RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

კრიტიკული ინფრასტრუქტურის დაცვა ევროპაში: მედეგობის გაძლიერება ვაშინგტონის ხელშეკრულების მესამე მუხლის შესაბამისად

მეგი გენია

166

ექსპერტის აზრი

საქართველოს სტრატეგიისა და საერთაშორისო ურთიერთობათა კვლევის ფონდი
GEORGIAN FOUNDATION FOR STRATEGIC AND INTERNATIONAL STUDIES

ექსპერტის აზრი

მეგი ბენია

კრიტიკული ინფრასტრუქტურის დაცვა ევროპაში: მედეგობის გაძლიერება ვაშინგტონის ხელშეკრულების მესამე მუხლის შესაბამისად

166

2021

პუბლიკაცია დაიბეჭდა ამერიკის შეერთებული შტატების საელჩოს ფინანსური მხარდაჭერით. გამოცემაში გამოთქმული მოსაზრებები ეკუთვნის ავტორებს და შეიძლება არ ასახავდეს საელჩოს თვალსაზრისს.

ტექნიკური რედაქტორი: არტემ მელიქ-ნუბაროვი

ISSN 1512-4835
ISBN

ნატო არის უმსხვილესი სამხედრო ორგანიზაცია, რომელიც პასუხისმგებელია ევროატლანტიკური რეგიონის უსაფრთხოებაზე. შესაბამისად, მსოფლიოში და, განსაკუთრებით, ევროპაში ამჟამად არსებული უსაფრთხოების გარემო იწვევს დისკუსიას, თუ რამდენად შეუძლია ნატოს გაუძლოს შეიარაღებულ თავდასხმას. აღსანიშნავია, რომ ეს განხილვა ძირითადად შეეხება მე-5 მუხლს, რომელიც კოლექტიური თავდაცვის საკვანძო კომპონენტია და ამ პროცესში უგულებელყოფილია მე-3 მუხლის პრინციპები, რაც თავისთავად მცდარი მიდგომაა.

ნატოს მე-3 მუხლის თანახმად, „იმისათვის, რომ უფრო ეფექტიანად იქნეს მიღწეული ამ ხელშეკრულების ამოცანები, მხარეები, ცალ-ცალკე და ერთობლივად, განგრძობადი და ეფექტიანი თვითდახმარების და ურთიერთდახმარების საფუძველზე, შეინარჩუნებენ და განავითარებენ თავიანთ ინდივიდუალურ და კოლექტიურ შესაძლებლობებს შეიარაღებული შეტევის აღსაკვეთად“ (NATO, Resilience and Article 3 2020). შესაბამისად, მე-3 მუხლის ვალდებულებების შესრულება ორგანიზაციის კოლექტიური პრინციპის აღსრულების სასიცოცხლო ნაწილია, ვინაიდან ის აძლევს საშუალებას ნატოს, აღასრულოს მე-5 მუხლით განსაზღვრული ვალდებულებები.

მიუხედავად ამისა, აუცილებელია გვახსოვდეს, რომ თანამედროვე არაპროგნოზირებად უსაფრთხოების გარემოში „შეიარაღებული შეტევის მიმართ რეზისტენტულობა“ (NATO, Resilience and Article 3 2020) არ გულისხმობს მხოლოდ სამხედრო მზადყოფნას. იმისათვის, რომ შეიარაღებულმა ძალებმა ოპერაციის შესრულების ან სამხედრო შეტევის დროს შეძლონ ძალების სწრაფი გადასროლა, მათ სჭირდებათ სატრანსპორტო სისტემები, სატელიტური კომუნიკაციის საშუალებები, დენის წყაროები და ა.შ. თუმცა ცნობილი ფაქტია, რომ ეს სისტემები ყველაზე მეტად მოწყვლადია ნებისმიერი შეტევის დროს, როგორც მშვიდობის, ისე ომიანობის პერიოდში.

2014 წლის ყირიმის ანექსიის შემდეგ რუსეთმა გაზარდა ჰიბრიდული აქტივობები ევროპული სახელმწიფოების კრიტიკული ინფრასტრუქტურის წინააღმდეგ, ძირითადად, კიბერშეტევების საშუალებით. ამის მიზეზი კი ის არის, რომ „რუსეთისთვის კიბერშეტევის განხორციელება ოპონენტებზე გავლენის მოხდენის იაფფასიანი და მაღალი შედეგების მომტანი საშუალებაა, რომლისთვისაც ვინმეს პასუხისგებაში მიცემა რთულია. სამხედრო კონფრონტაციის დროს რუსეთს შეუძლია ფართომასშტაბიანი კიბერშეტევის გამოყენება

მოწინააღმდეგეების კრიტიკული ინფრასტრუქტურის დროებით მწყობრიდან გამოსაყვანად“ (Dina 2019).

