DE GRUYTER OPEN

Land Forces Academy Review
Vol. XXIII, No 1(89), 2018

CYBER SECURITY POLICY AND STRATEGY IN THE EUROPEAN UNION AND NATO

László KOVÁCS
National University of Public Service, Budapest, Hungary
kovacs.laszlo@uni-nke.hu

ABSTRACT

Nowadays it is clear not only for professionals but also for outsiders that our advanced Western societies cannot operate without the infrastructure based on information technologies. The security of these infrastructures, which are present in public utilities, economic life, public administration, defence sector or even in the smallest detail of everyday life, have a vital importance. The reason for this is very simple: if these systems do not work, then society does not work either. The importance of cyberspace can no longer be questioned. Accordingly, the challenges and threats to cyberspace have to be addressed at strategic level. This paper presents the most important cyber security principles and strategies of the European Union and NATO.

KEYWORDS: cyber, policy, strategy, NATO, European Union

1. Introduction

Both the European Union as well as NATO are major international economic, political and military organizations. However, they are facing serious challenges and threats that occur in cyberspace every day. Both organizations and their member states recognized the importance of strategic regulation of cyberspace many years ago.

The European Union in its cyber security strategy, which was born in 2013, is planning to create the safest Internet environment in the world to enable the development of the digital economy. The strategy itself is the EU's strategic vision for preventing and responding to European telecommunication systems' failures and attacks, as well as for responding to such cases. The proposal for the strategy was published in two parts in the beginning of 2013, of which the first part is the Communication from the European Commission and the High Representative for Foreign Affairs and Security Policy on the EU cyber security strategy. The second part is the European Commission's proposal for a directive on network and information security which is one of the most important strategic directives on cyber security for the future of EU (European Commission, 2013).

Similarly to the EU, NATO has its own processes and measures in the field of cyber security. However, in accordance with the official NATO terminology it is called cyber defence instead of cyber security as EU terminology says. NATO has been very intensively focusing on cyber issues since the Estonian cyber crisis in 2007. In addition to technical IT issues, serious political and international legal matters have arisen within the Alliance since 2007. All of these questions have led to serious strategic steps being taken in NATO referring to cyber defence.

DOI: 10.2478/raft-2018-0002

The present study looks to the most important steps that were taken at strategic level to define the EU cyber security as well as NATO and cyber defence issues in the last few years.

2. The Cyber Security Strategy of the European Union

In the wake of the 2008 global economic crisis, in order to reduce the exposure and vulnerability of the European economy and to increase the EU's competitiveness, in 2010 the European Commission announced a strategy with the title "Europe 2020", which consists of five main objectives. These objectives are based on pillars and sub-pillars. The first pillar focuses on the key growth which includes the Digital Agenda for Europe (European Commission, 2010).

The key objective of the European Digital Agenda is to create a unified digital market for EU member states, relying on sustainable economic and social benefits for all European citizens. The Agenda is to explore and analyse the existing economic, social challenges and shortcomings of the European Union (i.e. segmentation of the digital market, interoperability challenges, the spread of cybercrime, lack of network investments, low level of R & D, low level of digital human capability) to make proposals for development and to define various actions (European Commission, 2010).

Based on the above mentioned findings of the European Digital Agenda, the EU Cyber Security Strategy was completed in 2013, referring to the dependence on information technology and information systems that are present in all segments of our society and economy.

Consequently, the security of cyberspace must also be initiated, because if these information systems fail to work, it causes serious disruptions, in some cases inefficiency, not only in economic but also in social functions (European Commission, 2013).

This new strategy was the first effective and very important step towards laying the foundations for unified European cyber security. The strategy includes the EU's strategic vision to prevent and respond to European telecommunications systems' failures and responses to such cases.

Following a rather long and controversial negotiation and coordination process, in February 2013 the proposal for the strategy was published in two parts. The first part is the Communication from the European Commission and the High Representative for Foreign Affairs and Security Policy on the EU Cyber Security Strategy, which is the strategy itself, and the second part is the European Commission's proposal for a directive on network and information security, which has become known as a package for the NIS Directive.

