველოს ეროვნული უშიშროების სტრატეგიის გაძლიერების მიმართულებით.

ნაშრომი დაწერილია მაღალი აკადემიური სტანდარტების დაცვით, გამოყენებულია უახლესი სამეცნიერო ლიტერატურა და წყაროები. ტექსტი ლოგიკურად არის სტრუქტურირებული, რაც მკითხველს საშუალებას აძლევს ეტაპობრივად გაიაზროს გადასვლა ტრადიციული სახელმწიფო ინსტიტუტებიდან ციფრული ეპოქის მმართველობის ფორმებზე. ეს წიგნი ქმნის სრულყოფილ მეთოდურ ჩარჩოს კიბერუშიშროებისა და ინფორმაციული ომების კურსისთვის.

მეთოდური და პრაქტიკული ღირებულება: ცალკე აღნიშვნის ღირსია ნაშრომის სასწავლო-მეთოდური სტრუქტურა: **თითოეულ თავს ერთვის დასკვნა და საკონტროლო კითხვები**, ასევე კონკრეტულად მოცემული თავის **მეთოდური ასპექტი**. ნაშრომს ერთვის მნიშვნელოვანი **დანართი**, რომელიც მოიცავს **პრაქტიკულ სავარჯიშოებსა და „ქეის-სტადებს“ (Case Study)** ცამეტივე თავის მიხედვით, რაც კრიტიკულად მნიშვნელოვანია მასალის პრაქტიკული ათვისებისთვის.

მივიჩნევ, რომ წარმოდგენილი ნაშრომი სრულად პასუხობს სამეცნიერო-სახელმძღვანელო ლიტერატურისადმი წაყენებულ მოთხოვნებს და მისი გამოცემა მნიშვნელოვანი შენაძენი იქნება როგორც სტუდენტებისა და აკადემიური წრეებისთვის, ისე პრაქტიკოსი პოლიტიკოსებისა და ეროვნული უშიშროების სპეციალისტებისათვის.

ლუკა შონია

ინფორმატიკის დოქტორი, საქართველოს ტექნიკური უნივერსიტეტის ასისტენტ-პროფესორი

შესავალი

21-ე საუკუნე კაცობრიობის ისტორიაში შევიდა, როგორც ფუნდამენტური საინფორმაციო-ტექნოლოგიური ტრანსფორმაციის ეპოქა. ინფორმაციულმა რევოლუციამ არა მხოლოდ შეცვალა ჩვენი ყოველდღიურობა, არამედ რადიკალურად გარდაქმნა საერთაშორისო ურთიერთობების არქიტექტურა და ომის წარმოების ტრადიციული გაგება. დღეს სახელმწიფოთა შორის დაპირისპირების ხაზი აღარ გადის მხოლოდ ფიზიკურ საზღვრებზე; მან გადაინაცვლა უხილავ, მაგრამ ყოვლისმომცველ სივრცეში — **კიბერსივრცეში**.

მოცემული წიგნი, **„ინფორმაციული ომები და საერთაშორისო კიბერსივრცე“** მიზნად ისახავს მკითხველს გააცნოს ის რთული და მრავალშრიანი პროცესები, რომლებიც თანამედროვე გლობალურ უშიშროებას განსაზღვრავს.

ნაშრომში განხილულია ომის ევოლუცია პირველი თაობიდან დღევანდელ, მეოთხე თაობამდე, სადაც მთავარი იარაღი არა ტყვია და ჭურვი, არამედ ინფორმაცია და ფსიქოლოგიური ზემოქმედებაა.

წიგნის აქტუალობას რამდენიმე ფაქტორი განაპირობებს:

1. **სუვერენიტეტის სრულიად ახალი განზომილება:** სახელმწიფო როგორ ინარჩუნებს კონტროლს მაშინ, როდესაც ქსელური სტრუქტურები ტრადიციულ იერარქიულ მმართველობას ანაცვლებს?
2. **ე. წ. „რბილი ძალის“ პრიორიტეტულობა:** რატომ გახდა ინფორმაციული, კულტურული და

იდეოლოგიური გავლენა უფრო ეფექტური, ვიდრე პირდაპირი სამხედრო აგრესია?

3. **კიბერუშიშროების უზრუნველყოფა, როგორც ეროვნული ინტერესი:** კრიტიკული ინფრასტრუქტურის დაცვა და კიბერტერორიზმთან ბრძოლა დღეს მსოფლიოში ნებისმიერი სახელმწიფოს, მათ შორის საქართველოს ეროვნული უშიშროების უზრუნველყოფის ქვაკუთხედია.

წიგნში დეტალურადაა გაანალიზებული საქართველოს ეროვნული სტრატეგია და საერთაშორისო პარტნიორების (NATO, EU) როლი კოლექტიური თავდაცვის ჩამოყალიბებაში. ავტორი ცდილობს პასუხი გასცეს კითხვას: როგორ უნდა უზრუნველყოს სახელმწიფომ მედეგობა ჰიბრიდული საფრთხეების პირობებში?

ეს წიგნი განკუთვნილია სტუდენტებისთვის, რომლებიც ეუფლებიან პოლიტიკურ მეცნიერებებს, საერთაშორისო ურთიერთობებსა და სამართალს, უშიშროების სფეროს ექსპერტებისთვის და ყველასთვის, ვისაც სურს გაერკვეს თანამედროვე მსოფლიოს „ციფრულ ანატომიაში“. ინფორმაცია დღეს ძალაა, ხოლო მისი ფლობა და დაცვა — გადარჩენის გარანტი.

თავი I
გარდამავალი პერიოდი სახელმწიფო და სამხედრო ინსტიტუციებში

1.1. ქსელების მსოფლიო: ინტერნეტის გენეზისი და სამხედრო ფესვები

თანამედროვე ეპოქის დასაწყისის ყველაზე თვალსაჩინო თარიღად, სიმბოლურად, 1985 წლის 15 მარტი შეიძლება მივიჩნიოთ, როდესაც მსოფლიო ისტორიაში პირველი ინტერნეტ-დომენი (symbolics.com) დარეგისტრირდა. თუმცა, ამ მოვლენას წინ უძღოდა აშშ-ში მიმდინარე საიდუმლო სამხედრო კვლევები, რომლებმაც საფუძველი ჩაუყარა ინფორმაციული ომების თანამედროვე არენას — ინტერნეტს.

ინტერნეტის იდეა დაიბადა აშშ-ის თავდაცვის უწყებაში 1950-იანი წლების ბოლოს. ცივი ომის პერიოდში, მას შემდეგ, რაც საბჭოთა კავშირმა 1957 წელს პირველი ხელოვნური თანამგზავრი გაუშვა, ამერიკელი სტრატეგები მიხვდნენ, რომ ბირთვული ომის პირობებში ქვეყანას ინფორმაციის გადაცემის რადიკალურად განსხვავებული სისტემა სჭირდებოდა. ტრადიციული იერარქიული ქსელების მთავარი ნაკლი მათი ცენტრალიზებულობა იყო — ერთი მართვის ცენტრის განადგურება მთელი სისტემის პარალიზებას იწვევდა.

ამ გამოწვევის საპასუხოდ შეიქმნა მოწინავე პროექტების კვლევის სააგენტო **ARPA** (Advanced Research Projects Agency). ARPA-ს მიზანი იყო შეექმნა დეცენტრალიზებული ქსელი, რომელსაც არ ექნებოდა ერთიანი მართვის ცენტრი და მისი რომელიმე სეგმენტის

გათიშვა არ შეაფერხებდა მთლიანი ქსელის მუშაობას. ამ კონცეფციას ეწოდა **ARPANET**. 1969 წლის 29 ოქტომბერს მოხდა ისტორიული ფაქტი: კალიფორნიის უნივერსიტეტსა და სტენფორდის კვლევით ინსტიტუტს შორის დამყარდა პირველი კავშირი, როდესაც **ჩარლი კლაინმა** (Charley Kline)[1] 640 კილომეტრით დაშორებულ კომპიუტერზე სიტყვა „LOGIN“ გაუგზავნა **ბილ დიუვალს** (Bill Duvall)[2].

ინტერნეტის განვითარების შემდგომი ეტაპები ელვისებურად წარიმართა:

- **1972 წელი:** ელექტრონული ფოსტის გამოგონება.
- **1989 წელი: თიმ ბერნერს-ლი**ს (Tim Berners-Lee) მიერ მსოფლიო ქსელის (**WWW**) იდეის შემოთავაზება, HTTP სისტემისა და HTML ენის შემუშავება.
- **1991 წელი:** პროექტ World-Wide Web-ის რეალიზაცია, რამაც ინტერნეტი საყოველთაო და ხელმისაწვდომი გახადა.

დღეს მსოფლიო ქსელების „აბლაბუდაში“ მოექცა, რომლებიც არა მხოლოდ ადამიანის ნებისგან დამოუკიდებელ თვითგანვითარებად სისტემებად იქცა, არამედ ფუნდამენტურად შეცვალა ეროვნული და საერთაშორისო უშიშროების პარადიგმა.

1.2. სახელმწიფო და არმია ქსელების სამეფოში: იერარქიიდან ჰორიზონტალურ მართვამდე

[1]Computer Hope. (2017). Charley Kline. http://www.computerhope.com/people/charley_kline.htm [25.12.2025]
[2] Computer Hope. (2025). Bill Duvall. https://www.computerhope.com/people/bill_duvall.htm [25.12.2025]

ინფორმაციული რევოლუცია, რომელიც კომპიუტერიზაციამ და საკომუნიკაციო ტექნოლოგიების პროგრესმა გამოიწვია, გარდამავალი პერიოდის საწყისად იქცა სახელმწიფო და სამხედრო ინსტიტუციებისთვის. ინფორმაცია გადაიქცა სტრატეგიულ რესურსად, რომელიც პოსტინდუსტრიულ ეპოქაში უფრო ფასეულია, ვიდრე ქვანახშირი, ფოლადი ან კაპიტალი და სამუშაო ძალა იყო ინდუსტრიულ ხანაში.

ამ პროცესმა მნიშვნელოვნად შეასუსტა გაბატონებული ტრადიციული იერარქიული სტრუქტურების როლი. ინფორმაციის „სიუხვეში“ გადასვლამ ინდივიდებსა და მცირე ჯგუფებს შესაძლებლობა მისცა, გვერდი აუარონ ცენტრალიზებულ სახელმწიფოებრივ იერარქიებს. ინფორმაციის დამუშავებისას ქსელური ორგანიზაციული ფორმები ბევრად უფრო ეფექტური აღმოჩნდა, ვიდრე ხისტი ვერტიკალური სტრუქტურები.

ამ კონტექსტში შეიარაღებული ძალები ყველაზე რთული გამოწვევისა და პრობლემების წინაშე აღმოჩნდა. მათი ბუნება მთლიანად იერარქიულობაზეა აგებული, თუმცა თანამედროვე ომის დინამიკა მოითხოვს ქსელურობას. ამერიკელი პოლიტოლოგის, ეკონომიკური ომების ექსპერტის, იელის მენეჯმენტის უმაღლესი სკოლის პროფესორის, **პოლ ბრაკენისა** (Paul Bracken) და ავსტრო-ამერიკელი მკვლევრის, მენეჯმენტის თეორეტიკოსის, **პიტერ დრუკერის** (Peter Drucker) კვლევები ადასტურებს, რომ წარმატება თანამედროვე, ახალ ინფორმაციულ ეპოქაში აუცილებლად მოითხოვს სახელმწიფოსა და არმიის ძირეულ ტრანსფორმაციას:

1. **ორგანიზაციული ადაპტაცია:** ტექნოლოგიური უპირატესობა არაფერია ორგანიზაციული უპირატესობის გარეშე;
2. **დეცენტრალიზაცია:** გადაწყვეტილების მიღების პროცესი უნდა დაუახლოვდეს მოქმედების ადგილს;
3. **პარტნიორობა:** სახელმწიფომ უნდა ისწავლოს მოქმედება არასახელმწიფო აქტორებთან (კერძო სექტორი, ჰაკერული დაჯგუფებები, სამოქალაქო ქსელები) კოორდინაციაში.

ნაციონალური სახელმწიფოები კარგავს „ოპერაციულ სუვერენიტეტს“ — კვლავ აქვს ფორმალური კონტროლი ტერიტორიაზე, მაგრამ სულ უფრო უჭირს იმ ინფორმაციული ნაკადების გაკონტროლება, რომლებიც ამ ტერიტორიაზე გაედინება.

1.3. ინფორმაცია და ტერმინების დიალექტიკა: ობიექტურიდან სუბიექტურ აღქმამდე

სამყარო ურთიერთდაკავშირებული სისტემების ერთობლიობაა, ხოლო ამ სისტემების მდგომარეობათა სიმრავლე არის **თავისთავადი (ობიექტური) ინფორმაცია**. იგი არსებობს ადამიანის ცნობიერებისგან დამოუკიდებლად.

თუმცა, საინფორმაციო ომების კონტექსტში ჩვენთვის პრიორიტეტულია **მეორეული (ადამიანური) ინფორმაცია**. ეს არის რეალობის ის შინაარსი, რომელიც აღიქმება ადამიანის ან სპეციალური მოწყობილობის მიერ. ადამიანის ფიზიოლოგიური შესაძლებლობები შეზღუდულია — ჩვენ რეალობას მხოლოდ გარკვეულ სპექტრში აღვიქვამთ (მაგალითად, მხედველობის

შეზღუდულობა). სწორედ ამ შეზღუდულ აღქმაზე — სუბიექტურ ცნობიერებაზე ხდება ზემოქმედება ინფორმაციული ომის დროს.[3]

ინფორმაციის თვისებები, რომლებიც მას იარაღად აქცევს, ოთხია:

1. **რესურსებისადმი მცირე მოთხოვნილება:** კიბერშეტევას არ სჭირდება ქარხნები და მძლავრი ინდუსტრია.
2. **ტრანსპორტირების სიმარტივე:** ბიტები მყისიერად გადაადგილდება.
3. **შეღწევადობა:** ინფორმაციულ ნაკადებს ვერ აჩერებს ფიზიკური კედლები.
4. **გაზიარების აუცილებლობა:** ინფორმაცია მრავლდება გაზიარებისას, რაც მას „ვირუსულს“ ხდის.

1.4. ინფორმაციული რევოლუციის სტადიები და გლობალური ანატომია

ინფორმაციულ რევოლუციაში გამოიყოფა სამი ძირითადი სტადია:

I სტადია (1837–1963): ტელეგრაფისა და რადიოს ეპოქა.

II სტადია (1964–1985): კომპიუტერიზაციის დასაწყისი (IBM 360).

[3] Kuprashvili, H. (2002). Aspects of Georgia's Information Policy. Report at the Conference: Cyberspace of emerging threats to national security. The George C. Marshall European Center for Security Studies. 02-05.12.2002 Munich, Germany

III სტადია (1985-დღემდე): ინტერნეტიზაცია და ციფრული ეკონომიკის დაბადება.

ამ პროცესმა წარმოშვა „ვირტუალური რეალობა“, სადაც პოლიტიკა, რელიგია და ომი გადაჯაჭვულია. ინფორმაციულ ეპოქაში ქვეყნის გავლენა მსოფლიოზე დამოკიდებულია არა მხოლოდ მის შეიარაღებაზე, არამედ საინფორმაციო ინფრასტრუქტურაზე. ძლიერ სახელმწიფოებს შეუძლია სხვა ქვეყნების ინტელექტუალური პოტენციალის ექსპლუატაცია და მათი სულიერ-ზნეობრივი საფუძვლების შერყევა ინფორმაციული ექსპანსიით.

პირველი თავის დასკვნა

დღეს ბევრი საუბრობს „პოსტადამიანურ საზოგადოებაზე“, სადაც ადამიანური აზრი უშუალო საწარმოო ძალაა. ინფორმაციული რევოლუცია ცვლის იმას, თუ როგორ ვცხოვრობთ, ვმუშაობთ და ვკვდებით. სახელმწიფო, რომლიც ეძებს სტრატეგიულ უპირატესობას, უნდა გააცნობიეროს: ძალისა და ინფორმაციის ბუნება იცვლება ელვისებურად. წარმატებას მიაღწევს მხოლოდ ის, ვინც შეძლებს იერარქიული სიხისტის ჩანაცვლებას ქსელური მოქნილობით და ინფორმაციის, როგორც სტრატეგიული რესურსის, ეფექტურ მართვას.

პირველი თავის საკონტროლო კითხვები:

1. *როგორ შეცვალა ქსელურმა სტრუქტურებმა ტრადიციული იერარქიული მმართველობა?*
2. *რა განსხვავებაა მონაცემებსა და სტრატეგიულ ინფორმაციას შორის?*

მეთოდური ასპექტი:

ამ თავის შესწავლის შემდეგ სტუდენტმა უნდა გააცნობიეროს, რომ ინფორმაციული ომი არ არის მხოლოდ ტექნიკური პრობლემა, არამედ ცივილიზაციური ცვლილებაა, რომელიც მოითხოვს სახელმწიფო და სამხედრო ინსტიტუციების ფუნდამენტურ რესტრუქტურიზაციას.

თავი II
კაცობრიობა განვითარების ახალ ეტაპზე: ინფორმაციული ეპოქის ანატომია და სტრატეგიული რესურსი

2.1. ახალი ეპოქის წანამძღვრები და საკომუნიკაციო რევოლუციები

კაცობრიობის ისტორია შეიძლება განვიხილოთ, როგორც ინფორმაციის გადაცემისა და შენახვის მეთოდების მუდმივი სრულყოფის პროცესი. თანამედროვე ინფორმაციულ ეპოქაში გადასვლა არ ყოფილა მოულოდნელი; მას წინ უძღოდა ე.წ. „საკომუნიკაციო-ინფორმაციული რევოლუციები“, რომლებმაც ფუნდამენტურად შეცვალა ადამიანთა შორის ურთიერთობის მასშტაბები:

პირველი რევოლუცია: ბორბლის გამოგონება. მან საფუძველი ჩაუყარა ტრანსპორტს და გააფართოვა ფიზიკური კომუნიკაციის არეალი.

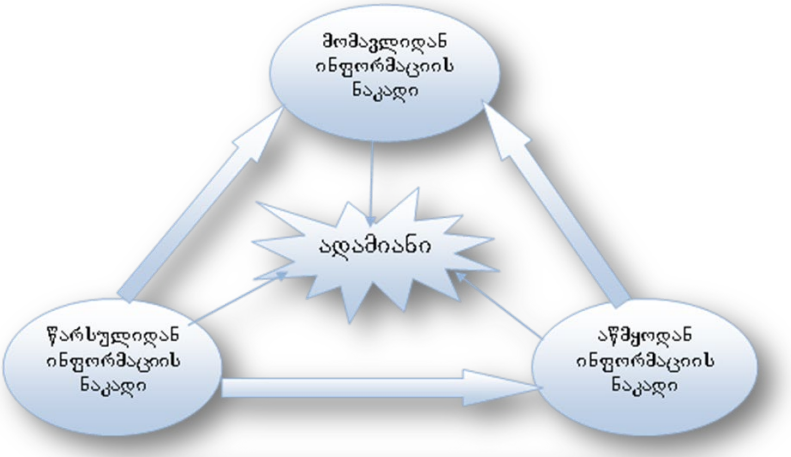
მეორე რევოლუცია: ანბანისა და დამწერლობის გაჩენა. ამან შესაძლებელი გახადა ინფორმაციის ფიქსაცია და დროში შენახვა.

მესამე რევოლუცია: სტამბის გამოგონება და წიგნების ბეჭდვის შემოღება. ინფორმაცია გახდა მასობრივი და ხელმისაწვდომი ფართო ფენებისთვის.

მეოთხე რევოლუცია: ელექტრობის, ტელეგრაფის, ტელეფონის, რადიოსა და ტელევიზიის ეპოქა. კომუნიკაცია გახდა მყისი.

მეოცე საუკუნის მეორე ნახევრიდან კი იწყება თვისებრივად ახალი ეტაპი — ინფორმატიკის მეცნიერების

დაბადება. 1970-იან წლებში გამომთვლელი მანქანების, ხოლო 90-იან წლებში პერსონალური კომპიუტერებისა და ინტერნეტის ფართო დანერგვამ საფუძველი ჩაუყარა **საინფორმაციო საზოგადოებას**. ამ ახალ რეალობაში კეთილდღეობის მთავარი პირობა გახდა არა მატერიალური დოვლათი, არამედ **ინფორმაცია**.

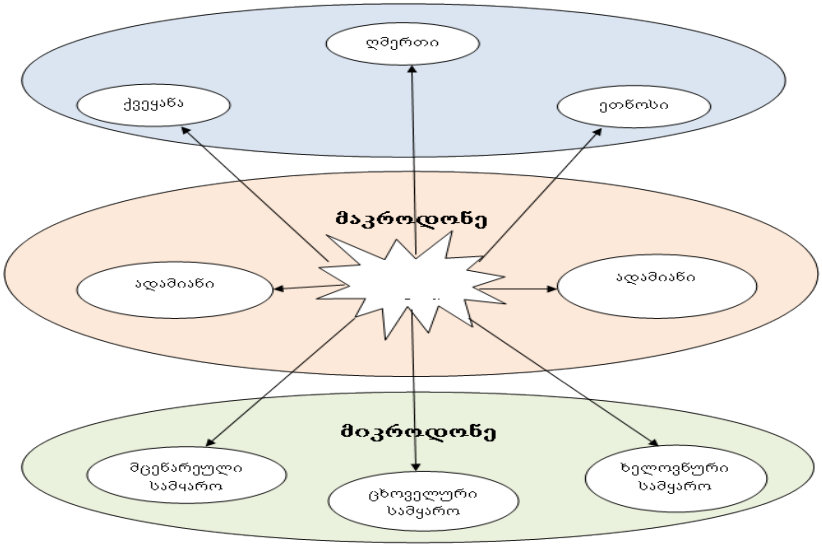


წახ. 2. წარსულის, აწმყოსა და მომავლის ურთიერთკავშირი და მათი ინფორმაციული ზემოქმედებიდ სივრცე

2.2. ინფორმაცია, როგორც სამყაროს სისტემური დომინანტი

ინფორმაცია, როგორც **სამეცნიერო ტერმინი** (Information), კიბერნეტიკის განვითარებასთან ერთად შემოვიდა XX საუკუნის მეორე ნახევრიდან. მიუხედავად მისი პოპულარობისა, იგი კვლავ რჩება მეცნიერების ერთ-ერთ ყველაზე რთულ და მრავალწახნაგოვან ცნებად.

სამყაროს სისტემური ხედვა გვეუბნება, რომ ყველაფერი — სუბატომური ნაწილაკიდან მეტასამყარომდე —



ნახ. 2. ადამიანის პასუხისმგებლობის დონეების იერარქია და მათი ინფორმაციული ზემოქმედებიდ სივრცე

ურთიერთდაკავშირებული ქვესისტემების ერთობლიობაა. ამ სისტემების მდგომარეობათა სიმრავლე თავისთავად ინფორმაციას წარმოადგენს. აქ უნდა გავმიჯნოთ ინფორმაციის ორი დონე:

- **თავისთავადი (ობიექტური) ინფორმაცია:** არსებობს ადამიანის ნებისა და ცნობიერებისგან დამოუკიდებლად. ეს არის მატერიის საერთო თვისება. **ნორბერტ ვინერი** მიიჩნევდა, რომ ამ ტიპის „ნამდვილი“ ინფორმაციის გაზომვა პრაქტიკულად შეუძლებელია.
- **მეორეული (ადამიანური) ინფორმაცია:** ეს არის მატერიალური სამყაროს ობიექტების აზრობრივი შინაარსი, რომელიც ფორმირებულია ადამიანის სუბიექტური ცნობიერებით.

ადამიანი, როგორც სისტემის მცირე ნაწილაკი, გარე სამყაროს საკუთარი „ნაჭუჭიდან“, ამ „ნაჭუჭის“ თვალსაწიერიდან, მხოლოდ „შიგნიდან“ აკვირდება ანუ „სადამდეც ხელი მიუწვდება“, ამიტომ ჩვენი ცოდნა მუდამ სუბიექტური და არასრულყოფილია. აბსოლუტური ინფორმაცია მხოლოდ „აბსოლუტური დამკვირვებლისთვის“ არის ხელმისაწვდომი.

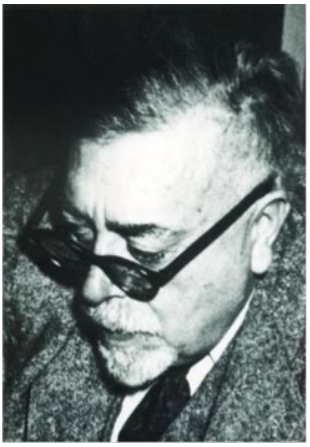
2.3. ინფორმაციის თვისებები და კლასიფიკაცია საზოგადოებაში

საზოგადოებაში ინფორმაცია ცირკულირებს არა მხოლოდ როგორც მონაცემები, არამედ როგორც სოციალურ-საზოგადოებრივი ურთიერთობების ანაბეჭდი. მისი კლასიფიკაცია რამდენიმე კრიტერიუმით ხდება:

1. **დანიშნულების მიხედვით:** პოლიტიკური, ეკონომიკური, სოციალური, ტექნიკური, იდეოლოგიური.
2. **დროითი ფაქტორის მიხედვით:** ინფორმაცია წარსულის, აწმყოსა და მომავლის (პროგნოზული) შესახებ.
3. **აღქმის ფორმით:** ვიზუალური, აუდიალური, ტაქტილური, გემოვნებითი და სურნელებითი.

ნორბერტ ვინერი

(Norbert Wiener; 1894-1964) ამერიკელი მათემატიკოსი. ფუნდამენტურ ნაშრომში "კიბერნეტიკა" მოგვცა ახალი მეცნიერების, კიბერნეტიკის ძირითადი ამოცანების ფორმულირება.



"ინფორმაცია, ინფორმაციაა და არა მატერია ან ენერგია"

"წამდვილი ინფორმაციის გაზომვა შეუძლებელია"

განსაკუთრებით მნიშვნელოვანია ინფორმაციის **ხარისხობრივი პარამეტრები**, რომლებიც განსაზღვრავს მის სტრატეგიულ ფასს:

- **ობიექტურობა და უტყუარობა:** რამდენად ზუსტად ასახავს ინფორმაცია რეალობას.
- **რელევანტურობა და აქტუალურობა:** რამდენად პასუხობს იგი დღევანდელ მოთხოვნებს.
- **სისრულე და ხელმისაწვდომობა:** არის თუ არა ინფორმაცია საკმარისი გადაწყვეტილების მისაღებად.
- **დაცულობა:** ინფორმაციის მდგრადობა არასანქცირებული ცვლილებების მიმართ.

2.4. ინფორმაციული რევოლუციის სტადიები და პერსონალიები

თანამედროვე ინფორმაციულ რევოლუციაში პირო-

ამერიკელი ინჟინერი და მათემატიკოსი, ინფორმაციის თეორიის ფუძემდებელი კლოდ შენონი (**Claude Elwood Shannon**, 1916-2001);

პოსტინდუსტრიული (ინფორმაციული) საზოგადოების თეორიის ფუძემდებელი, ამერიკელი სოციოლოგი და პუბლიცისტი დენიელ ბელი (**Daniel Bell**; 1919—2011);

ბითად გამოიყოფა სამი ძირითადი სტადია:

1. **1837–1963 წწ.:** ტელეგრაფისა და რადიოს დანერგვა.
2. **1964–1985 წწ.:** IBM 360 სერიის კომპიუტერების გამოჩენა.
3. **1985 წლიდან დღემდე:** საყოველთაო ინტერნეტიზაცია.

ამ ეპოქის სულისჩამდგმელები არიან **ნორბერტ ვინერი** (Norbert Winer), რომელმაც შექმნა კიბერნეტიკა და **კლოდ შენონი** (Claude Elwood Shannon), რომელმაც ინფორმაციის მათემატიკური თეორია ჩამოაყალიბა. **მათმა შრომებმა ინფორმაცია აქცია სიდიდედ, რომლის გაზომვა და დიდ მანძილზე დანაკარგის გარეშე გადაცემა შესაძლებელი გახდა.**

ესპანური წარმოშობის ამერიკელი სოციოლოგი, ინფორმაციული საზოგადოების თეორიის უდიდესი სპეციალისტი მანუელ კასტელსი (**Manuel Castells**, დ. 1942);

კანადელი ფილოსოფოსი, ფილოლოგი, კომუნიკაციის საშუალებების ადამიანსა და საზოგადოებაზე ზემოქმედების სფეროს თეორეტიკოსი მარშალ მაკლუენი (**Herbert Marshall McLuhan**, 1911-1980)

პარალელურად, საზოგადოებრივ მეცნიერებებში გაჩნდა ახალი ტერმინები: **ზბიგნევ ბჟეზინსკის** „ტექნოტრონული ერა“, **დანიელ ბელის** (Daniel Bell) „პოსტინდუსტრიული საზოგადოება“, **ელვინ ტოფლერის** „სუპერინდუსტრიული საზოგადოება“ და **მანუელ კასტელსის** (Manuel Castells) „ინფორმაციონალიზმის ეპოქა“.

2.5. მანუელ კასტელსი და ქსელური საზოგადოების ლოგიკა

ესპანელმა სოციოლოგმა **მანუელ კასტელსმა** ფუნდამენტურად შეისწავლა ინფორმაციული ეპოქის სტრუქტურა. მისი აზრით, ახალი ტექნოლოგიური პარადიგმის ბირთვი ინფორმაციისა და კომუნიკაციის დამუშავების ტექნოლოგიებთანაა დაკავშირებული.