იმისათვის, რომ ნატომ აღნიშნული მიმართულებით გააუმჯობესოს საკუთარი შესაძლებლობები, 2018 წელს ალიანსმა შეიმუშავა „ეროვნული მედეგობის შვიდი საბაზისო მოთხოვნა, რომელთა მიხედვითაც წევრმა სახელმწიფოებმა უნდა გაზომონ საკუთარი მომზადების დონე“ (NATO, Resilience and Article 3 2020). ერთ-ერთი მათგანი არის „კრიტიკული კომუნიკაციის მედეგი სისტემები, რომლებიც მიზნად ისახავს ტელეკომუნიკაციისა და კიბერქსელების შეუფერხებელ ფუნქციონირებას კრიზისული სიტუაციების დროსაც კი“ (NATO, Resilience and Article 3 2020), ანუ სხვა სიტყვებით რომ ვთქვათ, კრიტიკული ინფრასტრუქტურის დაცვას.

ამასთან, ნატომ მიიღო „გაღრმავებული კიბერთავდაცვის პოლიტიკა“ 2014 წლის უელსის სამიტზე, რომლის განახლებაც შემდგომში მოხდა ვარშავის სამიტზე, 2016 წელს, სადაც მოკავშირეებმა კიბერსივრცე ოპერაციების დომეინად აღიარეს და მიიღეს „კიბერთავდაცვის დათქმა“ (Cyber Defense Pledge) (Kačič 2019). დოკუმენტის თანახმად, მოკავშირეებმა უნდა უზრუნველყონ ეროვნული ქსელებისა და ინფრასტრუქტურის გაძლიერება, ვაშინგტონის ხელშეკრულების მესამე მუხლის შესაბამისად (Kačič 2019). ამასთან, 2018 წლის ბრიუსელის სამიტზე წევრმა ქვეყნებმა გადაწყვიტეს კიბერსივრცეში ოპერაციების ცენტრის (Cyberspace Operations Centre) დაარსება და ეროვნული კიბერშესაძლებლობების ინტეგრირება ნატოს მისიებსა და ოპერაციებში (NATO, Cyber defence 2020) (Kačič 2019)

მიუხედავად ყველა ამ ძალისხმევისა, რომლებიც მიმართულია ალიანსის მოდერნიზაციისა და ადაპტაციისაკენ საერთაშორისო უსაფრთხოების თანამედროვე გამოწვევების მიმართ, ნატოს სჭირდება მიიღოს ყოვლისმომცველი და ეფექტიანი მიდგომა ევროპაში კრიტიკული უსაფრთხოების დაცვასთან დაკავშირებით. წინამდებარე ნაშრომი მიზნად ისახავს სამი ძირითადი მიმართულების იდენტიფიცირებას, რომლებიც უნდა შეიმუშაოს ნატომ კრიტიკული უსაფრთხოების დაცვისა და, შესაბამისად, მედეგობის გაზრდისათვის ვაშინგტონის ხელშეკრულების მე-3 მუხლის შესაბამისად.

ნატოს მედეგობის უზრუნველყოფა კრიტიკული ინფრასტრუქტურის გაუმჯობესებული დაცვით

იმისათვის, რომ გაუმჯობესდეს კრიტიკული ინფრასტრუქტურის დაცვა, ნატომ უნდა:

1. ***შეიმუშაოს კრიტიკული ინფრასტრუქტურის დაცვის ეფექტიანი სტრატეგია***

კრიტიკული ინფრასტრუქტურის უკეთ დასაცავად მოკავშირეებმა უნდა შეიმუშაონ ქსელურ მიდგომაზე დაფუძნებული სტრატეგია. ეს მიდგომა ჩამოაყალიბა ტედ ლიუისმა საკუთარ წიგნში კრიტიკული ინფრასტრუქტურის შესახებ. 9/11-ის ტერორისტულ შეტევაზე ამერიკის შეერთებული შტატების სადაზვერვო სისტემების რეაგირების ანალიზისას ლიუისმა დაასკვნა, რომ „დროში გაწელილმა რეაგირებამ და სხვადასხვა ინსტიტუტებს შორის, ასევე სადაზვერვო და სამართალდაცვითი სისტემების იერარქიულ წყობაში არსებულმა სუსტმა კოორდინაციამ ტერორისტებს წარმატების მიღწევის საშუალება მისცა, მიუხედავად მათ მიერ დაშვებული უამრავი შეცდომისა“ (Lewis 2006). ამიტომ, მისი აზრით, საჭიროა „ისეთი იერარქიული სისტემის შექმნა, სადაც არ იქნებიან შუამდგომლები მმართველობის სხვადასხვა რგოლს შორის. ამის მაგივრად ხელმძღვანელები ჩართული იქნებიან ქსელურ სტრუქტურაში, რომელიც უზრუნველყოფს მონაცემების, დისკუსიებისა და გადაწყვეტილებების წერტილოვან გადაცემას. იერარქიის თითოეული რგოლის მეთაურებს აქვთ უშუალო წვდომა სპეციალისტებთან, რომლებიც ფლობენ სწორ ინფორმაციას და სათანადო ექსპერტიზას. შესაბამისად, გადაწყვეტილებები მიიღება სწრაფად“ (Lewis 2006). ლიუსი მიიჩნევს, რომ ვინაიდან კრიტიკული ინფრასტრუქტურის დაცვაში უმთავრეს პრობლემას ინფორმაციის გაცვლა წარმოადგენს, შემოთავაზებული მოდელი კარგად მოერგება კრიტიკული ინფრასტრუქტურის დაცვას.

იმისათვის, რომ ეს მიდგომა ნატოს რეალობას მოერგოს, წევრი სახელმწიფოები უნდა განვიხილოთ, როგორც ერთი დიდი სტრუქტურის სხვადასხვა სააგენტოები/სექტორები/მეთაურები, რითაც შევქმნით ქსელურ სტრუქტურას შუამდგომლების გარეშე. ისევე, როგორც ერთიანი სისტემის სხვადასხვა ნაწილები პასუხისმგებელი არიან, პირველ რიგში, საკუთარ უსაფრთხოებაზე, ასევე „ნატოს თითოეული წევრი ვალდებულია იყოს მედეგი, რათა

შეინარჩუნოს რეზისტენტულობა და ჰქონდეს აღდგენის უნარი ბუნებრივი კატასტროფის, კრიტიკული ინფრასტრუქტურის მწყობრიდან გამოსვლის, ჰიბრიდული ან შეიარაღებული შეტევით გამოწვეული შოკის შემდეგ“ (NATO, Resilience and Article 3 2020), რაც გათვალისწინებულია ვაშინგტონის ხელშეკრულების მესამე მუხლში. „ქსელური ანალიზი არის ინოვაციური მიდგომა კრიტიკული ინფრასტრუქტურის მოწყვლადობის ანალიზისას და ის უნდა იყოს კრიტიკული ინფრასტრუქტურის დაცვის შესახებ მიღებული ნებისმიერი სტრატეგიის ცენტრალური ხაზი. „მართლაც, ამ მიდგომას ბუნებრივად და ლოგიკურად მივყავართ შესაბამის პრინციპებამდე, რომლებიც შეიძლება მოიცავდეს ნებისმიერ ეფექტიან სტრატეგიას თითქმის ყველა სექტორისთვის“, - ასკვნის ლიუსი.

2. *გააძლიეროს თანამშრომლობა კერძო სექტორთან*

ცნობილია, რომ კრიტიკული ინფრასტრუქტურის ობიექტები, ძირითადად, კერძო საკუთრებაა. შესაბამისად, ისინი არიან ყველაზე მოწყვლადი ნებისმიერი შეტევის შემთხვევაში. მაგალითად, „2014 წელს კიბერუსაფრთხოების კომპანიებმა CrowdStrike და Symantec გამოააშკარავეს რუსეთთან დაკავშირებული ჯგუფების მიერ ჩატარებული კიბეროპერაციები, რომელთა სამიზნე იყო დასავლური გაზისა და ნავთობის კომპანიები, ასევე ენერგეტიკის სფეროში საინვესტიციო კომპანიები, რომელთა ნაწილსაც ხსენებული სამიზნე კიბერინფრასტრუქტურის დისტანციური მართვა ჰქონდათ დანერგილი, რამაც ბევრად გაამარტივა საბოტაჟის განხორციელება“ (Schmitt 2019). ამის შემდგომ, „2015 წლის დეკემბერში, რუსეთმა განახორციელა NotPetya კიბეროპერაციები უკრაინის ენერგეტიკულ ქსელზე. ამავე დროს, რუსეთის ჰაკერულმა ჯგუფებმა დაიწყეს შეტევა ამერიკის ინფრასტრუქტურაზე, მათ შორის, ენერგოქსელსა და ატომურ ელექტროსადგურებზე (Schmitt 2019).

