Scientific and Practical Cyber Security Journal (SPCSJ) 2(3): 08-19 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

INTELLIGENCE FACTORS OF CYBER WARFARE IN INFORMATION SPACE

Ilia Khutsishvili,
The Ministry Of Internal Affairs Of Georgia, LEPL - Security Police Department

ABSTRACT . The state informative process has since been established since the creation of the world in terms of the proper management of the governing system as well as its control. The functioning of the state governing apparatus, its sovereignty, strategic policies, domestic and foreign relations are dependent on the timely, completed and faithful information provision about the processes around the country as well as the various processes taking place outside its borders.

The use and development of modern information-communication technologies in the XXI century is an integral part of any country and society. Protection from the harmful impact of the external forces of the modern state is impossible without the existence of appropriate information technologies. In addition to the state critical infrastructure dependence on information technologies, the need for cyber security is increasing, as analysis of conflicts in the past decade proves that hostilities are not only on land, air and sea but also in information space.

KEYWORDS: National Security, Information Security, Cyber Security, Cyber War, Information War, Misinformation, Hybrid War;

შესავალი

არსებობის თვალსაზრისით, საზოგადოება განაპირობებს სახელმწიფოს, რადგან სწორედ საზოგადოებას შეუძლია, დადებითი ან უარყოფითი კუთხით ზემოქმედება მოახდინოს სახელმწიფოს განვითარებაზე. უცხო სახელმწიფოთა სპეცსამსახურების მნიშვნელოვანი დაინტერესებისა და ზემოქმედების მიმართულებას კონკრეტული სახელმწიფოს საზოგადოება და მასში არსებული განწყობები წარმოადგენს, რადგან საზოგადოებრივი აზრით მანიპულირება (წინასწარ გათვლილი შედეგის მისაღწევად გარკვეული მოქმედებების განხორციელება რასაც საბოლოოდ მოჰყვება ამ შედეგის დადგომა) ერთ-ერთი მძლავრი ბერკეტია სპეცსამსახურების წარმატებული სამოქმედო არეალის შესაქმნელად, რომლის ძირითად მიზანს ძალაუფლების მოპოვება ან არსებულის შენარჩუნება წარმოადგენს. ამ მიზნით უძველესი დროიდან აქტუალურია ინფორმაციულ-ფსიქოლოგიური ომი, რომელშიც მნიშვნელოვანი ადგილი უკავია საზოგადოებრივი აზრით მანიპულირების მეთოდებს.

სოციალურ-პოლიტიკურ ლექსიკონში არსებული განმარტების თანახმად, საზოგადოებრივი აზრი - ესაა, ქვეყნის მოსახლეობის დიდი ნაწილის დამოკიდებულება საზოგადოებრივი ცხოვრების პრობლემებისადმი, რაც გამოიხატება მათ შეფასებებში, მსჯელობასა და განწყობაში. საზოგადოებრივი აზრი არის

იდეოლოგიურ-ფსიქოლოგიური დამოკიდებულება ქვეყენაში არსებული წესრი-გისადმი, მას შეუძლია შეცვალოს, მხარი დაუჭიროს ან უარყოს გარკვეული საკითხები, რომლებიც ეხება ქვეყნის საზოგადოებრივი ცხოვრების სხვადასხვა სფეროს.[1]

მ.ჭაბაშვილის განმარტებით, საზოგადოებრივი აზრით მანიპულირების ერთ-ერთი მიზანია ის, რომ დადგეს წინასწარ გათვლილი შედეგი[2], რომელიც სასურველი იქნებოდა კონკრეტული დაინტერესებული სახელმწიფოსათვის ან ამ სახელმწიფოს პოლიტიკის გამტარებელი ხელისუფალისათვის.[3]

აღნიშნულიდან გამომდინარე, ინფორმაციული ომის პირობებში, არსებობს მაღალი ალბათობა საზოგადოებრივი აზრის არარეალურზე მიმხრობისა, რაც საზოგადოების მიერ სახელმწიფოს წინააღმდეგ მოქმედების მაპროვოცირებელი გარემოება შეიძლება გახდეს. სახელმწიფოს ეროვნული ინტერესების უზრუნველ-ყოფა წარმატებული სადაზვერვო და კონტრსადაზვერვო საქმიანობით, შესაბამისად, სრულყოფილი, ობიექტური და დროული ინფორმაციული უზრუნ-ველყოფით მიიღწევა. შეიძლება ითქვას, რომ სახელმწიფოს განვითარების დონე ინფორმაციული უზრუნველყოფის ხარისხის პირდაპირპროპორციულია, ის, ვინც ინფორმაციას ფლობს, ფლობს ასევე ძალაუფლებასაც.

თავი I. ინფორმაციული უსაფრთხოება როგორც ეროვნული უსაფრთხოების ერთ-ერთი სეგმენტი

სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველმყოფელ ერთ-ერთ უმნიშვნელოვანეს სექტორს ინფორმაციული უსაფრთხოება წარმოადგენს, რომელზეც დამოკიდებულია სახელმწიფოებრივი განვითარების უამრავი სხვა ფაქტორი, მათ შორის თავდაცვისუნარიანობა, სამხედრო-სტრატეგიული მდგომარეობა და უსაფრთხოება. უსაფრთხოების უზრუნველმყოფელ სექტორებს ასევე წარომადგენენ სახელმწიფოს პოლიტიკური, ეკონომიკური, სამეცნიერო-ტექნიკური, თავდაცვის, ეკოლოგიური და სხვა სფეროები.