კასტელსის ხედვით, ინფორმაციულ-ტექნოლოგიური რევოლუციის შედეგად **ადამიანის აზრი უშუალო საწარმოო ძალა გახდა**. მანქანებსა და აზრებს შორის ინტეგრაცია აუქმებს „მეოთხე განზომილებას“ — განხეთქილებას ადამიანსა და მანქანას შორის. ეს პროცესი ცვლის იმას თუ როგორ ვცხოვრობთ, ვმუშაობთ, ვაწარმოებთ და ვიბრძვით.

2.6. ინფორმაცია, როგორც სტრატეგიული რესურსი და გლობალური იარაღი

ინფორმაციულ ეპოქაში ინფორმაცია გახდა უფრო მძლავრი რესურსი, ვიდრე ადრე ინდუსტრიულ ეპოქაში ქვანახშირი და ფოლადი იყო. იგი არის ნებისმიერი სფეროს სიცოცხლისუნარიანობის წყარო. **საერთაშორისო არენაზე ქვეყნის გავლენა პირდაპირ დამოკიდებულია მისი საინფორმაციო ინფრასტრუქტურის განვითარებაზე.**

ინფორმაციული რესურსის ფლობა სახელმწიფოს აძლევს შესაძლებლობას:

- **გაავრცელოს საკუთარი კულტურული და სულიერი ღირებულებები;**
- **მოახდინოს სხვა ქვეყნების ინტელექტუალური პოტენციალის ექსპლუატაცია;**

- **შეაფერხოს მტრული ექსპანსია და შეარყიოს**

ამერიკელი სოციოლოგი და ფუტუროლოგი, პოსტინდუსტრიული საზოგადოების კონცეფციის ერთ-ერთი ავტორი ელვინ ტოფლერი (**Alvin Toffler**, დ. 1928);

ავსტრიული წარმოშობის ამერიკელი მეცნიერი, **XX** საუკუნის მენეჯმენტის თეორეტიკოსი, "ინფორმაციული მუშაკის" კონცეფციის ავტორი პიტერ დრუკერი (**Peter Ferdinand Drucker**, 1909-2005);

მოწინააღმდეგის ზნეობრივი საფუძვლები.

ინტერნეტმა მოსპო დროითი და პოლიტიკური საზღვრები. ინფორმაციის ნაკადებს შეუძლიათ დაუბრკოლებლად გადალახონ სახელმწიფო საზღვრები, რაც განუზომლად ზრდის ინფორმაციის ზემოქმედებით გავლენას.

2.7. ვირტუალური რეალობა და პოსტადამიანური საზოგადოება

დღეს სულ უფრო ხშირად საუბრობენ „პოსტადამიანურ საზოგადოებაზე". ადამიანები სცილდებიან ტრადიციულ ყოფას და ექცევიან „ვირტუალურ რეალობაში". იცვლება დროის შეგრძნება და კლასიური ცხოვრების რიტმი.

ინფორმაციული რევოლუცია გულისხმობს არა მხოლოდ ტექნოლოგიების გავრცელებას, არამედ საზოგადოებრივ ურთიერთობათა ახალი ტიპის დამკვიდრებას. მოქალაქეებს სულ უფრო ნაკლები საერთო კულტურული გამოცდილება უგროვდებათ, რაც სამოქალაქო საზოგადოებას ფრაგმენტულს ხდის. ეს კი, თავის მხრივ, წარმოშობს ეროვნული სახის დაკარგვის რისკებს.

მეორე თავის დასკვნა

ინფორმაცია არის ცივილიზაციის შემდგომი განვითარების მამოძრავებელი ფაქტორი. მისი როლის ახლებურად გააზრება და მართვა არა მხოლოდ სამეცნიერო ამოცანაა, არამედ თანამედროვე მსოფლიოს ბედის განმსაზღვრელიც. ინფორმაციული რევოლუციის შედეგად შექმნილი ციფრული სამყარო მოითხოვს ახლებურ მიდგომებს ეროვნული უშიშროების, ეკონომიკისა და სახელმწიფოებრივი მმართველობის სფეროებში.

მეორე თავის საკონტროლო კითხვები:

1. *რატომ ითვლება ინფორმაცია 21-ე საუკუნის მთავარ რესურსად?*
2. *რა გავლენას ახდენს ციფრული ტრანსფორმაცია გლობალურ ეკონომიკაზე?*

მეთოდური ასპექტი:

სტუდენტმა უნდა გაიაზროს, რომ ინფორმაცია გახდა თანამედროვეობის მთავარი სტრატეგიული რესურსი, რომელიც ენერგომატარებლებზე მეტად განსაზღვრავს სახელმწიფოს ძლიერებასა და მის ადგილს გლობალურ იერარქიაში.

თავი III
ინფორმაციული ომის წარმოშობის პერიპეტიები

3.1. ომის ფენომენი ადამიანთა ცივილიზაციაში

კაცობრიობის ისტორია, გარკვეულწილად, ომების ისტორიაა. მკვლევართა მონაცემებით, ძვ.წ. 3500 წლიდან მე-20 საუკუნის ბოლომდე დედამიწაზე 14 500-მდე ომი მოხდა, რომელმაც 3.5 მილიარდი ადამიანის სიცოცხლე შეიწირა. ცივილიზაციამ მშვიდობიან პირობებში მხოლოდ 300-მდე წელი გაატარა. ომის, როგორც ორგანიზებული სოციალური მოვლენის, სათავეები ნეოლითურ ხანას (საკვებწარმოებით რევოლუციას) უკავშირდება, როდესაც ნამატი პროდუქტის დაგროვებამ მისი მიტაცების სურვილი წარმოშვა.

პირველი სრულყოფილად ორგანიზებული არმიები შუმერულ და ეგვიპტურ ცივილიზაციებში ჩამოყალიბდა. ჯერ კიდევ ძვ.წ. III ათასწლეულში შუამდინარეთის ქალაქ-სახელმწიფოებს 10 000-მდე მეომრის გამოყვანა შეეძლო. ომის წარმოების ტექნოლოგიური ევოლუცია ბრინჯაოს იარაღიდან და საბრძოლო ეტლებიდან (რომლებიც თავისი ეფექტურობით ანტიკური ხანის ტანკებს წარმოადგენდნენ) დენთისა და ინდუსტრიული ეპოქის გამანადგურებელ იარაღამდე განვითარდა. მეოცე საუკუნის გლობალურმა კონფლიქტებმა კი კაცობრიობა სრულიად ახალი რეალობის წინაშე დააყენა, სადაც ინფორმაციული ფაქტორი გადამწყვეტი გახდა.

3.2. ომის ოთხი თაობა: ტრადიციულიდან პოსტმოდერნულ დაპირისპირებამდე

თანამედროვე სამხედრო თეორიაში (**უილიამს ლინდი** (William S. Lind), **კეიტი ნაიტინგეილი** (Keith Nightengale), ***ჯონ შმიტი*** (John F. Schmitt), **ჯოზეფ სუტონი** (Joseph W. Sutton), ***გარი ვილსონი*** (Gary I. Wilson),[4] მიღებულია ომის თაობებად დაყოფის კონცეფცია, რაც გვეხმარება გავიგოთ ინფორმაციული ომის ადგილი ისტორიულ პროცესში:

1. **პირველი თაობის ომი (1648–1860):** ვესტფალიის ზავის შემდგომი პერიოდი. მას ახასიათებს არაორგანიზებული შეტაკებებიდან დისციპლინირებულ, გაშლილი მწყობრით ბრძოლაზე გადასვლა. ჩამოყალიბდა სამხედრო იერარქია, უნიფორმა და მისალმების ფორმა. მთავარი იარაღი გლუვლულიანი მუშკეტი იყო.
2. **მეორე თაობის ომი (ინდუსტრიული პერიოდი):** დაკავშირებულია საცეცხლე ძალის ზრდასთან (არტილერია, ტყვიამფრქვევი). ამ პერიოდში გაშლილი მწყობრით გადაადგილება სარისკო გახდა, რამაც ჯარისკაცთა მცირე ჯგუფების დამოუკიდებელი მანევრების საჭიროება გამოიწვია. ცენტრალიზებული კონტროლი და

[4] Lind, W. S; Nightengale, Keith; Schmitt, John F.; Sutton, Joseph W.; Wilson, Gary I. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, October 1989, Pages 22-26 https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf http://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html [05.07.2017].

სინქრონიზე-ბული საცეცხლე ძალა ამ თაობის მთავარი ნიშანია.

3. **მესამე თაობის ომი (მანევრული ომი):** ფოკუსი-რებულია სისწრაფეზე, მოულოდნელობასა და მოწინააღმდეგის გვერდის ავლაზე (ბლიცკრიგი). აქ მნიშვნელოვანია არა ფიზიკური განადგურება, არამედ მოწინააღმდეგის კოლაფსი ტაქტიკური მანევრების გზით.

4. **მეოთხე თაობის ომი (4GW):** პოსტმოდერნული ომი, სადაც იშლება ზღვარი ომსა და პოლიტიკას, ჯარისკაცსა და სამოქალაქო პირს შორის. სახელმწიფო კარგავს ომზე მონოპოლიას და მხარეებად ტერორისტული ორგანიზაციები (ალ-ქაედა, ჰამასი და სხვა) გვევლინება. ფრონტის ხაზი აღარ არსებობს — ბრძოლა ყველგან მიმდინარეობს.

3.3. ინფორმაციული ომის ცნება და "შეუზღუდავი ომის" მოდელი

ინფორმაციულმა ეპოქამ შეცვალა ომის სტანდარტები. ჩინელი პოლკოვნიკების – **ქიაო ლიანგისა** (Qiao Liang) და **ვანგ სიანგშუის** (Wang Xiangsui) კონცეფცია **„შეუზღუდავი ომი“ (Unrestricted Warfare)**[5] ამტკიცებს, რომ ძალადობა აღარ არის ომის ერთადერთი

[5] Qiao, L., Wang, X. (2002). Unrestricted Warfare: China's Master Plan to Destroy America. Pan American Publishing Company, Panama City, Panama https://books.google.ge/books?id=ejFV1568hqAC&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [21.09.2025].

განმსაზღვრელი. ომი თანაბრად მიმდინარეობს ფინანსურ, ეკოლოგიურ, ენერგეტიკულ და ინფორმაციულ სფეროებში.

ინფორმაციული ეპოქის პირმშოა ინფორმაციული ომი, რომელსაც საფუძვლად უდევს ახალი ეპოქის – ინფორმაციული ეპოქის შინაარსის გამომხატველი, კაცობრიობის განვითარების სრულიად ახალი სტრატეგიული რესურსი – ინფორმაცია. თანამედროვე ეპოქის შინაარსის განმსაზღვრელი ფაქტორი „ინფორმაცია“ არის თანამედროვე ომების შინაარსის განმსაზღვრელიც, საფუძველიც და ამოსავალიც და როგორი სახეცვლილებითაც არ უნდა მოგვევლინოს, მისი მთავარი განმსაზღვრელიდან გამომდინარე, ფართო გაგებით, ეწოდება ინფორმაციული ომი. ინფორმაციულმა ეპოქამ ეპოქის შესატყვისი ომი მოიტანა.

ამიტომ ამ ომისათვის რა ახალი მოდური სახელის შერქმევაც არ უნდა სცადოს ზოგიერთმა თანამედროვე მკვლევარმა, ეს მხოლოდ ახალი სახელების მოგონების მოდისათვის ხარკის გადახდა იქნება და არა არსებითი შინაარსის გადმოცემა.[6]

მაგალითად, ტერმინი „ჰიბრიდული ომი“ არსებითად ინფორმაციული ომის (ფართო გაგების) ნაირსახეობაა, რომელიც მართვადი ქაოსის მეშვეობით მოწინააღ-

[6] კუპრაშვილი, ჰ. (2022). „ჰიბრიდული ომი - ომის ახალი ფილოსოფია თუ ახალი ტერმინი.“ „სამართლის მაცნე“, №5 (524), გვ. 6-17. E ISSN 2667-9434 http://heraldoflaw.com/ge/journal/hibriduli-omi-omis-akhali-filosofia-tu-akhali-termini/

მდეგის მორალურ და პოლიტიკურ დამარცხებას ისახავს მიზნად.

3.4. ინფორმაციული ომების თეორიის განვითარების ოთხი ეტაპი

საკომუნიკაციო ტექნოლოგიების ცნობილი უკრაინელი სპეციალისტი **გიორგი პოჩეპცოვის** (Гео́ргій Гео́ргійович Почепцо́в) კლასიფიკაციით,[7] ინფორმაციული ომების თეორიამ განვითარების ოთხი მნიშვნელოვანი ეტაპი გაიარა:

პირველი ეტაპი (90-იანების დასაწყისი): აშშ-ის სამხედრო-საჰაერო ძალების მეცნიერთა ჯგუფმა იწინასწარმეტყველა, რომ მომავლის ომის ყველაზე სუსტი წერტილი ჯარისკაცის ტვინი იქნებოდა. **ჯორჯ სტაინ-მა** (George J. Stein)[8] და **რი-ჩარდ შაფრანსკიმ** (Richard Szafranski)[9] ყურადღება გაამახვილეს „მენტალურ განზომილებასა “ და მოწინააღ-მდეგის ნებაზე მოქმედებაზე.

[7] Почепцов Г. Г. (2015). Информационные войны. Новый инструментарий политики. Москва: Алгоритм.
[8] Stein G. J. (2025). Information Attack: Information Warfare In 2025, research paper presented to 'Air Force 2025', August 1996. http://csat.au.af.mil/2025/volume3/vol3ch03.pdf
[9] Szafranski, R. (1997). Neocortical warfare? The acme of skill // In Athena's camp. Ed. By J. Arquilla, D. Ronfeldt. - Santa Monica.

მეორე ეტაპი (90-იანების დასასრული): ჯონ არქუილამ (John Arquilla) და **დევიდ რონფელდმა** (David Ronfeldt) ჩამოაყალიბეს „კიბერომისა“ და „ქსელური ომის“ ფუნდამენტური პრინციპები. მათ ნაშრომში „ათენის ბანაკი“ გაანალიზდა კონფლიქტების მზადება ინფორმაციულ ეპოქაში.[10]

მესამე ეტაპი (XXI საუკუნის დასაწყისი): პრაქტიკოსი სამხედროების გააქტიურება, რომლებმაც აქცენტი „გავლენის ოპერაციებზე“ (Influence Operations) გადაიტანეს.

მეოთხე ეტაპი (მიმდინარე): ეპოქა, რომელიც საჭიროებს ახალ თეორიებსა და ანალიტიკას სწრაფად ცვალებადი ტექნოლოგიური გარემოს საპასუხოდ.

3.5. ინფორმაციული ომის "ადამიანური" და "ტექნიკური" განზომილებები

თეორიის განვითარებისას აქცენტი მუდმივად მონაცვლეობს ადამიანურ და ტექნიკურ ფაქტორებს შორის:

დოროთი დენინგი (Dorothy E. Denning) აქცენტს ტექნიკურ განზომილებაზე აკეთებს, სადაც ომი მიმართულია ინფორმაციული რესურსებისკენ.[11]

მარტინ ლიბიკი (Martin C. Libicki)[12] გამოყოფს „ციხესიმაგრეებსა“ (დაცული სისტემები) და „მოედნებს“ (ღია

[10] Arquilla, J., Ronfeldt, D (1997). In Athena's Camp: Preparing for Conflict in the Information Age, RAND Corporation (MR-880).
[11] Denning, D. E. (1999). *Information warfare and security*. - Reading etc., https://archive.org/details/informationwarfa00denn
[12] Libicki M. (2007). Conquest in cyberspace. National security and information warfare. - Cambridge, p. 216.

სისტემები), სადაც მთავარია ნარატივების შესწავლა და მოწინააღმდეგის გადაწყვეტილებათა მიღების სისტემაში შეღწევა.

ფინანსური ომი: დუაიტ ეიზენჰაუერის (Dwight D. Eisenhower) მიერ 1956 წელს სუეცის კრიზისის დროს გამოყენებული ფინანსური ბერკეტები ინფორმაციული და ეკონომიკური ომის შეხამების კლასიკური მაგალითია.

3.6. კიბერომი და ქსელური ომი (ჯონ არქუილას ხედვა)

ჯონ არქუილას (John Arquilla)[13] კონცეფციით, თანამედროვე კონფლიქტი ორ პოლუსს შორის თავსდება: **კიბერომი** (მაღალი ინტენსივობის) და **ქსელური ომი** (დაბალი ინტენსივობის, სადაც იერარქიის ნაცვლად ქსელები მოქმედებს). მისი აზრით, ინფორმაციული ომი საშუალებას იძლევა ფარულად და ანონიმურად ჩაერიო ნებისმიერ წერტილში „ბიტებითა და ბაიტებით“. არქუილა წინმსწრები დარტყმის მომხრეა და მაგალითად 2008 წლის რუსეთ-საქართველოს ომი მოჰყავს, სადაც რუსულ ტანკებს გზა კიბერშეტევამ გაუკვალა.

3.7. ინფორმაციული ოპერაცია და ინფორმაციული ომი

აშშ-ის თავდაცვის სამინისტრომ 1998 წელს მკაფიოდ გამიჯნა ეს ორი ცნება:

[13] Arquilla J. (2011). Insurgents, raiders, and bandits. How masters of irregular warfare have shaped our world. – Chicago.

- **ინფორმაციული ოპერაცია:** კონკრეტული მოქმედება მოწინააღმდეგის ინფორმაციული ნაკადების შესაფერხებლად და საკუთარის დასაცავად.
- **ინფორმაციული ომი:** კომპლექსური ზემოქმედება (ოპერაციების ერთობლიობა), რომელიც მიზნად ისახავს მოწინააღმდეგის სახელმწიფო და სამხედრო მმართველობის სრულ პარალიზებას.

ტექნიკური თვალსაზრისით, ეს მოიცავს რადიოელექტრონულ ბრძოლას, ჰაკერულ შეტევებსა და ფსიქოტრონულ ზემოქმედებას, ჰუმანიტარული კუთხით კი — სამყაროს საკუთარი მოდელის თავისმოხვევას მოწინააღმდეგისთვის.

მესამე თავის დასკვნა

ინფორმაციული ომი არის ყოვლისმომცველი სტრატეგია, სადაც ინფორმაციის ღირებულება განუზომლად გაიზარდა. იგი აღარ შემოიფარგლება მხოლოდ სამხედრო სფეროთი და მოიცავს საბანკო სისტემებს, ენერგეტიკას, ტრანსპორტსა და სამოქალაქო ცნობიერებას. როგორც პენტაგონის ექსპერტები აღნიშნავენ, ჩვენ ვუახლოვდებით ეპოქას, სადაც „ყველა მონაწილეა საბრძოლო მოქმედებების“, ხოლო ამოცანა არა ცოცხალი ძალის განადგურება, არამედ სოციუმის დაშლა და მოწინააღმდეგის მსოფლმხედველობის შერყევაა.

მესამე თავის საკონტროლო კითხვები:

1. *დაახასიათეთ ომის მეოთხე თაობა და მისი ძირითადი ნიშნები.*

2. ვინ იყვნენ ინფორმაციული ომის თეორიის ფუძემდებლები?

მეთოდური ასპექტი:

თავის ათვისების შემდეგ სტუდენტმა უნდა შეძლოს ომის ევოლუციის დანახვა და გაცნობიერება, რომ მეოთხე თაობის ომში ზღვარი „მშვიდობასა“ და „ომს“ შორის პრაქტიკულად წაშლილია.

თავი IV
კიბერსივრცე: თავდაცვის თანაბარუფლებიანი სფერო ზღვასთან, ჰაერთსა და ხმელეთთან ერთად

4.1. ვირტუალური რეალობის სოციოლოგიური და ფილოსოფიური საფუძვლები

თანამედროვე ცივილიზაციამ განვითარების ისეთ ეტაპს მიაღწია, სადაც ქსელური კომუნიკაციები აღარ არის მხოლოდ დამხმარე ინსტრუმენტი; ისინი იქცა სოციალური, პოლიტიკური და ეკონომიკური ორგანიზაციის ძირითად ფორმად. ჯერ კიდევ XX საუკუნის შუა წლებში, **მარშალ მაკლუენი** (Herbert Marshall McLuhan) აღნიშნავდა, რომ ელექტრული ეპოქა ქმნის გლობალურ ქსელს, რომელიც თავისი ბუნებით ადამიანის ცენტრალურ ნერვულ სისტემას ჰგავს. ამ „ნერვულმა სისტემამ“ წარმოშვა ქსელური საზოგადოება, რომელიც ხასიათდება სტრუქტურული კომპლექსურობითა და მუდმივი დინამიკურობით.

სოციოლოგი **ჯონ ური** (John Urry)[14] ადამიანის არსებობის გარემოს სამი ფონის მიხედვით ყოფს: ბუნებრივი, ხელოვნური და ვირტუალური. თუ კაცობრიობის ისტორიის უმეტესი ნაწილი ბუნებრივ ლანდშაფტში მიმდინარეობდა, მესამე და მეოთხე ინდუსტრიულმა რევოლუციამ შექმნა **ვირტუალური ობიექტების ფონი**. ეს არის კიბერსივრცე — პროგრამული სისტემების ერთობლიობა, რომელიც ადამიანის უშუალო ჩარევის გარეშეც ახორციელებს განმეორებად მოქმედებებს. **ური** გვთავა-

[14] Urry, J. (2007). *Mobilities*. Cambridge, UK ; Malden, MA : Polity https://archive.org/details/mobilities0000urry

ზობს ტრადიციული „საზოგადოების“ ნაცვლად გამოვიყენოთ ტერმინი „მობილურობა“, რაც უკეთ ასახავს ინფორმაციის, ობიექტებისა და ცოცხალი ორგანიზმების მუდმივ გადაადგილებას ციფრულ ეპოქაში.

4.2. კიბერსივრცის დეფინიცია და მისი მრავალშრიანი სტრუქტურა

კიბერსივრცე არ არის მხოლოდ ინტერნეტი. ეს არის სოციალური ურთიერთქმედების განსაკუთრებული სფერო, რომელიც მოიცავს:

- **მსოფლიო კომპიუტერულ ქსელებს:** სადაც მიედინება ინფორმაციული ნაკადები;
- **ტრანსნაციონალურ ფინანსურ ქსელებს:** რომლებიც მართავენ გლობალურ საბირჟო და საკრედიტო ოპერაციებს;
- **კრიტიკული ინფრასტრუქტურის მართვის სისტემებს:** ენერგეტიკა, ტრანსპორტი, წყალმომარაგება, სამრეწველო ტუმბოებისა და ლიფტების მართვის პანელებიც კი.

ეს ახალი გარემო ეფემერული, ინტერაქტიული და ანონიმურია. მასში იქმნება სოციალური წარმოების გლობალური სისტემა, სადაც სოციალური სტრატიფიკაცია აღარ ეფუძნება ტრადიციულ პრინციპებს, არამედ დამოკიდებულია **აქტორის ცოდნის დონეზე**. კიბერსივრცის „პრივილეგირებულ ფენას“ ქმნიან ისინი, ვინც უკეთ ფლობენ ინფორმაციულ ნაკადებს და წვდომა აქვთ დახურულ მონაცემებთან.

4.3. ვარშავის სამიტი: ისტორიული გარდატეხა სამხედრო სტრატეგიაში

2016 წლის 8 ივლისი ისტორიულ თარიღად იქცა საერთაშორისო უშიშროების ისტორიაში. ნატოს ვარშავის სამიტზე კიბერსივრცე ოფიციალურად იქნა აღიარებული **თავდაცვის თანაბარუფლებიან სფეროდ**, ხმელეთის, ზღვის, ჰაერისა და კოსმოსის გვერდით. **იენს სტოლტენბერგმა** (Jens Stoltenberg) მკაფიოდ განაცხადა, რომ კიბერშეტევა ისეთივე რეალური აგრესიაა, როგორც შეიარაღებული თავდასხმა და მასზე რეაგირება კოლექტიური თავდაცვის პრინციპით უნდა მოხდეს.

ამ გადაწყვეტილებამ წაშალა ზღვარი „ვირტუალურ“ და „რეალურ“ კონფლიქტებს შორის. კიბერსივრცეში მიმდინარე ეკონომიკური შპიონაჟი, ფინანსური დივერსიები და საინფორმაციო ბრძოლები აღარ განიხილება როგორც იზოლირებული ინციდენტები — ისინი გლობალური სამხედრო-პოლიტიკური დაპირისპირების განუყოფელი ნაწილია.

4.4. კიბერომი, როგორც ომის მეხუთე ფორმა

ინფორმაციულმა ერამ შეცვალა სამხედრო მოქმედებათა ჩატარების წესი. კიბერომი საშუალებას იძლევა:

1. მოხდეს მოწინააღმდეგის პირდაპირი მანიპულირება ინფორმაციით, რაც მას პოტენციურ იარაღად აქცევს;
2. გამოყენებულ იქნეს ციფრული ტექნოლოგიები საბრძოლო ოპერაციების კოორდინაციისთვის.

მსოფლიო ქსელის გაჩენამ გააუქმა ბუნებრივი საზღვრები. „მებრძოლ არმიებს“ შეუძლია შეიჭრას სხვის ტერიტორიაზე ფიზიკური გადაადგილების გარეშე და პარალიზება გაუკეთონ ქვეყნის სასიცოცხლო სისტემებს. პენტაგონი, რუსეთი, ჩინეთი და სხვა წამყვანი სახელმწიფოები უკვე წლებია იყენებს ინფორმაციულ იარაღს, რომელიც მიმართულია არა მხოლოდ ტექნიკაზე, არამედ ადამიანის მსოფლმხედველობაზეც.

4.5. ცნობიერებით მანიპულაცია და რიჩარდ შაფრანსკის თეორია

ამერიკელი პოლკოვნიკი **რიჩარდ შაფრანსკი** (Richard Szafranski) თავის ნაშრომებში ხაზს უსვამს, რომ ინფორმაციული ომის მთავარი მიზანია მოწინააღმდეგის ქცევაზე ისეთი ზემოქმედება, რომ მან ვერც კი გააცნობიეროს სხვისი გავლენის ქვეშ ყოფნა. წარმატებული კამპანია მტერს აიძულებს მიიღოს გადაწყვეტილებები, რომლებიც მისსავე ინტერესებს ეწინააღმდეგება.

შაფრანსკის აზრით, ინფორმაციული ტექნოლოგიები საშუალებას იძლევა „იმართოს“ პროცესები მინიმალური სისხლისღვრით. უსისხლოდ მიღწეული გამარჯვება — მტრის დამორჩილება და მასზე აბსოლუტური ძალაუფლების დამყარება — ინფორმაციული ომის უმაღლესი მწვერვალია. ამ პროცესში ინტერნეტი ასრულებს გამაბრუებელი ვირტუალური გარემოს როლს, სადაც ადამიანის აზროვნება აუტისტური და მანიპულაციის მიმართ მოწყვლადი ხდება.

4.6. სუვერენიტეტი კიბერსივრცეში: ვირტუალური და ქსელური განზომილება

ციფრულ ეპოქაში სახელმწიფო სუვერენიტეტის ცნებამ ტრანსფორმაცია განიცადა. გაჩნდა ტერმინები: „ვირტუალური სუვერენიტეტი“ და „ქსელური სუვერენიტეტი“. ვინაიდან კიბერსივრცეს არ ახასიათებს ტერიტორიალურობა, სახელმწიფო ხელისუფლების პროეცირება ამ სფეროზე სირთულეებთანაა დაკავშირებული.

დღეს სახელმწიფო კიბერსივრცეში გვევლინება როგორც ერთ-ერთი აქტორი, თუმცა ყველაზე მძლავრი რესურსებით. მას შეუძლია შეზღუდოს სხვა აქტორების წვდომა ქსელზე, მაგრამ კიბერსივრცის ეფემერულობა და ანონიმურობა ტრადიციულ კონტროლს შეუძლებელს ხდის. კიბერომებში გამარჯვება პირდაპირ განსაზღვრავს სახელმწიფოს პოლიტიკურ და ეკონომიკურ სუვერენიტეტს 21-ე საუკუნეში.

4.7. საქართველოს ხედვა და მომავლის გამოწვევები

საქართველოს თავდაცვის სამინისტრო და „თავდაცვის ხედვა 2030“ ადეკვატურად პასუხობს კიბერსივრცის გამოწვევებს. აღიარებულია, რომ ხელოვნური ინტელექტის, უპილოტო სისტემებისა და დისტანციური მართვის განვითარება ამცირებს ტრადიციული საცეცხლე საშუალებების როლს.

მომავლის ომებში წარმატების ფორმულაა **Network Centric** (ქსელურ-ცენტრული) მართვა, რაც გულისხმობს:

- რეალურ დროში ბრძოლის ველის სრული სურათის ფლობას;
- C4I (მართვა, კონტროლი, კავშირგაბმულობა, კომპიუტერული სისტემები და დაზვერვა) სისტემების განვითარებას;
- კონვენციური და არაკონვენციური მეთოდების ერთ სტრატეგიაში გაერთიანებას (ჰიბრიდული საფრთხეების მოგერიება).

საქართველოს ამოცანაა არა მხოლოდ მტრის შემოტევების მოგერიება, არამედ საკუთარი მყარი კიბერსივრცის შექმნა, რათა თავიდან აიცილოს სხვა სახელმწიფოთა მხრიდან მანიპულირების ობიექტად ქცევა.