ამრიგად, გასაგები ხდება, რომ კრიტიკული ინფრასტრუქტურის დაცვა თითქმის შეუძლებელია კერძო სექტორის წარმომადგენლებთან წარმატებული თანამშრომლობის გარეშე.

უნდა აღინიშნოს, რომ ნატო განსაკუთრებულ ყურადღებას აქცევს კერძო სექტორთან თანამშრომლობას. 2014 წლის უელსის სამიტზე მოკავშირეებმა გადაწყვიტეს NATO Industry Cyber Partnership-ის (NICP) დაარსება (Kačič 2019). NICP-ის საშუალებით ხდება კიბერთავდაცვის შესახებ ინფორმაციისა და ცოდნის გაზი-

არება, საუკეთესო პრაქტიკის შემუშავება, კიბერრისკების გაგების გაუმჯობესება და სწავლება ნატოს კიბერთავდაცვის მიმართულებით (Kačič 2019).

მიუხედავად ამისა, კერძო სექტორთან თანამშრომლობა უნდა იყოს უფრო ღრმა და მეტად ეფექტიანი. ამისათვის ელსა ლი გვთავაზობს საინტერესო მიდგომას. ავტორის აზრით, საფრთხეების შესახებ მონაცემების მოქნილი წვდომა და ინფორმაციის გაცვლა უნდა იყოს ასეთი ტიპის თანამშრომლობის საფუძველი. ლის აზრით, სამართალდამცავმა სტრუქტურებმა უნდა მისცენ უფლება კერძო სექტორის წარმომადგენლებს ჰქონდეთ წვდომა უკვე ცნობილი საფრთხეების შესახებ მონაცემებზე, რასაც დაეყრდნობიან არსებული ტენდენციის ანალიზისას. სხვადასხვა ორგანიზაცია ისედაც აწარმოებს მომხდარი ინციდენტებისა და მოვლენების საკუთარ შიდა აღრიცხვას. დამატებითი სარგებლის მომტანი იქნებოდა მათ რომ ჰქონდეთ საშუალება, შეხედონ სხვა ორგანიზაციების ინციდენტებს და შეიტყონ მათკენ მიმართული შეტევის, მათ სისტემებში შეღწევისა თუ თვალთვალის შესახებ და გააზიარონ ინფორმაცია. ეს მისცემდა მათ საშუალებას, განეხილათ მათ სისტემებზე ამგვარი შეტევების განხორციელების შესაძლებლობა და ინციდენტი წინასწარ აღეკვეთათ. საფრთხეები შეიძლება ერთ ღამეში შეიცვალოს. სწორედ ამიტომ ინფორმაციის შეგროვება, ანალიზი, შეფასება, საპასუხო ზომების შემუშავება და განხილვა საჭიროა მიმდინარეობდეს უწყვეტად. ამის მიზანია საფრთხე დავინახოთ მანამ, სანამ ის გახდება რეალური, აქტიურად ჩართული რომელიმე დაწესებულების წინააღმდეგ შეტევაში ან უკვე შეღწეული რომელიმე შენობაში, რაც შემდგომში იწვევს კატასტროფას“ (Lee 2009). ასეთი მიდგომა უნდა იყოს საკმაოდ ეფექტიანი, რადგან ერთად უყრის თავს მოწყვლადი სექტორის წარმომადგენლებს და ეხმარება გაიგონ სხვადასხვა ინდუსტრიის ძირითადი მახასიათებლები, რაც პრობლემის გადაჭრის კიდევ ერთი სასიცოცხლო ასპექტია.