სხვა მნიშვნელოვან სექტორებთან ერთად, ზემოთ ჩამოთვლილი სეგმენტები ეროვნული უსაფრთხოების ერთიანი ჯაჭვის მაკავშირებელნი არიან, თუმცა აღსანიშნავია, რომ სახელმწიფოს ძლიერი თავდაცვა ვერ ეყოლება თუ ინფორმაციული უსაფრთხება არ არის სათანადოდ უზრუნველყოფილი, ვერ მიიღწევა საზოგადოებრივი თანხმობა და სოლიდარობა თუ ქვეყანაში იქნება უცხო სახელმწიფოთა სპეცსამსახურების მიერ შექმნილი ინფორმაციული ვაკუუმი და დეზინფორმაციის გავრცელების ხელსაყრელი პირობები.

---

[1] სოციალურ და პოლიტიკურ ტერმინთა ლექსიკონი-ცნობარი, თბილისი, გამომცემლობა „ლოგოს პრესი," 2004 წ. გვ. 258;

[2] მიხეილ ჭაბაშვილი, უცხო სიტყვათა ლექსიკონი, თბილისი, გამომცემლობა „განათლება", 1973 წ. გვ. 231;

[3] „საზოგადოებრივი აზრი", საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა, განმარტებითი ლექსიონი, www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=6359; [07/08/2018];

სწორედ აღნიშნულიდან გამომდნარე შეიძლება ითქვას, რომ სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველმყოფელი სექტორებიდან ინფორმაციულ უსაფრთხოებას საკმაოდ დიდი მნიშვნელობა ენიჭება ეროვნული უსაფრთხოების უზრუნველყოფის პროცესში.[4]

ინფორმაციულ უსაფრთხოებას პირდაპირ უკავშირდება პოლიტიკურ დამოუკიდებლობა და სუვერენიტეტი, რადგან სახელმწიფოს ტერიტორიული ხელშეუხებლობა, მისი სუვერენიტეტი სათანადო ინფორმაციული უზრუნველყოფის პირდაპირპროპორციული დამოკიდებულებით მიიღწევა, რადგან „სუვერენიტეტი გულისხმობს ქვეყნის შესაძლებლობას, თავისუფლად აწარმოოს საშინაო და საგარეო საქმეები და არ დაუშვას მის საქმიანობაში საგარეო ან შიდა ძალები“.[5]

სწორედ ამიტომ, მტრულად განწყობილი ქვეყნები სადაზვერვო სამსახურების გამოყენებით იწვევენ დაზვერვას დაქვემდებარებული ქვეყნის ინფირმაციული უსაფრთხოების შემადგენელი ელემენტებისა და (კიბერუსაფრთხოება, კიბერთავდაცვა და სხვ.) სხვადასხვა ბერკეტების გამოყენებით დაზიანებასა და ახარხებენ მაქსიმალურ კონტროლის დაწესებას.

ინფორმაციული უსაფრთხოების უზრუნველყოფა როგორც საჯარო ისე კერძო სექტორების ვალდებულებას წარმოადგენს. ვინაიდან მისი დაუცველობით შესაძლებელია მოპოვებულ იქნას ინფორმაცა რომელიც შეეხება ენერგეტიკის სფეროდან ჰესების სიმძლავრის, მათი დაცვის დონეების შესახებ, ასევე ინფორმაცია ტრანსპორტის, კავშირგაბმულობის, ქვეყნის ინფრასტრუქტურის სხვა დარგებისა და ობიექტების დაცვის სისტემისა და რეჟიმის შესახებ. ინფორმაცია საფინანსო სფეროდან, რომელიც შეეხება ეროვნულ ბანკში დაცულ ინფორმაციას ბანკნოტებისა და მონეტების დამზადებას, გაყალბების თავიდან აცილებას, მიმოქცევას, გაცვლას ან მიმოქცევიდან ამოღებას, რომლის ნაადრევმა გამჟღავნებამ შეიძლება ზიანი მიაყენოს სახელმწიფოს ეკონომიკურ ინტერესებს.

ინფორმაციული უსაფრთხოების უზრუნველყოფა საზოგადოებისა და სახელმწიფოს ჩამოყალიბების დღიდან ერთ-ერთი აქტუალური პრობლემაა, მას კაცობრიობის განვითარების მთელი ისტორიის მანძილზე ყოველთვის გადამწყვეტი მნიშვნელობა ჰქონდა სახელმწიფოს არსებობისთვის. ზოგჯერ იგი დაკავშირებული იყო ქვეყნის სამხედრო ძლიერებასთან, განვითარებასთან, მაგრამ მისი მთავარი ამოცანა ყოველთვის იყო და მომავალშიც იქნება სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველყოფა.

აღნიშნულიდან გამომდინარე შეიძლება ითქვას, რომ სახელმწიფოში ინფორმაციული უსაფრთხოების უზრუნველყოფის ხარისხი განაპირობებს სახელმწიფოს პოლიტიკური დესტაბილიზაციისა და დივერსიებისგან დაცვის ხარისხს.

[4] საქართველოს კანონი „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“, საკანონმდებლო მაცნე, 04/03/2015;

[5] გ.ინწკირველი, „სახელმწიფოსა და სამართლის ზოგადი თეორია“, თბილისი, თბილისის უნივერსიტეტის გამომცემლობა, 2003 წ., გვ. 42.