მეოთხე თავის დასკვნა

კიბერსივრცე აღარ არის მხოლოდ „ტექნიკური დანამატი“ რეალობაზე; იგი არის დამოუკიდებელი, ყოვლისმომცველი სფერო, სადაც წყდება თანამედროვე სახელმწიფოების ბედი. ვარშავის სამიტის გადაწყვეტილება იყო პასუხი იმ რეალობაზე, სადაც ინფორმაციული ნაკადები ისეთივე დამანგრეველია, როგორც ბომბები. ინფორმაციულ ეპოქაში გამარჯვება მოითხოვს არა მხოლოდ ტექნოლოგიურ აღჭურვილობას, არამედ ახლებურ სოციალურ და სამხედრო აზროვნებას, რომელიც მზად იქნება ქსელურ სამყაროში სუვერენიტეტის დასაცავად.

მეოთხე თავის საკონტროლო კითხვები:

1. *რა არის „რბილი ძალის“ (Soft Power) არსი და რით განსხვავდება ის ტრადიციული „ხისტი ძალისგან“?*

2. *როგორ გამოიყენება კულტურა და იდეოლოგია ინფორმაციულ ომში სტრატეგიული უპირატესობის მოსაპოვებლად?*
3. *განმარტეთ ფსიქოლოგიური ოპერაციების (PSYOPS) როლი საზოგადოებრივი აზრის ფორმირებაში.*

მეთოდური ასპექტი:

სტუდენტმა უნდა გააცნობიეროს, რომ თანამედროვე კონფლიქტებში ადამიანის ცნობიერება არის მთავარი სამიზნე, ხოლო „რბილი ძალა“ წარმოადგენს ყველაზე ეფექტურ ინსტრუმენტს ქვეყნის ინტერესების უსისხლოდ გასატარებლად.

თავი V
ინფორმაციული ომის ორი შემადგენელი: საინფორმაციო-ფსიქოლოგიური და კიბერომი

5.1. ტერმინოლოგიური დიალექტიკა: ფსიქოლოგიური ზემოქმედება და ტექნიკური შეტევა

თანამედროვე მეცნიერულ დისკურსში ტერმინი „ინფორმაციული ომი“ ხშირად გამოიყენება როგორც ქოლგა-ცნება, რომელიც ორ ფუნდამენტურ, თუმცა განსხვავებულ მიმართულებას აერთიანებს. 21-ე საუკუნის რეალობაში ინფორმაციული ომის სრულყოფილი გააზრება მოითხოვს **საინფორმაციო-ფსიქოლოგიური ბრძოლისა** და **კიბერბრძოლის** გამიჯვნასა და მათი ურთიერთქმედების ანალიზს:

- **საინფორმაციო-ფსიქოლოგიური ომი** – დაპირისპირების უძველესი ფორმა, რომელიც ინფორმაციულ ეპოქაში ახალი ინსტრუმენტებით აღიჭურვა. მისი სამიზნეა ადამიანის ფსიქიკა, სოციალური ჯგუფების ცნობიერება და გადაწყვეტილების მიღების პროცესი. მარტივად რომ ვთქვათ, ეს არის მასმედიის, სოციალური ქსელებისა და სხვადასხვა ნარატივის მეშვეობით წარმოებული მიზანმიმართული პროპაგანდა და მანიპულაცია.
- **კიბერომი** – ტექნოლოგიური რევოლუციისა და ინტერნეტის პირმშო. მისი ობიექტია ინფორმაციული ტექნოლოგიების ინფრასტრუქტუ-

რა — კომპიუტერული ქსელები, მონაცემთა ბაზები და მართვის სისტემები. კიბერომი მიზნად ისახავს სისტემების პარალიზებას, მონაცემთა მოპარვას ან განადგურებას ტექნიკური კოდებისა და ალგორითმების მეშვეობით.

ამ ორ შემადგენელს შორის დიალექტიკური კავშირი მდგომარეობს იმაში, რომ კიბერშეტევა ხშირად ამზადებს ნიადაგს ფსიქოლოგიური ოპერაციისთვის, ხოლო ფსიქოლოგიური ზემოქმედება აადვილებს ტექნიკურ შეღწევას (მაგალითად, სოციალური ინჟინერიის გზით).

5.2. ისტორიული რეტროსპექტივა: "ცივი ომიდან" ციფრულ აგრესიამდე

ინფორმაციული ომის მასშტაბების საილუსტრაციოდ საუკეთესო მაგალითია „ცივი ომის“ პერიოდი (1946-1991). ეს იყო კაცობრიობის ისტორიაში ყველაზე ხანგრძლივი და მასშტაბური საინფორმაციო-ფსიქოლოგიური დაპირისპირება ორ ზესახელმწიფოს — აშშ-სა და სსრკ-ს შორის. ამ ომში საბჭოთა კავშირის დამარცხება არ ყოფილა მხოლოდ ეკონომიკური კოლაფსის შედეგი; ეს იყო იდეოლოგიური და ფსიქოლოგიური მარცხი, სადაც დასავლურმა ნარატივებმა და ინფორმაციულმა ღიაობამ ჩაკეტილი საბჭოთა პროპაგანდა დაამარცხა.

პოსტსაბჭოთა პერიოდში ინფორმაციული ომის ხასიათი შეიცვალა. რუსეთის ფედერაციამ, **ვლადიმერ პუტინის** მმართველობის პერიოდში, შეიმუშავა ინფორმაციული უშიშროების დოქტრინა, სადაც პოსტსაბჭოთა სივრცეში წამყვანი ადგილი სწორედ საინფორმაციო-ფსიქოლოგიურ კომპონენტს ეთმობა. რუსული სტრატეგია ეყრ-

დნობა ჩინელი მხედართმთავარის და სამხედრო თეორეტიკოსის, სამხედრო ხელოვნების ტრაქტატის „ომის ხელოვნების“ ავტორის, **სუნ ძის** კლასიკურ პრინციპს: „საუკეთესო ომია — მტრის ჩანაფიქრის ჩაშლა“. ისინი არა მხოლოდ ტექნიკურად გვიტევენ, არამედ ღრმად სწავლობენ სამიზნე აუდიტორიის ფსიქოლოგიურ პორტრეტს, კულტურულ კოდებსა და ტრადიციებს, რათა მანიპულაცია მაქსიმალურად ეფექტური იყოს.

5.3. საქართველოს გამოწვევები: კიბერუსაფრთხოების კალკირება და რეალური საფრთხეები

საქართველოს ეროვნული უშიშროების პოლიტიკის ანალიზი სერიოზულ ხარვეზს აჩვენებს: სახელმწიფო სტრატეგიულ დონეზე აქცენტს აკეთებს თითქმის ექსკლუზიურად კიბერუსაფრთხოებაზე (ტექნიკურ მხარეზე). არაფერია ნათქვამი საინფორმაციო-ფსიქოლოგიური უშიშროების უზრუნველყოფაზე, რაც რუსეთის მთავარი იარაღია საქართველოს წინააღმდეგ. ტექნოლოგიური ინფრასტრუქტურის აღდგენა შესაძლებელია, მაგრამ ფსიქოლოგიური ომით მიყენებული ზიანი ხშირად აუნაზღაურებელია.

საქართველოში მიღებული კანონები ძირითადად დასავლური, მაღალტექნოლოგიური ქვეყნების დოკუმენტების კალკირებაა. ამერიკის შეერთებული შტატებისთვის, რომელიც გლობალურად დომინირებს ინფოსფეროში, კიბერუსაფრთხოება მართლაც პრიორიტეტულია, რადგან მათი ეკონომიკა და არმია სრულადაა დამოკიდე-

ბული ციფრულ ქსელებზე. თუმცა, საქართველოსთვის, რომელიც რუსული პროპაგანდისა და „რბილი ძალის“ პირდაპირი სამიზნეა, ფსიქოლოგიური ასპექტების უგულებელყოფა სტრატეგიული შეცდომაა.

რუსეთის მიერ წარმოებულ ინფორმაციულ ომში ქართული სპეციფიკა ზედმიწევნითაა გათვალისწინებული. რუსეთის სპეცსამსახურები იყენებენ ორასწლოვანი ბატონობის პერიოდში დაგროვებულ ქართველების ფსიქიკის, ტრადიციებისა და ღირებულებების შესახებ ცოდნას. ისინი მანიპულირებენ მასობრივი ცნობიერებით, რაც გაცილებით დიდ პოლიტიკურ და იდეოლოგიურ ზარალს გვაყენებს, ვიდრე ტექნიკური კიბერშეტევები.

კრემლი მაღალ პროფესიულ დონეზე იყენებს ჩვენს კულტურულ და სულიერ ღირებულებებს ჩვენსავე წინააღმდეგ, ახდენს საზოგადოების პოლარიზაციას და მანიპულირებს მასობრივი ცნობიერებით. ამ ფონზე, **მხოლოდ** კიბერსივრცეში სახელმწიფო ინტერესების დაცვა (ტექნიკური კუთხით) ვერ იქნება ადეკვატური პასუხი ყოვლისმომცველ აგრესიაზე.

5.4. საინფორმაციო-ფსიქოლოგიური ომის საბრძოლო არსენალი

საინფორმაციო-ფსიქოლოგიური ომის წარმოების მეთოდები მრავალფეროვანია და მიზნად ისახავს მოწინააღმდეგის სრულ დემორალიზებას:

1. **დეზინფორმაცია და „ფეიკ ნიუსი“:** მითების შექმნა და გავრცელება, რომლებიც საფუძველს უთხრის სახელმწიფო ინსტიტუტებისადმი ნდობას;

2. **ცნობიერებით მანიპულაცია:** სოციალურ ჯგუფებზე მიზანმიმართული ზემოქმედება მათი ქცევის შესაცვლელად (მაგალითად, ანტიდასავლური განწყობების გაღვივება);
3. **ისტორიული ნარატივების გამრუდება:** კოლექტიური მეხსიერების ტრანსფორმაცია მოწინააღმდეგისთვის სასურველი მიმართულებით;
4. **სოციალური ინჟინერია:** ადამიანური ფაქტორის გამოყენება ინფორმაციულ სისტემებში შეღწევის ან დესტაბილიზაციის მიზნით.

განსაკუთრებით საშიშია ინტერნეტის როლი ამ პროცესში. ვირტუალურ სივრცეში ჩაფლული ადამიანის აზროვნება ხდება „აუტისტური“, იგი კარგავს კავშირს რეალობასთან, რაც მანიპულატორს საშუალებას აძლევს დანერგოს მასში ნებისმიერი სასურველი ცოდნა თუ სურვილი.

5.5. ეროვნული უშიშროების საინფორმაციო-ფსიქოლოგიური უზრუნველყოფის ამოცანები

საქართველოს წინაშე არსებული რეალური საფრთხეებიდან გამომდინარე, აუცილებელია ჩამოყალიბდეს „ინფორმაციული უშიშროების დოქტრინა“, სადაც წამყვანი ადგილი ფსიქოლოგიურ კომპონენტს დაეთმობა. სტრატეგიული ამოცანები უნდა მოიცავდეს:

- **მოსახლეობის ფსიქიკის დაცვა:** მოქალაქეების მედეგობის გაზრდა დესტრუქციული საინფორმაციო ზემოქმედების მიმართ (მედიაწიგნიერება და კრიტიკული აზროვნება).

- **აღქმის პროცესების მანიპულირების აღკვეთა:** მტრულად განწყობილი ძალების მიერ მოსახლეობის ცნობიერებაში შეღწევის მცდელობების იდენტიფიცირება და ნეიტრალიზაცია.
- **მუდმივი მონიტორინგი და დიაგნოსტიკა:** საზოგადოებრივი აზრისა და ფსიქიკური მდგომარეობის მუდმივი კვლევა, რათა დროულად გამოვლინდეს უცხოური გავლენის ოპერაციების კვალი.
- **ეროვნული ინტერესების პროექცია:** გლობალურ და რეგიონულ საინფორმაციო სივრცეში საკუთარი, ქართული ნარატივისა და ღირებულებების აქტიური დაცვა და გავრცელება.

მეხუთე თავის დასკვნა

ინფორმაციული ომი 21-ე საუკუნეში არის ორთავიანი ჰიდრა, სადაც ერთი თავი ტექნიკურია (კიბერომი), ხოლო მეორე — კოგნიტური (საინფორმაციო-ფსიქოლოგიური ომი). სახელმწიფოს მხრიდან მხოლოდ ერთ კომპონენტზე აქცენტირება მას დაუცველს ხდის მეორის წინაშე.

საქართველოსთვის, რომლის მოწინააღმდეგეც ფლობს ქართველთა ფსიქოლოგიური მანიპულირების ორასწლოვან გამოცდილებას, სასიცოცხლოდ მნიშვნელოვანია საინფორმაციო-ფსიქოლოგიური უშიშროების პრიორიტეტულად აღიარება. ინფორმაციულ ომში გამარჯვება მოიპოვება არა მხოლოდ კარგად დაცული სერვერებით, არამედ, პირველ რიგში, მყარი ეროვნული ცნობიერებითა და ინფორმირებული საზოგადოებით.

მეხუთე თავის საკონტროლო კითხვები:

1. რას გულისხმობს „ქსელური ომის“ (Netwar) კონცეფცია და რა როლს ასრულებს მასში არასახელმწიფოებრივი აქტორები?

2. როგორ ცვლის იერარქიული მმართველობის ქსელურით ჩანაცვლება კონფლიქტის დინამიკას?

3. განიხილეთ სოციალური ქსელების გავლენა თანამედროვე პოლიტიკურ მობილიზაციაზე.

მეთოდური ასპექტი:

სტუდენტმა უნდა გაიაზროს ქსელური სტრუქტურების უპირატესობა ტრადიციულ იერარქიებთან მიმართებაში და გააცნობიეროს, როგორ შეუძლია მცირე, კარგად ორგანიზებულ ჯგუფებს გლობალურ უშიშროებაზე ზემოქმედება.

თავი VI
საერთაშორისო კიბერსივრცე და თანამედროვე ომების თავისებურებანი: ინფორმაციული იარაღი

6.1. ჰიბრიდული ომი და ინფორმაციული ეპოქის საბრძოლო პარადიგმა

თანამედროვე სამხედრო ექსპერტები და ანალიტიკოსები ერთხმად აღნიშნავენ, რომ 21-ე საუკუნის კონფლიქტები სულ უფრო ხშირად იღებს ჰიბრიდულ ხასიათს. ჰიბრიდული ომი არ არის მხოლოდ სამხედრო ტაქტიკა, ის არის კომპლექსური სტრატეგია, სადაც ბრძოლა ადამიანთა გონებისა და გულებისათვის მიმდინარეობს. ამ პროცესში მასმედიისა და ციფრული საკომუნიკაციო არხების მეშვეობით შექმნილი ინფორმაციული სურათი ხშირად უფრო მნიშვნელოვანია, ვიდრე რეალური მდგომარეობა ფრონტის ხაზზე.

ზოგიერთი მკვლევარი მიიჩნევს, რომ ჰიბრიდული მეთოდები (დეზინფორმაცია, პარტიზანული ბრძოლა, ეკონომიკური შანტაჟი) ისტორიულად ყოველთვის არსებობდა, თუმცა ინფორმაციულმა ეპოქამ მათ სრულიად ახალი მასშტაბი და ეფექტურობა შესძინა. ინფორმაცია, როგორც კაცობრიობის განვითარების სტრატეგიული რესურსი, გახდა თანამედროვე ომების საფუძველი და ამოსავალი წერტილი. სწორედ ამიტომ, ნებისმიერი „ჰიბრიდული“ დაპირისპირების ბირთვს წარმოადგენს ინფორმაციული ომი, რომელიც თავისი დამანგრეველი ძალით უკვე უთანაბრდება მასობრივი განადგურების იარაღს.

6.2. ინფორმაციული იარაღის ტრიადა და მისი ზემოქმედების ობიექტები

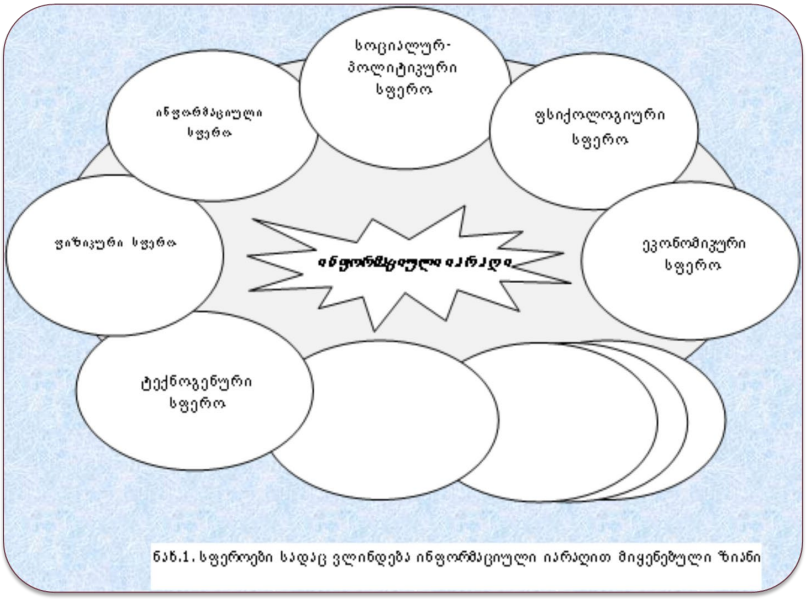
ინფორმაციული ტექნოლოგიების განვითარებამ ჩამოაყალიბა ინფორმაციული სივრცის სპეციფიკური ტრიადა: **ადამიანი — ინფორმაცია — ტექნიკური საშუალებები.** ამ გარემოში ფუნქციონირებს ე.წ. „ჰუმანური იარაღი“, რომლის მიზანია არა ფიზიკური განადგურება, არამედ მოწინააღმდეგის ცნობიერებისა და ინფრასტრუქტურის მართვა.

ინფორმაციული იარაღის მოქმედების სპექტრი უაღრესად ფართოა და ერთდროულად აზიანებს რამდენიმე შრეს:

1. **კოგნიტური დონე:** აზიანებს ადამიანის ცნობიერებას, გარდაქმნის მეხსიერების მატრიცას და ხელოვნურ მოთხოვნილებებს აყალიბებს;
2. **იდენტობის დონე:** არღვევს პიროვნების თვითგამორკვევის გზებს და ფორმებს, ადამიანს აიძულებს რეალობა არაადეკვატურად აღიქვას.
3. **ტექნიკური დონე:** მწყობრიდან გამოჰყავს სახელმწიფოსა და შეიარაღებული ძალების მართვის სისტემები, ანადგურებს მონაცემთა ბაზებს.

6.3. ინფორმაციული იარაღის დეფინიცია და სოციალური საშიშროება

აკადემიური თვალსაზრისით, ინფორმაციული იარაღი უნდა განვიხილოთ როგორც საინფორმაციო-ფსიქოლოგიური ზემოქმედების კომპლექსური ტექნოლოგიები.



ნახ.1. სფეროები სადაც ვლინდება ინფორმაციული იარაღით მიყენებული ზიანი

მისი მთავარი დანიშნულებაა ადამიანის ცენტრალური ნერვული სისტემის დაზიანება და „უმაღლესი ნერვული მოქმედების“ მართვა.

ხშირად ისმის კითხვა: რატომ მივიჩნევთ იარაღად ტექნოლოგიებს და არა თავად ინფორმაციას? პასუხი იმაში მდგომარეობს, რომ **ინფორმაცია (თუნდაც დეზინფორმაცია) იარაღად მხოლოდ მაშინ იქცევა, როდესაც ის კომპლექსური ტექნოლოგიური დამუშავების შედეგად აღწევს ადამიანის ფსიქიკამდე, ანგრევს მის ბუნებრივ დამცავ ბარიერებს და ცვლის ქცევას.** ამგვარად, ინფორმაციული იარაღის მიზანია ცოცხალი სამიზნის — ადამიანის ფსიქიკური და სოციალური პარალიზება.

6.4. პრაქტიკული ქეისები და მანიპულაციის ტექნოლოგიები

ინფორმაციული იარაღის გამოყენების თვალსაჩინო მაგალითები გვიჩვენებს მის ეფექტურობას სხვადასხვა კონტექსტში:

- **ცნობიერების კორექტირება (ერაყის ომის მაგალითი):** ერაყში სამხედრო ოპერაციის დროს, საზოგადოებრივი უკმაყოფილების გადასაფარად, ეფექტურად იქნა გამოყენებული ატიპიური პნევმონიის (ვირუსის) შესახებ მასობრივი შიშის დათესვა. ინფორმაციულმა იარაღმა ადამიანები აიძულა დაევიწყებინათ პოლიტიკური პროცესები და გადართულიყვნენ გადარჩენის ინსტინქტზე.
- **ბრბოს მართვის ტექნოლოგიები:** პოლიტიკურ ბრძოლაში ხშირად გამოიყენება ბრბოს ფსიქოლოგიაზე გათვლილი მეთოდები, რომლებიც კანონმორჩილ მოქალაქეებს აგრესიულ, მართვად მასად აქცევს.
- **ნეირო-ლინგვისტური პროგრამირება (NLP):** შიგაპოლიტიკურ თუ ეკონომიკურ ბრძოლაში NLP ტექნოლოგიები გამოიყენება ოპონენტის „დასაპროგრამებლად“, რათა მან გაუცნობიერებლად შეასრულოს სხვისი ნება.

6.5. შეიარაღების ახალი ფილოსოფია: CHAMP-რაკეტები და უხილავი დარტყმა

ინფორმაციული ომების ტექნიკურ განზომილებაში რევოლუციური გარდატეხა მოახდინა CHAMP (Counter-

Electronics High Power Microwave Advanced Missile) ტექნოლოგიამ. კორპორაცია Boeing-ისა და პენტაგონის ერთობლივი ძალისხმევით შექმნილი ეს იარაღი „მართული ენერგეტიკული იარაღია“.

CHAMP-ის უნიკალურობა იმაში მდგომარეობს, რომ შეუძლია ფიზიკური ნგრევის გარეშე, ელექტრომაგნიტური იმპულსების მეშვეობით:

- გაანადგუროს მოწინააღმდეგის ელექტროენერგიის სისტემები და ქსელები;
- მწყობრიდან გამოიყვანოს კომპიუტერები, რაკეტები, ტანკები და უპილოტო აპარატები;
- მოახდინოს მონაცემთა ბაზების გადაპროგრამება და კონტროლის ქვეშ აყვანა.

ეს არის იარაღი, რომელიც ატომურ ბომბსაც კი გამოუსადეგარს ხდის. CHAMP არის შეიარაღების ახალი ფილოსოფიის დასაწყისი, სადაც მთავარია არა ობიექტის აფეთქება, არამედ მისი ინფორმაციული და ენერგეტიკული „გულიდან“ გათიშვა.

6.6. გლობალური ინფორმაციული იარაღი და მედიის როლი

თანამედროვე ეტაპზე შემოდის „გლობალური ინფორმაციული იარაღის“ ცნება. მძლავრი ტელეკომპანიები (მაგალითად, CNN) და სოციალური მედია პლატფორმები ახდენს ომების დემონსტრირებას რეალურ დროში. ეს გავლენას ახდენს პოლიტიკური გადაწყვეტილებების მიღებაზე, რადგან საზოგადოებრივი აზრი

ყალიბდება იმაზე სწრაფად, ვიდრე სამხედრო შტაბები ანალიზს დაასრულებენ. გლობალური ინფორმაციული სივრცე დღეს ისეთივე მნიშვნელოვანი საბრძოლო გარემოა, როგორიც გეოგრაფიული ტერიტორია.

მეექვსე თავის დასკვნა

ინფორმაციული იარაღი, იქნება ეს ფსიქოლოგიური მანიპულაცია თუ CHAMP-ის მსგავსი ელექტრონული საშუალებები, საფუძვლიანად ცვლის ომის წარმოების წესებს. იგი შლის ზღვარს მშვიდობასა და ომს შორის და ნებისმიერ ადამიანს აქცევს პოტენციურ სამიზნედ. მომავლის უშიშროება დამოუკიდებელი იქნება არა მხოლოდ თავდაცვითი შეიარაღების რაოდენობაზე, არამედ იმაზე, თუ რამდენად დაცულია ქვეყნის ინფორმაციული ინფრასტრუქტურა და მისი მოქალაქეების ცნობიერება გარე დესტრუქციული ზემოქმედებისგან.

მეექვსე თავის საკონტროლო კითხვები:

1. *რატომ მიიჩნევა ინფორმაციული იარაღი მასობრივი განადგურების იარაღის ტოლფასად და რა სფეროებს აზიანებს იგი?*
2. *განმარტეთ განსხვავება ინფორმაციასა და ინფორმაციულ ტექნოლოგიას (როგორც იარაღს) შორის. რატომ არის ტექნოლოგია უფრო საშიში?*
3. *რაში მდგომარეობს CHAMP-ტექნოლოგიის რევოლუციური მნიშვნელობა და როგორ ცვლის ის ტრადიციული შეიარაღების ღირებულებას?*

მეთოდური ასპექტი:

ამ თავის შესწავლისას სტუდენტმა უნდა გააცნობიეროს, რომ კიბერსივრცე არის დამოუკიდებელი საბრძოლო პლატფორმა, სადაც თავდასხმა უფრო იაფი და ეფექტურია, ვიდრე თავდაცვა, რაც სრულიად ახლებურ სტრატეგიულ აზროვნებას მოითხოვს.

თავი VII
ინფორმაციული უშიშროება — ეროვნული უშიშროების სისტემის სტრატეგიული კომპონენტი

7.1. ეროვნული უშიშროების ფენომენი და მისი ევოლუცია

სახელმწიფოს არსებობა და მისი სუვერენიტეტის შენარჩუნება პირდაპირ კავშირშია მის უნართან, მუდმივ რეჟიმში უპასუხოს თანამედროვეობის მრავალფეროვან გამოწვევებს. უშიშროების მოთხოვნილება ადამიანის, საზოგადოებისა და სახელმწიფოსთვის მარადიული პრიორიტეტია. თუმცა, ინდუსტრიული ეპოქიდან ინფორმაციულ ეპოქაში გადასვლამ რადიკალურად შეცვალა ამ პრობლემის გააზრების მეთოდოლოგია. ინფორმაციის ქცევამ ცივილიზაციის დომინანტად წარმოშვა ახალი ტენდენციები პოლიტიკურ, სამხედრო და სოციალურ სფეროებში.

7.2. ეროვნული უშიშროების სტრუქტურა და ობიექტები

ტერმინი „უშიშროება“ ნაწარმოებია ძველი ქართული სიტყვისგან „უშიშობა“ და გვხვდება თხუთმეტსაუკუნოვან ქართულ წერილობით წყაროებში („ქართლის ცხოვრება“ და სხვა). როგორც პოლიტიკური მეცნიერების კატეგორია, „უშიშროება“ არის ადამიანის (საზოგადოების...) მიერ თავისი ძირითადი მოთხოვნილებების დაკმაყოფილებისა და საკუთარი უფლებების დაცულობის უზრუნველყოფაში მდგრადობის შეგრძნება; სხვანაირად -

პიროვნების, საზოგადოებისა და სახელმწიფოს სასიცოცხლო ინტერესების დაცული მდგომარეობა პოტენციური და რეალურად არსებული საშიშროების, გამოწვევისა და მუქარისაგან ან ამგვარი საშიშროების არარსებობა.

ეროვნული უშიშროება არის რთული, მრავალდონიანი სისტემა, რომელიც სამ ძირითად ობიექტზეა ორიენტირებული: **პიროვნება:** 1. მისი უფლებები და თავისუფლებები; 2. **საზოგადოება (ერი):** მისი მატერიალური და სულიერი ფასეულობები; 3. **სახელმწიფო:** მისი კონსტიტუციური წყობილება, სუვერენიტეტი და ტერიტორიული მთლიანობა.

თანამედროვე ეტაპზე ამ სისტემის შემადგენლობაში მოიაზრება არა მხოლოდ სამხედრო, არამედ ინფორმაციული, ეკონომიკური, ეკოლოგიური, ენერგეტიკული, დემოგრაფიული და სხვა უშიშროების ქვესისტემები. თითოეული ეს ქვესისტემა ურთიერთკავშირშია და ერთის დასუსტება მთლიანი ეროვნული მედეგობის რღვევას იწვევს.

ეროვნული უშიშროება უზრუნველყოფილია მაშინ, როდესაც სახელმწიფო ავლენს უნარს, დროულად ამოიცნოს მოსალოდნელი საფრთხეები და დროულად აირიდოს ისინი, ამით განამტკიცოს ერის მდგრადობა და სიცოცხლისუნარიანობა.

7.3. ტერმინოლოგიური დიფერენციაცია: „უშიშროება“ და „უსაფრთხოება“

ქართულ სამეცნიერო სივრცეში აუცილებელია მკაფიო ზღვრის გავლება ტერმინებს – „უსაფრთხოებასა“ და „უშიშროებას“ შორის:

- ტერმინ „უსაფრთხოების“ გენეზისი: ენობრივი ანალიზი აჩვენებს, რომ ეს ტექნიკური ტერმინი ქართულ მეტყველებაში 1932 წელს, რუსული ენიდან თარგმნის შედეგად, ხელოვნურად შემოვიდა (მაგ., „Техника безопасности“ – „უსაფრთხოების ტექნიკა“). იგი ისტორიულად ასოცირდება ფიზიკურ და ტექნიკურ დაზიანებებთან (შრომის უსაფრთხოება, საგზაო უსაფრთხოება) და არა პოლიტიკურ სტრატეგიებთან.

- ტერმინ „უშიშროების“ ისტორიული კონტექსტი: განსხვავებით „უსაფრთხოებისგან“, „უშიშროება“ არის ძირძველი ქართული სოციალურ-პოლიტიკური ტერმინი, რომელიც უძველესი დროიდან გამოიყენებოდა მატიანეში, პოლიტიკურ ნაწერებსა და კონსტიტუციურ დონეზე (1921 და 1995 წლების კონსტიტუციები).

