NATO and EU Cybersecurity Environment and Standards

Alika Guchua

Ph.D. in Political Science, Associate Professor,
Caucasus International University (Tbilisi, Georgia)
E-mail: alika_guchua@ciu.edu.ge
https://orcid.org/0000-0003-0347-9574

Thornike Zedelashvili

Ph.D. in Political Science, Caucasus International University (Tbilisi, Georgia)
E-mail: ThomasZetelashvili@gmail.com
https://orcid.org/0000-0003-2630-1779

Gochua, Alika, and Thornike Zedelashvili (2021) NATO and EU Cybersecurity Environment and Standards. *Ukrainian Policymaker,* Volume 9, 4-11. https://doi.org/10.29202/up/9/1

The states face many dangers in modern international politics. The size of threats and risks is growing, which requires great effort and struggle from states to ensure security. One of the major challenges in the 21st century is the threats posed by cyberspace, such as cybercrime, cyber terrorism, and so on. The role of states and international or regional organizations should be in ensuring a safe environment, in improving protective mechanisms, as well as in improving the economic and environmental situation through the use of technological advances, and in caring for public order and other welfare, for which the developed countries of the world are working today, also by joint efforts of the EU and NATO. However, more effort and involvement are needed. The research raises important questions: What are the consequences for the world? Where are we, and where are we going? A pandemic, a crisis, a lot of dangers in both the real and the irreal world, that is, in cyberspace, which does not even lag behind the real one. The paper discusses the standards and mechanisms of how governmental institutions and international or local organizations should operate to minimize the damage from cyber-attacks. The paper also discusses the introduction of cyber threats and what solutions can be found to neutralize and mitigate the threats. It is impossible to localize cyber threats at this stage fully, and why it is impossible, this issue is also discussed in the paper. NATO and EU cyber security policies and existing standards are also discussed. We also talk about the cyber security environment and policy of Ukraine and Georgia.

Keywords: Cybersecurity, EU, NATO, Challenges, Ukraine, Georgia, Russia

Received: 19 September 2021 / Accepted: 22 October 2021 / Published: 1 December 2021

Introduction

In the modern world, the issue of cyber security is quite relevant for all states. They are actively trying to introduce new technologies to protect their cyberspace, but it requires quite large financial and human resources, which many states do not have. After the air, sea, and land space, cyberspace has become a new space of confrontation. Various states often use it to achieve political, military, and geopolitical goals. The United States, England, France, Germany, Russia, and a number of other European countries have their own official cyber armies. In addition, NATO, the United Nations, and the European Union are engaged in the development of various doctrines. For example, the US equates cyber-attacks with traditional military operations. The issue of Russian cyber security also occupies a large place in the Russian national security doctrine. Consequently, the role and importance of cyber security are growing: "The EU and NATO are targeted by the very same vectors, notably by cybercrime syndicates, politically motivated non-state actors, and sophisticated state actors. These hostile cyber activities undermine all levels of society in EU and NATO countries, threatening civil, political, economic, and military security. Even though cyberattacks are a very real threat, many of these activities go undetected, unacknowledged, or inadequately addressed by decision-makers. Stakeholders in various sectors are becoming more informed and engaged around cybersecurity and cyber defense issues, but the challenges remain daunting" (Lété & Pernik, 2017: 1).

We can also say that cybercriminals, spies, hackers, and other criminal mafia and criminal gangs have so well kept pace with technological progress. In many cases, the protective mechanisms simply do not work; it is impossible to find out, find, punish the culprit, and so on. Standards and mechanisms exist to enable government agencies and international or local organizations to minimize the damage from cyber-attacks. These standards are ISO (International Organization for Standardization) standards divided into different areas, including information and cyber security issues. Various structural units from more than 160 countries are members of this international organization. Also, CEN (European Committee for Standardization) combines the national standards bodies of all countries of the EU and EFTA (European Free Trade Association), NATO standards, and cyber policy.

Ignoring or inadequately assessing cyber threats will expose the country to such risks as the vulnerability of state and economic structures, insufficient protection of critical infrastructure, weakness in military and hybrid threats, and decreased self-defense. Therefore, ensuring a high level of cyber security is vital.

NATO and EU Cyber Security Policy

Today, Russia's and some countries' continuous cyberattacks on the Alliance and its members threaten NATO's security. To accomplish its mission of deterrence and defense, NATO needs to implement a strategy of proactive, continuous responses to Russia and some countries in cyberspace, where great power competition is playing out in real-time. Russia and some countries "…challenge NATO and its members in cyberspace daily as part of ongoing hybrid campaigns to undermine the transatlantic community. The Kremlin's actions have involved intrusions into Allies' critical infrastructures, manipulating Allies' elections through hacks and disinformation, and even blocking GPS information critical to NATO activities. Russia, North Korea, and some countries "…government has engaged in cyber espionage against Allies' military capabilities; intellectual property theft related to sensitive technologies,

industries, and infrastructure; and disinformation against transatlantic countries, including around the coronavirus. These efforts to weaken NATO countries and Alliance cohesion represent a persistent threat to Allied security" (Kramer et al., 2020: 1).