თავი II. „ჰიბრიდული კონფლიქტები“ და კიბერ უსაფრთხოების სადაზვერვო მნიშვნელობა

XXI საუკუნის დასაწყისიდან მსოფილოს წამყვანი სახელმწიფოების მიერ, (აშშ, რუსეთი, ჩინეთი და სხვ.) თანდათან უფრო დაიხვეწა ინფორმაციული ომის წარმოების ხერხები და მეთოდები, რომლებსაც ისინი საკუთარი მიზნების მისაღწევად და გავლენის სფეროების გასაფართოვებლად იყენებენ. სახელმწიფოს ინფორმაციული უზრუნველყოფის პროცესს სამყაროს წარმოშობიდან დღემდე მნიშვნელოვანი ადგილი უკავია, როგორც მმართველობითი სისტემის სწორი ორგანიზაციის, ისე მისი კონტროლის საშუალებად გამოყენების თვალსაზრისით.

ინფორმაციული უსაფრთხოიების ერთ-ერთ შემადგენელ კომპონენტს წარმოადგენს კიბერ უსაფრთხოება, რომელიც ტექნოლოგიების განვითარებასთან ერთად სულ უფრო და უფრო აქტუალური ხდება სახლემწიფოთათვის. ბოლო ათწლეულში მსოფლიოში მომხდარი კონფლიქტების დროს, სახელმწიფოთა სპეცსამსახურების მიერ აქტიურად გამოიყენება კიბერშეტევები. კიბერდანაშაული დამაზიანებელი სადაზვერვო-ინფორმაციული ომის წარმოების ხელშემწყობ ერთ-ერთ ეფექტურ საშუალებას წარმოადგენს თანამედროვე ჰიბრიდულ კონფიქტებში, რომლებიც ხორციელდება კონფლიქტის მსვლელობისას, რაც გამოიხატება იმაში, რომ ომის დაწყებისთანავე ხდება სახელმწიფოს მთავრობისა და საინფორმაციო საიტების სერვერების კიბერშეტევებით დაზიანება, (ამ კუთხით, 2008 წლის აგვისტოს ომის დროს არც საქართველო იყო გამონაკლისი, კიბერშეტევები ხორციელდებოდა მასობრივად სახელმწიფოს საინფორმაციო-ტექნოლოგიურ სისტემაზე, რაც მიზნად ისახავდა სახელმწიფოს კრიტიკული ინფრასტრუქტურის პარალიზებას).[6]

აღნიშნული სახის შეტევებით მოწინააღმდეგე სახელმწიფოები აფერხებენ სამიზნე სახელმწიფოს მიერ გადაწყვეტილების მიღების უნარს ისევე, როგორც მისი კომუნიკაციის უნარს მსოფლიოს განვითარებულ ქვეყნებთან, რაც ასევე ამცირებს სამიზნე სახელმწიფოს სამხედრო ძალების ოპერატიულ მოქნილობას.

საომარი მიმდინარეობის დროს სამხედრო კიბერშეტევების განხორციელება მოწინააღმდეგე სახელმწიფოზე ზუსტად ერგება ე.წ. ჰიბრიდული ომის კონცეფციას.[7]

პრაქტიკულად კიბერშეტევებით ხდება სახელმწიფოს იზოლაცია ცივილიზებული სამყაროსაგან და მისი მოქცევა ინფორმაციულ ვაკუუმში, რაც დამაზიანებლად მოქმედებს როგორც შეიარაღებული ძალების კოორდინირებულად მოქმედებაზე, ისე ქვეყნის მოსახლეობაზე, ვინაიდან ასეთ შემთხვევაში მოწინააღმდეგე სახელმწიფოს სპეცსამსახურების მიერ ადგილი აქვს დეზინფორმაციის გავრცელებას, რაც იწვევს შიშს, პანიკასა და არეულობას მოსახლეობაში რომელიც უარყოფითად აისახება სახელმწიფოს თავდაცვისუნარიანობაზე.

---

[6] *საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში,* კიბერუსაფრთხოება, 01.08.2015-31.12.2015, 15.

[7] *საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისია,* ტომი II, სექტემბერი, 2009, 256-258.

2008 წლის აგვისტოს ომის დროს საქართველოზე განხორციელებულმა კიბერ შეტევებმა დღის წესრიგში დააყენა ინფორმაციული ინფრასტრუქტურების უსაფრთხოების საკითხი. შეიქმნა შესაბამისი საკანონმდებლო ბაზა და ქვეყანაში ინფორმაციული უსაფრთხოების განვითარების პროცესების კოორდინაცია იუსტიციის სამინისტროს მონაცემთა გაცვლის სააგენტოს დაეკისრა.[8] სააგენტოს ფარგლებში შეიქმნა კომპიუტერულ ინციდენტებზე რეაგირების ჯგუფი (CERT.GOV.GE). აღსანიშნავია, რომ მონაცემთა გაცვლის სააგენტოს კომპეტენციის სფეროა მთავრობის სამოქალაქო ნაწილი, თავდაცვის სტრუქტურებში ინფორმაციული უსაფრთხოების განვითარებაზე კი თავდაცვის სამინისტროს კიბერ უსაფრთხოების ბიურო ზრუნავს.[9]

კიბერუსაფრთხოების უზრუნველყოფის ფარგლებში საქართველოს მთავრობის მიერ მიღებულ იქნა დადგენილება კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ,[10] რომლიც წარმოადგენს კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელ ძირითადი დოკუმენტს. იგი ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს ამოცანებსა და მათ შესასრულებლად განსაზღვრავს შესაბამის აქტივობებს. კიბერუსაფრთხოების განმტკიცების აუცილებლობა განსაზღვრულია ასევე საქართველოს ეროვნული უსაფრთხოების კონცეფციაში.[11]