ტერმინოლოგიური დიფერენციაცია:
უშიშროება (Security) და უსაფრთხოება (Safety)

მახასიათებლები	უშიშროება (Security)	უსაფრთხოება (Safety)
საფრთხის ბუნება	განზრახული, მიზანმიმართული, ორგანიზებული და მტრული.	შემთხვევითი, ტექნიკური ან ბუნებრივი, უყურადღებობა...
სუბიექტი	არსებობს ცნობიერი მოწინააღმდეგე (მტერი, აგრესორი).	მოწინააღმდეგე არ არსებობს, არსებობს მხოლოდ რისკი.
პრევენციის მეთოდი	სტრატეგიული დაგეგმვა, სოციალურ-პოლიტიკური აქტივობები.	საინჟინრო-ტექნიკური და სანიტარიულ-ჰიგიენური ზომები.
ისტორიული კონტექსტი	ძირძველი ქართული აკადემიური ტერმინი.	1932 წელს რუსული ენიდან გადმოქართულებული ტექნიკური ტერმინი.
მოქმედების სფერო	სახელმწიფო, პოლიტიკა, კიბერსივრცე, დაზვერვა...	ტექნიკა, მშენებლობა, ეკოლოგია, საყოფაცხოვრებო..
მაგალითები	ეროვნული უშიშროება, სახელმწიფო უშიშროება...	საგზაო უსაფრთხოება, სახანძრო უსაფრთხოება...

7.4. კიბერუსაფრთხოებიდან კიბერუშიშროებამდე: სოციოტექნოლოგიური ტრანსფორმაცია და ტერმინოლოგიური დიფერენციაცია

საინფორმაციო ეპოქის თანამდევმა პროცესებმა ფუნდამენტურად შეცვალა კიბერსივრცეში არსებული გამოწვევების ბუნება. თუ ადრე კიბერუსაფრთხოების უზრუნველყოფა განიხილებოდა როგორც წმინდა ტექნიკური ხასიათის საქმიანობა, დღეს იგი გასცდა ინფორმაციული ტექნოლოგიების ვიწრო სფეროს და კომპლექსურ პოლიტიკურ ამოცანად იქცა. შესაბამისად, პრობლემის გადაჭრის პროცესში, ტექნიკურ მეცნიერებებთან ერთად, აქტიურად ერთვება სოციალური და ჰუმანიტარული დისციპლინები.

ამ სოციოტექნოლოგიურ გარდაქმნას ადასტურებს საერთაშორისო სამეცნიერო პრაქტიკაც. კერძოდ, ციურიხის უშიშროების კვლევის ცენტრის მკვლევრების - **მირიამ დან კაველტისა** (M. Dunn Cavelty) და **ანდრიას ვენგერის** (A. Wenger) რედაქტორობით გამოცემული ნაშრომი „კიბერუშიშროების პოლიტიკა: სოციალურ-ტექნოლოგიური გარდაქმნები და პოლიტიკური ფრაგმენტაცია“ ნათლად აჩვენებს, რომ კიბერუშიშროება დღეს სხვადასხვა სფეროს მრავალ ავტორთა მიერ განიხილება, როგორც სოციალურ-ტექნოლოგიური გაურკვევლობით განსაზღვრული საკითხი. მკვლევრები ხაზს უსვამენ, რომ ტექნიკური სისტემების ინტეგრაცია საზოგადოებრივ და ეკონომიკურ ცხოვრებაში გარდაუვალს ხდის კიბერპრობლემების გავრცელებას პოლიტიკის სფეროზე, რაც მოითხოვს ტექნიკური

კვლევების სინთეზს პოლიტიკურ და სოციალურ მეცნიერებებთან.

პრაქტიკული გამოყენების სფეროები და კლასიფიკაცია. დღეს არსებული ვითარება ორგვარ მიდგომას საჭიროებს.

თუ კვლევის ობიექტია კომპიუტერული ქსელების, პროგრამებისა და მონაცემთა ბაზების ტექნიკური დაცვა ციფრული თავდასხმებისგან, მართებულია ტერმინ „**კიბერუსაფრთხოების**“ გამოყენება.

თუმცა, როდესაც საუბარია სახელმწიფო პოლიტიკაზე, ეროვნულ ინტერესებზე, სტრატეგიულ დაგეგმარებასა და საერთაშორისო ურთიერთობებზე, უნდა დამკვიდრდეს ტერმინი „**კიბერუშიშროება**“.

ამ განსხვავების მეცნიერულ დონეზე ასასახად, საქართველოში მიზანშეწონილია კლასიფიკატორების (UDC, SCOPUS, სწავლის სფეროების კლასიფიკატორი) მიხედვით შემდეგი გამიჯვნა:

- **„უსაფრთხოება“**: ინფორმაციული ტექნოლოგიები, კომპიუტერული მეცნიერებები (UDC 004; SCOPUS 1700-1708).
- **„უშიშროება“**: სოციალური მეცნიერებები, პოლიტიკა, სამართალი, საერთაშორისო ურთიერთობები, თავდაცვა (UDC 3; SCOPUS 3300; 2000).

ამრიგად, კიბერუშიშროება უნდა მოვიაზროთ, როგორც ქვეყნის ეროვნული უშიშროების ერთიანი სისტემის შემადგენელი ნაწილი, ხოლო „კიბერუსაფრთხოება“ — მის ტექნიკურ კომპონენტად. აუცილებელია,

საქართველოს განათლებისა და მეცნიერების სამინისტრომ ასახოს ეს შინაარსობრივი სხვაობა ეროვნული კვალიფიკაციების ჩარჩოსა და სწავლის სფეროების კლასიფიკატორში, რათა თავიდან იქნეს აცილებული აზრობრივი აღრევა და უზრუნველყოფილ იქნეს დარგობრივი სიზუსტე.

ტერმინოლოგიური დიფერენციაცია:
კიბერუშიშროება და კიბერუსაფრთხოება

მახასიათებლები	კიბერუშიშროება	კიბერუსაფრთხოება
მეცნიერული სფერო ⇨	სოციალური მეცნიერებები, პოლიტიკა, სამართალი	ინფორმაციული ტექნოლოგიები, კომპიუტერული მეცნიერებები
განათლების კლასიფიკატორი ⇨	UDC 3; SCOPUS 3300; 2000	UDC 004; SCOPUS 1700-1708
პრევენციის მეთოდი ⇨	სტრატეგიული დაგეგმვა, სოციალურ-პოლიტიკური აქტივობები, კანონი, დიპლომატია...	კოდი, ალგორითმი ან აპარატურა
მიზანი ⇨	ეროვნული ინტერესებისა და სუვერენიტეტის დაცულობა	მონაცემთ მთლიანობისა და სისტემური მდგრადობის უზრუნველყოფა
მოქმედების სფერო ⇨	სახელმწიფო, პოლიტიკა, სტრატეგიული დაგეგმარება, საერთაშორისო ურთიერთობები...	კომპიუტერული ქსელების, პროგრამებისა და ბაზების ტექნიკური დაცვა
აქტორები ⇨	სახელმწიფო უწყებები, სპეცსამსახურები, პოლიტიკური სუბიექტები	პროგრამისტები, IT სპეციალისტები, სისტემური ადმინისტრატორები

7.5. ინფორმაციული უშიშროება: აქტორები და მუქარები

ინფორმაციული უშიშროება გულისხმობს ინფორმაციულ სფეროში ქვეყნის ეროვნული ინტერესების დაცულობას. ინფორმაციულ ეპოქაში იგი იქცა ეროვნული უშიშროების უმნიშვნელოვანეს კომპონენტად. ამ სფეროში წარმატების გარეშე სახელმწიფო ვერ მიაღწევს უპირატესობას

ვერც ეკონომიკურ და ვერც სამხედრო-პოლიტიკურ ასპარეზზე.

ინფორმაციული უშიშროების საფრთხეები შეიძლება გამოვლინდეს სხვადასხვა დონეზე:

- **სახელმწიფო დონეზე:** როდესაც მტრული ძალები მანიპულირებს გადაწყვეტილებათა მიღების პროცესით.
- **ტექნოლოგიურ დონეზე:** ქვეყნის დამოკიდებულება უცხოურ საინფორმაციო ინფრასტრუქტურაზე და ტექნოლოგიური ჩამორჩენა.
- **სოციალურ დონეზე:** საზოგადოების ეროვნულ-სახელმწიფოებრივი საფუძვლების მორყევა დეზინფორმაციისა და საინფორმაციო ექსპანსიის გზით.

სუსტი სახელმწიფოებისთვის მუდმივ მუქარას წარმოადგენს საგარეო აქტორების ჩარევა შიგა პოლიტიკურ პროცესებში, რაც იწვევს ინსტიტუტების დელეგიტიმაციას და სახელმწიფო მმართველობის დეზორგანიზაციას.

მეშვიდე თავის დასკვნა

ეროვნული უშიშროება არის დინამიკური სისტემა, რომლის ეფექტურობა დამოკიდებულია საფრთხეების სწორ კლასიფიკაციასა და მართვაზე. ინფორმაციული უშიშროება ამ სისტემის ის „ხერხემალია“, რომელიც აკავშირებს პიროვნებას, საზოგადოებასა და სახელმწიფოს. ტერმინოლოგიური სიზუსტე („უშიშროება“ და „უსაფრთხოება“) არ არის მხოლოდ ლინგვისტური საკითხი — ეს არის მეთოდოლოგიური საფუძველი,

რომელიც განსაზღვრავს სახელმწიფო პოლიტიკის მიმართულებასა და ქვეყნის მზაობას გლობალური გამოწვევებისადმი.

ქართულ სამეცნიერო სივრცეში ტერმინოლოგიური წესრიგის აღდგენა არ არის მხოლოდ ლინგვისტური საკითხი; ეს არის ეროვნული უშიშროების სისტემის ეფექტური ფუნქციონირების წინაპირობა.

მეშვიდე თავის საკონტროლო კითხვები:

1. *განმარტეთ ტერმინების — „კიბერუშიშროება“ და „კიბერუსაფრთხოება“ შინაარსობრივი განსხვავება და მოიყვანეთ მათი გამოყენების მაგალითები.*
2. *ჩამოთვალეთ ეროვნული უშიშროების ძირითადი ობიექტები და ქვესისტემები. რატომ ითვლება ინფორმაციული უშიშროება მათ დამაკავშირებელ რგოლად?*
3. *როგორ ვითარდება საფრთხის, გამოწვევისა და მუქარის დინამიკური ჯაჭვი და რა როლი აქვს ამ პროცესში სახელმწიფოს პროგნოზირების უნარს?*

მეთოდური ასპექტი:

სტუდენტმა უნდა გაიაზროს, რომ ციფრული ტექნოლოგიების ხელმისაწვდომობამ ტერორიზმს მისცა გლობალური მასშტაბი და შექმნა საფრთხე, რომელსაც ფიზიკური საზღვრები არ გააჩნია.

თავი VIII
საერთაშორისო სამოქმედო სტრატეგია კიბერსივრცეში

8.1. კიბერსივრცის გლობალური მილიტარიზაცია და პოლიტიკური დილემები

დღეისათვის მსოფლიოს მრავალი სახელმწიფო აქტიურად ავითარებს შეტევით შესაძლებლობებს კიბერსივრცეში. ეს პროცესი, რომელსაც ხშირად კიბერსივრცის „მილიტარიზაციას“ უწოდებენ, საერთაშორისო ურთიერთობების ერთ-ერთ ყველაზე მწვავე გამოწვევად იქცა. გაეროს წევრ ქვეყნებს შორის არსებობს ფუნდამენტური აზრთა სხვადასხვაობა ამ სფეროს რეგულირების შესახებ:

- **ავტორიტარული მოდელი (რუსეთი, ჩინეთი, ირანი):** ისინი ოფიციალურად ითხოვენ კიბერსივრცეში შეტევითი ოპერაციების აკრძალვას და უარს ამბობენ საკუთარი შეტევითი პოლიტიკის აღიარებაზე. მოითხოვენ ახალი, სავალდებულო საერთაშორისო ხელშეკრულებების მიღებას, რადგან მიიჩნევენ, რომ არსებული საერთაშორისო ჰუმანიტარული სამართალი არასაკმარისია.
- **დასავლური მოდელი (აშშ და მოკავშირეები):** კიბერშესაძლებლობების ღიად განხილვისა და გამჭვირვალობის პრინციპების დაცვის მომხრეა. მათი პოზიციით, არსებული საერთაშორისო სამართალი სრულად ფარავს კიბერსივრცესაც. დასავლეთისთვის მთავარია არა აკრძალვა,

არამედ ქცევის წესების სტანდარტიზაცია და პროგნოზირება.

ამ კონტექსტში განსაკუთრებით მნიშვნელოვანია **კიბერ-შეკავების ინიციატივა (CDI)**, რომელიც აშშ-მა 2019 წელს დანერგა და მიზნად ისახავს მოკავშირეებთან ერთობლივი მოქმედებით ნებისმიერი აგრესიის მოგერიებას.

8.2. წამყვანი სახელმწიფოების კიბერსტრატეგიები

საერთაშორისო ასპარეზზე კიბერპოლიტიკას განსაზღვრავს რამდენიმე ძირითადი აქტორის მიდგომა:

1. **აშშ:** ეროვნული უშიშროების აქტის (განსაკუთრებით 1642-ე მუხლის) მიხედვით, აშშ-ის თავდაცვის დეპარტამენტს უფლებამოსილება აქვს განახორციელოს შეტევითი ოპერაციები ოთხი სახელმწიფოს — რუსეთის, ჩინეთის, ჩრდილოეთ კორეისა და ირანის წინააღმდეგ. აშშ უფლებას იტოვებს იმოქმედოს სხვა ქვეყნების თანხმობის გარეშე, თუ საფრთხე მის ეროვნულ ინტერესებს ემუქრება.
2. **დიდი ბრიტანეთი:** სამთავრობო კომუნიკაციების შტაბის (GCHQ) მეშვეობით აქტიურად უპირისპირდება კიბერკრიმინალებს. ლონდონი მიიჩნევს, რომ საერთაშორისო სამართლის ინტერპრეტაცია კიბერსივრცეში ჯერ კიდევ ბუნდოვანია და მეტ პრაქტიკულ დაზუსტებას საჭიროებს.
3. **ავსტრალია და კანადა:** ორივე ქვეყანამ ოფიციალურად აღიარა შეტევითი კიბერშესაძლებლო-

ბების განვითარების აუცილებლობა. კანადის „კომუნიკაციების უსაფრთხოების აქტი“ პირდაპირ იძლევა შეტევითი ოპერაციების წარმოების უფლებას ქვეყნის გარეთ.

8.3. ნატოს ხედვა და კოლექტიური უშიშროება

ნატოს 2021 წლის თავდაცვის მინისტრების შეხვედრაზე საერთაშორისო ტერორიზმთან ერთად კიბერსაფრთხეები პირველი რიგის ამოცანად დასახელდა. ალიანსი აძლიერებს მუშაობას რამდენიმე მიმართულებით:

- კრიტიკული ინფრასტრუქტურის წინააღმდეგ კიბერშეტევების პრევენცია;
- კიბერთავდაცვის ინტეგრირება სახმელეთო, საზღვაო და საჰაერო ოპერაციებთან;
- ზარალის მინიმიზაცია და სისტემების სწრაფი აღდგენა. ნატოს გენერალური მდივნის განცხადებით, იგეგმება ახალი კიბერფორმირებების შექმნა, რომლებიც ალიანსის წევრებს „სახიფათო საგარეო აქტორებისგან“ დაიცავს.

8.4. კიბერსივრცის ანატომია: ფიზიკურიდან ვირტუალურამდე

კიბერსივრცე (Cyberspace) არის გლობალური და მუდმივცვალებადი სფერო, რომელიც მოიცავს:

- **ფიზიკურ შრეს:** კომპიუტერები, სერვერები, კაბელები, სატელიტური მოწყობილობები.

- **ლოგიკურ შრეს:** პროგრამული უზრუნველყოფა და კოდები, რომლებიც სისტემის ფუნქციონირებას უზრუნველყოფს.
- **ქსელურ შრეს:** ინტერნეტი (ქსელთა ქსელი) და ინტრანეტი (შიგა ქსელები).
- **მონაცემთა შრეს:** თავად ციფრული ინფორმაცია.

ამ სფეროს მთავარი თვისება ის არის, რომ არ არსებობს ცენტრალური სუბიექტი, რომელიც მას სრულად აკონტროლებს. ძალაუფლება აქ გაფანტულია ათასობით ნაკადში. ფილოსოფოსი **მიშელ ფუკო** ასეთი სივრცეების აღსაწერად იყენებდა ტერმინს **ჰეტეროტოპია** — ადგილი, რომელიც ერთდროულად ფიზიკურიცაა და ფსიქიკურიც.

8.5. ტერმინის ევოლუცია: უსინგიდან გიბსონამდე

საინტერესოა ტერმინ „კიბერსივრცის“ წარმოშობა. იგი პირველად მხატვრობაში გაჩნდა **სუზანა უსინგთან** (Susanne Ussing) და **კარსტენ ჰოფთან** (Carsten Hoff), როგორც ღია სისტემების პრინციპზე დაფუძნებული „სენსორული სივრცე“. თუმცა, მისი თანამედროვე პოპულარიზაცია მწერალ **უილიამ გიბსონს** (William Gibson) უკავშირდება. მან რომანში „ნეირომანსერი“ კიბერსივრცე აღწერა, როგორც „კონსენსუალური ჰალუცინაცია“ — კომპიუტერული სისტემების ჩანაცვლება ადამიანის გონებაში.

მაიკლ ბეტი (Michael Batty) კი კიბერსივრცის ოთხ დონეს გამოყოფს: **ადგილი, ვირტუალური სივრცე, კიბერსივრცე და კიბერადგილი.** ეს მოდელი გვიჩვენებს,

რომ ციფრული სამყარო მუდმივად „შეხებაშია“ რეალურ გეოგრაფიულ გარემოსთან.

8.6. საპროექტო კიბერსივრცის 4 ძირითადი მახასიათებელი

თანამედროვე ინტერპრეტაციით, კიბერსივრცე შემდეგი ნიშნებით ხასიათდება:

1. **ინფრასტრუქტურულობა:** ინტერნეტი, მისი რესურსები და მომსახურება.
2. **ვირტუალურობა:** კომპიუტერული ქსელების მიერ შექმნილი ალტერნატიული რეალობა.
3. **სოციალურობა:** მეგაქსელი, სადაც ინდივიდები და ჯგუფები გლობალურ რესურსებს იყენებს.
4. **დინამიკურობა:** ევოლუციონირებადი, რთული სისტემა, რომელიც მუდმივად იცვლება.

მერვე თავის დასკვნა

კიბერსივრცეში საერთაშორისო სტრატეგიები დღეს პოლიტიკური და სამხედრო ძალაუფლების გადანაწილების მთავარი იარაღია. აშშ-ის მცდელობა, შექმნას პარტნიორული კიბერუშიშროების სისტემა, პასუხია იმ საფრთხეებზე, რომლებიც ეროვნულ ეკონომიკასა და სტაბილურობას ემუქრება. კიბერსივრცის დაცვა აღარ არის მხოლოდ ტექნიკური ამოცანა, ეს არის გლობალური დიპლომატიისა და კოლექტიური თავდაცვის ახალი ფრონტი, სადაც გამარჯვება დამოკიდებულია საერთაშორისო თანამშრომლობასა და ტექნოლოგიურ უპირატესობაზე.

მერვე თავის საკონტროლო კითხვები:

1. *რა ძირითადი განსხვავებაა კიბერსივრცის რეგულირების „დასავლურ“ და „ავტორიტარულ“ (რუსეთი, ჩინეთი) მოდელებს შორის?*
2. *განმარტეთ აშშ-ის „კიბერშეკავების ინიციატივის“ (CDI) არსი და მისი მნიშვნელობა საერთაშორისო პარტნიორობისთვის.*
3. *ჩამოთვალეთ კიბერსივრცის ოთხი ძირითადი მახასიათებელი და ახსენით, რატომ არის ინტერნეტი ამ ფართო ცნების მხოლოდ ნაწილი.*

მეთოდური ასპექტი:

სტუდენტს უნდა ჩამოუყალიბდეს ხედვა, რომ ქვეყნის უშიშროება მისი საინფორმაციო, ენერგეტიკული და ფინანსური სისტემების მდგრადობის პირდაპირპრო-პორციულია.

თავი IX
საერთაშორისო სამართალი და ომი კიბერსივრცეში

9.1. კიბერსივრცე, როგორც საერთაშორისო სამართლის ახალი ობიექტი

ინფორმაციულ ეპოქაში სახელმწიფოთა დაპირისპირება სცილდება კლასიკური სამხედრო კონფლიქტის ჩარჩოებს. დღეს სულ უფრო ხშირად საუბრობენ ეკონომიკურ, დიპლომატიურ და ინფორმაციულ ომებზე. თუმცა, საერთაშორისო სამართლისთვის მთავარი გამოწვევა კიბერსივრცეში წარმოებული ოპერაციების სამართლებრივი კვალიფიკაციაა.

კიბერსივრცეში ომის პრობლემატიკა აიძულებს იურისტებს, ახლებურად გააზრონ ტრადიციული ნორმები. ტერმინი „ინფორმაციული ომი“, რომელიც თომას რონამ (Thomas P. Rona) ჯერ კიდევ 1976 წელს შემოიტანა, დღეს უკვე მოითხოვს მკაცრ საერთაშორისო-სამართლებრივ რეგულირებას. ინფორმაციული ზემოქმედება შეიძლება მიმართული იყოს სახელმწიფოს ეროვნული უშიშროების ისეთი კრიტიკული ობიექტების წინააღმდეგ, როგორიცაა საბანკო-საფინანსო სისტემები, ენერგეტიკული ქსელები და ნავიგაცია. ასეთი ქმედებების შეზღუდვა და პასუხისმგებლობის დაკისრება თანამედროვე სამართლის უმთავრესი ამოცანაა.

9.2. ინფორმაციული ომი და შეიარაღებული კონფლიქტის დეფინიცია

სამართლებრივი თვალსაზრისით, რთულია გაივლოს ზღვარი „არამეგობრულ მოქმედებასა“ და „შეიარაღებულ კონფლიქტს“ შორის კიბერსივრცეში. **გრეგორი რატრეი** (Gregory J. Rattray) და სხვა ექსპერტები აღნიშნავენ, რომ ინფორმაციული ომის შედეგები შეიძლება იყოს ისეთივე მასშტაბური, როგორც კლასიკური ომის — მოიტანოს მსხვერპლი და ნგრევა.

მთავარი სამართლებრივი კითხვებია:

- ვინ ჩაითვალოს ასეთი ომის მონაწილედ და როგორ განისაზღვროს **კომბატანტის** სტატუსი ციფრულ სამყაროში?
- მიიღებენ თუ არა სამხედრო ტყვის სტატუსს სამოქალაქო პირები, რომლებიც სხვა კონტინენტიდან კლავიატურით ახორციელებენ შეტევას?
- არის თუ არა ინფორმაციული ომი შეიარაღებული კონფლიქტის ნაირსახეობა, თუ ის საერთაშორისო სამართლის მიღმა მყოფი „არასამხედრო“ ქმედებაა?

ინფორმაციული ომი შეიძლება განვიხილოთ, როგორც საბრძოლო მოქმედების წარმოების ერთ-ერთი ხერხი, სადაც ინფორმაციული იარაღი (ვირუსები, ლოგიკური ბომბები) სტრატეგიული უპირატესობის მისაღწევად გამოიყენება.

9.3. საერთაშორისო ჰუმანიტარული სამართლის ნორმები და კიბერსივრცე

მიუხედავად იმისა, რომ ზოგიერთი მკვლევარი ეჭვქვეშ აყენებს „ინფორმაციული ომის“ კლასიკურ გაგებას,

საყოველთაოდ მიღებულია, რომ ნებისმიერი კონფლიქტი უნდა დარჩეს საერთაშორისო ჰუმანიტარული სამართლის (სჰს) ჩარჩოებში. ეს ნიშნავს, რომ კიბერსივრცეში ომის წარმოებისას გამოყენებული უნდა იქნეს როგორც **ჟენევის**, ისე **ჰააგის სამართალი**.

პროფესორი **მიხაელ ნ. შმიდტი** (Michael N Schmitt) მიიჩნევს, რომ ინფორმაციული ეპოქის იარაღი (თვითდამიზნებადი სისტემები) პირიქით, ეხმარება ჰუმანიტარული სამართლის პრინციპების რეალიზაციას, რადგან სამხედრო და სამოქალაქო ობიექტების მკაფიო გამიჯვნის საშუალებას იძლევა. იარაღის შერჩევითობა ამცირებს უდანაშაულო მსხვერპლს, თუმცა ადამიანის ბოროტ განზრახვას შეუძლია იგივე ტექნოლოგია სამოქალაქო ინფრასტრუქტურის წინააღმდეგ მიმართოს.

9.4. ინფორმაციული იარაღის კლასიფიკაცია და სამართლებრივი აკრძალვები

საერთაშორისო სამართალი ინფორმაციულ იარაღს სამ ძირითად კატეგორიად ყოფს:

1. **დისტანციური განადგურების სისტემები:** კომპიუტერული ვირუსები და ლოგიკური ბომბები.
2. **ელექტრონული ჯაშუშები:** არასანქცირებული წვდომისა და ინფორმაციის მოპარვის სისტემები.
3. **ფსიქოლოგიური ზემოქმედების სისტემები:** მულტიმედიური საშუალებები, რომლებიც გავლენას ახდენენ მომხმარებლის ფსიქიკაზე.

ინფორმაციული შეტევა ატომურ ელექტროსადგურზე ან წყალმომარაგების სისტემაზე, მიუხედავად იმისა, რომ

ტანკებს არ საჭიროებს, თავისი შედეგებით მასობრივი განადგურების იარაღის ტოლფასია. ჟენევის კონვენციის დამატებითი ოქმები პირდაპირ კრძალავს თავდასხმას ისეთ ობიექტებზე, რომლებიც „ბუნების საშიშ ძალებს“ შეიცავს.

9.5. შიმოდის საქმე და ახალი იარაღის ლეგალურობა

საინტერესო სამართლებრივი პრეცედენტია „შიმოდისა და სხვათა საქმე იაპონიის წინააღმდეგ“ (1955-1963). ტოკიოს სასამართლომ დაადგინა, რომ ახალი სახის იარაღის გამოყენება ნებადართულია მანამ, სანამ არ იარსებებს მისი ამკრძალავი სპეციალური ხელშეკრულება. თუმცა, სასამართლომ ხაზი გაუსვა, რომ იარაღი, რომელიც იწვევს **ზედმეტ ტანჯვას** ან **არაშერჩევით ზიანს**, საერთაშორისო სამართლის პრინციპებს ეწინააღმდეგება.

ეს პრინციპი სრულად ვრცელდება ინფორმაციულ იარაღზეც. ჟენევის კონვენციის 36-ე მუხლი ავალდებულებს სახელმწიფოებს, ახალი იარაღის შექმნისას გაარკვიონ, ხვდება თუ არა მისი გამოყენება საერთაშორისო სამართლის აკრძალვებში.

9.6. საშინაო საქმეებში ჩაურევლობის პრინციპი და "ცივი" კიბერომი

შეუიარაღებელი ინფორმაციული დაპირისპირება (იდეოლოგიური ჩარევა, პროპაგანდა) აკრძალულია სახელმწიფოს საშინაო საქმეებში ჩაურევლობის პრინციპით. ჯერ კიდევ 1953 წელს სსრკ ცდილობდა „იდეოლოგიური

აგრესიის“ დეფინიციის დამკვიდრებას, თუმცა საერთაშორისო თანამეგობრობამ იგი პროპაგანდისტულად მიიჩნია.

დღეს ინტერნეტის პირობებში ძალზე რთულია გაკონტროლდეს ზემოქმედების წყარო. თუ ინფორმაციული ზემოქმედების მიზანია სხვა სახელმწიფოს იძულება, დამორჩილდეს მას საკუთარი სუვერენული უფლებების განხორციელებისას, ეს ცალსახად საერთაშორისო სამართლის დარღვევაა, თუმცა „ომის“ ცნების გაფართოებას და მასში ეკონომიკური ან ინფორმაციული მუქარის შეტანას მსოფლიო სახელმწიფოები კვლავ სიფრთხილით ეკიდებიან.

მეცხრე თავის დასკვნა

ინფორმაციული ომები უნდა რეგულირდებოდეს საერთაშორისო ჰუმანიტარული სამართლით. მიუხედავად იმისა, რომ კიბერსივრცეში კომბატანტისა და იარაღის დეფინიციები კვლავაც დისკუსიის საგანია, ფუნდამენტური პრინციპები — სამოქალაქო პირების დაცვა, შერჩევითობა და ზედმეტი ტანჯვის აკრძალვა უცვლელი რჩება. მომავლის სამართლებრივი სისტემა მზად უნდა იყოს, რათა „პროცესორითა და კლავიატურით შეიარაღებული“ პირების ქმედებები საერთაშორისო პასუხისმგებლობის ჩარჩოებში მოაქციოს.

