RONDELI FOUNDATION

GEORGIAN FOUNDATION FOR
STRATEGIC AND INTERNATIONAL STUDIES

# CRITICAL INFRASTRUCTURE PROTECTION IN EUROPE: STRENGTHENING RESILIENCE UNDER ARTICLE 3 OF THE WASHINGTON TREATY

MEGI BENIA

166

EXPERT OPINION

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

# EXPERT OPINION

MEGI BENIA

## CRITICAL INFRASTRUCTURE PROTECTION IN EUROPE: STRENGTHENING RESILIENCE UNDER ARTICLE 3 OF THE WASHINGTON TREATY

166

2021

The publication is made possible with the support of the US Embassy in Georgia. The views expressed in the publication are the sole responsibility of the author and do not in any way represent the views of the Embassy.

Technical Editor: Artem Melik-Nubarov



ISSN 1512-4835
ISBN

NATO is a major military organization responsible for security in the Euro-Atlantic space. Consequently, the current security environment in the world and, especially, in Europe stimulates debates about NATO's readiness to resist an armed attack. However, these debates are normally held around the Alliance's Article 5 as a key component of collective defense and in this process, the principles of Article 3 are ignored, something which is a wrong approach.

NATO's Article 3 states that: "In order to more effectively achieve the objectives of this Treaty, the parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack" (NATO, Resilience and Article 3 2020). Therefore, fulfilling obligations under Article 3 is a crucial part of the organization's main idea of collective defense as it enables NATO to fulfil the obligations of Article 5.

However, one must remember that in today's unpredictable security situation, "capacity to resist armed attack" (NATO, Resilience and Article 3 2020) means not only military readiness. To be able to deploy rapidly during operations or a potential armed attack, military forces need the support of transport systems, satellite communications and power supplies, etc. However, it is a well-known fact that these systems are highly vulnerable during an attack in both peace and war.

After the annexation of Crimea in 2014, Russia increased its hybrid activities against the critical infrastructure (CI) of European nations, mainly in the form of cyberattacks. The reason for this is that "launching a cyber-attack for Russia is a cost-effective, high-impact and difficult-to-attribute tool to influence, intimidate and blackmail its opponents. In the event of a military confrontation, Russia can use full-fledged cyber-attacks to temporarily incapacitate the vital infrastructure of its adversaries" (Dina 2019).

In order to improve NATO's capacity in this direction, the Alliance developed "seven baseline requirements in 2018 for national resilience against which member states can measure their level of preparedness" (NATO, Resilience and Article 3 2020). One of them is "resilient civil communications systems: ensuring that telecommunications and cyber networks function even under crisis conditions with sufficient back-up capacity" (NATO, Resilience and Article 3 2020) or, in other words, the protection of critical infrastructure.

Moreover, NATO adopted the Enhanced Cyber Defense Policy at the Wales Summit in 2014 which was further updated at the Warsaw Summit in

2016 where the allies recognized cyberspace as a domain of operations and approved the Cyber Defense Pledge (Kačič 2019). The Cyber Defense Pledge ensures that the allies are committed to strengthening the cyber defense of national networks and infrastructure in line with Article 3 of the Washington Treaty (Kačič 2019). In addition, at the Brussels Summit in 2018, the member states decided to establish a new Cyberspace Operations Centre as a part of NATO's strengthened Command Structure and called for the integration of cyber sovereign national capabilities into NATO-led operations and missions (NATO, Cyber defence 2020) (Kačič 2019).

However, despite all of these efforts that are directed towards the modernization of the Alliance and its adaptation to the modern challenges of international security, NATO needs to adopt a comprehensive and effective approach for CI protection in Europe. This paper aims at identifying two major developments that NATO should implement for CI protection and thus strengthening its resilience under Article 3 of the Washington Treaty.

## Ensure NATO Resilience through Improved CI Protection

To improve the protection of the Critical Infrastructure NATO needs to:

1. ***Develop an effective strategy for CI protection***

To ensure the better protection of the CI, the allies need to develop a strategy based on a network-structured approach. The solution was developed by Ted G. Lewis in his book on Critical Infrastructure. While analyzing the response of the US intelligence agencies against the terrorist attacks of 9/11, Lewis concluded, that "seams between agencies, low reaction times and poor coordination within the hierarchical command structure of the US intelligence and law enforcement organizations created ample opportunity for the attackers to succeed even when they made several mistakes" (Lewis 2006). Instead, he suggested to develop a "disintermediated command hierarchy where decision makers are embedded within a network structure that encourages the point-to-point movement of data, discussions and decisions. Commanders can access the specialists possessing the right expertise as easily as the next in command executive or leader. Therefore, decisions are made more quickly because information is shared more widely. Disintermediation means flattening an organization by removing layers" (Lewis 2006). As long as "one prominent unresolved issue in infrastructure protection is the problem of information

sharing" (Lewis 2006), Lewis suggested that this approach can be simply applied to the CI protection.

To apply this approach in the NATO reality, member states should have been viewed as different agencies/sectors of one unified entity, thus creating the disintermediated network structure. Similar to independent agencies/sectors which are responsible for their internal security, "each NATO member country needs to be resilient in order to resist and recover from a major shock such as a natural disaster, the failure of critical infrastructure or a hybrid or armed attack" (NATO, Resilience and Article 3 2020) which is anchored in Article 3 of the founding treaty. "Network analysis is an 'out-of-the-box' approach to critical infrastructure vulnerability analysis that should be the centerpiece of any strategy for critical infrastructure protection. Indeed, this approach leads naturally and logically to subsequent principles that can be incorporated into an effective strategy for nearly all sectors," Lewis concludes.