სადაზვერვო ინფორმაციის მოპოვება ხორციელდება როგორც ღია ისე დახურული წყაროებიდან. ამ მიზნით, განსაკუთრებული შესწავლის ობიექტებს სახელმწიფო და კერძო სექტორში შემავალი ორგანიზაცია-დაწესებულებები წარმოადგენენ. სწორედ ამიტომ სახელმწიფოს მნიშვნელოვან საზრუნავს საჯარო და კერძო სექტორის კონტრსადაზვერვო, ხოლო საერთაშორისო არენაზე მტრულად განყობილ სახელმწიფოებში იმავე სეგმენტის სადაზვერვო უზრუნველყოფა წარმოადგენს.

2014 წელს, რუსეთ-უკრაინის კონფლიქტის დროს განხორციელდა ისეთი კიბერ აქტივობები, როგორიცაა კიბერ შპიონაჟი, ანტისახელმწიფოებრივი და პროპაგანდისტული კამპანიები, კიბერ შეტევები უკრაინული მედიისა და სამთავრობო საიტებზე, NATO-ისა და არასამთავრობო ორგანიზაციების საიტებზე.[12]

გარდა ამისა, რუსეთის დაზვერვის მიერ, ინტერნეტში არსებულ მონაცემები გამოიყენებოდა აღმოსავლეთ უკრაინაში განთავსებული უკრაინული სამხედრო შენაერთების ადგილმდებარეობის დასადგენად. აგრეთვე ხდებოდა დეზინფორმაციის გავრცელება ფორუმებზე, სოციალურ ქსელებში და საინფორმაციო სისტემაში. ყოველივე ზემოაღნიშნული ადასტურებს, რომ

[8] საქართველოს კანონი, „საჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“, საკანონმდებლო მაცნე, 17/07/2009;

[9] საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, საკანონმდებლო მაცნე, 05/06/2012;

[10] საქართველოს მთავრობის დადგენილება №14, „საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ“, 13/01/2017;

[11] საქართველოს პარლამენტის დადგენილება „საქართველოს ეროვნული უსაფრთხოების კონცეფციის“ დამტკიცების შესახებ, საკანონმდებლო მაცნე, 23/12/2011;

[12] *Col. Kowalik T.K., and Jankowski D.P.*, Hybrid warfare – a known unknown?, Monday, 04 July 2016. http://neweasterneurope.eu/2016/07/04/hybrid-warfare-a-known-unknown/ [წვდომის თარიღი: 09.08.2018].

სახელმწიფოთა შორის საომარი მოქმედებების მიმდინარეობამდე ობიექტი ქვეყნის საკომუნიკაციო არხების შესაძლებლობების შესახებ სადაზვერვო ხასიათის ინფორმაციის შეგროვება ხორციელდებოდა.

როგორც აღინიშნა სახელმწიფოს ეროვნული უსაფრთხოების უზრუნველყოფა არამარტო სახელმწიფო სტრუქტურების, არამედ კერძო სექტორისა და თითოეული მოქალაქის სათანადო ინფორმირებით, კოორდინირებული მუშაობითა და ერთსულოვანი, კომპლექსური მიდგომით მიიღწევა. კერძო სექტორზე კიბერ შეტევების მასშტაბის საილუსტრაციოდ 2015 წლის დეკემბერში უკრაინის შემთხვევაც გამოდგება,[13] როდესაც ივანო-ფრანკივსკის რეგიონს, ელექტროსისტემაზე ჰაკერული შეტევების შედეგად ელექტრომომარაგება შეუწყდა.[14]

კიბერ უსაფრთხოების უზრუნველყოფას ერთ-ერთი მნიშვნელოვანი ადგილი უკავია სახელმწიფოთა ეროვნული თავდაცვის განმსაზღვრელ დოკუმენტებში. ამერიკის შეერთებული შტატების 2017 წლის ეროვნული უსაფრთხოების სტრატეგიაში განსაზღვრულია კიბერ უსაფრთხოების უზრუნველყოფის ეტაპები, რომელიც ითვალისწინებს: 1) ქვეყნის კრიტიკული ინფრასტრუქტურების წინააღმდეგ კიბერ შეტევების თავიდან აცილებას; 2) კიბერ შეტევების წინააღმდეგ ქვეყნის დაცვის დონის ამაღლებას და 3) განხორციელებული კიბერ შეტევების შემთხვევაში ზარალისა და შედეგების გამოსწორების დროის მინიმუმამდე დაყვანას.[15]

გარდა კიბერშეტევებისა, ჰიბრიდული კონფლიქტის დროს, სახელმწიფოთა მიერ აქტიურად გამოიყენება სწრაფი რეაგირების, არაიდენტიფიცირებადი, შეიარაღებული დანაყოფები ამოსაცნობი ნიშნების გარეშე, რომლებიც აქტიური საბრძოლო ქმედებებით ახორციელებენ შეტევებს სხვადასხვა ობიექტზე.[16] აღნიშნული სახის კონფლიქტები ზუსტად შეესაბამება ე.წ „ჰიბრიდული ომის“ კონცეფციას, რომელშიც გადამწყვეტი როლი უკავია კრიტიკული ინფრასტრუქტურის უსაფრთხოების უზრუნველყოფის საკითხებს, განსაკუთრებით კი საომარი მოქმედებების მიმდინარეობის დროს.