მეცხრე თავის საკონტროლო კითხვები:

1. *ვინ ითვლება „კომბატანტად“ საერთაშორისო სამართალში და რა სირთულეებს აწყდება ეს დეფინიცია კიბერომის კონტექსტში?*

2. *როგორ იცავს ჟენევისა და ჰააგის სამართალი ობიექტებს, რომლებიც „ბუნების საშიშ ძალებს“ შეიცავს (მაგ., ატომური ელექტროსადგური) კიბერშეტევისგან?*
3. *განიხილეთ „შიმოდის საქმის“ მნიშვნელობა ახალი ტიპის იარაღის ლეგალურობის შეფასების პროცესში.*

მეთოდური ასპექტი:

სტუდენტმა უნდა ისწავლოს ჰიბრიდული საფრთხეების ამოცნობა და გააცნობიეროს, რომ დეზინფორმაცია იარაღია, რომელიც მიმართულია საზოგადოების ერთიანობისა და სახელმწიფო ინსტიტუტებისადმი ნდობის რღვევისკენ.

თავი X
ინფორმაციული ომი და სახელმწიფო საინფორმაციო პოლიტიკა

10.1. საინფორმაციო გარემო და სახელმწიფო უშიშროების პრიორიტეტები

საზოგადოების სტაბილური ფუნქციონირება პირდაპირდამოკიდებულია საინფორმაციო გარემოს განვითარების დონესა და მის უშიშროებაზე. ვინაიდან ინფორმაციული ინფრასტრუქტურა თანამედროვე ინფორმაციული იარაღის მთავარ სამიზნეა, მისი დაცვა სახელმწიფო პოლიტიკის უპირველეს პრიორიტეტად იქცა. ამ სფეროში არსებული საფრთხეების დროული აღმოჩენა, შეფასება და რანჟირება ეროვნული უშიშროების სისტემის ეფექტურობას განსაზღვრავს.

საერთაშორისო კიბერსივრცეში ინფორმაციული ომის წარმოების პირობებში, სახელმწიფო ვალდებულია განახორციელოს წინმსწრები ეკონომიკური, პოლიტიკური და ორგანიზაციული ღონისძიებები. ინფორმაციული იარაღის ნეიტრალიზაციისათვის აუცილებელი საბრძოლო არსენალი მოიცავს როგორც ტექნიკურ დაცვას, ისე სამართლებრივ და საგანმანათლებლო კომპონენტებს.

10.2. ინფორმაციული უშიშროების უზრუნველყოფის სტრატეგიული ნაბიჯები

კიბერსივრცეში წარმატებული თავდაცვისა და სახელმწიფო ინტერესების დაცვისათვის აუცილებელია შემდეგი კომპლექსური ღონისძიებების რეალიზაცია:

1. **ობიექტების დაცვა:** მონაცემთა ბაზებისა და მატერიალურ-ტექნიკური ობიექტების უწყვეტი ფუნქციონირების გარანტირება.
2. **არასანქცირებული წვდომის აღკვეთა:** ინფორმაციის დაცვა დამახინჯებისა და განადგურებისაგან.
3. **მონიტორინგი:** საერთაშორისო ქსელებში ინფორმაციის გაცვლაზე მუდმივი კონტროლის დაწესება.
4. **საერთაშორისო თანამშრომლობა:** პარტნიორობა ღია ქსელებში ტექნიკური უსაფრთხოების საერთო სტანდარტების დასამკვიდრებლად.
5. **საკანონმდებლო ბაზა:** ეროვნული კანონმდებლობის შექმნა, რომელიც დაარეგულირებს მსოფლიო ქსელების მომხმარებელთა უფლებებსა და პასუხისმგებლობებს.
6. **კადრების მომზადება:** როგორც მასობრივი მომხმარებლის, ისე მაღალკვალიფიციური სპეციალისტების მომზადება და გადამზადება.
7. **ინფორმაციული ჰიგიენა:** ღია ქსელებით გადასაცემად დაუშვებელი ინფორმაციის ნუსხის მკაცრი განსაზღვრა.
8. **კულტურული მედეგობა:** ტრადიციული სულიერი ფასეულობების, კულტურული და ისტორიული მემკვიდრეობის დაცვა გარე ინფორმაციული ექსპანსიისაგან.

10.3. საინფორმაციო პოლიტიკის დიალექტიკა: ფართო და ვიწრო გაგება

პოლიტოლოგიურ ჭრილში „საინფორმაციო პოლიტიკა“ ორ დონეზე განიხილება:

- **ფართო გაგებით:** პოლიტიკური ზემოქმედება ყველა სფეროში (ეკონომიკა, სამხედრო საქმე, სამართალი) ხორციელდება ინფორმაციული მეთოდებით. ინფორმაცია მმართველობის მთავარი ინსტრუმენტია.
- **ვიწრო გაგებით:** საორგანიზაციო და საკონტროლო საქმიანობა უშუალოდ ინფორმაციული მეთოდების სფეროში (მაგ., ახალი ტექნოლოგიების მხარდაჭერა, კიბერუშიშროებისა და კიბერუსაფრთხოების სტანდარტების დაწესება).

ეს ორი დონე ერთმანეთთან მიმართებაშია, როგორც სისტემა და ქვესისტემა. ვიწრო გაგების საინფორმაციო პოლიტიკა ამზადებს ინსტრუმენტებს, რათა ფართო გაგების საინფორმაციო პოლიტიკამ მიაღწიოს დასახულ სტრატეგიულ მიზნებს. ამ ორი დონის ჰარმონიული შერწყმის გარეშე ინფორმაციულ ეპოქაში სახელმწიფო მმართველობა არაეფექტურია.

10.4. საინფორმაციო კანონმდებლობა და სუვერენიტეტის დაცვა

საერთაშორისო კიბერსივრცეში სუვერენიტეტის დაცვის ერთადერთი გზა მყარი ეროვნული საინფორმაციო კანონმდებლობის ჩამოყალიბებაა. საინფორმაციო სამართლის ნორმებმა უნდა განსაზღვროს კიბერსივრცეში საქმიანობის ერთიანი წესები.

სამეცნიერო კვლევასა და სამართლებრივ რეგულირებას პრაქტიკული მნიშვნელობა აქვს: სახელმწიფომ უნდა შეძლოს საკუთარი კიბერსივრცის „შემოსაზღვრა“ არა ფიზიკური კედლებით, არამედ იურიდიული და ტექნოლოგიური მექანიზმებით. ეს არის ერთადერთი გზა, რათა საქართველო არ გახდეს სხვა სახელმწიფოების მანიპულირების ობიექტად.

10.5. სახელმწიფო საინფორმაციო პოლიტიკის ფუნქციური ამოცანები

სახელმწიფომ უნდა ჩამოაყალიბოს ერთიანი საერთო-სახელმწიფოებრივი სტრუქტურა, რომელიც მოიცავს:

1. **საინფორმაციო რესურსების სისტემას:** სახელმწიფო და არასახელმწიფო მონაცემთა ერთობლიობა.
2. **საინფორმაციო ინდუსტრიას:** ადგილობრივი ტექნოლოგიური და საწარმოო პოტენციალის განვითარება.
3. **პროფესიულ განათლებას:** კადრების მომზადება კიბერომებისა და ინფორმაციული ანალიზის სფეროში.
4. **პროგნოზირების ტექნოლოგიებს:** შესაძლო ინფორმაციული შეტევების შედეგების წინასწარი მოდელირება.

10.6. ტექნოლოგიური პერსპექტივა: Li-Fi და ინფორმაციის გადაცემის მომავალი

საინფორმაციო პოლიტიკამ უნდა გაითვალისწინოს ტექნოლოგიური ინოვაციების ტემპი. მაგალითად, Li-Fi სისტემა, რომელიც ინფორმაციის გადასაცემად რადიოტალღების ნაცვლად სინათლის სპექტრს (LED ნათურებს) იყენებს, გვთავაზობს 100-ჯერ უფრო სწრაფ კავშირს (1 გბ/წმ და მეტი), ვიდრე Wi-Fi.

მიუხედავად გარკვეული შეზღუდვებისა (მაგ. მზის სინათლის ზემოქმედება), Li-Fi რადიკალურად შეცვლის ინფორმაციულ უშიშროებას, რადგან სინათლის ტალღები არ გადის კედლებში, რაც ამცირებს გარედან არასანქცირებული შეღწევის რისკს. ასეთი ინოვაციების დანერგვა სახელმწიფო სტრატეგიის ნაწილი უნდა გახდეს.

მეათე თავის დასკვნა

სახელმწიფო საინფორმაციო პოლიტიკა არის ეროვნული უშიშროების უზრუნველყოფის ყველაზე ქმედითი საშუალება 21-ე საუკუნეში. ინფორმაციული ომების ეპოქაში გამარჯვება მოითხოვს არა მხოლოდ ტექნოლოგიურ აღჭურვილობას, არამედ მწყობრ სამართლებრივ სისტემას, განათლებულ საზოგადოებას და კულტურული იდენტობის მყარ დაცვას. საქართველოსთვის ეფექტური საინფორმაციო პოლიტიკის შემუშავება არის გადაუდებელი პრიორიტეტი, რომელიც განსაზღვრავს ქვეყნის ადგილს ციფრულ ცივილიზაციაში.

მეათე თავის საკონტროლო კითხვები:

1. *განმარტეთ განსხვავება საინფორმაციო პოლიტიკის „ფართო“ და „ვიწრო“ გაგებას შორის. რატომ არის მათი ურთიერთქმედება აუცილებელი?*

2. *ჩამოთვალეთ ინფორმაციული უშიშროების უზრუნველყოფის ძირითადი ღონისძიებები და ახსენით, რატომ არის კულტურული მემკვიდრეობის დაცვა ამ სიაში?*
3. *რა არის Li-Fi ტექნოლოგიის უპირატესობა Wi-Fi-თან შედარებით ინფორმაციული უშიშროების კონტექსტში?*

მეთოდური ასპექტი:

სტუდენტმა უნდა გააცნობიეროს, რომ სახელმწიფო საინფორმაციო პოლიტიკა არის არა მხოლოდ ცენზურის ან პროპაგანდის არქონა, არამედ ქვეყნის „ციფრული სუვერენიტეტის“ დაცვის გააზრებული სტრატეგია.

თავი XI
კიბერუშიშროებისა და კიბერუსაფრთხოების ორგანიზაციები, მუშაობის პრინციპები და სტანდარტები

11.1. სტაბილურობა კიბერსივრცეში: გლობალური თანხმობის ძიება

კიბერსივრცეში სტაბილურობა განისაზღვრება, როგორც მდგომარეობა, როდესაც ყველა მომხმარებელი დარწმუნებულია ციფრული შესაძლებლობების საიმედოობასა და უსაფრთხოებაში. ეს გულისხმობს მონაცემთა მთლიანობის გარანტიას და წარმოქმნილი წინააღმდეგობების მშვიდობიან რეგულირებას ესკალაციის გარეშე.

ვინაიდან კიბერსივრცე თავისი არსით ტრანსსასაზღვროა, მისი უშიშროების პრობლემა ვერ მოგვარდება ცალკეული სახელმწიფოების იზოლირებული ძალისხმევით. ტრადიციული იურისდიქცია, რომელიც ტერიტორიულ პრინციპს ეყრდნობა, ციფრულ სამყაროში არაეფექტურია. ეს მოითხოვს საერთაშორისო-სამართლებრივი ნორმების ჰარმონიზაციას და ახალი, გლობალური მიდგომების შემუშავებას.

11.2. საერთაშორისო თანამშრომლობის პარადოქსი და ფრაგმენტაცია

კიბერსივრცეში თანამშრომლობა თანამედროვე საერთაშორისო ურთიერთობების შინაგან პარადოქსს ავლენს: ერთი მხრივ, ქვეყნებისთვის კოოპერაცია სასიცოცხლოდ აუცილებელია საფრთხეების მოსაგერიებლად, მეორე მხრივ კი — ეს თანამშრომლობა ზრდის სახელმწიფოს

მოწყვლადობას, რადგან იგი იძულებულია შეზღუდოს საკუთარი სუვერენიტეტი ორ მგრძნობიარე სფეროში: სამართალსა და ინფორმაციის დაცვაში.

დღეისათვის საერთაშორისო თანამშრომლობა ხასიათდება შემდეგი ნიშნებით:

- **ფრაგმენტაცია:** რეგიონალური ორგანიზაციები (მაგ., ევროკავშირი) ქმნის თანამშრომლობის საკუთარ, ლოკალურ მექანიზმებს.
- **სამართლებრივი ვაკუუმი:** საკანონმდებლო საქმიანობა არსებითად ჩამორჩება ტექნოლოგიურ პროგრესს.
- **ცნებათა დისონანსი:** არ არსებობს ძირითადი ტერმინების (მაგ., „კიბერაგრესია“) საყოველთაოდ აღიარებული განმარტებები.

11.3. ექსპერტული კონცენტრაციის საკვანძო მიმართულებები

საერთაშორისო დონეზე ეფექტური გამოძიებისა და პრევენციისთვის აუცილებელია ტექნიკური ექსპერტების, სამართალდამცავების და სამეცნიერო წრეების კოორდინაცია. ექსპერტთა ძალისხმევა უნდა მიიმართოს შემდეგი საკითხებისკენ:

- **კრიტიკული ინფრასტრუქტურის დაცვა:** ინფორმაციული იარაღის გამოყენების შეზღუდვა სტრატეგიულ ობიექტებთან მიმართებაში.

- **ელექტრონული მტკიცებულებები:** საერთაშორისო მექანიზმების შექმნა ციფრული მტკიცებულებების მოპოვებისა და აღიარებისათვის.
- **ნაციონალური კანონმდებლობის დაახლოება:** დანაშაულთა კლასიფიკაციისა და პასუხისმგებლობის უნიფიცირება.
- **საერთაშორისო დახმარება:** ინფორმაციული შეტევების მსხვერპლი ქვეყნებისათვის რეაბილიტაციისა და მხარდაჭერის მექანიზმების ამოქმედება.

11.4. წამყვანი საერთაშორისო ორგანიზაციები და ასოციაციები

კიბერუშიშროების გლობალურ არქიტექტურაში რამდენიმე ორგანიზაცია ასრულებს გადამწყვეტ როლს:

1. **ISACA (ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაცია):** დაარსდა 1969 წელს და 100 000-ზე მეტ წევრს აერთიანებს 120 ქვეყანაში. ISACA არის მსოფლიო ლიდერი IT-მართვის, კონტროლისა და აუდიტის სფეროში. იგი გასცემს პრესტიჟულ საერთაშორისო სერტიფიკატებს, როგორიცაა CISA (სერტიფიცირებული აუდიტორი) და CISM (სერტიფიცირებული მენეჯერი), რაც პროფესიული კვალიფიკაციის უმაღლეს სტანდარტად ითვლება.
2. **CIS (ინტერნეტუსაფრთხოების ცენტრი):** არაკომერციული ორგანიზაცია, რომელიც კომპანიებს ეხმარება ელექტრონულ კომერციაში

რისკების მართვასა და უსაფრთხოების დონის გაზომვაში. CIS არ არის მიბმული კომერციულ პროდუქტებთან, რაც მის რეკომენდაციებს ობიექტურს ხდის.

3. **ISAlliance (ინტერნეტი - ინფორმაციული უშიშროების კავშირი):** კომერციული ასოციაცია, რომელიც იცავს წევრი კომპანიების ინფორმაციულ აქტივებსა და კორპორატიულ რეპუტაციას. მისი მთავარი სერვისია მჭიდრო თანამშრომლობა CERT-თან (კომპიუტერული ინციდენტების შესწავლის საერთაშორისო ცენტრი) წარმოქმნილ საფრთხეებზე მყისი რეაგირებისათვის.

11.5. საერთაშორისო სტანდარტები და მათი გამოყენების პრაქტიკა

კიბერუშიშროების სფეროში სტანდარტიზაცია არის „საერთო ენა“, რომელიც სახელმწიფოებსა და კერძო სექტორს შორის კომუნიკაციას შესაძლებელს ხდის. სტანდარტების დანერგვა უზრუნველყოფს:

- უსაფრთხოების მართვის სისტემების უნიფიცირებას;
- რისკების შეფასების ობიექტურ კრიტერიუმებს;
- ინფორმაციული პროდუქტებისა და სერვისების ურთიერთთავსებადობას.

საქართველოსთვის ასეთ საერთაშორისო ფორმატებში ჩართვა, გაერთიანებული ერების ორგანიზაციის ეგიდით თუ რეგიონულ დონეზე, სასიცოცხლოდ მნიშვნელოვანია

საკუთარი კანონმდებლობისა და ტექნიკური მექანიზმების სრულყოფისათვის.

11.6. არასახელმწიფო აქტორების როლი

კიბერსივრცის სპეციფიკიდან გამომდინარე, საკანონმდებლო და უსაფრთხოების ბაზის შექმნაში ჩართულია არა მხოლოდ სახელმწიფოები, არამედ კერძო კომპანიები და დამოუკიდებელი ექსპერტებიც. სწორედ კერძო სექტორი ფლობს უახლეს ტექნოლოგიურ რესურსებს, რაც მათ ინფორმაციული უშიშროების უზრუნველყოფის თანასწორუფლებიან პარტნიორებად აქცევს.

მეთერთმეტე თავის დასკვნა

კიბერსივრცეში უშიშროების უზრუნველყოფა კოლექტიური პასუხისმგებლობაა. საერთაშორისო ორგანიზაციები, როგორიცაა ISACA, CIS და სხვები, ქმნიან იმ „ცოდნის ბაზას“ და სტანდარტებს, რომლებზეც უნდა დაშენდეს ეროვნული უშიშროების სისტემები. ინფორმაციული ეპოქის გამოწვევებთან გამკლავება შესაძლებელია მხოლოდ მულტილატერალური თანამშრომლობის, სამართლებრივი ჰარმონიზაციისა და მაღალი ტექნოლოგიური კულტურის დანერგვის გზით.

მეთერთმეტე თავის საკონტროლო კითხვები:

1. *რატომ ითვლება ტერიტორიული პრინციპი არაეფექტურად კიბერსივრცეში იურისდიქციის განსაზღვრისას?*

2. *ჩამოთვალეთ კიბერუშიშროების სფეროში მოქმედი მინიმუმ სამი საერთაშორისო ორგანიზაცია და განმარტეთ მათი ძირითადი ფუნქციები.*
3. *რაში მდგომარეობს საერთაშორისო თანამშრომლობის „ფრაგმენტაციის ტენდენცია“ და რა გავლენას ახდენს იგი გლობალურ უშიშროებაზე?*

მეთოდური ასპექტი:

სტუდენტმა უნდა გაიაზროს, რომ კიბერუსაფრთხოება ეფუძნება მკაცრ საერთაშორისო პროტოკოლებსა და სტანდარტებს, რომელთა გარეშე შეუძლებელია ერთიანი, დაცული გლობალური ციფრული სივრცის არსებობა.

თავი XII
კიბერუშიშროების ნაციონალური სტრუქტურები, მათი მუშაობის მეთოდები და მოქმედების პრინციპები

12.1. უშიშროების ეროვნული პოლიტიკის საკვანძო ელემენტები

თანამედროვე ეპოქაში ძლიერი კიბერთავდაცვის სისტემის არსებობა სახელმწიფოს ეროვნული უშიშროების ქვაკუთხედია. ქვეყნების უმეტესობა კიბერსივრცეს აღიქვამს არა მხოლოდ ტექნოლოგიურ გარემოდ, არამედ სამხედრო მოქმედებათა ახალ თეატრად. ეროვნული სტრატეგიები დღეს ფოკუსირებულია საფრთხეების პროგნოზირებაზე, კრიტიკული ინფრასტრუქტურის დაცვასა და აქტიურ (შემტევ) კიბეროპერაციებზე.

12.2. აშშ-ის მოდელი: კიბერსარდლობა და "წინწაწეული თავდაცვა"

ამერიკის შეერთებული შტატების კიბერპოლიტიკამ ევოლუციის რამდენიმე ეტაპი გაიარა. 2010 წლიდან შეიქმნა **აშშ-ის კიბერსარდლობა (USCYBERCOM)**, რომელმაც 2018 წლიდან დამოუკიდებელი სამეთაურო ერთეულის სტატუსი მიიღო.

ამერიკული სტრატეგიის საკვანძო ელემენტია **„წინწაწეული თავდაცვა“ (Defend Forward)**. ეს კონცეფცია გულისხმობს:

- მოწინააღმდეგის მავნე მოქმედებების წინასწარ დაზვერვას მისსავე ქსელებში.

- ყოველდღიურ ჰაკერულ რეიდებს პოტენციური საფრთხეების ნეიტრალიზაციისთვის.
- სამ საფეხურიან მართვას: ფედერალური უწყებები (DHS, DoD), ოპერატიული ცენტრები (CERT, USCYBERCOM) და ლოკალური ქვედანაყოფები.

12.3. ესტონეთის ფენომენი: ციფრული მედეგობა და ნატოს ცენტრი

ესტონეთი ევროკავშირის ლიდერია კიბერუშიშროების სფეროში. ქვეყნის წარმატება განაპირობა მჭიდრო თანამშრომლობამ კერძო სექტორთან და მოხალისეობრივი **„კიბერთავდაცვის დანაყოფის“** შექმნამ, რომელიც პროფესიონალ ჰაკერებსა და IT-ექსპერტებს აერთიანებს.

ტალინში განთავსებული **ნატოს კიბერთავდაცვის დახელოვნების ცენტრი** (NATO CCDCOE) გლობალური ანალიტიკური ჰაბია, სადაც იქმნება კიბერომის საერთაშორისო წესები (მაგ., „ტალინის სახელმძღვანელო“). ესტონური მოდელის უნიკალურობაა **VSR (ვირტუალური სიტუაციების ოთახი)** პლატფორმა, რომელიც კრიზისის დროს უწყებებს შორის კოორდინაციასა და ინციდენტების სრულ ანალიზს უზრუნველყოფს.

12.4. ლიეტუვისა და რუსეთის სტრატეგიული ხედვები

ლიეტუვას 2018 წლის სტრატეგია 5 ძირითად მიზანს ემყარება, სადაც აქცენტი კეთდება კიბერუშიშროების

კულტურის ამაღლებასა და საჯარო-კერძო პარტნიორობაზე.

რაც შეეხება რუსეთის ფედერაციას, მისი სამხედრო დოქტრინა 23 ძირითად საფრთხეს გამოყოფს. რუსული ხედვით, კიბეროპერაციები განიხილება როგორც „სულიერი და პატრიოტული ტრადიციების შერყევის“ და „შიგა პოლიტიკური უთანხმოების პროვოცირების“ იარაღი. ეს ადასტურებს, რომ რუსეთი ინფორმაციულ ომს აღიქვამს, როგორც კოგნიტურ დაპირისპირებას.

12.5. საქართველოს ეროვნული სტრატეგია 2021–2024

საქართველოს კიბერუშიშროების მესამე სტრატეგია სახელმწიფოს 3-წლიანი გეგმაა, რომელიც აერთიანებს კიბერთავდაცვასა და კიბერდანაშაულთან ბრძოლას. დოკუმენტი განსაზღვრავს 4 პრიორიტეტულ მიზანს:

1. **კიბერკულტურის განვითარება:** მოსწავლეებისა და სტუდენტების განათლება და საზოგადოების ცნობიერების ამაღლება.
2. **მმართველობითი სისტემის მდგრადობა:** ეროვნულ დონეზე რეპორტინგისა და ინციდენტებზე რეაგირების ეფექტური სისტემის შექმნა.
3. **ადამიანური რესურსები:** დარგის სპეციალისტების კვალიფიკაციის ამაღლება და ტექნიკური ბაზის გაძლიერება.
4. **საერთაშორისო როლი:** საქართველოს ჩართულობა გლობალურ კიბერსწავლებებსა და პარტნიორულ ფორმატებში.

სტრატეგიის მთავარი ამოცანაა **C4I** სისტემების განვითარება და კიბერსივრცეში საქართველოს სუვერენიტეტის განმტკიცება რუსული ჰიბრიდული საფრთხეების ფონზე.

12.6. კიბერმდგრადობის ორგანიზაციის პრინციპები

ეროვნულ დონეზე კიბერმდგრადობა (Cyber Resilience) მოითხოვს არა მხოლოდ კედლების შენებას, არამედ სისტემის უნარს — გაუძლოს დარტყმას და სწრაფად აღდგეს. დადებითი გამოცდილება აჩვენებს, რომ წარმატებული სტრუქტურა ეფუძნება:

- **ინფორმაციის გაზიარებას:** უწყებებს შორის საფრთხეების შესახებ მონაცემების მყის მიმოცვლას.
- **უწყვეტ წვრთნებს:** პერსონალის მომზადებას რეალური სიმულაციების პირობებში.
- **ტექნიკურ უნიფიკაციას:** მართვისა და ანალიზის საშუალებების ერთიან სტანდარტს.

მეთორმეტე თავის დასკვნა

კიბერუშიშროების ნაციონალური ჩარჩოები დღეს აღარ არის მხოლოდ IT-დეპარტამენტების პრეროგატივა; ის მაღალი დონის პოლიტიკური და სამხედრო მმართველობის სფეროა. წამყვანი ქვეყნების გამოცდილე-ბა აჩვენებს, რომ გამარჯვება მოიპოვება იქ, სადაც სახელმწიფო ახერხებს ტექნოლოგიური ინოვაციების, მოხალისეობრივი რესურსისა და შემტევი

თავდაცვის სტრატეგიის სინთეზს. საქართველოსთვის მესამე სტრატეგიის რეალიზაცია არის სასიცოცხლო ნაბიჯი ციფრულ სამყაროში უსაფრთხო ადგილის დასამკვიდრებლად.

მეთორმეტე თავის საკონტროლო კითხვები:

1. *რა არის აშშ-ის „წინწაწეული თავდაცვის“ (Defend Forward) სტრატეგიის არსი და რით განსხვავდება იგი ტრადიციული პასიური თავდაცვისგან?*
2. *ჩამოთვალეთ ესტონეთის კიბერმოდელის ძირითადი კომპონენტები (NATO CCDCOE, CERT-EE, VSR) და ახსენით მათი როლი.*
3. *განიხილეთ საქართველოს 2021–2024 წლების კიბერუსაფრთხოების სტრატეგიის 4 პრიორიტეტული მიზანი. რომელი მათგანი მიგაჩნიათ ყველაზე კრიტიკულად მიმდინარე გეოპოლიტიკურ ვითარებაში?*

მეთოდური ასპექტი:

თავის შესწავლის შემდეგ სტუდენტმა უნდა გააცნობიეროს, რომ მცირე სახელმწიფოებისათვის კოლექტიური კიბერთავდაცვა არის ეროვნული უშიშროების უზრუნველყოფის ერთადერთი საიმედო გარანტია საერთაშორისო ასპარეზზე.

თავი XIII
კიბერსივრცის დაცვის ევროპული სისტემის ფორმირების პრობლემები

13.1. ერთიანი ევროპული კიბერუშიშროების კონცეფცია

ევროპის განვითარების თანამედროვე ეტაპზე ინფორმაციული უშიშროების ერთიანი სისტემის ფორმირება ევროკავშირის სტრატეგიულ პრიორიტეტად იქცა. კიბერუშიშროება აქ აღიქმება, როგორც მდგომარეობა, სადაც რისკები დაყვანილია მინიმალურ ზღვრამდე, ხოლო სისტემის ეფექტურობა დამოკიდებულია მისი ცალკეული ელემენტების (წევრი სახელმწიფოების) კოორდინირებულ მუშაობაზე.

ევროპული მიდგომა არ შემოიფარგლება მხოლოდ ტექნიკური დაცვით; იგი მოიცავს პროფილაქტიკურ ღონისძიებებსა და პოლიტიკურ-ეკონომიკურ ფაქტორებს. ევროკავშირი, როგორც გლობალური აქტორი, დიდ ყურადღებას უთმობს კრიტიკული ინფრასტრუქტურის დაცვასა და ინფორმაციული საზოგადოების ფორმირებას, რაც პირდაპირ აისახება ბიზნესის, ჯანდაცვისა და განათლების სფეროებზე.

13.2. ევროკავშირის კიბერსტრატეგია (2020-2025)

2020 წლის დეკემბერში წარმოდგენილი სტრატეგია არის ევროპის ციფრული მომავლის ფორმირების საკვანძო კომპონენტი. მისი მიზანია „გლობალური, ღია და უსაფრთხო კიბერსივრცის“ შექმნა, რომელიც დაეფუძნება ადამიანის უფლებებსა და დემოკრატიულ ღირე-

ბულებებს. სტრატეგია სამ ძირითად მიმართულებაზე ფოკუსირდება:

1. **მდგრადობა და ტექნოლოგიური სუვერენიტეტი:** ევროკომისიის ინიციატივით, ხდება კრიტიკული სფეროების (ენერგოქსელები, ტრანსპორტი, საავადმყოფოები) კიბერმდგრადობის რეფორმირება. იქმნება **უსაფრთხოების ოპერატიული ცენტრების ქსელი (Security Operations Centres)**, რომელიც ხელოვნური ინტელექტის გამოყენებით გახდება ევროკავშირის „კიბერუშიშროების ფარი“.

2. **რეაგირების შესაძლებლობების გაძლიერება:** ჩამოყალიბდა **ევროკავშირის გაერთიანებული კიბერგანყოფილება (Joint Cyber Unit)**. ეს არის პლატფორმა, რომელიც აერთიანებს სამოქალაქო, სამხედრო და სამართალდამცავ რესურსებს ფართომასშტაბიანი შეტევების მოსაგერიებლად.

3. **გლობალური თანამშრომლობა:** ევროკავშირი აყალიბებს „კიბერდიპლომატიურ ქსელს“, რათა საერთაშორისო ორგანიზაციებში (გაერო, ICANN) პოპულარიზაცია გაუწიოს საკუთარ სტანდარტებსა და ღირებულებებს.