3. *ევროკავშირთან თანამშრომლობის გაღრმავება*

2016 წლის 8 ივლისს ევროპული საბჭოს პრეზიდენტმა, ევროკომისიის პრეზიდენტმა და ნატოს გენერალურმა მდივანმა ხელი მოაწერეს ვარშავის ერთობლივ დეკლარაციას (NATO, Joint declaration 2016). დოკუმენტის თანახმად, ევროპაში მედეგობის კიდევ უფრო გასაძლიერებლად ორი ორგანიზაცია, სხვა მრავალ საკითხთან ერთად, „მიზნად ისახავს ჰიბრიდული საფრთხეების წი-

ნააღმდეგ საკუთარი ბრძოლის უნარის გაზრდას, რაც გულისხმობს მედეგობის გაძლიერებას, ანალიზის, პრევენციისა და ადრეული გამოვლენისას თანამშრომლობას, ინფორმაციის დროულად გაცვლის საფუძველზე; ასევე, შეძლებისდაგვარად, თანამშრომელთა შორის სადაზვერვო ინფორმაციის გაცვლის საშუალებით და თანამშრომლობას სტრატეგიული კომუნიკაციებისა და საპასუხო ზომების შემუშავების მიმართულებით". გარდა ამისა, ორგანიზაციები შეთანხმდნენ, რომ გააფართოებდნენ კოორდინაციას კიბერუსაფრთხოებისა და კიბერთავდაცვის სფეროებში, მათ შორის, მისიებისა და ოპერაციების, წვრთნების, სწავლებებისა და ტრენინგების მიმართულებით" (NATO, Joint declaration 2016).

აქედან გამომდინარე, ბოლო წლებში ჰიბრიდული საფრთხეებისა და კიბერუსაფრთხოების სფეროებში ევროკავშირსა და ნატოს შორის არსებული თანამშრომლობა მნიშვნელოვნად წინ წავიდა. ნატოსა და ევროკავშირს შორის არსებული საერთო შეთავაზებების განხორციელების შეფასების მეექვსე ანგარიშის თანახმად, ორმა ორგანიზაციამ გააღრმავა თანამშრომლობა ჰიბრიდული გამოწვევებისა და კიბერსაფრთხეების საპასუხო ზომების შემუშავების მიმართულებით, თემატური დისკუსიების, ერთობლივი სემინარებისა და წვრთნების, რეგულარული კონსულტაციებისა და ინფორმაციის გაცვლის საშუალებით. დასახული მიზნისთვის გამოიყენება სხვადასხვა მექანიზმი, კერძოდ: ჰიბრიდულ საფრთხეებთან ბრძოლის სრულყოფის ცენტრი (Countering Hybrid Threats in Helsinki (Hybrid CoE)), ევროკავშირის სწრაფი შეტყობინების სისტემა (the EU's Rapid Alert System (RAS)), ნატოს სტრატეგიული კომუნიკაციების სრულყოფის ცენტრი (the NATO Strategic Communications Centre of Excellence (StratCom CoE)), ნატოს სამოქალაქო საგანგებო დაგეგმვის კომიტეტი (NATO's Civil Emergency Planning Committee (CEPC)), ნატოს კატასტროფებზე რეაგირების კოორდინაციის ევროატლანტიკური ცენტრი (NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC)), ევროკავშირის საგანგებო რეაგირების კოორდინაციის ცენტრი (the EU's Emergency Response Coordination Centre (ERCC)) და სხვა (NATO, Sixth progress report 2021).

მიუხედავად იმისა, რომ ჰიბრიდული საფრთხეებისა და კიბერუსაფრთხოების სფეროებში წარმატებული თანამშრომლობა სასიცოცხლოდ მნიშვნელოვანია ევროპული სახელმწიფოებისთვის, ევროკავშირისა და ნატოს წევრ სახელმწიფოებში სათანადოდ არ არის დაცული კრიტიკული ინფრასტრუქტურა. არსებულ პოზი-

ტიურ გამოცდილებაზე დაყრდნობით, ნატოს შეუძლია გააღრმაოს თანამშრომლობა ევროკავშირთან კრიტიკული ინფრასტრუქტურის უკეთ დასაცავად და ალიანსის მედეგობის გასაძლიერებლად.