თავი III. „გერასიმოვის დოქტრინა“ და მაკკუენის „ჰიბრიდული ომები“

[13] Michael J. Assante, Confirmation of a Coordinated Attack on the Ukrainian Power Grid, 09 Jan 2016, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid; [წვდომის თარიღი: 10.08.18]

[14] Roya T. Gordon, M.A. Security and Intelligence Specialist INL Applicant, 2015 Cyber-attack on Ukraine's Power Grid Implications on US Grid Security, September 29, 2016, P.8-11;

[15] National Security Strategy of the United States of America, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, December 2017, [წვდომის თარიღი: 10.08.18];

[16] *Kofman M., Migacheva K., Nichiporuk B., Radin A., Tkacheva O., Oberholtzer J.,* Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, Santa Monica, Calif, 2017, 5-16.

განსაკუთრებით მნიშვნელოვანია „ჰიბრიდული ომის“ ხერხებისა და მეთოდების გასაგებად ე.წ „გერასიმოვის დოქტრინა“.[17] მისი ავტორი რუსეთის ფედერაციის შეიარაღებული ძალების გენერალური შტაბის უფროსი ვალერი გერასიმოვია, რომელმაც აღნიშნული დოქტრინა ერთ-ერთ სამხედრო საიტზე გამოაქვეყნა. დოქტრინაში, გერასიმოვის მიერ ჩამოყალიბებულია რუსეთის შეიარაღებული ძალების მიერ ომის ხერხებსა და მეთოდებში არსებითი ცვლილებები.

გერასიმოვის მიერ „არაბული გაზაფხულის“ გაანალიზების გზით, გაკეთებულია დასკვნები, რომ ნებისმიერი სახელმწიფო, მისი განვითარების დონის მიუხედავად, შეიძლება ჩათრეულ იქნას ომსა და ქაოსში და ამის მისაღწევად მოწინააღმდეგე სახელმწიფოს სულაც არ სჭირდება აქტიური საბრძოლო მოქმედებები, მას აღნიშნულის მიღწევა პოლიტიკური, ეკონომიკური, საინფორმაციო, იდეოლოგიური და სხვა არასამხედრო მოქმედებების გამოყენებით შეუძლია, რომელშიც მნიშვნელოვანია სახელმწიფოს სპეცსამსახურების მეშვეობით ინფორმაციული ომის წარმოება.

გერასიმოვის დოქტრინის მიხედვით, თანამედროვე ომის პირობებში, წარმატების მისაღწევად აუცილებელია მოწინააღმდეგე სახელმწიფოში ქაოსისა და არეულობის განცდის გაჩენა მოსახლეობაში დეზინფორმაციის გავრცელებითა და სადაზვერვო ოპერაციების განხორციელების გზით. დოქტრინის ავტორი გამოყოფს თანამედროვე ომის[18] ხერხებსა და მეთოდებს, რომლებსაც სახელმწიფოები ახორციელებენ ჰიბრიდული ომის წარმოებისას, ესენია:

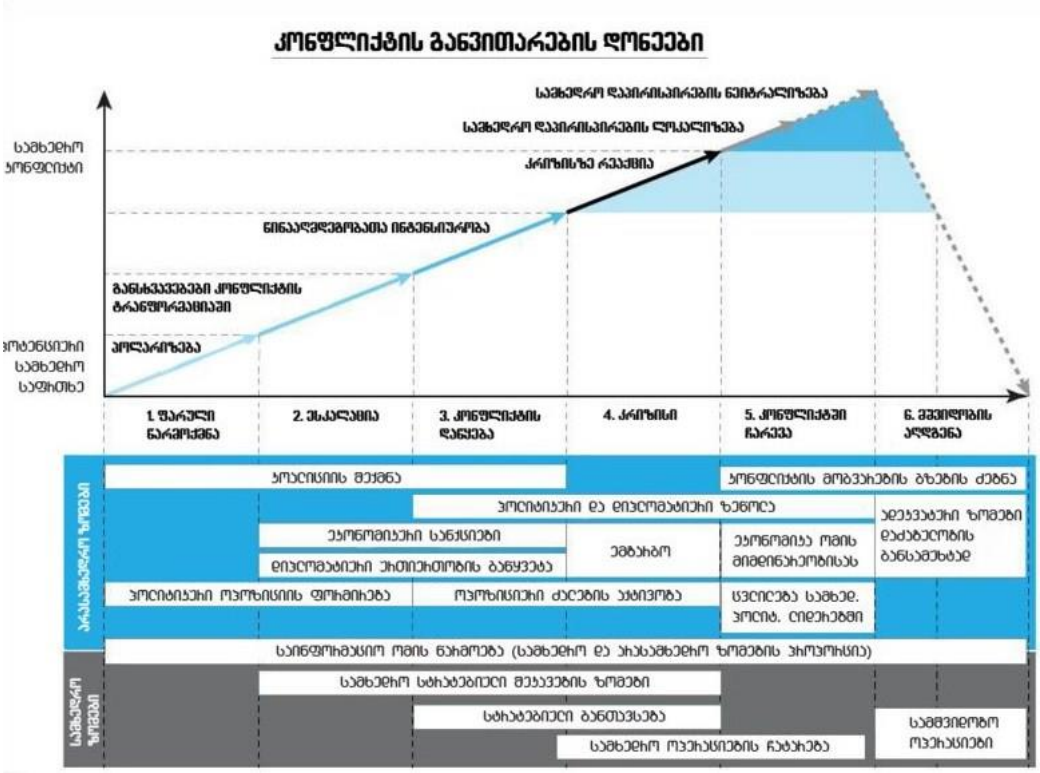
- სამხედრო მოქმედებების დაწყება შეიარაღებული დანაყოფების გადაჯგუფებით მშვიდობიანობის პერიოდში (მაშინ როდესაც ომი არაა გამოცხადებული);
- საბრძოლო დანაყოფების მართვის ერთიანი საინფორმაციო სივრცის უზრუნველყოფა;
- ერთდროული საბრძოლო მოქმედებების განხორციელება სხვადასხვა მიმართულებით: მიწაზე, ჰაერში, ზღვასა და საინფორმაციო სივრცეში;
- დაქირავებული მებრძოლების, ე.წ „მეამბოხეების“, გამოყენება საბრძოლო მოქმედებებში;
- სპეციალური ოპერაციებისა და მაღალტექნოლოგიური იარაღების, (ლაზერული, ბგერითი და სხვ.), რობოტების, გამოყენება საბრძოლო მოქმედებების დროს კომბინირებულად;
- სტრატეგიულ, სამხედრო და სამოქალაქო ინფრასტრუქტურაზე ზუსტი დარტყმების მიყენებით (მათ შორის კიბერ შეტევებით) მოწინააღმდეგეზე სამხედრო და ეკონომიკური ბერკეტებით კონტროლის უზრუნველყოფა;