2. ***Enhance cooperation with the private sector***

It is a well-known fact that many subjects of critical infrastructure are in private ownership. Hence, they are one of the most vulnerable to any type of attack. For instance, "in 2014 the cyber security firms CrowdStrike and Symantec uncovered cyber operations by a group with ties to Russia targeting hundreds of Western oil and gas companies, as well as energy investment firms, some of which enabled remote control of the affected cyber infrastructure that would make possible sabotage (Schmitt 2019). Then, "in December 2015, Russia conducted its NotPetya cyber operations against the Ukrainian electrical grid. It was also around this time that a "Russian hacking unit began targeting critical American infrastructure, including the electricity grid and nuclear power plants," and "by 2016, the hackers were scrutinizing the systems that control the power switches at the plants" (Schmitt 2019).

To this end, it is understandable that CI protection is nearly impossible without the successful cooperation with representatives of the private sector.

Before we go to specific recommendations for the nature of such cooperation, it is worth mentioning that NATO pays attention to the importance of the private sector in this regard. Allies at the Wales Summit in 2014 decided to establish the NATO Industry Cyber Partnership (NICP)

(Kačič 2019). The NICP enables the sharing of information and expertise on cyber defense, developing best practices, improving understanding of cyber risks and improving NATO's cyber defense education, training and exercises (Kačič 2019).

However, the nature of this cooperation should be deeper and more effective. To this end, Lee provides a good approach to the nature of such interactions between the private and the public sectors. The author believes that flexible access to the data of threats and information sharing should have been the baseline of this collaboration. Lee suggests that "with a strong commitment to improving communications between the private sector and the public sector — one of the things that has not been addressed by law enforcement is the ability to access a databank of known threats and conduct a trend analysis. Various public and private sector organizations have their own internal logs of incidents and events. What would be useful for the owners and operators of critical infrastructure would be for them to have an ability to look through the window of incidents of other infrastructure and learn about attempted attacks, probing or surveillance — and share information. It would alert them that the same suspicious activities may be going on at other similar facilities or even in the local area. Threats can change overnight. That is why threat gathering, analysis, assessment, countermeasures and reviews need to be continuously ongoing. The goal is to be able to see the threats before they become imminent, actively engaged against one's facility or even inside one's own building thereby creating a catastrophe" (Lee 2009). The approach seems to be effective as it will bring representatives or vulnerable sectors together and make them understand the key features of different industries which is another essential aspect of problem-solving.

3. ***Enhance cooperation with the EU***

On July 8, 2016, the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization signed the Warsaw Joint Declaration (NATO, Joint declaration 2016). According to the document, to better strengthen the resilience in Europe, among many things, two organizations aim to "boost their ability to counter hybrid threats, including by bolstering resilience, working together on analysis, prevention and early detection through timely information sharing and, to the extent possible, intelligence sharing between staff while also cooperating on strategic communication and

response" as well as "expand the coordination on cyber security and defense including in the context of missions and operations, exercises, education and training" (NATO, Joint declaration 2016).

Accordingly, over the past years, the EU-NATO partnership has made significant progress in countering the hybrid threats and challenges as well as strengthening cyber security. According to the sixth progress report on the implementation of the common set of proposals endorsed by the EU and NATO Councils, the two organizations have enhanced cooperation on how to better respond to hybrid challenges and cyber threats through increased scenario-based discussions, joint workshops and exercises, regular consultations and information exchange using various mechanism such as: Countering Hybrid Threats in Helsinki (Hybrid CoE), NATO Drone Single Local Air Picture project, the EU's Rapid Alert System (RAS), the NATO Strategic Communications Centre of Excellence (StratCom CoE), NATO's Civil Emergency Planning Committee (CEPC), NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC), the EU's Emergency Response Coordination Centre (ERCC) and so on (NATO, Sixth progress report 2021).

Even though the successful cooperation in the field of hybrid activities and cyber security is of tremendous importance for the European nations, it does not ensure the proper protection of critical infrastructure in the member states of both the EU and NATO. Following this positive experience, NATO can enhance its cooperation with the European Union to better protect critical infrastructure and bolster the resilience of the Alliance.

The EU has already developed various mechanisms in this direction. In 2006, "the European Commission launched the European Programme for Critical Infrastructure Protection (EPCIP). This is a package of measures aimed at improving the protection of critical infrastructure in Europe across all EU states and in all relevant sectors of economic activity. The EU initiative on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures" (EU 2021). In addition, the "Joint Research Centre of the European Commission coordinates the European Reference Network for Critical Infrastructure Protection (ERNCIP), provides technical support for the review of the Directive on European Critical Infrastructures and carries out different research activities such as the development of methods and tools for international cyber security exercises, the assessment of the

vulnerability of networked infrastructures in the case of extreme space weather events and the evaluation of the resistance of buildings and transport systems against explosions" (EU 2021).

Through regular consultations and information exchange, NATO can use the EU's experience in the protection of critical infrastructure. The increased number of discussions at all levels and the boosted practical cooperation in operations and capability development will bring tangible results. The reinforcement of a strategic partnership in this area is highly important amid the security challenges which the two organizations face in the modern world.

**Conclusion**

Despite the fact that NATO is one of the most successful alliances in the history of mankind and it tries to constantly adapt to the new security realities as well as being eager to improve its policies and performances in CI protection, it still requires to work on certain directions that are presented in this paper. Article 3 of the founding document of the North Atlantic Treaty Organization requires that member states build a resilience against armed attacks and work on the security of both the civilian and the military subjects of their security architecture. The aforementioned three recommendations provided herein on elaborating a strategy base for a network-structured approach and enhanced cooperation with the private sector and the EU seem to be the most effective steps which the Alliance should take in the short-term perspective for the better protection of the critical infrastructure.

## Bibliography


- 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.