ევროკავშირმა ამ მიმართულებით უკვე შეიმუშავა გარკვეული მექანიზმები. 2006 წელს ევროპულმა კომისიამ წამოიწყო ევროპული პროგრამა კრიტიკული ინფრასტრუქტურის დაცვის შესახებ (European Programme for Critical Infrastructure Protection (EPCIP)). ეს არის იმ ზომების პაკეტი, რომლებიც მიზნად ისახავს ევროკავშირის წევრ ქვეყნებსა და ეკონომიკური აქტივობის ყველა რელევანტურ სექტორში კრიტიკული ინფრასტრუქტურის გაუმჯობესებულ დაცვას. ევროკავშირის ინიციატივა კრიტიკული საინფორმაციო ინფრასტრუქტურის დაცვასთან დაკავშირებით (EU initiative on Critical Information Infrastructure Protection (CIIP)) მიმართულია კრიტიკული საინფორმაციო და საკომუნიკაციო ტექნოლოგიების უსაფრთხოებისა და მედეგობის გაძლიერებისაკენ (EU 2021). ამასთან, ევროპული კომისიის ერთობლივი კვლევის ცენტრი (Joint Research Centre of the European Commission) კოორდინაციას უწევს კრიტიკული ინფრასტრუქტურის დაცვის ევროპულ საინფორმაციო ცენტრს (coordinates the European Reference Network for Critical Infrastructure Protection (ERNCIP)), ტექნიკურ მხარდაჭერას უწევს დირექტივას ევროპული კრიტიკული ინფრასტრუქტურის შესახებ და მონაწილეობს სხვადასხვა კვლევაში, როგორიცაა, მაგალითად, საერთაშორისო კიბერუსაფრთხოების წვრთნებისთვის მეთოდოლოგიის შემუშავება, ქსელური ინფრასტრუქტურის მოწყვლადობის შეფასება უამინდობით გამოწვეული მოვლენების დროს და აფეთქებების მიმართ შენობებისა და სატრანსპორტო სისტემების მედეგობის ანალიზი (EU 2021).

რეგულარული კონსულტაციებისა და ინფორმაციის გაცვლის შედეგად, ნატოს შეუძლია გამოიყენოს კრიტიკული ინფრასტრუქტურის დაცვის ევროკავშირის გამოცდილება. დისკუსიების რაოდენობის გაზრდა ყველა დონეზე და ოპერაციებისა და შესაძლებლობების განსავითარებლად პრაქტიკული თანამშრომლობის გაძლიერება ხელშესახებ შედეგებს გამოიღებს. ამ სფეროში სასიცოცხლოდ მნიშვნელოვანია სტრატეგიული პარტნიორობის გაძლიერება, განსაკუთრებით, უსაფრთხოების იმ გამოწვევების ფონზე, რომელთა წინაშეც დგას თანამედროვე მსოფლიოში ეს ორი ორგანიზაცია.

დასკვნა

მიუხედავად იმისა, რომ ნატო არის ყველაზე წარმატებული ალიანსი კაცობრიობის ისტორიაში, რომელიც არსებული მექანიზმებისა და პოლიტიკის მოდერნიზაციით მუდმივად ცდილობს ადაპტაციას უსაფრთხოების თანამედროვე გარემოსთან, მასაც ჯერ კიდევ სჭირდება გარკვეული მიმართულებებით მუშაობა, რაც წარმოდგენილია წინამდებარე ნაშრომში. ჩრდილოატლანტიკური ხელშეკრულების ორგანიზაციის დამფუძნებელი დოკუმენტის მე-3 მუხლი მოითხოვს წევრი სახელმწიფოებისგან მედეგობის გაძლიერებას შეიარაღებული შეტევის დროს, რაც მათი მხრიდან გულისხმობს საკუთარი უსაფრთხოების არქიტექტურის სამხედრო და სამოქალაქო ობიექტების უსაფრთხოებაზე მუშაობას. ზემოთ წარმოდგენილი რეკომენდაციები ეფექტიანი სტრატეგიის შემუშავების, კერძო სექტორთან და ევროკავშირთან თანამშრომლობის გაღრმავების ყველაზე ეფექტური ნაბიჯებია, რომლებიც ალიანსმა უნდა მიიღოს მოკლევადიან პერსპექტივაში კრიტიკული ინფრასტრუქტურის დაცვის გასაძლიერებლად.

ბიბლიოგრაფია

- Dina, Sebastiano. 2019. *Cyberwarfare and Critical Infrastructure.* Strategic Brief, Washington: Center for European Policy Analysis (CEPA).
- Kačič, Matjaž. 2019. "Commentary on Articles 2 and 3 of the Washington Treaty." *Emory International Law Review.*
- Lee, Elsa. 2009. *Homeland Security and Private Sector Business: Corporation's Role in Critical Infrastructure Protection.* Taylor & Francis Group.
- Lewis, Ted G. 2006. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* John Wiley & Sons, Inc: Hoboken.
- NATO. 2020. "Cyber defence." March 17.
- NATO. 2016. "Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization." July 8. https://www.nato.int/cps/en/natohq/official_texts_133163.htm.
- NATO. 2020. "Resilience and Article 3." 31 March.
- NATO. 2021. *Sixth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf.
- Schmitt, Michael. 2019. "U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?" *Just Security*, June 18.