The strategy is based on five principles that will be priorities for the future of the European Union. It is very important to highlight the recognition that the EU's official communications also emphasize: cyber security is equally important as security in the physical space. In accordance with the official text of the Strategy its five principles (priorities) are the following:

- *"Achieving cyber resilience,*
- *Drastically reducing cybercrime,*
- *Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP),*
- *Develop the industrial and technological resources for cyber security,*
- *Establish a coherent international cyberspace policy for the European Union and promote core EU values"* (European Commission, 2013, p. 4).

In order to achieve cyber resilience, the strategy emphasizes the unity of public authorities and the private sector, and the development of cyber capacities, resources and efficiency. However, achieving this goal cannot be imagined without improving the prevention, detection and management

of cyber security events and without coordinating them at EU level. The strategy has a special and prominent role for ENISA (European Union Agency for Network and Information Security) to strengthen the cyber resilience across the Member States.

The Strategy notes that, although there is some progress in this area, namely the creation of coordinated resilience as a priority, there are still serious gaps in many Member States, mainly in terms of national capabilities, coordination in handling of cross-border cyber incidents, or promotion of the private sector's preparedness areas. Therefore, the strategy must be followed by a legislative process.

This legislation should focus laying down minimum requirements which will be the basis for national authorities, creating well-functioning network security emergencies or CERTs (Computer Emergency Response Teams) and adopting a national strategy and national co-operation plan in different cyber issues (European Commission, 2013).

One of the key segments of cyber resilience is the cyber awareness. In the area of awareness, the strategy aims to maximize the security of users' online activities: *"End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them"* (European Commission, 2013, p. 8).

To achieve the increased cyber security awareness, the strategy is highly relying on ENISA and other organizations such as Europol and Eurojust. The document highlights the European Cyber Security Month series initiated by ENISA. This initiative has been regularly organized in many Member States since its launch in 2013.

In the strategy, the European Commission requests the Member States to comply with a specific call. The request states that in order to increase awareness, member countries will participate in the Safe Internet program, and should introduce safety-related training in schools from 2014. Additionally, this call of the European Commission forces that training for IT specialists should include secure software development and personal data protection issues, and some initial cyber security training for the public administration staff needs to be established (European Commission, 2013).

To achieve the drastic reduction of cybercrime, the strategy calls for a single, more powerful and stricter but effective legislative environment to control cybercrimes. Although earlier, international conventions have been recognised in the area of cybercrime, such as the Council of Europe's Convention on Cybercrime (or as widely used 'the Budapest Convention'), which is an otherwise binding international treaty for the signatory countries and which provides an effective legal basis for the adoption of national laws on cybercrime or the use of online sex exploitation and the fight against child pornography, nevertheless a real breakthrough in the field has not yet been made. On the basis of the strategy, the European Commission has a major role to play in countering cybercrime for its work and the effective actions of the European Cybercrime Centre (EC3) within Europol. In addition to EC3, the European Commission also names and encourages CEPOL, the European Police College, to launch training courses that provide relevant knowledge to law enforcement officers (European Commission, 2013).

The next priority of the strategy is to develop cyber defence policy and capabilities along the Common Security and Defence Policy (CSDP) of the EU. This would mean the protection of civil and military infocommunication systems in closer cooperation with NATO. Within this work, the strategy states: *"To increase the resilience of the communication and information systems supporting Member*

States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats" (European Commission, 2013, p. 11).

To achieve this goal, the European Commission calls for assistance from the European Defence Agency (EDA).

One of the most important objectives of the strategy is the development of cyber security industrial and technological resources. It covers the creation of a single market for existing and emerging products as well as the use of NIS directive by manufacturers of cyber security products. The financing and support background defined for accomplishing the goals is also shown here. The strategy encourages R & D investment and further innovation, which can be realised, inter alia, through the "Horizon 2020" programme of the EU. Apart from that, the strategy also calls for the creation of an international policy that, in keeping with the existing international rules can contribute to the overcoming of digital divide, while preserving the openness and freedom of the Internet. This objective also includes the fact that, as mentioned above, the EU should make cyberspace issues the part of its common foreign and security policy and also to strengthen the role of third countries (non-EU members) in cyber defence, and the EU must play a significant role in this work (European Commission, 2013).

On 13 September 2017, Jean-Claude Juncker, President of the European Commission, stated in his regular annual report on the Union: *"in the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks. This is why, today, the Commission is proposing new tools, including a European Cybersecurity Agency, to help defend us against such attacks"* (European Commission, 2017a).