13.3. ერთობლივი კიბერდანაყოფი (Joint Cyber Unit) და კოლექტიური დაცვა

2021 წლის ივლისში შექმნილი ეს სტრუქტურა ევროპული კიბერთავდაცვის „ოპერატიული ტვინია“. მისი ფუნქციაა:

- ევროკავშირის წევრ სახელმწიფოებს შორის ინფორმაციის აქტიური მიმოცვლა საფრთხეების შესახებ.
- ფართომასშტაბიან კიბერინციდენტებზე კოლექტიური რეაგირების კოორდინაცია.
- სწრაფი რეაგირების ჯგუფების მობილიზება და ურთიერთდახმარების ოქმების გამარტივება.

ეს დანაყოფი სასიცოცხლოდ მნიშვნელოვანია გლობალური კიბერსაფრთხეებისაგან მთავრობების, ბიზნესისა და მოქალაქეების დასაცავად. იგი ქმნის საერთაშორისო თანამშრომლობის პრეცედენტს, სადაც ტექნიკური და დიპლომატიური უწყებები ერთიან რეჟიმში მუშაობს.

13.4. ნატოს კიბერპოლიტიკა და ევროპული უშიშროება

ვინაიდან ნატო ევროპის კონტინენტის უშიშროების გარანტია, მისი კიბერპოლიტიკა მჭიდროდ არის გადაჯაჭვული ევროკავშირის ინტერესებთან. ალიანსის კიბერსარდლობის სრულად დაკომპლექტება 2023 წელს დასრულდა. აქ იკვეთება ორი სტრატეგიული გამოწვევა:

- **სამართლებრივი ატრიბუცია:** მიუხედავად იმისა, რომ საერთაშორისო სამართალი აღიარებულია კიბერსივრცეშიც, კვლავ პრობლემურია აგრესორის იდენტიფიცირება (ატრიბუცია) და ბრალდების მყარი მტკიცებულებებით გამყარება.
- **კიბერიარაღის ლეგიტიმაცია:** წევრი ქვეყნები (მაგ. დიდი ბრიტანეთი) სულ უფრო ხშირად

საუბრობს საკუთარ დოქტრინებში შეტევითი კიბერიარაღის შექმნის აუცილებლობაზე, რათა მზარდ საფრთხეებს უპასუხონ.

13.5. ინვესტიციები და პროგრამა "ციფრული ევროპა"

ევროკავშირი გეგმავს 2021-2027 წლებში 4.5 მილიარდი ევროს ინვესტიციას კიბერუშიშროების სექტორში. პროგრამა „ციფრული ევროპის“ ფარგლებში, ევროკომისიამ გამოყო მნიშვნელოვანი გრანტები (დაახლოებით 2 მილიარდი ევრო) შემდეგი მიზნებისთვის:

- ხელოვნური ინტელექტის და კვანტური კავშირის ინფრასტრუქტურის განვითარება.
- მოქალაქეების ციფრული უნარების ამაღლება.
- დეზინფორმაციასთან ბრძოლა და ბავშვების ონლაინ უსაფრთხოება.

ასევე იქმნება **ციფრული ინოვაციების ევროპული ცენტრების ქსელი (EDIH)**, რომელიც კერძო და საჯარო სექტორს ციფრულ ტრანსფორმაციაში დაეხმარება.

13.6. ტექნოლოგიური სტანდარტები და ICANN

ევროკავშირის პოლიტიკა ორიენტირებულია იმაზე, რომ საერთაშორისო ტექნიკური რეგულაციები (მაგალითად, ICANN-ის ფარგლებში) ასახავდეს ევროპულ ღირებულებებს. ეს მოიცავს მონაცემთა დაცვის მაღალ სტანდარტებსა და ინტერნეტის მართვის მულტისტეიკჰოლდერულ მოდელს, რაც უზრუნველყოფს კიბერსივრცის ღიაობასა და თავისუფლებას.

მეცამეტე თავის დასკვნა

კიბერსივრცის დაცვის ევროპული სისტემა ყალიბდება, როგორც მრავალშრიანი მექანიზმი, სადაც ტექნოლოგიური ინოვაცია, სამართლებრივი რეგულირება და საერთაშორისო პარტნიორობა ერთ მთლიანობას ქმნის. „კიბერუშიშროების ფარისა“ და ერთობლივი დანაყოფების შექმნით, ევროპა ცდილობს დაიცვას თავისი ციფრული სუვერენიტეტი და გახდეს უშიშროების გარანტი არა მხოლოდ თავისი წევრებისთვის, არამედ პარტნიორი ქვეყნებისთვისაც, მათ შორის საქართველოსთვის.

მეცამეტე თავის საკონტროლო კითხვები:

1. *რას წარმოადგენს ევროკავშირის „კიბერუშიშროების ფარი“ და რა როლს ასრულებს მასში ხელოვნური ინტელექტი?*
2. *განმარტეთ „ერთობლივი კიბერდანაყოფის“ (Joint Cyber Unit) ფუნქციები და მისი მნიშვნელობა კოლექტიური რეაგირების პროცესში.*
3. *რა სამართლებრივ პრობლემებს აწყდება ნატო და ევროკავშირი კიბერშეტევების ატრიბუციისა და საერთაშორისო სამართლის გამოყენების თვალსაზრისით?*

მეთოდური ასპექტი:

სტუდენტმა უნდა შეძლოს თეორიული ცოდნის პროეცირება საქართველოს რეალობაზე და გააცნობიეროს საკუთარი როლი, როგორც მომავალი სპეციალისტისა, ქვეყნის კიბერმედეგობისა და ეროვნული ინტერესების დაცვაში.

დასკვნა

ნაშრომის **ინფორმაციული ომები და საერთაშორისო კიბერსივრცე** ფარგლებში განხორციელებულმა კვლევამ და ანალიზმა ცხადყო, რომ თანამედროვე სამყარო იმყოფება გლობალური უშიშროების პარადიგმის ფუნდამენტური ცვლილების პროცესში. ინფორმაციული რევოლუცია აღარ არის მხოლოდ ტექნოლოგიური პროგრესის ნაწილი, იგი იქცა გეოპოლიტიკური ძალაუფლებისა და სახელმწიფოებრივი გადარჩენის მთავარ ინსტრუმენტად.

წიგნში განხილული მასალების საფუძველზე შეიძლება ჩამოყალიბდეს რამდენიმე უმთავრესი დასკვნა:

1. **ომის ტრანსფორმაცია.** ტრადიციული, კინეტიკური ომები ჩაანაცვლა ან შეავსო მეოთხე თაობის კონფლიქტებმა, სადაც მთავარი საბრძოლო ველი ადამიანის ცნობიერება და ციფრული ინფრასტრუქტურაა. ინფორმაციული ომი გახდა უწყვეტი პროცესი, რომელსაც არ გააჩნია მკაფიო ზღვარი მშვიდობიანობასა და საომარ მდგომარეობას შორის.

2. **სახელმწიფო ინსტიტუტების მედეგობა.** იერარქიული მმართველობის სტრუქტურები იძულებულია მოერგოს ქსელურ (Network-centric) რეალობას. სახელმწიფოს სიძლიერე დღეს განისაზღვრება არა მხოლოდ სამხედრო არსენალით, არამედ მისი „რბილი ძალითა“ და კიბერსივრცეში ეფექტური მანევრირების უნარით.

3. **კოლექტიური უშიშროების აუცილებლობა.** კიბერტერორიზმისა და ჰიბრიდული საშიშროების მასშტაბი იმდენად დიდია, რომ მათთან გამკლავება ინდივიდუალურად შეუძლებელია. ნატოს, ევროკავშირისა და საერთაშორისო სტანდარტების (ISACA, CIS) როლი კრიტიკულად მნიშვნელოვანია ერთიანი თავდაცვითი ფარის შესაქმნელად.

4. **საქართველოს სტრატეგიული არჩევანი.** საქართველოსთვის, როგორც რთულ გეოპოლიტიკურ რეგიონში მყოფი ქვეყნისთვის, კიბერმედეგობის ამაღლება და ეროვნული კიბერუშიშროების სტრატეგიის იმპლემენტაცია ეგზისტენციალური მნიშვნელობისაა. განათლებული კადრები და ტექნოლოგიური მზაობა ჩვენი ქვეყნის სუვერენიტეტის დაცვის გარანტიაა.

დასასრულს, უნდა აღინიშნოს, რომ ინფორმაციული ეპოქა გვთავაზობს როგორც უპრეცედენტო შესაძლებლობებს, ისე კრიტიკულ რისკებს. მოცემული ნაშრომი არის მცდელობა, შეიქმნას მყარი თეორიული და პრაქტიკული საფუძველი მომავალი სპეციალისტებისათვის, რათა მათ შეძლონ ამ გამოწვევების ადეკვატური აღქმა და მართვა. ამ ახალ რეალობაში გამარჯვება ეკუთვნის მათ, ვინც ფლობს ინფორმაციას, მართავს მას და, რაც მთავარია, იცის მისი დაცვის ფასი.

გამოყენებული ლიტერატურა

1. ჰ. კუპრაშვილი. (2024). ტერმინები უშიშროება და უსაფრთხოება და მათი გამოყენების წესი. ტერმინოლოგია - მემკვიდრეობა და თანამედროვეობა IV საერთაშორისო კონფერენციის მასალების კრებული. თბილისი: თსუ, ა. ჩიქობავას სახელობის ენათმეცნიერების ინსტიტუტი, გვ. 235-253;
2. ჰ. კუპრაშვილი. (2024). აკადემიური სამეცნიერო კვლევების სფეროსა და არეალის გაფართოება ინფორმაციულ ეპოქაში. სტუ-ის შრომები – Work of GTU, №1 (531), გვ. 108-120. ISSN 1512-0996
3. ჰ. კუპრაშვილი. (2023). ეროვნული უშიშროების თეორიის კვლევის მეთოდოლოგიის თავისებურება. სტუ-ის შრომები – Work of GTU, №4 (530), გვ. 154-166. ISSN 1512-0996
4. ჰ. კუპრაშვილი. (2023). პრობლემები საინფორმაციო-ფსიქოლოგიური უშიშროების უზრუნველყოფაში. ფსიქოლოგია და თანამედროვეობა. სამეცნიერო-პრაქტიკული კონფერენციის ნაშრომთა კრებული. სსიპ - დავით აღმაშენებლის სახელობის საქართველოს ეროვნული თავდაცვის აკადემია. გვ. 68-75. ISBN-978-9941-8-5577-1 https://eta.edu.ge/uploads/kvleviti_centri/fsiqologiada_tamnamedrov.pdf
5. ჰ. კუპრაშვილი. (2022). „ჰიბრიდული ომი - ომის ახალი ფილოსოფია თუ ახალი ტერმინი.“ „სამართლის მაცნე“, №5 (524), გვ. 6-17. E ISSN 2667-9434 http://heraldoflaw.com/ge/journal/hibriduli-omi-omis-akhali-filosofia-tu-akhali-termini/
6. ჰ. კუპრაშვილი. (2022). საქართველოს ეროვნული უშიშროება. მონოგრაფია, მთ. რედ. ი. გაბისონია. თბილისი: უნივერსალი, 702 გვ.

7. ჰ. კუპრაშვილი. (2022). „კიბერსივრცის კვლევა და ახალი აკადემიური დისციპლინები.“ სტატიების კრებული საერთაშორისო სამეცნიერო კონფერენციისა „თანამედროვე მსოფლიო წესრიგი - პოლიტიკურ-სამართლებრივი გამოწვევები“, სტუ, სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტი. თბილისი, გვ.82-88. http://law.gtu.ge/საერთაშორისო-სამეცნიერ-11/
8. ჰ. კუპრაშვილი. (2022). „კიბერსივრცე და ტერმინები: კიბერუშიშროება და კიბერუსაფრთხოება.“ სტუ-ის შრომები – Work of GTU, №2 (524), გვ. 167-177. ISSN 1512-0996
9. საქართველოს მთავრობის დადგენილება. (2021). საქართველოს კიბერუსაფრთხოების 2021 – 2024 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ https://www.matsne.gov.ge/ka/document/view/5263611?publication=0
10. Arquilla J. (2011). Insurgents, raiders, and bandits. How masters of irregular warfare have shaped our world. – Chicago.
11. Arquilla, J., Ronfeldt, D (1997). In Athena's Camp: Preparing for Conflict in the Information Age, RAND Corporation (MR-880).
12. Computer Hope. (2017). Charley Kline. http://www.computerhope.com/people/charley_kline.htm ბოლო მონახულება 25.12.2025
13. Computer Hope. (2025). Bill Duvall. https://www.computerhope.com/people/bill_duvall.htm ბოლო მონახულება 26.12.2025

14. Denning, D. E. (1999). *Information warfare and security*. - Reading etc. https://archive.org/details/informationwarfa00denn
15. Dewar R. (2022). Cyberspace is a Consensual Hallucination. P. 2. Available from: https://www.researchgate.net/publication/325216608_Cyberspace_is_a_Consensual_Hallucination
16. Dunn Cavelty, M., Eriksen, Ch., Scharte, B. (2023). Making cyber security more resilient: adding social considerations to technological fixes. Journal of Risk Research, 26 (7), 801-814 https://doi.org/10.1080/13669877.2023.2208146 https://www.tandfonline.com/doi/full/10.1080/13669877.2023.2208146
17. Dunn Cavelty, M., & Wenger, A. (Eds). (2022). Cyber security politics: socio-technological transformations and political fragmentation. New York, NY: Routledge https://www.routledge.com/Cyber-Security-Politics-Socio-Technological-Transformations-and-Political/Cavelty-Wenger/p/book/9780367626747
18. Dunn Cavelty, M., Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41:1, DOI: 10.1080/13523260.2019.1678855, 83. 22-23. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn%20Cavelty_Wenger_2019_Contemporary%20Security%20Policy_Cyber%20security%20meets%20secu

rity%20politics%20Complex%20technology%20fragmented%20politics%20and%20networked%20science.pdf
19. Egloff, F. J. (2019). Contested Public Attributions of Cyber Incidents and the Role of Academia. Contemporary Security Policy, 41(1): 55–81;
20. Eggenschwiler, J. (2022). Big Tech's Push for Norms to Tackle Uncertainty in Cyberspace; and others.
21. Jackson, K. (2025). The Unseen War: Cyber Warfare in the Shadow of Global Conflicts. Cobalt. https://www.cobalt.io/blog/the-unseen-war-cyber-warfare-in-the-shadow-of-global-conflicts
22. Kuprashvili, H. (2002). Aspects of Georgia's Information Policy. Report at the Conference: Cyberspace of emerging threats to national security. The George C. Marshall European Center for Security Studies. 02-05.12.2002 Munich, Germany
23. Lind, William S; Nightengale, Keith; Schmitt, John F.; Sutton, Joseph W.; Wilson, Gary I. The Changing Face of War: Into the Fourth Generation. Marine Corps Gazette, October 1989, Pages 22-26 https://www.mca-marines.org/files/The%20Changing%20Face%20of%20War%20-%20Into%20the%20Fourth%20Generation.pdf http://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html [05.07.2017].
24. Libicki M. (2007). Conquest in cyberspace. National security and information warfare. Cambridge, p. 216.
25. Olejnik, L. (2025). Russian cyber and information warfare and its impact on the EU and UK. King's College London.

https://www.kcl.ac.uk/russian-cyber-and-information-warfare-and-its-impact-on-the-eu-and-uk

26. Qiao, L., Wang, X. (2002). Unrestricted Warfare: China's Master Plan to Destroy America. Pan American Publishing Company, Panama City, Panama https://books.google.ge/books?id=ejFV1568hqAC&printsec=frontcover&hl=ru&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false [21.09.2025].
27. Stein, G. J. (2025). Information Attack: Information Warfare In 2025, research paper presented to 'Air Force 2025', August 1996. http://csat.au.af.mil/2025/volume3/vol3ch03.pdf
28. Szafranski, R. (1997). Neocortical warfare? The acme of skill // In Athena's camp. Ed. By J. Arquilla, D. Ronfeldt. - Santa Monica.
29. Urry, J. (2007). Mobilities. Cambridge, UK ; Malden, MA : Polity https://archive.org/details/mobilities0000urry
30. Wilson, T. L., & Hershey, D. A. (1996). The research methods script. Teaching of Psychology, 23(2), 97-99. https://doi.org/10.1207/s15328023top2302_5
31. Почепцов Г. Г. (2015). *Информационные войны. Новый инструментарий политики*. Москва: Алгоритм.

დანართი. პრაქტიკული სავარჯიშოები და „ქეის-სტადები“ (Case Study) თავების მიხედვით

I თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 1. **გარდამავალი პერიოდი სახელმწიფო და სამხედრო ინსტიტუციებში** - ეს თავი მიმოიხილავს ინტერნეტის სამხედრო გენეზისს და სახელმწიფო მართვის სისტემების ტრანსფორმაციას)*

I. პრაქტიკული სავარჯიშო - „იერარქია და ქსელი“

სავარჯიშოს მიზანი: *სტუდენტებმა პრაქტიკულად აღიქვან განსხვავება ტრადიციულ (ვერტიკალურ) და ქსელურ (ჰორიზონტალურ) მართვის მოდელებს შორის კრიზისულ სიტუაციაში.*

ინსტრუქცია. *დაყავით ჯგუფი ორ ნაწილად:*

1. ***ჯგუფი A (იერარქია) -*** *გადაწყვეტილების მიღება შეუძლია მხოლოდ „ლიდერს“. ინფორმაცია ჯერ ადის ლიდერთან, ის იღებს გადაწყვეტილებას და მერე ჩამოდის ქვემოთ.*
2. ***ჯგუფი B (ქსელი) -*** *ყველა წევრი თანასწორია, მათ აქვთ საერთო მიზანი და ინფორმაციის გაცვლა ხდება მყისიერად ყველას შორის.*

დავალება. *ორივე ჯგუფს მიეცით ერთი და იგივე რთული ლოგიკური ამოცანა (მაგალითად, დაშიფრული ტექსტის ამოცნობა).*

- *დააკვირდით, რომელი ჯგუფი უფრო სწრაფად მოახდენს რეაგირებას „ინფორმაციულ ხმაურზე“ (როცა ამოცანის პირობა მოულოდნელად იცვლება).*

სადისკუსიო კითხვები

- *რატომ გაუჭირდა იერარქიულ ჯგუფს ცვალებად გარემოსთან ადაპტაცია?*
- *რა საფრთხეები ახლავს ქსელურ მართვას (ჯგუფი B) პასუხისმგებლობის თვალსაზრისით?*

II. ქეის-სტადი (Case Study) - „ARPANET-იდან კიბერსუვერენიტეტამდე“

კონტექსტი: *1960-იან წლებში ARPA-ს მიზანი იყო სისტემა, რომელიც გაუძლებდა ბირთვულ დარტყმას. დღეს კი სახელმწიფოები დგას ახალი გამოწვევის წინაშე: მათ აქვთ ტერიტორიული სუვერენიტეტი, მაგრამ ვერ აკონტროლებენ „ბიტებს“, რომლებიც მათ საზღვრებში მოძრაობს.*

ქეისი: *წარმოიდგინეთ პირობითი სახელმწიფო „X“, რომლის საჯარო უწყებები (სამინისტროები, ჯარი) კვლავ მუშაობს მკაცრი საბჭოური ტიპის იერარქიით (ყველაფერს წყვეტს მინისტრი). ამ დროს, ქვეყნის წინააღმდეგ იწყება კიბერშეტევა, რომელსაც ახორციელებს დეცენტრალიზებული ჰაკერული დაჯგუფება. ჰაკერები არიან მსოფლიოს სხვადასხვა წერტილში, არ აქვთ ერთიანი ოფისი და მოქმედებენ ავტონომიურად.*

დავალება სტუდენტებისთვის

1. ***ანალიზი.*** *რატომ არის სახელმწიფო „X“-ის იერარქიული სტრუქტურა განწირული მარცხისთვის ამ „ქსელურ ომში“?*
2. ***სტრატეგია.*** *ტექსტში ნახსენები პოლ ბრაკენისა და პიტერ დრუკერის პრინციპების (ორგანიზაციული ადაპტაცია, დეცენტრალიზაცია, პარტნიორობა) გამოყენებით, შესთავაზეთ სახელმწიფოს რეფორმის გეგმა.*
3. ***გადაწყვეტა.*** *როგორ უნდა შეინარჩუნოს სახელმწიფომ „ოპერაციული სუვერენიტეტი“, როცა ინფორმაცია ფიზიკურ კედლებს არ ცნობს?*

III. ანალიტიკური დავალება - „ინფორმაციის 4 თვისება“

ტექსტში მოცემულია ინფორმაციის 4 თვისება (მცირე რესურსები, ტრანსპორტირება, შეღწევადობა, გაზიარება).

დავალება. *მოიყვანეთ ბოლო 2 წლის განმავლობაში მომხდარი ერთი რეალური საერთაშორისო მოვლენის მაგალითი (მაგ., უკრაინის ომი, არჩევნებში ჩარევა, გლობალური პროტესტები), სადაც ინფორმაციის ეს ოთხივე თვისება იქნა გამოყენებული, როგორც „იარაღი“.*

მე-2 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 2. **კაცობრიობა განვითარების ახალ ეტაპზე** - ეს თავი კიდევ უფრო ღრმად შედის ინფორმაციის ბუნებასა და მის სოციოლოგიურ ასპექტებში. აქ ცენტრალური ფიგურა მანუელ კასტელსია, რომელიც "ქსელური საზოგადოების" კონცეფციას გვთავაზობს.)*

I. პრაქტიკული სავარჯიშო. „ინფორმაციული რევოლუციების ქრონოლოგია და გავლენა“

სავარჯიშოს მიზანი. *სტუდენტებმა დაუკავშირონ ისტორიული გამოგონებები თანამედროვე ციფრულ ეფექტებს.*

დავალება. *ჯგუფმა უნდა შეავსოს „გავლენის მატრიცა“. თითოეულ რევოლუციას უნდა მიუსადაგოს ერთი თანამედროვე ანალოგი და იმ საფრთხის ტიპი, რომელიც მან წარმოშვა.*

რევოლუცია	**თანამედროვე ანალოგი**	**რისი საფრთხე წარმოიშვა?**
I (ბორბალი/ტრანსპორტი)	გლობალური ლოგისტიკა/დრონები	ფიზიკური საზღვრების მოშლა
II (დამწერლობა)	მონაცემთა ბაზები/Cloud	ინფორმაციის გაჟონვა/არქივის წაშლა
III (სტამბა)	სოციალური მედია (X, FB)	დეზინფორმაციის მასობრივი ტირაჟირება
IV (ელექტრობა/რადიო)	Real-time სტრიმინგი	მყისი პანიკის დათესვა

კითხვა დისკუსიისთვის. *რატომ ამბობს მანუელ კასტელსი, რომ დღეს „ადამიანის აზრი უშუალო საწარმოო ძალაა“? მოიყვანეთ მაგალითი, სადაც მხოლოდ იდეამ შექმნა მილიარდობით დოლარის ღირებულება.*

II. ქეის-სტადი. „ობიექტური და სუბიექტური ინფორმაცია კრიზისის დროს“

კონტექსტი.

ტექსტში ნახსენებია ნორბერტ ვინერის ხედვა, რომ ობიექტური ინფორმაცია მატერიის თვისებაა, ხოლო ადამიანური ინფორმაცია — სუბიექტური აღქმა.

ქეისი.

წარმოიდგინეთ, რომ გარკვეულ რეგიონში მოხდა ტექნოგენური კატასტროფა (მაგ., ქიმიური გაჟონვა).

1. ***ობიექტური ინფორმაცია -*** *სენსორები აჩვენებს ჰაერში ნივთიერების კონცენტრაციას (ციფრები, ბიტები).*
2. ***სუბიექტური ინფორმაცია -*** *სოციალურ ქსელებში ვრცელდება პანიკური ვიდეოები, სადაც ადამიანები ამბობენ, რომ „ხელისუფლება სიმართლეს მალავს“ და „სიტუაცია ბევრად უარესია“.*

დავალება სტუდენტებისთვის

- ***როგორც სტრატეგიული კომუნიკაციის სპეციალისტებმა****, როგორ უნდა გამოიყენოთ ინფორმაციის ხარისხობრივი პარამეტრები*

*(**აქტუალურობა, უტყუარობა, სისრულე**), რათა სუბიექტურმა აღქმამ (პანიკამ) არ დაანგრიოს სახელმწიფოებრივი წესრიგი?*

- *დაასაბუთეთ, რატომ არის ამ შემთხვევაში ინფორმაცია უფრო „ფასეული რესურსი“, ვიდრე კატასტროფის სალიკვიდაციო ტექნიკა.*

III. ანალიტიკური დავალება - „ვირტუალური რეალობის საფრთხეები“

ტექსტში ნახსენებია, რომ მოქალაქეებს სულ უფრო ნაკლები საერთო კულტურული გამოცდილება უგროვდებათ, რაც სამოქალაქო საზოგადოებას ფრაგმენტულს ხდის.

დავალება.

1. *შეარჩიეთ ერთი პოპულარული სოციალური პლატფორმა (მაგ: TikTok ან YouTube).*
2. *აღწერეთ, როგორ ქმნის ამ პლატფორმის ალგორითმი „საინფორმაციო ბუშტებს“ (Echo Chambers).*
3. *უპასუხეთ კითხვას: როგორ უშლის ხელს ეს „ბუშტები“ ერთიან ეროვნულ-სახელმწიფოებრივ ინტერესებზე შეთანხმებას?*

დასკვნითი კითხვა სტუდენტებისთვის

თუ ინფორმაცია 21-ე საუკუნის „ქვანახშირი და ფოლადია“, ვინ არიან თანამედროვე ეპოქის „ინფორმაციული ოლიგარქები“ და რა გავლენა აქვთ მათ სახელმწიფო სუვერენიტეტზე?

მე-3 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 3. **ინფორმაციული ომის წარმოშობის პერიპეტიები** - მესამე თავი ფუნდამენტურია, რადგან ის ომის ევოლუციასა და "მეოთხე თაობის ომის" (4GW) კონცეფციას ეხება. აქ მნიშვნელოვანია იმის გააზრება, რომ იარაღი აღარ არის მხოლოდ კინეტიკური (ფიზიკური), არამედ კოგნიტურია (აზროვნებაზე მიმართული)*

I. პრაქტიკული სავარჯიშო - „ომის თაობების დიაგნოსტიკა“

სავარჯიშოს მიზანი. *სტუდენტებმა ისწავლონ კონფლიქტის ტიპის ამოცნობა მისი მახასიათებლების მიხედვით.*

ინსტრუქცია. *ქვემოთ მოცემულია ომის წარმოების სხვადასხვა ელემენტი. სტუდენტებმა უნდა გადაანაწილონ ისინი უილიამ ლინდის მიერ კლასიფიცირებულ ოთხ თაობაში:*

1. ***ელემენტები -*** *მუშკეტი, ბლიცკრიგი, კიბერშეტევა ბანკებზე, არტილერიის მასირებული ცეცხლი, ხაზოვანი მწყობრი, დეზინფორმაციული კამპანია არჩევნების წინ, ტერორისტული უჯრედების მოქმედება.*

სადისკუსიო დავალება. *წაუკითხეთ სტუდენტებს ციტატა ჩინური მოდელიდან „შეუზღუდავი ომი“: "ომის პირველი წესი არის ის, რომ არ არსებობს წესები". სთხოვეთ მათ დაასაბუთონ, როგორ ცვლის ეს მიდგომა საერთაშორისო სამართალს (მაგ., ჟენევის კონვენციას).*

II. ქეის-სტადი (Case Study) - „ოპერაცია: ნეოკორტიკალური ომი“

კონტექსტი. *რიჩარდ შაფრანსკი საუბრობს „ნეოკორტიკალურ ომზე“ (ტვინის ქერქზე ზემოქმედება), სადაც მიზანია მოწინააღმდეგის ნების გატეხვა ფიზიკური განადგურების გარეშე.*

ქეისი. *წარმოიდგინეთ ქვეყანა „Y“, რომელიც აპირებს მნიშვნელოვანი ენერგეტიკული ხელშეკრულების გაფორმებას დასავლეთთან. მოწინააღმდეგე ქვეყანა „Z“ ამის წინააღმდეგია, თუმცა ღია ომს ვერ იწყებს. „Z“ იწყებს ინფორმაციულ ოპერაციას:*

1. *სოციალურ ქსელებში ავრცელებს ყალბ კვლევას, რომ ეს პროექტი გამოიწვევს ეკოლოგიურ კატასტროფას;*
2. *ჰაკერული შეტევით დროებით თიშავს ელექტროენერგიას დედაქალაქში, რათა მოსახლეობაში დაუცველობის განცდა გააჩინოს;*
3. *ავრცელებს ფარულ ჩანაწერებს (შესაძლოა „Deepfake“), სადაც ლიდერები პროექტის „გაყიდვაზე“ საუბრობენ.*

დავალება სტუდენტებისთვის

- ***ანალიზი.*** *პოჩეპცოვის ეტაპების მიხედვით, რომელ ეტაპს მიეკუთვნება ეს ოპერაცია?*
- ***განსხვავება.*** *განმარტეთ, სად მთავრდება ამ ქეისში „ინფორმაციული ოპერაცია“ და სად იწყება „ინფორმაციული ომი“?*

- ***კონტრზომა.*** *მარტინ ლიბიკის „ციხესიმაგრეებისა“ და „მოედნების“ კონცეფციით, როგორ უნდა დაიცვას ქვეყანა „Y“-მა საკუთარი მოსახლეობის ცნობიერება (ნეოკორტექსი)?*

III. როლური თამაში - „ჯონ არქუილას შტაბი“

დავალება. *სტუდენტები ორ ჯგუფად იყოფიან:* ***„იერარქიული არმია“*** *და* ***„ქსელური მოწინააღმდეგე“****.*

- *ქსელურმა ჯგუფმა უნდა მოიფიქროს 3 დაბალი ინტენსივობის დარტყმა (მაგ: ჭორის გავრცელება, მცირე კიბერსაბოტაჟი).*
- *იერარქიულმა ჯგუფმა უნდა სცადოს ამაზე რეაგირება ბრძანების ჯაჭვის დაცვით.*
- ***მიზანი.*** *დაამტკიცეთ არქუილას თეზისი, რომ „ქსელებთან ბრძოლა მხოლოდ ქსელებს შეუძლიათ“.*

საკონტროლო კითხვა. *ჯონ არქუილას მაგალითზე დაყრდნობით, როგორ ფიქრობთ, რატომ იყო 2008 წლის აგვისტოს ომი საქართველოში ინფორმაციული ომის ახალი ეტაპის დასაწყისი?*

მე-4 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 4. **კიბერსივრცე თავდაცვის თანაბარუფლებიანი სფერო ზღვასთან, ჰაერსა და ხმელეთთან ერთად** - მეოთხე თავი საკვანძოა, რადგან ის კიბერსივრცეს განიხილავს არა როგორც დამხმარე ინსტრუმენტს, არამედ როგორც დამოუკიდებელ საბრძოლო არენას — ხმელეთის, ზღვისა და ჰაერის თანაბარუფლებიან სფეროს. აქ შემოდის ნატოს ვარშავის სამიტის ისტორიული გადაწყვეტილება და რიჩარდ შაფრანსკის "უსისხლო ომის" კონცეფცია.)*

I. პრაქტიკული სავარჯიშო - „კიბერდომენის ანატომია“

სავარჯიშოს მიზანი. *სტუდენტებმა ისწავლონ კიბერსივრცის მრავალშრიანი ბუნების გარჩევა და კრიტიკული წერტილების იდენტიფიცირება.*

დავალება. ჯგუფმა უნდა შექმნას "კიბერრუკა" პირობითი ქალაქისთვის. მათ უნდა დააჯგუფონ ობიექტები ჯონ ურის სამი ფონის (ბუნებრივი, ხელოვნური, ვირტუალური) მიხედვით და მონიშნონ, სად გადის კიბერსივრცის ხაზი.