We often hear and see that NATO and the EU are working together to tackle a variety of challenges, including cyber and information attacks: "NATO has recognized the collective dangers of these hybrid attacks in cyberspace. Up to this point, however, the Alliance has taken a reactive approach, responding as if Russian, North Korea, and some countries cyber-attacks are each isolated incidents. The cyber efforts are part of continuous campaigns directed at the overall capability of the Alliance, NATO's response has been insufficient, failing to reduce or dissuade further attacks. To assure the security of its members going forward, NATO needs its own continuous response campaign to these threats" (Kramer et al., 2020: 1).

However, different countries try to defend themselves individually at the expense of technology. Nevertheless, the question is often asked: where is the solution? What should the world, state, NATO, EU, international or local organizations oppose? There are ambiguous answers to this as well. For example, it is clear that NATO and the EU have been actively working on cyber and information warfare for years, developing this sphere and spending more money than ever before, but that is not really enough. Of course, we can talk a lot about the achievements of NATO, the EU, the US, and even France or Germany. We can give many examples of cyber-attacks and information warfare, but we ask ourselves: where is the solution, how should we do developed humanity to defeat cyber-terrorism? We will try to answer this question based on the existing reality: "Three of the most prominent examples of cyber aggression between nation-states are those on Estonia (2007), Georgia (2008), and Ukraine (2014, 2015) by Russia and its proxies. These examples demonstrate a growing threat to European security from an increasingly aggressive Russia and the trend toward a single concept of conflict that makes cyber and kinetic aggression inseparable. It is important to note that Iran, and North Korea, to varying extents, also have the capability and intent to threaten the security of NATO and EU member states through cyber means" (Ilves et al., 2016: 128).

The topic of cyber security is so multifaceted that it is difficult to consider it in one direction. Cyber security standards actually work as a set of policies that define methods and/or approaches to secure systems in government agencies or private organizations. In the 21st century, there are already several standards of cyber security on the market – almost every organization operating at a high level is required to adhere to these standards as they fully define security.

First of all, we should mention NATO and the European Union, and the leading countries that spend billions of dollars on cyber security. Most money is consumed by the US, France, and Germany. Therefore, we should also talk about the NATO Standardization Office (NSO), which has the issue of cyber security at the forefront. This organization coordinates, supports, and manages NATO standardization activities under a Special Committee (CS) authority. The NSO also assists the NATO Military Committee in developing military operational standards that help increase the effectiveness of the Alliance's military forces.

As you know, in June 2021, a summit was held in Brussels, where NATO leaders made a statement. This reaffirms the commitment to collective security: "At the Brussels Summit in June 2021, Allies acknowledged the changing threat landscape, recognizing that cyberspace is continually contested. Allies endorsed a new Comprehensive Cyber Defence Policy to support NATO's three core tasks of collective defense, crisis management and cooperative security, as well as its overall deterrence and defense posture. NATO must actively deter, defend against and counter the full spectrum of cyber threats at all times – during peacetime, crisis and conflict – and

at the political, military and technical level" (Cyber defense, 2021: 1). The statement discusses current strategic issues that highlight NATO's defensive role in cyberspace. NATO policy allows the application of Article 5. In some cases, the Alliance says some cyber-attacks could equate to an armed attack, which could automatically lead to the enactment of Article 5 of NATO.

However, it should be noted here that most cyber-attacks are below the force limit. How does NATO respond proportionately to "low-level" cyber-attacks? Some experts may criticize NATO's defensive portion in cyberspace, but it should still be noted that responding to so-called low-level cyber-attacks poses the least risk to the Alliance. For example, in low-level cyber-attacks, we may consider an attack that steals information or financial resources, it may be state or sanctioned, and behind the attack, as is well known, often stands Russia or Iran. NATO clarifies that such cyber-attacks do not cause long-term economic losses.

Consequently, a collective response to them cannot be considered appropriate. In the case of low-level cyber-attacks, they are mainly satisfied with the expulsion of the diplomatic corps and the use of economic influence, namely, with sanctions. The value of the attack should determine the magnitude of the reaction. If the loss is estimated at $10 million, the sanction should also be proportionate to $10 million. This statement has been met with mixed reviews as it is difficult to pinpoint the consequences of sanctions and the deterioration of diplomatic relations. Moreover, it is possible that state-sanctioned attackers were not under the complete control of the government (Watson, 2021: 1).