According to President Juncker the European Commission had come up with a package of proposals envisaging a complete reform of the European cyber security situation in September 2017. This is the recognition of the fact that the European Union is not fully prepared to handle cyber-attacks and cyber incidents, such as the events of 2016 ransomware attacks, the actions and interventions – essentially in cyberspace – into the democratic electoral systems of the French and then the German elections in 2017. This recognition has led the European Commission and the High Representative for Foreign Affairs and Security Policy to develop a new package of proposals to strengthen cyber security. The proposal includes, inter alia, the idea of setting up a new European Union Cyber Security Agency to help Member States manage cyber incidents and develop a new European certification system that would guarantee the safe use of digital products and services (European Commission, 2017a).

The new European Union Cyber Security Agency, based on ENISA, becomes a permanent EU institution to assist the Member States prevent and respond to cyber-attacks. The Agency will be responsible for organizing and conducting European cyber security exercises. Within the Union, the information- and knowledge-sharing related to the cyber threats can move to a higher level with this Agency and the establishment of new information sharing and analysis centres. We can realize (read between the lines of the abovementioned communication) that the new Agency will also receive quasi-official duties covering the implementation of the NIS Directive in the Member States and, in particular, monitoring the reporting of serious cyber incidents to national authorities. In addition, the Cyber Security Agency would be responsible for contributing to the development and implementation of a new EU-wide certification scheme for digital

security for products and services to be developed by the European Commission (European Commission, 2017b).

Obviously, the strategic environment must be complemented by several laws (in the meaning of EU these are directives), to reach the full spectrum of cyber security. These new laws or recommendations include, inter alia, the previously mentioned NIS and the GDPR (General Data Protection Regulation) Directive, which is a breakthrough in the field of data protection. The GDPR is not directly aiming at cyber security but indirectly it will greatly influence the cyber sphere.

As we referred earlier, the NIS Directive is an important segment of the EU Cyber Security Strategy, which has a rather long and therefore slightly difficult to understand official title: *"Directive concerning measures for a high common level of security of network and information systems across the Union"* (NIS Directive, 2016).

The adopted Directive sets out mandatory requirements for all Member States. The most important of these binding factors is that each Member State must develop a national strategy for security of network and information systems. The NIS specifies that dedicated and unique national contact points or CSIRTs (Computer Security Incident Teams) are to be set up in the Member States, whose operating conditions must be ensured. For CSIRTs, the Directive also orders to establish and operate these organizations by a critical sector or sub-sector, and to ensure that these CSIRTs have to create a network within the Union, thereby promoting trust and effective and operational cooperation. All this is accompanied by the obvious fact that: *"Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in Annex III within the Union"* (NIS Directive, 2016, art. 16 1).

The directive and its entry into force in May 2018 is a huge step forward in the field of cyber security, as the directive itself states, for the unified digital economic and social activities and especially for the functioning of the internal market, since the security of networked information systems can finally be read from a common scenario by the Member States.

The other important directive, the GDPR, replaces the former EU Data Protection Directive of 1995 and represents a harmonized data protection law for the EU Member States. Its core objective is to protect the personal and private data of EU citizens. Since 1995, when the last Data Protection Directive was issued, the management of citizens' personal data has been fundamentally changed and transformed thanks to information technology. Therefore, a fundamentally new regulation is needed which is based on a totally new philosophy inspired by the information technology (GDPR, 2016).

The General Data Protection Regulation, which enters into force on 25 May 2018, brings enormous changes to all EU countries. Regarding the GDPR, one of the most cited regulations is a very severe sanction tool. This penalty is no less than 4% of the annual turnover of the organization that violates the rules or 20 million euros (whichever is greater). This serious penalty is the maximum fine that can be imposed for the most serious infringements, processing and handling of personal data without authorization. The directive also applies a penalty rate equivalent to 2 % of the annual turnover in case of failure to notify the supervisory authority, or in case of incorrect data record or breach of the law. These penalties should apply to data controllers and data processors; therefore, the cloud service providers are also subject to this regulation (GDPR, 2016).

The GDPR, which is based on *"lawfulness, fairness and transparency"* (GDPR, 2016, Article 5 [1] a), stipulates that data subjects (slightly simplified for customers) have the right to be informed by the data controller about when and how their personal data are processed, where and how they are stored, or to whom they may be handed over (if this is legally possible at all). This can increase the transparency of data management. In addition, the data controller must provide the customer with a copy of the personal data in electronic form free of charge.

