sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXVI No 1 2020

GENERAL ASPECTS ON CYBER SECURITY AND ITS IMPORTANCE FOR ENSURING COLLECTIVE SECURITY

Ionuț Alin CÎRDEI, Laviniu BOJOR

"Nicolae Bălcescu"Land Forces Academy, Sibiu, Romania
cirdei_alin@yahoo.com, laviniu.bojor@gmail.com

Abstract: *The cyber domain is a fundamental element of modern life, which together with the energy field sets the whole society in motion, makes it work and develop, but at the same time, it hides numerous dangers and offers numerous challenges, which can have consequences for both the individual and collective levels, which could endanger the security of states and regions. Ensuring security in the cybernetic environment is essential for the functioning of the whole society, which tends to be digitized and involves colossal efforts, both financially, humanly and technologically. Because the cyber environment offers many opportunities, but also multiplies and amplifies vulnerabilities, states pay particular attention to its understanding and security, aware that this extremely complex and difficult to control environment can pose a direct threat to national and collective security. In the cybernetic environment an individual can do the same damage that an entire army can do, and the consequences of any action can be difficult to determine, due to the interconnectedness and interdependencies that are established between domains and between states.*

Keywords: security, cyber, threat, challenge, protection

1. Introduction

Modern society is increasingly dependent on the cybernetic environment. Every aspect of life has connections to the cyber environment, and the possibilities offered by it are immense, both for those who want to use this environment for development and to improve all aspects of life, and for those who use this environment for negative purposes, either that we are talking here about individuals pursuing personal, strictly economic or affirmative purposes, whether we are talking about terrorist groups or even states that use the cyber environment to gain power, influence, to weaken an adversary or to spread chaos and terror in certain areas. When used by states or terrorist organizations, the cyber environment is a means of achieving economic, political, military and other type of objectives, and is used in combination with other direct or indirect means. Life, as we know it today, is almost impossible without the use of the online environment, the vulnerability of individuals and states growing every day, against the background of increasing dependence and penetration of new technologies in all areas, making it almost impossible for systems to work without interacting in cyber space [1].

The cyber space is extremely complex and has no borders, access to it can be achieved with relative ease and without leaving too many traces of presence in this area. Cyber environment is defined as "the electronic environment used by digital networks to store, modify or transmit information and includes the Internet and other information networks that support businesses, infrastructures or services" [2]. This

DOI: 10.2478/kbo-2020-0006

environment, which includes information, networks and physical or virtual connections has as entry points the equipment, through which actions can be initiated, actions that have the potential to affect the security status of individuals and states, because cyber space is not just used for positive purposes, to make life easier and to produce well-being, but it is also used for negative purposes, to cause damage, to illegally accumulate values, to gain power or influence or to weaken or destroy an adversary. Therefore, the impact of the actions carried out in the cyber environment can be significant both on the individuals and on the states, which can influence the state of individual or collective security.

2. The characteristics of cyber space

The cybernetic space is almost infinite, exceeding the geographical and geopolitical boundaries and reducing the distance between users and being integrated into the life of the whole society as it contributes to the functioning of critical infrastructures, as well as to the development of trade, governance and national security [3]. The cyber space ensures the development of the society and the increase of the level of well-being, as well as the reduction of the disparities between different regions, as well as the interconnection of the entities. At the same time, the intensification of the activities in the cyber space and the increase of the society's dependence on it has led to a multiplication and amplification of the vulnerabilities for individuals and for states.

The cyber space is characterized by the "lack of borders, dynamism and anonymity, generating both opportunities for development of the information society based on knowledge, but also risks to its functioning" (at individual, state level and even with cross-border and cross dimension manifestation) [4]. The use of cyber space offers opportunities and challenges for individuals, groups and states, opportunities that do not exist in the other fields or physical environments. The high speed of transmission of information and the interconnection of states and persons in a global network allows the use of cyber space as a basis for executing attacks behind the keyboard, without the need for physical contact between the attacker and the attacked one and without physical, moral and legal constraints. The objectives of organizations and states can be achieved without the need for military forces, without consuming resources and without registering human losses among the attacker, and the target will realize very late that it is attacked and that the security status is altered. This is possible because the cyber space is very complex and inside this space can be identified, according to Crowther [5], several component layers, such as: physical networks, consisting of hardware components, over which states can exercise sovereignty and which may be subject to domestic law and physical control to reduce security risks, virtual networks, represented by software components, immaterial ones, which ensure the information flow and which are extremely difficult to control and the cyber person, ie the people operating in the cyber space. These components play a vital role in the cyber environment and can represent the vectors or initiators of attacks that can affect the individual, national or collective security status.