ამ ქმედებების კომბინირებულად განხორციელება დასახული ამოცანის სწრაფად, მინიმალური დანაკარგებით, სრულმასშტაბიანი, ღია სამხედრო

[17] *Герасимов В.,* Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, Опубликовано в выпуске № 8 (476), за 27 февраля, 2013 года <http://www.vpk-news.ru/articles/14632 >, [წვდომის თარიღი: 13.08.2018].

[18] *Antonenko A., Bambals R., Bērziņš J., Bond I., Cepurītis M., Dobrokhotov R., Kažociņš J., Kudors A., Liuhto K., Nitsovych R., Pabriks A., Pavlenko O.*, The War in Ukraine: Lessons for Europe, The Centre for East European Policy, Studies University of Latvia Press Rīga, 2015, 44.

ინტერვენციის გარეშე გადაწყვეტას აადვილებს.[19] გერასიმოვის დოქტრინის მიხედვით გამოიყოფა ჰიბრიდული ომის წარმოების ექვსი ფაზა, რომლის თანმდევი და უწყვეტი პროცესია ინფორმაციული უზრუნველყოფა.[20]



გრაფიკული დიაგრამის წყარო:[21]

ანალოგიურად აღწერს ჰიბრიდული ომების არსს, ამერიკის შეერთებული შტატების არმიის გადამდგარი პოლკოვნიკი, მაკკუენი 2008 წელს სამხედრო ჟურნალში გამოქვეყნებულ სტატიაში,[22] რომელიც აანალიზებს ამერიკის შეერთებული შტატების მიერ წარმოებულ სამხედრო ოპერაციებს ვიეტნამში, ავღანეთსა და ერაყში და გამოყოფს ჰიბრიდული ომის ქმედებების სამ მთავარ ფრონტს:

1) პირველი, ეს არის ჩვეულებრივი ბრძოლის ველი, სადაც ომისათვის დამახასიათებელი ქმედებებით მიმდინარეობს ბრძოლები; 2) მეორე, არის მოწინააღმდეგე სახელმწიფოს მოსახლეობა, რომელზეც ხორციელდება ინფორმაციულ-იდეოლოგიური ზემოქმედება, რათა თავდამსახმელი სახელმწიფოს ქმედებების გამართლება მოხდეს; 3) მესამე ფრონტი კი არის

[19] Valery Gerasimov, "The Value of Science in Prediction," in The 'Gerasimov Doctrine' and Russian Non-Linear War, by Mark Galeotti, the Blog "In Moscow's Shadows," accessed at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linearwar/ [წვდომის თარიღი: 10.08.18]

[20] Charles K. Bartles, "Getting Gerasimov Right", Military Rreview, January-February 2016, P.35; https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf [წვდომის თარიღი: 10.08.18]

[21] ალექსანდე დუგინი, საინფორმაციო ომი რუსულად: პენტაგონის გასაჯაროებული მასალები, 2017, http://regresearch.ge;

[22] *Mccuen J. J.*, USA, Hybrid Wars, Military Review, Winning the Hybrid War, March-April, 2008, <http://www.au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf >, P.111, [წვდომის თარიღი: 12.08.2018].

საერთაშორისო თანამეგობრობა და საკუთარი ქვეყნის მოსახლეობა, რათა დაარწმუნო ქმედებების სისწორეში და თავიდან აიცილონ საერთაშორისო ზეწოლა და იზოლაცია.

გერასიმოვისა და მაკკუენის აღნიშნული თეორიები „ჰიბრიდული ომის“ წარმოებაზე მიესადაგება მე-20 საუკუნეში მოღვაწე ჩინეთის სამხედრო თეორიტიკოსისა და ლიდერის მაო ძედუნის თეორიას: „საბოლოო გამარჯვების ერთადერთი გზა სტრატეგიულად გაჭიანურებულ ომშია,“[23] სწორედ აღნიშნული თეორია ზუსტად ერგება ე.წ. ჰიბრიდული ომის კონცეფციას, ვინაიდან სახელმწიფოთა მიერ „ჰიბრიდული ომის“ დროს განხორციელებული ქმედებები მუდმივი დაძაბულობის, არეულობის, ქაოსისა და იდეოლოგიურ-ინფორმაციული ომის წარმოებაა, რაც ქმნის მუდმივი ომის განცდას მოსახლეობაში.