ობიექტის ტიპი	***ფონი (ურის მიხედვით)***	***კიბერკავშირი (მაგალითი)***
მდინარე/წყალსაცავი	*ბუნებრივი*	*წყლის დონის მართვის სენსორები (SCADA)*
ელექტროქვესადგური	*ხელოვნური*	*დისტანციური მართვის პანელი (IP მისამართით)*
საბანკო გადარიცხვა	*ვირტუალურ*	*ტრანსნაციონალურ*

ობიექტის ტიპი	ფონი (ურის მიხედვით)	კიბერკავშირი (მაგალითი)
	ი	ი ფინანსური ქსელი

სადისკუსიო კითხვა: *თუ კიბერსივრცეში საზღვრები არ არსებობს, როგორ უნდა დაიცვას საქართველომ თავისი "ქსელური სუვერენიტეტი"?*

II. ქეის-სტადი (Case Study) - „ვარშავის პრეცედენტი და მე-5 მუხლი“

კონტექსტი.

2016 წლის ვარშავის სამიტზე ნატომ აღიარა, რომ კიბერშეტევამ შეიძლება აამუშაოს კოლექტიური თავდაცვის (მე-5) მუხლი.

ქეისი.

წარმოიდგინეთ, რომ ნატოს წევრ ერთ-ერთ ქვეყანაში "ქვეყანა A" ერთდროულად ხდება შემდეგი მოვლენები:

1. *ქვეყნის ცენტრალური ბანკის სერვერები პარალიზებულია (ადამიანები ვერ იღებენ ფულს).*
2. *აეროპორტების სადისპეტჩერო სისტემაში შევიდა ვირუსი, რამაც ფრენების ქაოსი გამოიწვია.*
3. *სოციალურ ქსელებში ვრცელდება ინფორმაცია, რომ ეს ყველაფერი მეზობელი "ქვეყანა B"-ს გაკეთებულია, თუმცა ოფიციალური მტკიცებულება (Attribution) ჯერ არ არსებობს.*

დავალება სტუდენტებისთვის:

- ***იურიდიული ანალიზი.*** *ჩაითვლება თუ არა ეს ქმედება "შეიარაღებულ თავდასხმად" ვარშავის სამიტის დეკლარაციის მიხედვით?*
- ***შაფრანსკის ხედვა.*** *როგორ გამოიყენა "ქვეყანა B"-მ ინფორმაციული იარაღი მინიმალური სისხლისღვრით მაქსიმალური პარალიზების მისაღწევად?*
- ***სტრატეგიული გადაწყვეტილება.*** *თქვენ, როგორც ნატოს მრჩევლებმა, უნდა გადაწყვიტოთ: უნდა აამოქმედოს თუ არა ალიანსმა მე-5 მუხლი, თუ თავდამსხმელი ანონიმურია?*

III. ანალიტიკური დავალება - „Network Centric ომის ფორმულა"

*ტექსტში ნახსენებია **C4I** სისტემა (Command, Control, Communications, Computers, Intelligence).*

დავალება. მოიყვანეთ მაგალითი "თავდაცვის ხედვა 2030"-დან ან თანამედროვე კონფლიქტებიდან (მაგ: დრონების გამოყენება რეალურ დროში), სადაც Network Centric მართვამ დაამარცხა ტრადიციული, იერარქიული სამხედრო ძალა.

IV. კოგნიტური სავარჯიშო - „მანიპულაციის ამოცნობა"

რიჩარდ შაფრანსკი ამბობს, რომ წარმატებული ოპერაციისას მსხვერპლი ვერც კი ხვდება, რომ მანიპულირებენ.

დავალება. სტუდენტებმა უნდა მოძებნონ ბოლო ერთი კვირის განმავლობაში გავრცელებული ერთი

"ვირუსული" ნარატივი ქართულ ინტერნეტსივრცეში და გააანალიზონ:

1. *რა არის ამ ინფორმაციის მიზანი (ქცევის შეცვლა, პანიკა, თუ უნდობლობა)*
2. *როგორ ცდილობს ეს ნარატივი, რომ მსხვერპლის აზროვნება გახადოს "აუტისტური" (ჩაკეტილი მხოლოდ ერთი წყაროს მიმართ)?*

საკონტროლო კითხვა

რატომ არის კიბერომი "ომის მეხუთე ფორმა" და რატომ არის ის უფრო საშიში, ვიდრე ტრადიციული საავიაციო დაბომბვა?

მე-5 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 5. **ინფორმაციული ომის ორი შემადგენელი: საინფორმაციო-ფსიქოლოგიური და კიბერომი** - ეს თავი ერთ-ერთი ყველაზე კრიტიკული ნაწილია ამ კურსში, რადგან ის აშიშვლებს რეალურ საფრთხეს — საინფორმაციო-ფსიქოლოგიურ ზემოქმედებას, რომელიც ხშირად ტექნიკურ კიბერშეტევაზე ბევრად უფრო სახიფათოა. აქ მთავარი აქცენტი კეთდება იმაზე, რომ სერვერის აღდგენა ადვილია, ადამიანის ცნობიერების ტრანსფორმაცია კი — თითქმის შეუძლებელი)*

I. პრაქტიკული სავარჯიშო - „საფრთხეების დიაგნოსტიკა — კიბერ vs ფსიქო“

სავარჯიშოს მიზანი. *სტუდენტებმა ისწავლონ ინფორმაციული ომის ორი კომპონენტის გამიჯვნა და მათი ურთიერთკავშირის დანახვა.*

დავალება. *მოცემულია ოთხი მოვლენა. სტუდენტებმა უნდა განსაზღვრონ, რომელია „კიბერომი“ და რომელი „ფსიქოლოგიური ომი“, ასევე იპოვონ „გადაკვეთის წერტილი“.*

1. *სახელმწიფო უწყების ვებგვერდზე დროშის შეცვლა და შეურაცხმყოფელი ტექსტის განთავსება.*
2. *სოციალურ ქსელში ყალბი ვიდეოს (Deepfake) გავრცელება, სადაც პოლიტიკოსი ქვეყნის ღალატს აღიარებს.*
3. *საბანკო მონაცემების ბაზის დაშიფვრა და გამოსასყიდის მოთხოვნა (Ransomware).*

4. *ისტორიული ფაქტების ისეთი ინტერპრეტაცია, რომელიც მეზობელ ერებს შორის შუღლს აღვივებს.*

სადისკუსიო კითხვა. *რატომ არის დასავლური ქვეყნების სტრატეგიების „კალკირება“ (გადმოღება) შეცდომა საქართველოს კონტექსტში?*

II. ქეისი-სტადი (Case Study) - „სუნ ძის პრინციპი პრაქტიკაში“

კონტექსტი. *რუსული სტრატეგია ეყრდნობა სუნ ძის პრინციპს: „საუკეთესო ომია — მტრის ჩანაფიქრის ჩაშლა“. ისინი სწავლობენ სამიზნე აუდიტორიის „კულტურულ კოდებს“.*

ქეისი. *ქვეყანა „X“ აპირებს მნიშვნელოვანი რეფორმის გატარებას განათლების სისტემაში, რაც მის დასავლურ ინტეგრაციას დააჩქარებს. მოწინააღმდეგე ქვეყანა იწყებს საინფორმაციო კამპანიას:*

- *ავრცელებს ნარატივს, რომ ეს რეფორმა ეწინააღმდეგება „ეროვნულ ტრადიციებსა და რელიგიას“.*
- *იყენებს „ინფლუენსერებს“, რომლებიც საუბრობენ, რომ „ჩვენს იდენტობას საფრთხე ემუქრება“.*
- *პარალელურად, კიბერშეტევით აფერხებს განათლების სამინისტროს ბაზების მუშაობას, რათა ადმინისტრაციული ქაოსი შექმნას.*

დავალება სტუდენტებისთვის

1. ***სტრატეგიული ანალიზი.*** *როგორ გამოიყენა მოწინააღმდეგემ „კულტურული კოდი“ მანიპულაციისთვის?*

2. ***ეფექტის შეფასება.*** *რომელი უფრო დააზიანებს ქვეყანას — სამინისტროს საიტის გათიშვა თუ საზოგადოების პოლარიზაცია რეფორმის გარშემო?*

3. ***კონტრსტრატეგია.*** *შეადგინეთ „საინფორმაციო უშიშროების დოქტრინის“ 3 პუნქტი, რომელიც დაიცავდა საზოგადოებას მსგავსი ზემოქმედებისგან.*

III. როლური თამაში - „სოციალური ინჟინერიის ლაბორატორია“

ინსტრუქცია. *სტუდენტები იყოფიან „შემტევებად“ და „თავდაცვის სპეციალისტებად“.*

- ***შემტევები.*** *უნდა მოიფიქრონ ისეთი ფსიქოლოგიური ნარატივი, რომელიც აიძულებს სახელმწიფო მოხელეს, საკუთარი ნებით გახსნას საეჭვო ლინკი (სოციალური ინჟინერია).*

- ***თავდაცვა.*** *უნდა შეიმუშაონ „მედიაწიგნიერების ფილტრი“, რომელიც ამომცნობი იქნება ასეთი მანიპულაციისთვის.*

IV. ანალიტიკური დავალება - „აუტისტური აზროვნება და ინტერნეტი“

ტექსტში ნახსენებია, რომ ინტერნეტში ჩაფლული ადამიანის აზროვნება ხდება „აუტისტური“.

დავალება.

1. *აღწერეთ, როგორ უწყობს ხელს „ექო-კამერები“ (Echo Chambers) ადამიანის რეალობისგან მოწყვეტას.*
2. *მოიყვანეთ მაგალითი, როცა სოციალურმა ქსელმა გამოიწვია რეალური ფიზიკური დაპირისპირება საზოგადოებაში (მაგ., პროტესტი ან არეულობა).*

დასკვნითი კითხვა. *თუ კიბერომი არის „ბრძოლა ბიტებისთვის“, რა არის საინფორმაციო-ფსიქოლოგიური ომის მთავარი „საბრძოლო მასალა“?*

მე-6 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 6. **საერთაშორისო კიბერსივრცე და თანამედროვე ომების თავისებურებანი: ინფორმაციული იარაღი** - ეს თავი აჯამებს ინფორმაციული იარაღის არსს და შემოაქვს "ჰიბრიდული ომის" თანამედროვე გაგება. აქ განსაკუთრებით საინტერესოა გადასვლა წმინდა ფსიქოლოგიური მანიპულაციიდან (NLP, ბრბოს მართვა) მაღალტექნოლოგიურ, უხილავ ფიზიკურ იარაღზე (CHAMP)*

I. პრაქტიკული სავარჯიშო - „ინფორმაციული იარალის ტრიადა“

სავარჯიშოს მიზანი: *სტუდენტებმა გააანალიზონ, როგორ მოქმედებს ერთი და იგივე იარაღი სხვადასხვა დონეზე (კოგნიტური, იდენტობის, ტექნიკური).*

დავალება. წარმოიდგინეთ, რომ ქვეყნის წინააღმდეგ განხორციელდა კომპლექსური შეტევა. სტუდენტებმა უნდა შეავსონ ცხრილი და განსაზღვრონ, რომელი ქმედება რომელ დონეს აზიანებს:

ქმედება	***ზემოქმედების დონე***	***შედეგი (ეფექტი)***
სამხედრო კავშირგაბმულობის გათიშვა	*ტექნიკური*	*მართვის პარალიზება*
ყალბი ისტორიული ფილმების ტირაჟირება	*იდენტობის*	*ეროვნული თვითმყოფადობის შერყევა*
მასობრივი პანიკის დათესვა ვირუსის შესახებ	*კოგნიტური*	*გადარჩენის ინსტინქტის აქტივაცია / ლოგიკის გათიშვა*

II. ქეის-სტადი (Case Study) - „უხილავი დარტყმა — CHAMP-ის ეფექტი“

კონტექსტი.

CHAMP-რაკეტა ანადგურებს ელექტრონიკას ფიზიკური ნგრევის გარეშე. ეს არის "შეიარაღების ახალი ფილოსოფია".

ქეისი.

წარმოიდგინეთ, რომ დაპირისპირებისას ერთ-ერთმა მხარემ გამოიყენა CHAMP-ტექნოლოგია მოწინააღმდეგის დედაქალაქის წინააღმდეგ. 30 წამში ქალაქში:

1. *გაითიშა ყველა კომპიუტერული ქსელი და მობილური კავშირი;*
2. *მწყობრიდან გამოვიდა საავადმყოფოების აპარატურა და ბანკომატები;*
3. *სამხედრო შტაბმა დაკარგა კავშირი ქვედანაყოფებთან, თუმცა არც ერთი შენობა არ დანგრეულა და არც ერთი ტყვია არ გავარდნილა.*

დავალება სტუდენტებისთვის.

- ***სტრატეგიული ანალიზი.*** *შეიძლება თუ არა ეს ჩაითვალოს "ჰუმანურ იარაღად", რადგან ფიზიკური მსხვერპლი მინიმალურია? დაასაბუთეთ პასუხი.*
- ***საერთაშორისო სამართალი.*** *როგორ უნდა დაამტკიცოს დაზარალებულმა მხარემ აგრესია,*

თუ CHAMP-ი არ ტოვებს ნამსხვრევებსა და ნანგრევებს?

- ***რეაგირება.*** *თქვენ ხართ ამ ქვეყნის თავდაცვის მინისტრი. რა არის თქვენი პირველი ნაბიჯი ასეთ "ინფორმაციულ ვაკუუმში"?*

III. ანალიტიკური დავალება - „CNN-ის ეფექტი და გლობალური იარაღი“

ტექსტში საუბარია იმაზე, რომ მედია ახდენს ომების დემონსტრირებას რეალურ დროში, რაც ცვლის პოლიტიკურ დღის წესრიგს.

დავალება.

1. *გაიხსენეთ რომელიმე თანამედროვე კონფლიქტი (მაგ: უკრაინა-რუსეთის ომი).*
2. *მოიყვანეთ მაგალითი, როდესაც სოციალურ ქსელში გავრცელებულმა კადრებმა აიძულა დასავლეთის მთავრობები, მიეღოთ უფრო მკაცრი პოლიტიკური გადაწყვეტილებები (მაგ., სანქციები), ვიდრე მანამდე აპირებდნენ.*
3. *შეაფასეთ. ამ შემთხვევაში მედია იყო "დამკვირვებელი" თუ "ინფორმაციული იარაღი"?*

IV. მინისემინარი - „NLP და პოლიტიკური მანიპულაცია“

ინსტრუქცია. *სტუდენტებმა უნდა ნახონ რომელიმე ცნობილი პოლიტიკოსის გამოსვლის ვიდეო-ჩანაწერი (კრიზისულ სიტუაციაში) და ამოიცნონ ნეიროლინგვისტური პროგრამირების ელემენტები:*

- *გარკვეული ფრაზების მრავალჯერადი გამეორება (ინსტალაცია);*
- *ემოციური "ღუზების" გამოყენება (შიშის ან იმედის გაღვივება);*
- *"ჩვენ" და "ისინი" დაპირისპირების ხაზის გაძლიერება.*

დასკვნითი კითხვა.

თუ CHAMP-რაკეტა ატომურ ბომბსაც კი გამოუსადეგარს ხდის, ნიშნავს თუ არა ეს, რომ 21-ე საუკუნეში ფიზიკური ძალა (ჯარისკაცების რაოდენობა) მეორეხარისხოვანი გახდა?

მე-7 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 7. **ინფორმაციული უშიშროება - ეროვნული უშიშროების სისტემის სტრატეგიული კომპონენტი**)*

სავარჯიშო. ტერმინოლოგიური კლასიფიკატორი

ინსტრუქცია. ქვემოთ მოცემულია 5 სხვადასხვა სცენარი. თითოეული მათგანისთვის განსაზღვრეთ, რომელი ტერმინი უნდა იქნეს გამოყენებული — „კიბერუსაფრთხოება“ თუ „კიბერუშიშროება“ — ამ წიგნის თეორიული ჩარჩოს მიხედვით. დაასაბუთეთ პასუხი SCOPUS-ის ან UDC-ის კლასიფიკატორზე მითითებით.

1. ***სცენარი ა.*** *ბანკის სერვერზე განხორციელდა DDoS შეტევა, რამაც გამოიწვია ვებგვერდის დროებითი გათიშვა. IT ჯგუფი მუშაობს ფაირვოლის პარამეტრების შეცვლაზე.*

2. ***სცენარი ბ.*** *ქვეყნის პარლამენტი განიხილავს „ეროვნული კიბერსტრატეგიის“ დოკუმენტს, სადაც გაწერილია უწყებათაშორისი კოორდინაციის მექანიზმები კრიტიკული ინფრასტრუქტურის დასაცავად.*

3. ***სცენარი გ.*** *პროგრამისტი ქმნის ახალ დაშიფვრის ალგორითმს, რათა დაიცვას მომხმარებლის პირადი მონაცემები არაავტორიზებული წვდომისგან.*

4. ***სცენარი დ.*** *საერთაშორისო კონფერენციაზე განიხილავენ, თუ როგორ ცვლის კიბერშეტევები თანამედროვე ომის წარმოების წესებს და რა გავლენას ახდენს ეს გლობალურ პოლიტიკურ სტაბილურობაზე.*

5. ***სცენარი ე.*** *შინაგან საქმეთა სამინისტრო ამუშავებს საკანონმდებლო ცვლილებებს, რომლებიც განსაზღვრავს მოქალაქეთა უფლება-მოვალეობებს ციფრულ სივრცეში და სახელმწიფოს პასუხისმგებლობას მათ დაცვაზე.*

ქეის-სტადი (Case Study) - „ოპერაცია ციფრული სუვერენიტეტი“

კონტექსტი. *პირობით ქვეყანაში „X“ განხორციელდა მასშტაბური კიბერშეტევა ელექტროენერგიის გამანაწილებელ ქსელზე. შეტევის შედეგად დედაქალაქი 12 საათი დენის გარეშე დარჩა. გამოძიებამ აჩვენა, რომ შეტევა განახორციელა მეზობელი მტრული სახელმწიფოს მიერ დაფინანსებულმა ჰაკერულმა ჯგუფმა, მიზანი კი ქვეყანაში პანიკის დათესვა და მომავალი არჩევნების წინ ხელისუფლების დესტაბილიზაცია იყო.*

დავალება სტუდენტებისთვის. *თქვენ ხართ ეროვნული უშიშროების საბჭოს მრჩეველთა ჯგუფი. დაყავით პრობლემა ორ ნაწილად, წიგნის ავტორის მეთოდოლოგიის მიხედვით:*

ნაწილი 1 - „კიბერუსაფრთხოების“ ჭრილი (ტექნიკური დონე)

- *აღწერეთ, რა ტექნიკური ღონისძიებები უნდა გატარდეს სერვერების დასაცავად (UDC 004).*
- *ვისი კომპეტენციაა ეს საქმიანობა (ინფორმატიკოსები, სისტემური ადმინისტრატორები)?*

- *რა როლი აქვს აქ „უსაფრთხოების ტექნიკას“?*

ნაწილი 2 - „კიბერუშიშროების“ ჭრილი (სოციოპოლიტიკური დონე)

- *ჩამოაყალიბეთ სახელმწიფოს პოლიტიკური რეაგირების გეგმა (UDC 32).*
- *როგორ უნდა შეიცვალოს კანონმდებლობა ან ეროვნული სტრატეგია, რომ თავიდან ავიცილოთ პოლიტიკური დესტაბილიზაცია?*
- *რატომ არის ეს შემთხვევა „ეროვნული უშიშროების“ და არა მხოლოდ „ინფორმაციული უსაფრთხოების“ საკითხი?*

შეჯამება პრაქტიკოსებისთვის (Key Takeaways)

- ***თუ პრობლემას აგვარებს კოდი ან აპარატურა** - არის **კიბერუსაფრთხოება**.*
- ***თუ პრობლემას აგვარებს კანონი, პოლიტიკა, სტრატეგია ან დიპლომატია** - არის **კიბერუშიშროება**.*

მე-8 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 8. **საერთაშორისო სამოქმედო სტრატეგია კიბერსივრცეში.**)*
ეს თავი განსაკუთრებით საინტერესოა, რადგან ის გეოპოლიტიკურ ჭრილში განიხილავს კიბერსივრცეს. აქ ჩანს ფუნდამენტური იდეოლოგიური დაპირისპირება დასავლურ დემოკრატიებსა და ავტორიტარულ რეჟიმებს შორის, რაც პირდაპირ აისახება საერთაშორისო სამართალსა და უშიშროების არქიტექტურაზე)

I. პრაქტიკული სავარჯიშო - „კიბერ-დიპლომატიის დებატები“

სავარჯიშოს მიზანი. *სტუდენტებმა გაითავისონ სხვადასხვა ბლოკის პოლიტიკური არგუმენტაცია და ისწავლონ ინტერესთა კონფლიქტის ანალიზი.*

ინსტრუქცია. *ჯგუფი დაყავით სამ ნაწილად:*

1. ***დელეგაცია ა (დასავლური მოდელი) -*** *იცავენ პოზიციას, რომ არსებული საერთაშორისო სამართალი საკმარისია და მთავარია "ქცევის წესები";*
2. ***დელეგაცია ბ (ავტორიტარული მოდელი) -*** *მოითხოვენ ახალ ხელშეკრულებებს და კიბერიარაღის სრულ აკრძალვას (ოფიციალურ დონეზე);*
3. ***ექსპერტთა საბჭო (გაერო):*** *უნდა შეაჯერონ პოზიციები და გამოყონ საერთო წერტილები.*

სადისკუსიო დავალება. *რატომ არის აშშ-ის მიდგომა (აქტიური შეტევითი ოპერაციები 4 ქვეყნის წინააღმდეგ) სტრატეგიული აუცილებლობა და არა მხოლოდ აგრესია?*

II. ქეის-სტადი (Case Study) - „კოლექტიური თავდაცვა ციფრულ ეპოქაში“

კონტექსტი. *ნატოს 2021 წლის ხედვით, კიბერსაფრთხეები პირველი რიგის ამოცანაა. CDI (კიბერშეკავების ინიციატივა) კი პარტნიორების ერთიანობაზეა ორიენტირებული.*

ქეისი. *წარმოიდგინეთ, რომ ნატოს ერთ-ერთ წევრ ქვეყანაზე განხორციელდა კიბერშეტევა, რომელმაც მწყობრიდან გამოიყვანა ქვეყნის ელექტროგადამცემი ხაზები ზამთრის პერიოდში. კვალი მიდის რუსულ ჰაკერულ დაჯგუფებამდე, თუმცა კრემლი აცხადებს, რომ ეს "კერძო პირების ინიციატივაა" და სახელმწიფოსთან კავშირი არ აქვს.*

დავალება სტუდენტებისთვის.

1. ***სამართლებრივი ანალიზი.*** *გამოიყენეთ დასავლური მოდელის არგუმენტები — როგორ შეიძლება საერთაშორისო ჰუმანიტარული სამართლის მისადაგება ამ შემთხვევაზე?*
2. ***სტრატეგიული რეაგირება.*** *CDI-ის პრინციპების მიხედვით, რა ტიპის "ერთობლივი პასუხი" შეიძლება გასცეს აშშ-მა და მისმა მოკავშირეებმა ამ აქტზე?*
3. ***პოლიტიკური დილემა.*** *უნდა ჩაითვალოს თუ არა ეს შეტევა "შეიარაღებულ თავდასხმად", თუ ფიზიკური იარაღი არ გამოყენებულა, მაგრამ შედეგი (მოსახლეობის გაყინვა) კატასტროფულია?*

III. ანალიტიკური დავალება - „კიბერსივრცის ოთხი შრე“

ტექსტში მოცემულია კიბერსივრცის ანატომია: ფიზიკური, ლოგიკური, ქსელური და მონაცემთა შრეები.

დავალება. *შეარჩიეთ ერთი რეალური კიბერინციდენტი (მაგალითად, **Stuxnet** ან **NotPetya**) და აღწერეთ, როგორ დააზიანა მან თითოეული შრე:*

- ***ფიზიკური** - რა ტექნიკა დაზიანდა რეალურად?*
- ***ლოგიკური** - რომელი კოდი/ვირუსი იქნა გამოყენებული?*
- ***ქსელური** - როგორ გავრცელდა ის სისტემაში?*
- ***მონაცემთა** - რა ინფორმაცია იქნა მოპარული ან წაშლილი?*

IV. კოგნიტური დავალება - „კონსენსუალური ჰალუცინაცია“

უილიამ გიბსონი კიბერსივრცეს უწოდებს "კონსენსუალურ ჰალუცინაციას".

დავალება. *დაწერეთ მოკლე ესე (150-200 სიტყვა) თემაზე: **"როგორ ხდება კიბერსივრცე 'ადგილი' (Michael Batty-ს მიხედვით) და რატომ არის ამ 'ადგილის' დაცვა ისეთივე მნიშვნელოვანი, როგორც სახელმწიფო საზღვრის?"***

დასკვნითი კითხვა სტუდენტებისთვის. *თუ კიბერსივრცეში ძალაუფლება "გაფანტულია ათასობით ნაკადში", რატომ ცდილობენ სახელმწიფოები მის "მილიტარიზაციას" და ცენტრალიზებულ კონტროლს?*

მე-9 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 9. **საერთაშორისო სამართალი და ომი კიბერსივრცეში** - ამ თავს სამართლებრივ ჭრილში გადააქვს კიბერომის თემატიკა, რაც სტუდენტებისთვის ხშირად ყველაზე რთულად აღსაქმელი ნაწილია. აქ მთავარია იმის გააზრება, რომ ტექნოლოგიური პროგრესი წინ უსწრებს კანონმდებლობას, თუმცა არსებობს ფუნდამენტური პრინციპები, რომლებიც ციფრულ სამყაროზეც ვრცელდება)*

I. პრაქტიკული სავარჯიშო - „კომბატანტი თუ კრიმინალი?“

სავარჯიშოს მიზანი. *საერთაშორისო ჰუმანიტარული სამართლის (სჰს) მიხედვით პირთა სტატუსის განსაზღვრის სწავლება.*

ინსტრუქცია. *სტუდენტებს მიეცით სამი პერსონაჟის აღწერა. მათ უნდა დაადგინონ თითოეულის სტატუსი (კომბატანტი, სამოქალაქო პირი თუ „უკანონო მებრძოლი“) და განმარტონ, იცავს თუ არა მათ ჟენევის კონვენცია ტყვედ ჩავარდნის შემთხვევაში.*

1. ***გიორგი:*** *მუშაობს თავდაცვის სამინისტროს კიბერ-დანაყოფში, აცვია ფორმა და ასრულებს ბრძანებას მოწინააღმდეგის რადარების გათიშვის შესახებ.*
2. ***ანო:*** *სტუდენტი, რომელიც საკუთარი ინიციატივით (სახლის კომპიუტერიდან) „ტეხავს“ მოწინააღმდეგის სამთავრობო საიტებს პროტესტის ნიშნად.*
3. ***ლუკა.*** *კერძო IT კომპანიის თანამშრომელი, რომელიც სახელმწიფომ დაიქირავა*

მოწინააღმდეგის ენერგოსისტემაზე შეტევის განსახორციელებლად.