3. Cyber security and national and collective security

Due to the complexity of the cyber environment and the increasing dependence of human society on this environment, the states strive to know, understand and control this environment, even if the state intervention is quite difficult to perform, and the measures to regulate and sanction illicit acts or hostile acts are difficult to put into practice. However, all states strive to ensure cyber security, which is seen as a component of the overall security of

society. In the general sense, cyber security can be understood as "the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public or private resources and services" [6], from cyber space. The proactive and reactive measures adopted by states to ensure cyber security can include security policies, concepts, standards and guides, activities that include risk management, training people and conducting awareness campaigns, identifying and implementing cyber infrastructure protection solutions, adopting measures aimed at reducing the consequences of cyber attacks and increasing individual and organizational resilience, promoting a culture of security, and as a last resort, direct intervention to counter hostile actions in the cyber environment, especially if they are conducted by other states, through deployment of some defensive cyber operations.

In order to supplement the efforts of the states for achieving cyber security and for strengthening national security, effective measures have been taken at EU level, which are included in the European Cyber Security Strategy. EU efforts are focused on five strategic directions, thus [7]:

- achieving cyber resilience;
- drastic reduction of cyber crime;
- development of the cyber defense policy and capabilities related to the common security and defense policy;
- development of industrial and technological resources in the field of cyber security;
- establishing a coherent international policy of the European Union on cyber space and promoting the fundamental values of the EU.

To be effective, the measures proposed by the EU must be complemented by a continuous exchange of information, cooperation on all levels, the development of partnerships with states from other parts of the globe for regulating cyber space and for implementing control and intervention measures, respecting the legal provisions and the rights and freedoms of citizens. Securing and controlling cyber space can help strengthen the security of Member States and citizens.

The intervention of states in the cyber environment is necessary because the threats are increasingly complex, they are dynamic and they have an explosive growth, constantly increasing in terms of frequency, magnitude, purpose and impact [8]. A hostile action in the online environment implies a relatively low consumption of resources, a small number of people involved, is difficult to identify and counteract and can have devastating, long-term effects on individuals, the state and the whole society. However, cyber threats may come from individuals or groups who have financial motivations or who are involved in illicit activities that are profitable and beneficial for their reputation, may come from groups led by different ideologies, or may come from states. Threats from states are the most complex, are manifested, usually in several areas, are carried out on the basis of a well-developed plan and pursue strategic objectives that cannot be achieved by other means or attempt to create favorable conditions for the use of other means of pressure. These threats require considerable human and material efforts both for planning and execution, but also for their concealment, because states, as a rule, act by proxies and wish that the real attacker and the concrete objectives could not be identified, all actions and measures being part of a set of hybrid actions.

Any entity, in order to be able to evolve, must constantly adapt to changes in the environment. In order to increase the efficiency of any activity, it is necessary to interconnect and use the cyber environment as intensely as possible. In order to reduce

vulnerabilities and protect their data and valuable assets, organizations need to identify and implement concrete measures to ensure cyber security. In order for cyber protection to be as effective as possible, both physical and virtual protection measures are needed to discourage possible aggression, detect possible hostile actions, prevent access to their own systems and combat actions as they occur, because cyber attacks are often very effective and have a number of advantages that are unmatched by other hybrid offensive actions [9]. All these measures must be included in a coherent cyber security strategy, which will allow the protection of the operational processes, of the cyber and physical infrastructure, and of data and information of any kind.

In order to develop a cyber security strategy, which will contribute to achieving national security, states must focus on a few key directions, such as [10]: understanding the risks to cyber security, integrating measures aimed at strengthening personnel security, technical security, physical and information security, in an integrated, multilayered protection system, implementing preventive and deterrence measures, accepting that some attacks will have success and the development of resilience to enable the system to continue to function and recover as quickly as possible, creating an organizational culture of security, including cyber security.