დასკვნა

ნაშრომში მოყვანილი ფაქტების განხილვისა და გაანალიზების საფუძველზე შეიძლება ითქვას, რომ ინფორმაციული ომის წარმოებისას სახელმწიფოთათვის დროული, სრულყოფილი და ობიექტური სადაზვერვო ინფორმაციის მოპოვება და კონტრსადაზვერვო რეაგირება სასიცოცხლოდ მნიშვნელოვანია სწორი, საშინაო და საგარეო პოლიტიკური კურსის გასატარებლად, რომლის ერთ-ერთ მიმართულებას სწორედ კიბერ ომის წარმოება წარმოადგენს, ვინაიდან ინფორმაციული ომის ერთ-ერთი მიზანი სწორედ ქვეყნის მოსახლეობაზე ფსიქოლოგიური ზემოქმედების მოხდენაა.

აქედან გამომდინარე, ე.წ ინფორმაციული ომის პირობებში, უცხო სახელმწიფოთა მიერ საკუთარი მიზნების მისაღწევად, მათი სპეცსამსახურების დაინტერესების სფეროების, მიზნების, მისწრაფებებისა და ამოცანების გათვალისწინებით, შესაძლებელია გამოიკვეთოს ძირითადი მიმართულებები, საფრთხეები და რისკ-ფაქტორები, რომლებიც მიესადაგება ინფორმაციული ომის წარმოების კონცეფციას, რომლის მიხედვითაც:

- ობიექტი სახელმწიფოს წინააღმდეგ ინფორმაციული ომის საწარმოებლად კიბერ ომი, კიბერ ტერორიზმი, ჰაკერული შეტევები და სხვ. მიმართულია კრიტიკული ინფრასტრუქტურის პარალიზებისაკენ, რომელიც ემსახურება სამოქალაქო ან სამხედრო (ან კომბინირებულად ორივე ერთად) სექტორის დაზიანებას, დამთრგუნველი საზოგადოებრივი აზრის ჩამოყალიბებასა და დეზინფორმაციის გავრცელებას, რასაც თან სდევს სადაზვერვო შეღწევადობისათვის ხელსაყრელი პირობებისა და საზოგადოების მიერ ხელისუფლებისადმი უარყოფითი განწყობების, მასობრივი არეულობის, კანონიერი ხელისუფლების დამხობის წინაპირობების შექმნა;

- უცხო ქვეყნის სპეცსამსახურების მიერ, თავიანთი ე.წ „წარმომადგენლების“ დახმარებით, „ჰიბრიდული ომის“ მიზნებისა და ამოცანების

[23]იქვე, 109.

განსახორციელებლად ობიექტ სახელმწიფოში მიმდინარე პოლიტიკურ-ეკონომიკურ პროცესებში ჩართვა, ქვეყნის სოციალურ-დემოგრაფიული და ეკონომიკური განვითარების დონის შესწავლა და მტრულად განწყობილი სახელმწიფოსათვის სასარგებლო პროპაგანდის წარმოება მიმდინარეობს;

- ჰიბრიდული ომის პირობებში, სამიზნე ქვეყანის წინააღმდეგ ემბარგო, ეკონომიკური ბლოკადა და სხვ. სამიზნე სახელმწიფოს სოციალურ-ეკონომიკური სტაბილურიბის მოშლის, მოსახლეობაში უკმაყოფილების გაზრდის, მისი მასობრივ პროტესტსა და მასობრივ არეულობაში გადაზრდის ინსპირირების მიზნით ხორციელდება;

- უცხო სახელმწიფოს სპეცსამსახურების მიერ, მათი მომხრე გაერთიანებებისა და პოლიტიკური მოძრაობების ჩამოყალიბება, მათი დაფინასება და ძლიერ პოლიტიკურ პარტიებად გარდაქმნა ხელისუფლების სათავეში მათ პოლიტიკურ კურსზე ორიენტირებული პოლიტიკური ძალის მოყვანის ინსპირირების მიზნით ხორციელდება;

- სამიზნე სახელმწიფოში მოწინააღმდეგე ქვეყნის პოლიტიკაზე ორიენტირებული მასმედიის საშუალებების ფორმირება, ფინანსური მხარდაჭერა და მათი მეშვეობით უცხო სახელმწიფოს სასარგებლო პროპაგანდის წარმოება (ქვეყნის საგარეო და საშინაო პოლიტიკური კურსის დისკრედიტაცია და საკუთარი საგარეო კურსის პოლულარიზაცია, მოსახლეობის იდეოლოგიური დამუშავება, სეპარატისტული იდეების გაჟღერება, ეთნიკურ-რელიგიური შუღლის გაღვივება და სხვ.) მიმდინარეობს, რომელიც კონკრეტული სახელმწიფოს მოსახლეობაში უცხო სახელმწიფოსათვის ხელსაყრელი განწყობების ჩამოყალიბებას ემსახურება.