სადისკუსიო კითხვა. *არის თუ არა კლავიატურა „იარაღი“ და როდის ხდება პროგრამისტი „ლეგიტიმური სამხედრო სამიზნე“?*

II. ქეისს-სტადი (Case Study) - „ლოგიკური ბომბი და საშიში ძალები“

კონტექსტი. *ჟენევის კონვენცია კრძალავს თავდასხმას ისეთ ობიექტებზე, რომლებიც „ბუნების საშიშ ძალებს“ (კაშხლები, ატომური სადგურები) შეიცავს.*

ქეისი. *კონფლიქტის დროს, მხარე „A“-მ გამოიყენა „ლოგიკური ბომბი“ (მავნე კოდი), რათა გაეთიშა მხარე „B“-ს ჰიდროელექტროსადგურის წყლის დონის მაკონტროლებელი სისტემა. შედეგად, კაშხალი ავტომატურად გაიხსნა, რამაც ქვემოთ მდებარე დასახლებული პუნქტების დატბორვა და მშვიდობიანი მოსახლეობის მსხვერპლი გამოიწვია. მხარე „A“ ამტკიცებს, რომ მას არც ერთი რაკეტა არ უსვრია და ეს მხოლოდ „ტექნიკური ხარვეზი“ იყო.*

დავალება სტუდენტებისთვის.

1. ***სამართლებრივი შეფასება.*** *შმიდტისა და სჰს-ის პრინციპების მიხედვით, დაარღვია თუ არა მხარე „A“-მ საერთაშორისო სამართალი?*
2. ***შერჩევითობის პრინციპი.*** *შეეძლო თუ არა „ინფორმაციულ იარაღს“ ამ შემთხვევაში უფრო შერჩევითად (Selective) მოქმედება, რათა თავიდან აეცილებინა სამოქალაქო მსხვერპლი?*

3. ***პასუხისმგებლობა.*** *ვინ უნდა აგოს პასუხი ამ ქმედებაზე — პროგრამისტმა, რომელმაც კოდი დაწერა, თუ გენერალმა, რომელმაც შეტევის ბრძანება გასცა?*

III. ანალიტიკური დავალება - „შიმოდის საქმე და კიბერ-პრეცედენტი“

დავალება. *წაიკითხეთ ტექსტში მოცემული „შიმოდის საქმის“ არსი. წარმოიდგინეთ, რომ ხართ მოსამართლე თანამედროვე საერთაშორისო სასამართლოში.*

- *შეაფასეთ **AI-ზე დაფუძნებული ავტონომიური კიბერიარაღის** ლეგალურობა.*
- *გამოიყენეთ პრინციპი: „ნებადართულია ის, რაც პირდაპირ არ არის აკრძალული“ VS „აკრძალულია ის, რაც იწვევს ზედმეტ ტანჯვას“.*

IV. კოგნიტური დავალება - „საშინაო საქმეებში ჩაურევლობა“

ტექსტში საუბარია იმაზე, რომ იდეოლოგიური ჩარევა და პროპაგანდა აკრძალულია სახელმწიფოს საშინაო საქმეებში ჩაურევლობის პრინციპით.

დავალება. *მოიყვანეთ მაგალითი, როდესაც ერთი ქვეყნის მიერ მეორე ქვეყნის სოციალურ ქსელებში წარმოებული კამპანია (მაგ: არჩევნების წინ) სცილდება „აზრის გამოხატვის თავისუფლებას“ და ხდება „აგრესიული ჩარევა სუვერენიტეტში“. სად გადის ზღვარი?*

დასკვნითი კითხვა სტუდენტებისთვის. *თუ საერთაშორისო სამართალი კრძალავს სამოქალაქო*

ობიექტებზე შეტევას, რატომ არის კიბერსივრცეში „საბანკო სისტემა“ ყველაზე მოწყვლადი და ხშირად გამოყენებადი სამიზნე?

მე-10 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 10. **ინფორმაციული ომი და სახელმწიფო საინფორმაციო პოლიტიკა** - ეს თავი განსაკუთრებით მნიშვნელოვანია, რადგან ის თეორიული მსჯელობიდან გადადის სახელმწიფო მართვის პრაქტიკულ სიბრტყეზე. აქ მთავარი აქცენტი კეთდება იმაზე, რომ ინფორმაციული უსაფრთხოება და ინფორმაციული უშიშროება არ არის მხოლოდ IT სპეციალისტების საქმე, არამედ არის კომპლექსური სახელმწიფოებრივი პოლიტიკა, რომელიც მოიცავს კულტურას, კანონმდებლობასა და ინოვაციებს)*

I. პრაქტიკული სავარჯიშო - „საინფორმაციო პოლიტიკის დიზაინი“

სავარჯიშოს მიზანი. *სტუდენტებმა ისწავლონ განსხვავება საინფორმაციო პოლიტიკის „ფართო“ და „ვიწრო“ გაგებას შორის და შეძლონ მათი ინტეგრირება.*

დავალება. წარმოიდგინეთ, რომ ხართ სახელმწიფო უშიშროების საბჭოს მრჩეველი. უნდა შეადგინოთ მოკლე გეგმა ახალი სახელმწიფო ინიციატივისთვის: „საქართველოს ციფრული მედეგობა 2030“.

შეავსეთ ცხრილი შემდეგი ლოგიკით:

კომპონენტი	***დონე (ფართო თუ ვიწრო?)***	***კონკრეტული აქტივობა (მაგალითი)***
ტექნოლოგიური	*ვიწრო*	*Li-Fi ტექნოლოგიის დანერგვა სამთავრობო შენობებში*
საგანმანათლებლო	*ფართო*	*მედიაწიგნიერების გაკვეთილები სკოლებში*
საკანონმდებლო	*ვიწრო*	*კანონი კიბერსივრცეში მომხმარებლის პასუხისმგებლობაზე*
კულტურული	*ფართო*	*ისტორიული არქივების*

კომპონენტი	დონე (ფართო თუ ვიწრო?)	კონკრეტული აქტივობა (მაგალითი)
		ციფრული დაცვა და პოპულარიზაცია

II. ქეის-სტადი (Case Study) - „Li-Fi და Wi-Fi — უსაფრთხოების არჩევანი“

კონტექსტი.

Li-Fi იყენებს სინათლის სპექტრს და მისი ტალღები კედლებში არ გადის, რაც ინფორმაციის გარედან მოპარვას ფიზიკურად შეუძლებელს ხდის.

ქეისი.

სახელმწიფო სტრატეგიული ობიექტი (მაგ., თავდაცვის სამინისტროს ოპერატიული მართვის ცენტრი) დგას არჩევანის წინაშე:

1. *გამოიყენოს მაღალსიჩქარიანი Wi-Fi, რომელიც ხელმისაწვდომია შენობის გარეთაც (ავტოსადგომზე).*
2. *დაამონტაჟოს Li-Fi სისტემა, რომელიც მოითხოვს სპეციალურ LED განათებას და მუშაობს მხოლოდ ოთახის შიგნით.*

დავალება სტუდენტებისთვის.

- ***უსაფრთხოების ანალიზი.*** *დაასაბუთეთ, რატომ არის Li-Fi „ინფორმაციული ჰიგიენის“ ნაწილი და როგორ აზღვევს „არასანქცირებული წვდომის“ რისკს?*

- ***სუსტი წერტილები.*** *ტექსტში ნახსენებია მზის სინათლის ზემოქმედება. როგორ შეიძლება ამან შეაფერხოს მუშაობა და რა ალტერნატივა უნდა არსებობდეს?*

- ***პოლიტიკური გადაწყვეტილება.*** *რამდენად გამართლებულია ძვირად ღირებული ტექნოლოგიის დანერგვა მხოლოდ უსაფრთხოების გამო?*

III. ანალიტიკური დავალება - „კულტურული მემკვიდრეობა როგორც თავდაცვა“

ტექსტში საუბარია იმაზე, რომ კულტურული მემკვიდრეობის დაცვა გარე ინფორმაციული ექსპანსიისაგან სახელმწიფო პოლიტიკის ნაწილია.

დავალება. *მოიყვანეთ რეალური მაგალითი, როდესაც სხვა ქვეყნის საინფორმაციო პოლიტიკა ცდილობდა საქართველოს „ისტორიული ნარატივის გამრუდებას“ (მაგ., ისტორიული ფაქტების გადაკეთება).*

- *როგორ უნდა უპასუხოს ამას სახელმწიფომ „ფართო გაგების“ საინფორმაციო პოლიტიკით? (პასუხი არ უნდა იყოს მხოლოდ „აკრძალვა“).*

IV. კოგნიტური სავარჯიშო - „ინფორმაციული ჰიგიენა“

ინსტრუქცია.

სტუდენტებმა უნდა შეადგინონ 5 პუნქტიანი „ქცევის კოდექსი“ საჯარო მოხელეებისთვის, რომლებიც მუშაობენ სტრატეგიულ ინფორმაციაზე.

- *რა ინფორმაციის გატანაა დაუშვებელი ღია ქსელებში (მაგ., სოციალურ ქსელებში)?*
- *რა საფრთხეს უქმნის სახელმწიფო უშიშროებას სამუშაო მაგიდასთან გადაღებული „სელფი“, სადაც კომპიუტერის ეკრანი ჩანს?*

დასკვნითი კითხვა სტუდენტებისთვის

თუ სახელმწიფო საინფორმაციო პოლიტიკა მხოლოდ „ცენზურა“ არ არის, მაშინ როგორ უნდა დაიცვას სახელმწიფომ საკუთარი „ციფრული სუვერენიტეტი“ ისე, რომ არ დაარღვიოს სიტყვისა და გამოხატვის თავისუფლება?

მე-11 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 11. **კიბერუშიშროებისა და კიბერუსაფრთხოების საერთაშორისო ორგანიზაციები, პრინციპები და სტანდარტები** - ეს თავი ძალიან პრაქტიკული და ინსტიტუციურია. იგი სტუდენტებს აჩვენებს, რომ კიბერსივრცეში წესრიგი არა მხოლოდ კანონებზე, არამედ სტანდარტებსა და პროფესიულ ორგანიზაციებზე დგას. აქ მთავარია იმის გააზრება, რომ დიპლომატების გარდა, უშიშროების არქიტექტურას IT აუდიტორები და სერტიფიცირებული მენეჯერები ქმნიან)*

I. პრაქტიკული სავარჯიშო - „ორგანიზაციული შესაბამისობა“

სავარჯიშოს მიზანი. *სტუდენტებმა ისწავლონ კონკრეტული გამოწვევისთვის შესაბამისი საერთაშორისო პარტნიორის/ორგანიზაციის შერჩევა.*

დავალება. *წარმოიდგინეთ, რომ ხართ დიდი სახელმწიფო ორგანიზაციის უსაფრთხოების სამსახურის უფროსი. თქვენს წინაშე დგას 3 ამოცანა. აირჩიეთ ტექსტში ნახსენები ორგანიზაციებიდან (ISACA, CIS, ISAlliance/CERT) საუკეთესო პარტნიორი თითოეული ამოცანისთვის:*

1. ***ამოცანა 1.*** *გსურთ გადაამზადოთ კადრები და მიიღოთ საერთაშორისო დონის სერტიფიკატი IT-მართვასა და აუდიტში.*
2. ***ამოცანა 2.*** *გჭირდებათ ობიექტური, არაკომერციული რეკომენდაციები, რათა გაზომოთ თქვენი ორგანიზაციის უსაფრთხოების დონე და რისკები.*

3. ***ამოცანა 3.*** *თქვენს სისტემაზე ახლახან განხორციელდა უცნობი ტიპის შეტევა და გჭირდებათ მყისი ტექნიკური რეაგირება და ინფორმაციის გაცვლა სხვა მსხვერპლებთან.*

II. ქეის-სტადი (Case Study) - „სუვერენიტეტის პარადოქსი“

კონტექსტი. *ტექსტში ნახსენებია „საერთაშორისო თანამშრომლობის პარადოქსი“ - თანამშრომლობა აუცილებელია, მაგრამ ის ზღუდავს სუვერენიტეტს ინფორმაციის დაცვის სფეროში.*

ქეისი. *სახელმწიფო „A“-მ აღმოაჩინა, რომ მის კრიტიკულ ინფრასტრუქტურაში შეღწეულია ვირუსი, რომელიც მეზობელი ქვეყნის სერვერიდან იმართება. საერთაშორისო გამოძიებისთვის საჭიროა, რომ სახელმწიფო „A“-მ უცხოელ ექსპერტებსა და საერთაშორისო ორგანიზაციებს (მაგ., CERT) გაუზიაროს თავისი მონაცემთა ბაზების სტრუქტურა და დაზიანებული ფაილები, რომლებიც სახელმწიფო საიდუმლოებას შეიცავს.*

დავალება სტუდენტებისთვის.

- ***ანალიზი.*** *რატომ არის ეს სიტუაცია „სუვერენიტეტის პარადოქსის“ მაგალითი?*
- ***რისკის შეფასება.*** *რა უფრო საშიშია, სახელმწიფო საიდუმლოების ნაწილის გაზიარება საერთაშორისო პარტნიორებისთვის თუ ვირუსის სისტემაში დატოვება?*

- ***გადაწყვეტა.*** *ტექსტში ნახსენები რომელი „საერთაშორისო სტანდარტი“ დაეხმარებოდა სახელმწიფოებს შორის ასეთი კომუნიკაციის ნდობის ამაღლებაში?*

III. ანალიტიკური დავალება - „ელექტრონული მტკიცებულებები“

ტექსტში საუბარია ციფრული მტკიცებულებების მოპოვებისა და აღიარების საერთაშორისო მექანიზმების საჭიროებაზე.

დავალება.

1. *რატომ არის რთული ტრადიციული „ტერიტორიული იურისდიქციის“ გამოყენება, როდესაც დანაშაული ჩადენილია კიბერსივრცეში (მაგ., ჰაკერი ზის ბრაზილიაში, სერვერი დგას გერმანიაში, ხოლო მსხვერპლია საქართველოში)?*
2. *მოიყვანეთ მაგალითი, რატომ შეიძლება სასამართლომ არ მიიღოს ციფრული მტკიცებულება (მაგ., სქრინშოტი), თუ ის არ არის მოპოვებული საერთაშორისო სტანდარტების დაცვით?*

IV. კოგნიტური დავალება - „ცნებათა დისონანსი“

ინსტრუქცია. *ტექსტში ნათქვამია, რომ არ არსებობს „კიბერაგრესიის“ საყოველთაოდ აღიარებული განმარტება.*

- *სტუდენტებმა უნდა სცადონ შეადგინონ „კიბერაგრესიის“ ისეთი განმარტება, რომელიც მისაღები იქნება როგორც დემოკრატიული, ისე განვითარებადი ქვეყნებისთვის.*
- *რა უნდა იყოს მთავარი კრიტერიუმი: შეტევის განზრახვა, თუ მიყენებული ფიზიკური ზიანის მასშტაბი?*

დასკვნითი კითხვა სტუდენტებისთვის. *თუ კერძო კომპანიები (მაგ. Microsoft, Google, Cisco) ფლობენ უფრო მეტ ინფორმაციას კიბერშეტევების შესახებ, ვიდრე ბევრი სახელმწიფოს სპეცსამსახური, რამდენად უნდა ჰქონდეთ მათ ხმის უფლება საერთაშორისო ტექნიკური უსაფრთხოების სტანდარტების შემუშავებისას?*

XII თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 12. **კიბერუშიშროების ნაციონალური სტრუქტურები, მათი მუშაობის მეთოდები და მოქმედების პრინციპები** - ეს თავი კურსის დამაგვირგვინებელი ნაწილია. ის აერთიანებს წინა თავებში შესწავლილ თეორიულ საკითხებს და გვიჩვენებს, თუ როგორ ახორციელებს მსოფლიოს წამყვანი ქვეყნები (აშშ, ესტონეთი) და საქართველო საკუთარ ნაციონალურ კიბერპოლიტიკას. აქ მთავარი აქცენტი გადადის პასიური მოლოდინიდან აქტიურ თავდაცვაზე)*

I. პრაქტიკული სავარჯიშო - „ეროვნული კიბერარქიტექტურის შედარება“

სავარჯიშოს მიზანი. *სტუდენტებმა ისწავლონ სხვადასხვა ქვეყნის სტრატეგიული მიდგომების შედარება და საუკეთესო პრაქტიკის იდენტიფიცირება.*

დავალება. ჯგუფმა უნდა შეავსოს შედარებითი მატრიცა ტექსტში მოცემული ქვეყნების მიხედვით:

ქვეყანა	***მთავარი სტრატეგიული აქცენტი***	***უნიკალური კომპონენტი***
აშშ	*წინწაწეული თავდაცვა (Defend Forward)*	*USCYBERCOM და შეტევითი რეიდები*
ესტონეთი	*ციფრული მედეგობა და მოხალისეობა*	*VSR და NATO-ს დახელოვნების ცენტრი*
რუსეთი	*კოგნიტური და იდეოლოგიური ომი*	*„სულიერი ტრადიციების“ დაცვა*
საქართველო	*ჰიბრიდული საფრთხეების მოგერიება*	*C4I სისტემების განვითარება*

II. ქეის-სტადი (Case Study) - „წინწაწეული თავდაცვა პრაქტიკაში“

კონტექსტი.

აშშ-ის "Defend Forward" კონცეფცია გულისხმობს მოწინააღმდეგის ქსელებში შეღწევას, საფრთხის წინასწარი ნეიტრალიზაციისთვის.

ქეისი.

სახელმწიფო „A“-ს დაზვერვამ აღმოაჩინა, რომ სახელმწიფო „B“-ს ჰაკერული დაჯგუფება ამზადებს მასშტაბურ შეტევას სახელმწიფო „A“-ს საარჩევნო სისტემაზე. შეტევა 48 საათში უნდა დაიწყოს. სახელმწიფო „A“ იყენებს „წინწაწეული თავდაცვის“ სტრატეგიას და ახორციელებს პრევენციულ კიბერრეიდს — დისტანციურად თიშავს მოწინააღმდეგის იმ სერვერებს, საიდანაც შეტევა იგეგმებოდა.

დავალება სტუდენტებისთვის.

1. ***სტრატეგიული ანალიზი.*** *რით განსხვავდება ეს ქმედება ტრადიციული თავდაცვისგან (როდესაც ველოდებით შეტევას და მერე ვიგერიებთ)?*
2. ***ეთიკური და სამართლებრივი დილემა.*** *ჩაითვლება თუ არა ეს ქმედება აგრესიად, თუ ფიზიკური ზიანი არავის მიყენებია, მაგრამ მოწინააღმდეგის სუვერენულ ქსელში შეღწევა მოხდა?*
3. ***საქართველოს კონტექსტი.*** *რამდენად შესაძლებელია მცირე ქვეყანამ გამოიყენოს ასეთი*

აქტიური სტრატეგია რუსული ჰიბრიდული საფრთხეების წინააღმდეგ?

III. სიმულაციური თამაში - „ესტონური მოდელი — ვირტუალური სიტუაციების ოთახი (VSR)“

ინსტრუქცია.

კლასი დაყავით უწყებებად: თავდაცვის სამინისტრო, შინაგან საქმეთა სამინისტრო, კერძო ბანკების გაერთიანება და მოხალისე ექსპერტთა ჯგუფი.

- ***სცენარი.*** *ქვეყანაში გათიშულია ინტერნეტბანკინგი.*
- ***დავალება.*** *VSR-ის პრინციპით, როგორ უნდა მოხდეს ინფორმაციის გაზიარება ამ ოთხ სუბიექტს შორის მყისად? რა ინფორმაციას აწვდის ბანკი ჯარს და რას აკეთებენ მოხალისეები?*

IV. ანალიტიკური დავალება - „საქართველოს სტრატეგია 2021–2024“

დავალება.

ტექსტში მოცემულია საქართველოს სტრატეგიის 4 პრიორიტეტული მიზანი.

1. *დაასაბუთეთ, რატომ არის „კიბერკულტურის განვითარება“ (მოსწავლეების განათლება) ისეთივე მნიშვნელოვანი თავდაცვითი ღონისძიება, როგორც ტექნიკური აღჭურვა.*
2. *როგორ უკავშირდება C4I სისტემის განვითარება მე-4 თაობის ომის (3.2 თავიდან) მოთხოვნებს?*

მე-13 თავიდან პრაქტიკული სავარჯიშო და „ქეის-სტადი“ (Case Study)

*(თავი 13. **კიბერსივრცის დაცვის ევროპული სისტემის ფორმირების პრობლემები** - ეს თავი ასრულებს კურსს და გვიჩვენებს კიბერუშიშროების ევროპულ მოდელს, რომელიც გამორჩეულია თავისი აქცენტით ადამიანის უფლებებზე, დემოკრატიულ ღირებულებებსა და მრავალმხრივ (სამოქალაქო-სამხედრო) თანამშრომლობაზე. მთავარი სიახლეა ხელოვნური ინტელექტის ინტეგრირება თავდაცვაში და "კიბერდიპლომატიის" ცნების შემოტანა)*

I. პრაქტიკული სავარჯიშო - „ევროპული კიბერფარის მექანიზმი“

სავარჯიშოს მიზანი. *სტუდენტებმა გაიგონ, როგორ მუშაობს კოლექტიური თავდაცვის ევროპული პლატფორმები (SOCs და Joint Cyber Unit).*

დავალება. *წარმოიდგინეთ, რომ ევროკავშირის რამდენიმე ქვეყნის ენერგოსისტემაზე ერთდროულად დაიწყო ანომალიური აქტივობა. სტუდენტებმა უნდა გაანაწილონ ფუნქციები ევროპული სტრატეგიის მიხედვით:*

1. ***SOC (Security Operations Centres)*** *- რა როლი აქვს აქ ხელოვნურ ინტელექტს. (პასუხი: ადრეული იდენტიფიცირება და "ფარის" გააქტიურება)?*
2. ***Joint Cyber Unit*** *- როგორ მოახდენს ის სამოქალაქო (IT კომპანიები) და სამხედრო რესურსების კოორდინაციას?*
3. ***კიბერდიპლომატიური ქსელი*** *- რა ნაბიჯები უნდა გადაიდგას საერთაშორისო ასპარეზზე (მაგ., გაეროში) აგრესორის წინააღმდეგ?*

II. ქეის-სტადი (Case Study) - „ატრიბუციის დილემა და ევროპული პასუხი“

კონტექსტი. *ტექსტში ნახსენებია "სამართლებრივი ატრიბუციის" პრობლემა — რთულია დაამტკიცო, ვინ დგას შეტევის უკან ისე, რომ ეს იურიდიულად ვალიდური იყოს.*

ქეისი. *ევროკავშირის ერთ-ერთი წევრი ქვეყნის საავადმყოფოების ქსელი პარალიზებულია Ransomware შეტევით. ტექნიკური კვალი მიუთითებს მესამე ქვეყანაში მდებარე სერვერებზე, თუმცა ეს ქვეყანა უარყოფს კავშირს ჰაკერებთან. ევროკავშირმა უნდა გადაწყვიტოს "კიბერდიპლომატიური პასუხი" (Cyber Diplomacy Toolbox).*

დავალება სტუდენტებისთვის.

- ***ანალიზი.*** *რატომ არის აუცილებელი "ატრიბუცია" სანქციების დასაწესებლად?*
- ***გადაწყვეტილება.*** *თუ მტკიცებულებები მხოლოდ 90%-ითაა სანდო, უნდა გამოიყენოს თუ არა ევროკავშირმა პოლიტიკური სანქციები?*
- ***ღირებულებები.*** *როგორ უნდა დაიცვას ევროკავშირმა ადამიანის უფლებები (მაგ., პაციენტების მონაცემთა კონფიდენციალურობა) ამ შეტევის გამოძიებისას?*

III. ანალიტიკური დავალება - „ინვესტიცია მომავალში – ციფრული ევროპა“

ტექსტში საუბარია 4.5 მილიარდი ევროს ინვესტიციაზე, მათ შორის კვანტურ კავშირებსა და დეზინფორმაციასთან ბრძოლით.

დავალება.

1. *რატომ მიიჩნევს ევროკავშირი, რომ **კვანტური კავშირი** არის მომავლის უშიშროების გარანტი (მინიშნება: კვანტური დაშიფვრის გატეხა ტრადიციული კომპიუტერებით შეუძლებელია)?*
2. *დაასაბუთეთ, რატომ არის "ბავშვების ონლაინუსაფრთხოება" კიბერუშიშროების სტრატეგიის ნაწილი და არა მხოლოდ სოციალური საკითხი?*

IV. შემაჯამებელი დისკუსია - „საქართველო და ევროპული კიბერსივრცე“

ინსტრუქცია. *ტექსტის დასკვნაში ნათქვამია, რომ ევროპა ხდება უშიშროების გარანტი პარტნიორი ქვეყნებისთვისაც (საქართველო).*

კითხვები დისკუსიისთვის.

- *რა პრაქტიკული სარგებელი შეიძლება მიიღოს საქართველომ "ერთობლივი კიბერდანაყოფის" (Joint Cyber Unit) გამოცდილებიდან?*
- *რამდენად მნიშვნელოვანია საქართველოსთვის ევროპული "მულტისტეიკჰოლდერული მოდელის" მხარდაჭერა ინტერნეტის მართვისას (ავტორიტარული მოდელის საპირწონედ)?*

დასკვნითი კითხვები მთელი კურსისთვის

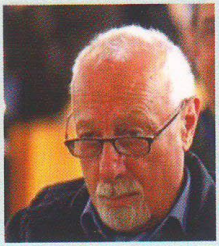
- *13 თავის შესწავლის შემდეგ, როგორ შეიცვალა თქვენი წარმოდგენა "ომზე"? არის თუ არა კიბერსივრცეში მშვიდობა, თუ ჩვენ მუდმივი "უხილავი კონფლიქტის" მდგომარეობაში ვართ?*
- *მთელი კურსის განმავლობაში განხილული მასალის საფუძველზე, რა არის უფრო გადამწყვეტი კიბერომში გამარჯვებისთვის: უახლესი ტექნოლოგიური კოდი თუ საზოგადოების მყარი ფსიქოლოგიური მედეგობა?*

რედაქტორი ლ. მამალაძე

გადაეცა წარმოებას 30.03.2026. ხელმოწერილია დასაბეჭდად 17.04.2026. ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 11,5. №3845.

საგამომცემლო სახლი „ტექნიკური უნივერსიტეტი“, თბილისი, კოსტავას 77

ჰენრი კუპრაშვილი



სტუ-ის პროფესორი; პოლიტიკის მეცნიერებათა დოქტორი; საერთაშორისო ურთიერთობების აკადემიური დოქტორი; ისტორიკოსი; ჟურნალისტი; I კლასის სახელმწიფო მრჩეველი (პრეზ. # 1299 განკ. 2003 წ;) სპორტის დამსახურებული მოღვაწე; ომის ვეტერანი; ვიცე-პოლკოვნიკი.

მეცნიერი, პედაგოგი და პუბლიცისტი: 50-ზე მეტი წლის პედაგოგიური სტაჟი; ავტორი 5 მონოგრაფიის, 10 სახელმძღვანელოსი, 200-მდე სამეცნიერო ნაშრომის, 400-ზე მეტი პუბლიცისტური სტატიისა და კონფერენციაზე წაკითხული 150-ზე მეტი მოხსენების; ხელმძღვანელი 27 დოქტორანტის.

ავტორი და ხელმძღვანელი: ეროვნული უშიშროების საბჭოში 1996 წელს შექმნილი სტრატეგიული ანალიზისა და გლობალური მოდელირების ავტომატიზებული სისტემისა „დიდგორი“ (პრეზიდ. # 05-ს განკარგ.,12.02.1996); იმავე აპარატში პოლიტიკურ მოვლენათა პოლიტომეტრიკული მეთოდით ანალიზისა და პროგნოზირების სისტემისა „აისი“; სტუ-ის სამართლისა და საერთაშორისო ურთიერთობების ფაკულტეტზე განხორციელებული პოლიტიკის მცოდნეობის მულტი და ინტერდისციპლინური სასწავლო-სამეცნიერო პროექტისა „პოლიტიკა სამსჯავროზე“ (საავტორო სერტიფიკატის # 7564).

ჯილდოები: ვახტანგ გორგასლის II ხარისხის ორდენი; „მხედრული მამაცობისათვის“ მედალი (საქართველო); „სამაგალითო სამსახურისთვის“ უკრაინის შჯ-ის მედალი (უკრაინა); ბაირონის საერთაშორისო საზოგადოების ოქროს მედალი (დიდი ბრიტანეთი); წლის ადამიანი-2002, გაზეთი "ახალი ეპოქა"; სტუ-ის აკადემიური საბჭოს საპატიო დიპლომი; ალ. ჩიკვაიძის სახელობის პრემია.

სპორტი: საქართველოს სპორტის დამსახურებული მოღვაწე; მსოფლიო რეკორდსმენი, მსოფლიოში სრუტეთა ახალი წესით გადაცურვისა და საქართველოში პარაცურვის ფუძემდებელი; სამგზის მსოფლიო ჩემპიონი ბიატლსა და ტრიატლში; შვიდ გზის მსოფლიო ჩემპიონი ზამთრის ცურვაში.

ეროვნული მოძრაობა: არჩეული იყო: ნახევრად არალეგალური «დავით აღმაშენებლის ჩოხოსანთა კავშირის - ჩოხოსნები 1973»-ის თავმჯდომარედ 1973 წელს; ერის ღირსების დამცველთა ასოციაცია «იმედის» საწინამძღვროს წევრად (1989-1991); საქართველოს სახალხო ფრონტის დარბაზის წევრად (1989-1992); ზღვისპირეთის დამცველთა ასოციაცია «აიეტის» თავმჯდომარედ 1990 წ.

9 789941 528125

საგამომცემლო სახლი

„ტექნიკური უნივერსიტეტი“

SCAN ME