The GDPR also defines the concept of *right to erasure ('right to be forgotten').* This means that the: *"data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay ..."* (GDPR, 2016, Article 17 [1]) if the specified conditions are realized.

This, for example, will make enormous changes to many social media service providers', such as Facebook, data management because many of them are known that no data was deleted from their users, even if apparently, the user did it on their own account.

3. Cyber Defence Policy of NATO

The Estonian cyber incidents in 2007 caused serious political and strategic dilemma within NATO. This was primarily due to the fact that during the existence of the Alliance it was the first series of attacks that did not occur in the physical dimension against a member state of the Alliance. Therefore, this was the beginning of a new era.

It should be noted that the closing declaration of the NATO Summit in Prague in 2002 already included the importance of cyber threats: *"We have therefore decided to: ...Strengthen our capabilities to defend against cyber-attacks"* (NATO, 2002). Although the closing statement of the Prague Summit included cyberspace as a term only once, that was a forward-looking phenomenon as all these dangers were proven by the 2007 Estonian events.

In April 2007, in the capital of Estonia, the removal of the "Soviet monument of the liberators of Tallinn" resulted in huge riots and street turmoil. In parallel with the riots, several online attacks also occurred mainly from outside Estonia, which were initially aimed at blocking the official communications lines and websites of the Estonian state administration. In the third week of cyber-attacks Estonia's Internet network was almost completely paralyzed and blocked in May 2007. The most powerful cyber actions were DDoS (Distributed Denial of Service) attacks targeting the Estonian Parliament, government offices, and even banks and media's computer centres. In the Estonian network, data traffic was often more than thousand times bigger than the normal for hours (Kovács, 2014).

After the Estonian cyber crisis, it became very clear, as several NATO officials also stressed, there was a need for central coordination and central roles in the area of cyber defence of the Alliance as well as in the Member States. In this new era one of the most important elements is cyberspace itself and the realization of the fact that a country can be attacked through cyberspace and not only in well-defined traditional dimensions, such as land, air, sea, or space. This recognition in NATO led to formulate a new level of defence of Alliance's military communications and IT systems in the organization's Strategic Concept after the 2010 NATO Summit in Lisbon.

After NATO's Lisbon Summit in 2010, the Alliance's Strategic Concept included that, due to increasingly sophisticated cyber-attacks, the Alliance's protection of information and communication systems is one of the most urgent and important tasks. The Lisbon Summit Declaration formulated as follows:

"Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO's permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO's doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber-attack against systems of critical importance to the Alliance" (NATO, 2010, Article 40).

On 8 June 2011, the Defence Ministers of NATO member states signed the new Cyber Policy of the Alliance. This document contained not only strategic ideas for cyber defence, but included an action plan as well. The detailed program of this Action Plan was adopted in October 2011 (Kovács, 2014).

In accordance with the action plan the NATO Cyber Incident Response Capability (NCIRC) was launched in February 2012, and a so-called Cyber Threat Awareness Cell also started to be set up (Kovács 2014).

As we discussed above cyber security took into the focus of the Alliance, and the Chicago Summit in 2012 dealt with the issue in a very detailed way, as follows: *"Cyber-attacks continue to increase significantly in number and evolve in sophistication and complexity. We reaffirm the cyber defence commitments made at the Lisbon Summit. Following Lisbon, last year we adopted a Cyber Defence Concept, Policy, and Action Plan, which are now being implemented. Building on NATO's existing capabilities, the critical elements of the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC), including protection of most sites and users, will be in place by the end of 2012"* (NATO, 2012, Article 49).

One of the most important elements in NATO's cyber defence efforts is the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which was established just after the Estonian cyber crisis in 2008. Today, the CCDCOE has 20 members as supporting nations. The main mission of the Centre is: *"is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation"* (CCDCOE, 2018).

The CCDCOE was one of the key facilitators and coordinators to make an international study on cyber warfare entitled "Tallinn Manual". The first version of this book was issued in 2013, and one of its main purposes was to investigate issues and the applicability of international law in the field of cyber warfare. Several experts from different universities and research institutes were involved into the work. The book itself is divided into two major parts: International Cyber Security Law and the Law of Cyber Armed Conflict. It has 7 chapters and 95 so-called rules have been identified and investigated in the context of international law's applicability in cyber warfare (Schmitt, 2013).