Thirty countries represented at the Brussels Summit issued a joint statement: "We will make greater use of NATO as a platform for political consultations between the Allies, in terms of sharing cyber-attack experience and national approaches. We will also consider the possibility of a collective retaliation and pass the cost to those who harm us. In confirmation of NATO's defense mandate, the Alliance is committed to using its full range of capabilities at all times to actively deter, protect and deal with the full range of cyber threats, including under international law in the framework of hybrid campaigns" (Watson, 2019: 1).

The statement also says that NATO, as an organization, will continue to adapt and improve its cyber defense policy and will further develop its capabilities.

Obviously, the aggressor states, including the most active Russia, are launching cyber-attacks in many directions, including on Georgia, Ukraine, and the United States, not to mention the rest of the post-Soviet space.

As mentioned above, despite great diligence and tireless work, NATO's fight to neutralize cyber-attacks is not enough, and as time goes on, more resources are needed. Today, all specialists recognize that the most effective solution, both internationally and individually, is to adhere to standards. The more people are aware of how to protect themselves from cyber-attacks, the less damage will be done to state structures, private or international organizations.

Let's expand on what international standards mean and what we have in this regard in terms of cyber security: we have already mentioned that the cornerstone of global standards is the International Organization for Standardization (ISO), which offers some theoretical and practical mechanisms for how to avoid harm publicly and internationally or privately by using the standards, guidelines, and adherence that this international organization provides.

The International Organization for Standardization was founded in 1947. It includes the relevant structure of more than 160 countries. ISO oversees the ongoing work of its technical committees. The total number of international technical committees is currently about 250. All bodies have the right to appoint members to committees.

ISO is a global body that collects and manages standards for various disciplines around the world. When the industry depends on the Internet and digital networks, more emphasis is placed on these standards, technological approaches. ISO approaches are best for ensuring that the internal process of public or private companies aims to meet customer demand at the highest level. When it is known that a government agency or other company is adhering to and certified following all ISO standards, it helps to build trust between the two parties. Today at the international level, it is already a major requirement; in case of cooperation, all stakeholders must have an ISO certificate (Watson, 2019: 1).

The most important standardization partner for ISO is the International Electrotechnical Commission (IEC). ISO and IEC have joint technical committees. For example, IT standardization was created through collaborative efforts in 1906. The IEC can be considered the first international standardization organization.

Electrical engineering was the first industry that recognized the need for common terminology. International Telecommunication Union ITU is a UN special organization. The goal of telecommunication standardization is the interoperability of communication networks, terminal devices, and communication services. ISMS (Information Security Management Systems) includei inspection and review. In this case, the auditors are looking for how your procedures are documented and reviewed on a regular basis. These procedures include human resource security, asset management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, supplier relations, information security incident management, information security aspects of business continuity management.

One of the mistakes many organizations make is that the entire responsibility for ISO certification lies with the local IT team. Although information technology is the core of ISO 27001, processes and procedures must still be shared by all parts of the organization.

One of the directions of the ISO is cyber security standards. In the modern dynamic era, everything works differently than in the old days. In terms of cyber security, different measures have been introduced in all regions. As we have mentioned, many international and local organizations are trying to innovate in this direction. Among them is NATO. However, since the worldwide Internet is integrated and used everywhere, some standards should be the same for everyone and remain unchanged.

More specifically, what is a cyber-security standard? It can be defined as a set of rules that a state structure and/or organization must meet to be entitled to certain issues (for example, online payment, patient data storage, etc.). These standards include the basic rules that the agency must obey.

Cybersecurity standards include several common vital points:

1. ISO 27001
   This standard protects an organization in terms of information security. According to this standard, the organization must introduce new technologies. Servers should be checked at regular intervals, periodically.
2. PCI DSS (Payment Card Industry Data Security Standard)
   This is the industry data security standard that is required for card payments. This can be considered as a standard to be chosen by the organization. The business structure that stores user data (name, surname, date of birth, card information) must comply with this standard and must comply with the updated technology. The system must continuously undergo security checks and assessments. This standard

is developed by world brands of card manufacturers: American Express, Visa, MasterCard, JCB, Discover.

3. HIPAA (Health Insurance Portability and Accountability Act)
   It is an act of health insurance portability and accountability. This is a standard that health clinics must follow. In this case, patient data must be protected. Any hospital should have a strong network security team that responds to all incidents. Quarterly security reports should be transparent. All transactions should be done in encrypted mode. The standard protects critical information related to the patient's health to make the person feel safe.
4. Finra (Financial Industry Regulatory Authority)
   It is the regulatory body of the financial industry. This standard is intended to ensure the safety of financial institutions that provide financing or are actively involved in financial transactions. In this standard, the system must be highly protected. Full data security and user data protection are essential. This is one of the most important standards that all financial institutions must meet.
5. GDPR (General Data Protection Regulation)
   This is a general regulation of data protection. It is defined by the European Union. In this case, too, customer data protection and security are paramount (Pedamkar, 2020: 1).