ბიბლიოგრაფია

1. საქართველოს პარლამენტის დადგენილება „საქართველოს ეროვნული უსაფრთხოების კონცეფციის“ დამტკიცების შესახებ, საკანონმდებლო მაცნე, 23/12/2011;
2. საქართველოს კანონი „ინფორმაციული უსაფრთხოების შესახებ“, საკანონმდებლო მაცნე, 05/06/2012;
3. საქართველოს მთავრობის დადგენილება №14, „საქართველოს კიბერუსაფრთხოების 2017-2018 წლების ეროვნული სტრატეგიისა და მისი სამოქმედო გეგმის დამტკიცების შესახებ“, 13/01/2017;
4. საქართველოს კანონი, „სჯარო სამართლის იურიდიული პირის – მონაცემთა გაცვლის სააგენტოს შექმნის შესახებ“, საკანონმდებლო მაცნე, 17/07/2009;
5. საქართველოს კანონი „ეროვნული უსაფრთხოების პოლიტიკის დაგეგმვისა და კოორდინაციის წესის შესახებ“, საკანონმდებლო მაცნე, 04/03/2015;

6. სოციალურ და პოლიტიკურ ტერმინთა ლექსიკონი-ცნობარი, თბილისი, გამომცემლობა „ლოგოს პრესი," 2004 წ. გვ. 258;
7. *საქართველოს სახელმწიფო უსაფრთხოების სამსახურის ანგარიში*, კიბერუსაფრთხოება, 01.08.2015-31.12.2015, 15;
8. მიხეილ ჭაბაშვილი, უცხო სიტყვათა ლექსიკონი, თბილისი, გამომცემლობა „განათლება", 1973 წ. გვ. 231;
9. „საზოგადოებრივი აზრი", საქართველოს პარლამენტის ეროვნული ბიბლიოთეკა, განმარტებითი ლექსიონი, www.nplg.gov.ge/gwdict/index.php?a=term&d=6&t=6359;
10. Cyril Thomas, "The Role of Intelligence in International Political Economy", University of Dundee, 21 Oct. 2006, https://www.scribd.com/doc/9495674/Role-of-Intelligence;
11. National Security Strategy of the United States of America, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, December 2017,
12. Michael J. Assante, Confirmation of a Coordinated Attack on the Ukrainian Power Grid, 09 Jan 2016, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid;
13. Roya T. Gordon, M.A. Security and Intelligence Specialist INL Applicant, 2015 Cyber-attack on Ukraine's Power Grid Implications on US Grid Security, September 29, 2016, P.8-11;
14. გ.ინწკირველი, „სახელმწიფოსა და სამართლის ზოგადი თეორია", თბილისი, თბილისის უნივერსიტეტის გამომცემლობა, 2003 წ., გვ. 42.
15. *საქართველოში მომხდარ კონფლიქტთან დაკავშირებული ფაქტების დამდგენი დამოუკიდებელი საერთაშორისო მისია,* ტომი II, სექტემბერი, 2009, 256-258.
16. *Col. Kowalik T.K., and Jankowski D.P.*, Hybrid warfare – a known unknown?, Monday, 04 July 2016. <http://www.neweasterneurope.eu/articles-and-commentary/2052-hybrid-warfare-a-known-unknown>
17. *Kofman M., Migacheva K., Nichiporuk B., Radin A., Tkacheva O., Oberholtzer J.,* Lessons from Russia's Operations in Crimea and Eastern Ukraine, RAND Corporation, Santa Monica, Calif, 2017, 5-16.
18. *Frost K. G.*, On Organizing Political Warfare, Blavatnik Family Foundation and Leon Levy Foundation, History and Public Policy Program Digital Archive, April 30, 1948, <https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c>.
19. *იმედაშვილი ა.,* თბილისში საერთაშორისო სამხრეთკავკასიური მედიაფორუმი გაიმართება, <https://sputnik-georgia.com/society/20170627/236441508/TbilisSi-saerTaSoriso-samxreTkavkasiuri-mediaforumi-gaimarTeba.html >, 27 ივნისი, 2017.

20. *ტულუში ლ., გაგუა მ., ღვედაშვილი გ., ლაფაჩი ნ.,* რუსეთის ხისტი და რბილი ძალის საფრთხეები საქართველოში, ევროპული ინიციატივა – ლიბერალური აკადემია, თბილისი, 2016, 24-32.
21. *ძველიშვილი ნ., კუპრეიშვილი თ.,* რუსული გავლენა ქართულ არასამთავრობო ორგანიზაციებსა და მედიაზე, თბილისი, 2015, 46;
22. *Герасимов В.,* Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, Опубликовано в выпуске № 8 (476), за 27 февраля, 2013 года <http://www.vpk-news.ru/articles/14632 >
23. *Antonenko A., Bambals R., Bērziņš J., Bond I., Cepurītis M., Dobrokhotov R., Kažociņš J., Kudors A., Liuhto K., Nitsovych R., Pabriks A., Pavlenko O.*, The War in Ukraine: Lessons for Europe, The Centre for East European Policy, Studies University of Latvia Press Rīga, 2015, 44.
24. Valery Gerasimov, "The Value of Science in Prediction," in The 'Gerasimov Doctrine' and Russian Non-Linear War, by Mark Galeotti, the Blog "In Moscow's Shadows," accessed at https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linearwar/
25. Charles K. Bartles, "Getting Gerasimov Right", Military Rreview, January-February 2016, P.35; https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art009.pdf
26. ალექსანდე დუგინი, საინფორმაციო ომი რუსულად: პენტაგონის გასაჯაროებული მასალები, 2017, http://regresearch.ge;
27. *Mccuen J. J.*, USA, Hybrid Wars, Military Review, Winning the Hybrid War, March-April, 2008, <http://www.au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf >,111.