Actions in the cyber environment may pose a threat to individual, state or collective security. If the target of a cyber attack is a person, then it is very likely that the effects of the actions taken against him will be felt only by that person or by a small group of people, which makes the attack a threat to individual security, the individual being directly or indirectly affected and may feel in danger. If the target of the attacks are the state institutions or basic elements of the society, which ensure the functioning of the economy, the systems that ensure the living conditions of the citizens, etc., then the attack can be perceived as a threat even to the national security. However, modern society is strongly interconnected and interdependent, and an event in one state can have consequences at the level of other neighboring states or even at significant distances, which means that an attack on one state can affect the security of other states and it can be treated as a direct threat to collective security.

4. NATO's position on the importance of cyber security

NATO member states have realized the importance of providing cyber security against the backdrop of the security environment and amplifying hybrid threats, and as cyber threats become more and more frequent, complex, have increasingly destructive effects [11]. Under these conditions, NATO must be prepared to carry out extensive cyber defense actions to protect communications networks and military operations themselves. NATO, as a political-military alliance, affirmed its determination to ensure the collective defense of its members, based on the provisions of Article 5 of the North Atlantic Treaty, including in the face of cyber threats, which could endanger the integrity of the territory, the functioning of the economy, including national and collective security and therefore strives to secure communications networks, energy and transport infrastructure, to know and identify cyber threats as early as possible, to train forces through instruction and exercises and to increase resilience, and complementarily states are trying to develops their own defensive capabilities in the cyber domain, establishing cyber defense commands and investing in specialized equipment and training. NATO was aware of the importance of the cyber domain even before the threats in this area multiplied and increased and before some states or entities carried out real cyber campaigns against other states.

Thus, at the Prague summit in 2002, NATO identified the need to strengthen cyber security at all levels of the alliance and of the Member States, and in 2008 adopted the first cyber defense policy. Against the backdrop of rising international tensions and the development of the cyber domain, the Enhanced NATO Cyber Defense Policy was adopted at the summit in Wales. The next step was taken at the 2018 Brussels summit, when NATO's position became very clear, leaving it to be understood that a cyber attack against a Member State can be associated with an armed attack and will be treated with all seriousness in the prism of the right to collective defense [12]. Collective defense against cyber threats can ensure the concentration of efforts and information sharing, avoiding duplication of capabilities and developing new ones, within the concept of smart defense. However, collective measures must be duplicated by individual measures adopted by each Member State, measures that include both preventive actions and the adoption of active and passive measures to counter cyber threats. The defense against cyber threats should not be based solely on a strictly defensive attitude, which should have only preventive and counteracting actions in the center, it should not be a reactive defense, but it must be more an active defense, which should combine passive measures with the active ones and which allows the early identification of the threats and the mode of action of the potential aggressors, it could be even the execution of preventive strikes in this domain, by virtue of the right to self-defense in the face of hostile acts or in front of some actors with clear hostile intentions.

To strengthen cyber security "NATO and many other armed forces see cyber space as a distinct military domain and have begun integrating defensive and offensive cyber capabilities into their operational planning through the following measures: developing cyber capabilities, combining cyber options with other types of operations, reorganising their command structures, devising cyber doctrines and embedding them in overall doctrine and examining how national and international law applies to actions in cyber space" [13].

In the future, NATO will act in several directions to counter threats in the cyber environment, both from individuals or criminal organizations, and especially those initiated or coordinated by terrorist organizations or hostile states. Among the measures the Alliance will take are [14]: developing the capabilities needed to defend national infrastructures and networks, also by integrating cyber defense into alliance operations, allocating the resources needed to strengthen cyber defense capabilities, promoting cooperation and the exchange of best practices between cyber defense specialists, improving the identification and the implementation of the most effective measures for cyber prevention and defense at all levels, promoting education, instruction and exercises to raise awareness, to know the situation and to consolidate a specific security culture and to observe the commitments aimed at strengthening cyber security and development specific cyber defense capabilities. By enhancing the level of protection and by adopting comprehensive measures that ensure increased cyber security, NATO contributes to securing the vital functions of the alliance and to ensuring the collective security of member states, as well as protecting NATO forces participating in various military operations.