The European Committee for Standardisation

In 2020, a new EU Cybersecurity Strategy and new rules were adopted to improve the resilience of critical physical and digital assets, according to which the new Cybersecurity Strategy "… allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values. The new Cybersecurity Strategy aims to safeguard a global and open Internet, while at the same time offering safeguards, not only to ensure security but also to protect European values and the fundamental rights of everyone" (New EU Cybersecurity Strategy, 2020: 1).

It should be noted that the European Committee for Standardization (CEN) was established in 1961. This association unites national organizations of state standardization. The same European standards apply in all CEN member countries. They are obliged to approve the European and abolish any conflicting standards. The standards approved by CEN are marked "EN." About 30 percent are based on global ISO standards.

CEN has more than 300 technical committees, i.e., European standardization groups. All members have the right to participate in the technical committees. The management of the Secretariat provides an opportunity to monitor the development of standards, in particular, to influence the content of future standards.

European Committee for Electrotechnical Standardization (CENELEC) manages the development of European electrotechnical standards. Its members are all EU countries and Eastern European countries. Seventy-five percent of CENELEC standards are based on global IEC (International Electrotechnical Commission) standards. The organization responsible for electrotechnical standardization in Finland is SESKO (Electrotechnical Standardization in Finland).

European Telecommunications Standards Institute (ETSI) develops international telecommunications standards. Its members are governing bodies in the field of information technology. Traficom (Finnish Transport and Communications Agency) is the organization responsible for telecommunications standardization in Finland. CEN, CENELEC, and ETSI will also develop standards at the request of the European Commission. Finally, harmonized standards provide more detailed guidance and specific directives: "Cybersecurity is a priority also reflected in the EU's next long-term budget (2021-2027). Under the Digital Europe Programme, the EU will support cybersecurity research, innovation and infrastructure, cyber defence, and the EU's cybersecurity industry. In addition, in its response to the Coronavirus crisis, which saw increased cyberattacks during the lockdown, additional investments in cybersecurity are ensured under the Recovery Plan for Europe" (New EU Cybersecurity Strategy, 2020: 1). It can be said that the EU and NATO cybersecurity and cyber threat response policies are working quite well.

Conclusions

To summarize, we can say, tackling cyber threats requires more cooperation and effort from governments and international or regional organizations. At the same time, it is important that, along with many factors, states must have the political will and the right management on which depends the proper provision of cyber security. Proper management, in turn, implies the proper redistribution of responsibilities and the refinement of coordination mechanisms. When a country is in a state of constant conflict, and the risk of a massive cyber-attack is high, the country's resources should be mobilized to refine and strengthen the existing organizational system (New EU Cybersecurity Strategy, 2020). It is necessary to take into account the existing policy on the example of Georgia and Ukraine. They need to implement their own cyber security system following European standards, as they are quite vulnerable countries and an important target for cyber-attacks from Russia or other states.

NATO and the EU are actively cooperating with each other on cyber security issues, which makes their protection against cyber threats more effective. It is also crucial that they actively develop new cyber security strategies and doctrines that help protect them from cyber threats. The cyber environment requires quite active work to create secure cyberspace. A complex approach to the problem is essential. In order to eliminate the deficiencies, first of all, it is crucial to identify the existing problems and take appropriate measures to stop them.

🕮 References

Cyber defense (2021) *North Atlantic Treaty Organization*. July 02, 2021. Available online: https://www.nato.int/cps/en/natohq/topics_78170.htm

Lété, Bruno, and Piret Pernik (2017) *EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions.* Available online: https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions

Kramer, Franklin D., Lauren Speranza, and Conor Rodihan (2020) NATO needs continuous responses in cyberspace". *Atlantic Council*, December 9, 2020. Available online: https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-needs-continuous-responses-in-cyberspace/

Ilves, Luukas K., Timothy J. Evans, Frank J. Cilluffo, and Alec A. Nadeau (2016) European Union and NATO Global Cybersecurity Challenges: A Way Forward. *Prism*, Vol. 6, no. 2, 126-141.

New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient, European Commission. Press release (2020) December 16, 2020. Available online: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

Pedamkar, Priya (2020) *Cyber Security Standards 2020*. Available online: https://www.educba.com/cyber-security-standards/

Watson, Tracy (2019) *Benefits of ISO 9001 and 27001 for companies and their clients.* October 03, 2019. Available online: https://skywell.software/blog/benefits-of-iso-9001-and-27001/

Watson, William (2021) *A Defence of Defence. NATO's Response to Low-Grade Cyber-Attacks*. June 15, 2021. Available online: https://icds.ee/en/a-defence-of-defence-natos-response-to-low-grade-cyber-attacks/