In 2016 the Tallinn Manual 2.0 was released, which is an updated and significantly expanded version of the first book. This volume includes all rules that were investigated in the first version. The title of the new book was partially modified, as it was referred to as "International Law Applicable to Cyber Operations" instead of displaying cyber warfare explicitly. The nearly 600-page study, divided into four sections, analyses 154 rules that could be applicable from international law to cyber operations (Schmitt, 2016).

However, the biggest breakthrough moment in NATO's history regarding to cyber defence took place at the Warsaw Summit in 2016 when the Alliance officially declared that cyber space can be considered as an operational dimension. In accordance with this declaration of NATO, cyber space, at least in the military

sense, also became a dimension of warfare beside the traditional four physical dimensions. The official NATO Declaration of Warsaw Summit announces it as: *"Cyber-attacks present a clear challenge to the security of the Alliance and could be as harmful to modern societies as a conventional attack. We agreed in Wales that cyber defence is part of NATO's core task of collective defence. Now, in Warsaw, we reaffirm NATO's defensive mandate, and recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea"* (NATO, 2016, Article 40).

4. Conclusion

Our society and economy are heavily dependent on information technology and cyber sphere. The more we rely on the cyber opportunities offered by cyberspace, the more we need to consider new types of threats that can significantly affect our everyday activities, the operation of critical infrastructures, and the access to various services.

To protect and defend the cyberspace and vital critical information infrastructure both the European Union and NATO need strategic thinking.

The new EU Cyber Security Strategy, developed jointly by the EU High Representative for Foreign Affairs and Security Policy and the European Commission, was launched in early 2013. This was the first comprehensive document created by the European Union in the field of cyber security, which determined the future of cyber era in the EU. The strategy identifies very clear goals and priorities for the EU's cyber policy, including the promotion of freedom and openness, compliance, cyber security capabilities, and international co-operation on cyberspace. With this strategy and NIS Directive the EU defines a very definite and common direction for its Member States in the field of cyber security.

Although NATO has several common actions with the European Union in the field of cyber security, the Alliance has its own cyber security policy and strategy. Since the Estonian cyber crisis in 2007, NATO and its member countries have treated cyber security and cyber defence as a priority area. In 2016, there was a breakthrough decision in the Alliance's history when NATO proclaimed the recognition of cyberspace as a domain of operations.

REFERENCES

European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe,* available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN, accessed on: 20 February 2018.

European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, accessed on: 20 February 2018.

European Commission. (2017a). *European Commission – Press release State of the Union 2017 – Cybersecurity: Commission scales up EU's response to cyber-attacks,* available at: http://europa.eu/rapid/press-release_IP-17-3193_en.htm, accessed on: 20 February 2018.

European Commission. (2017b). *Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification "Cybersecurity Act",* available at: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF, accessed on: 20 February 2018.

GDPR (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),* available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, accessed on: 20 February 2018.

Kovács, L. (2014). National security and military science issues in e-government service development. In: Nemeslaki, A. (ed.). *E-public service development: Theoretical basics and scientific research methods*, Budapest: National University of Public Service.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2018). *Our Mission and Vision*, available at: https://ccdcoe.org/structure-0.html, accessed on: 20 February 2018.

NIS Directive. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed on: 20 February 2018.

North Atlantic Treaty Organization (NATO). (2002). *Prague Summit Declaration.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Prague, Czech Republic, available at: https://www.nato.int/cps/en/natohq/official_texts_19552.htm, accessed on: 20 February 2018.

North Atlantic Treaty Organization (NATO). (2010). *Lisbon Summit Declaration*. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, available at: https://www.nato.int/cps/en/natohq/official_texts_68828.htm, accessed on: 20 February 2018.

North Atlantic Treaty Organization (NATO). (2012). *Chicago Summit Declaration.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, available at: https://www.nato.int/cps/en/natohq/official_texts_87593.htm, accessed on: 20 February 2018.

North Atlantic Treaty Organization (NATO). (2016). *Warsaw Summit Communiqué.* Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, available at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm, accessed on: 20 February 2018.

Schmitt, M. N. (ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare,* New York: Cambridge University Press.

Schmitt, M. N. (ed.). (2016). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* New York: Cambridge University Press.