5. Conclusions

Cyber security is a relatively recent concern for states, as they are aware that they are very vulnerable to threats from the virtual environment and that the cyber environment offers unlimited possibilities for attackers who can easily hide and carry out attacks with devastating effects. By taking the necessary measures to increase cyber security, each state actually

strengthens its national security and contributes directly and indirectly to achieving collective security, given that the current security environment is increasingly complex, more dynamic and unpredictable and when individual, state or non-state actors can act almost unimpeded using the opportunities offered by the cyber environment. When actions in the cyber environment are duplicated by actions in other areas, such as economic or military, national security can be affected in a quite serious manner, and the consequences of the attacks will be extremely difficult to manage.

Each state is responsible for its own security and also for the security of its allies, which is why it must strengthen its cyber security. In at the same time, NATO must support the individual efforts of the Member States by: developing cyber capabilities, investing in cyber defense, adapting command and control structures, integrating cyber effects in military operations, improving cyber strategies and policies, encouraging cooperation and the exchange good practices and information exchange, maintaining situational awareness, supporting and encouraging education and training activities, developing partnerships with related fields and other international organizations, etc [15].

Cyber security is an individual problem of the states but at the same time it is a problem of the international community. Efforts to know cyber space, identify threats and understand them, to combat cyber threats and aggressors must be coordinated, and resources of states with the same goals, which are part of the same political-military blocks, must be used in an efficient and integrated manner, based on the principles specific to the concept of smart defense.

References

[1] Bojor, L. (2017). *Security and Privacy in Smart Devices Era*, International conference KNOWLEDGE-BASED ORGANIZATION, 23(1), p. 44.

[2] https://www.cpni.gov.uk/cyber, accessed on 02.02.02.2020.

[3] Joint Publication 3-12, *Cyberspace Operations*, 8 June 2018, p. I-1.

[4] Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013, p. 4.

[5] G. Alexander Crowther, National Defense and the Cyber Domain, retrieved from https://www.heritage.org/military-strength-topical-essays/2018-essays/national-defense-and-the-cyber-domain, accessed on 23.01.2020.

[6] Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013, p.7.

[7] Comisia Europeană, Comunicare comună către Parlamentul european, Consiliu, Comitetul economic și social european și Comitetul regiunilor, *Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat*, Bruxelles, 7.2.2013, p. 5.

[8] https://www.nsa.gov/what-we-do/understanding-the-threat/, accessed on 18.02.2020.

[9] Marius PRICOPI*, Studiu privind efectele războiului hibrid asupra infrastructurilor critice,* in Ghiţă Bârsan, Anca Dinicu şi Dorel Badea (coordonatori), *Analiza şi modelarea conceptuală a situaţiilor complexe* (studii interdisciplinare), p. 59, Editura Academiei Forţelor Terestre "Nicolae Bălcescu", Sibiu, 2016.

[10] https://www.paconsulting.com/insights/developing-an-effective-cyber-security-strategy/.

[11] https://www.nato.int/cps/en/natohq/topics_78170.htm, accessed on 23.02.2020.

[12] Science and Technology Committee (STC), *NATO in the cyber age: strengthening security & defence, stabilising deterrence*, 087 STC 19 E, Draft General Report, 18 April 2019, p. 1, retrieved from https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence, accessed on 21.02.2020.
[13] Science and Technology Committee (STC), *NATO in the cyber age: strengthening security & defence, stabilising deterrence*, 148 STC 19 E rev. 1 fin, General Report, October 2019, p. 4, retrieved from https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence, accessed on 22.02.2020.
[14] NATO Cyber Defence Pledge, 08 Jul. 2016, retrieved from https://www.nato.int/cps/en/natohq/official_texts_133177.htm, accessed on 22.02.2020.
[15] Science and Technology Committee (STC), *NATO in the cyber age: strengthening security & defence, stabilising deterrence*, 148 STC 19 E rev. 1 fin, General Report, October 2019, p. 13, retrieved from https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence, accessed on 23.02.2020.