EUROPEAN UNION POLICIES ON CYBER SECURITY

Colonel (Ret.) Professor Gheorghe BOARU, PhD*

Abstract: *The benefits that the virtual environment and their adjacent technologies brought to mankind have been overshadowed by specific insecurity, manifested by new forms of threat – the cyber attacks.*

Europe has also been the target of such cyber attacks, which has prompted the European Union to develop its cyber-protection policies by developing a series of cyber-security strategies.

Romania, as a member of the European Union, has developed its own cyber security policy by developing specific documents and creating national structures in the field of cyber security in full compliance with European policies.

Keywords: *cyber threat, cyber security, cyber security policies, cyber security strategies, cyber attacks, resilience.*

The salience of cyber security in the European Union, Information and Communications Technologies (ICTs)[1], in particular the Internet, have been an increasingly important aspect of global social, political and economic life for two decades, and are the backbone of the global information society today. Their evolution and development have brought many benefits for individuals, as well as a plethora of public and private institutions and actors; witness the positive impact of social networks on the

* Corresponding Member of Academy of Romanian Scientists, Member of the Academy of National Security Sciences, e-mail: boarugheorghe@yahoo.com.

[1] Information and Communication Technology (ICT) is an extended term for information technology (IT), which emphasizes the role of unified communications and the integration of telecommunications (telephone and wireless signals), computers and business software, processing, storage, and audio-visual systems that allow users to access, store, transmit and operate with information, [https://en.wikipedia.org/wiki/Information_and_ communications technology].

uprisings in the Arab Spring in 2011, or the increased use of e-commerce among businessmen and individuals.

ICTs have also, however, brought the threat of serious cyber-attacks demonstrated in recent years through acts of cyber espionage and cyber crime within the virtual, networked ecosystem that we live in.

Securing cyberspace has become one of the most pressing security challenges of the twenty-first century through its importance to everyday life for government, business and citizens alike. The cyber world and its associated technologies have, on the one hand, created many social, cultural, economic and political opportunities for all, whilst on the other, its borderless nature has brought with it threats in the form of cyber attacks and cyber crime. The European Union (EU) is not immune to such threats. The Distributed Denial of Service attacks on Estonia's public and private networks and systems in 2007, and attacks on its own institutions in 2011(the European Commission, the European Parliament), among other cases of high-ranking cyber-attack[2] organizations demonstrate the realism of this statement.

Cyber attacks have included, to name but a few high-profile cases, attacks on Estonia's public and private institutions in 2007, Russian-sourced attacks on Georgian systems in 2008, the Stuxnet worm attack on the Iranian nuclear program in 2009, the re-routing by a Chinese Internet service provider (ISP) of sensitive US government e-mail traffic to China, the WikiLeaks affair in 2010.

Beyond such high-profile attacks, reports of attacks on companies have also proliferated in the last few years and also pointed out that the losses suffered by them were not negligible.

Such events have underlined the vulnerability of ICTs and have brought the European information security agenda to the forefront of important political issues.

All this has triggered a strong alarm signal for the EU and they have become convinced that cyber security must enter urgently to the top of the EU political agenda.

A Romanian specialist and writer, acknowledged in the field of intelligence, Professor George Cristian Maior also points out in a

[2] The predominant attacks were: DoS (Denial of Service), DDoS (Distributed Denial of Service), blog comments, Internet propaganda, and site damage.

specialized paper about the dangers of such cyber attacks: *"The dependence of most countries on IT infrastructures to meet basic needs can predict the risk of devastating effects as a result of disruptions, even briefly, of essential public services such as banking and commerce, communications, production or transport. From this perspective, hostile actions in cyberspace are broad, complex and direct threats to security"*[3].

The conclusion also highlights the global and multi-dimensional nature of the information assurance problem – with recognition that security governance developed to combat the cyber threat must engage the many levels, actors, institutions and individuals involved within the cyber ecosystem.

To prioritize the field and integrate its internal and external policies and actions, the EU subsequently produced its first Cyber Security Strategy in 2013. The EU was aware that it would not be able to address the cyber security challenges alone, given the global and open nature of the Internet.

In a wider international, regional and national context, this document analyzed the EU approach to the challenges it faces itself in the virtual space before and after publishing its Cyber Security Strategy.

Using the fusion of concepts of resilience and governance security, this strategy provides a new framework for understanding and assessing how much the EU has progressed in integrating the necessary conditions for a cyber, elastic and secure ecosystem to emerge in Europe and beyond. It is argued that the incorporation of such conditions will facilitate the emergence of adaptable and flexible passage capabilities necessary for the EU to promote security, safety and confidence in cyberspace.

An analyst and policy specialist George Christou[4] shows in his analysis in a specialized paper[5] that cyber security can be a basic condition for the social and cultural benefits of Europe as well as for our economic growth. He argues that specific security technologies (ICTs) are essential to achieve this.

---

[3] George Cristian Maior, *Un Război al Minții. Intelligence, servicii de informații și cunoaștere strategică în secolul XXI*, Editura RAO, București, 2010, p.231.

[4] George Christou, Associate Professor of European Policies, University of Warwick, UK.

[5] George Christou „*Cybersecurity in the European Union-Resilience and Adaptability in Governance Policy",* New Security Challenges Series, Macmillan Publishers Limited, London, 2016.

Often, politicians still believe and act roughly without a differentiated and refined approach to sensitive areas. Thus, there are opinions that claim that cyber war is defense, cyber crime is law enforcement, private life is dominated by justice, and so on. Unfortunately, technology and attackers do not distinguish between these different areas.

We ask ourselves the question: Was the Stuxnet attack cyber crime, cyber sabotage or cyber warfare?

Depending on the political interpretation, the answer may be different, but the attackers do not care. And next time, the same Stuxnet technology - which is now publicly known - can be used to attack a modern car, a passenger aircraft, or it can be a denial of service attack against the information systems of a European or national critical infrastructure.

Therefore, all actors and stakeholders need to work in a cooperative manner and, for this, processes such as incident reporting and information sharing are essential.

I fully share the view expressed by Prof. Udo Helmbrecht (Executive Director of the European Network Security Agency), who, in the preface to a paper by George Christou, sent the following message: *„Fostering trust and security in cyberspace is not an option for the EU; it is a requirement and pre-requisite for realizing its own ambitions, promoting its values, and (re)defining its identity in a dynamic global order that is increasingly reliant on digital interoperability and connectivity"*[6].

In this context, the European Union (EU) over the past ten years has been developing its policies towards cyber threats, even though this has often been quite fragmented. The EU's Internal Security Strategy (ISS, November 2010) and the Digital Agenda for Europe (2010) have provided the main broad guidance for its activities in this area in more recent times. However, the EU also produced more specific proposals through the European Strategy for Internet Security (ESIS 2011) and the Cyber Security Strategy for the European Union (EUCSS 2013).

Institutionally, the European External Action Service (EEAS) plays the role of central coordinative node in agreeing on and projecting EU cyber

[6] George Christou, Op.q, p. x.

security policy externally, whilst the EU Computer Emergency Response Team (CERT) fulfils the technical aspects of such a role internally.

The Directorate Generals Connect (DG Connect) and Home (DG HOME) take the lead in developing policy in relation to Network and Information Security (NIS) and cyber crime, respectively, with the European Parliament also playing a key role within the policy process with regard to relevant Regulations and Directives.

Beyond this, there are key EU agencies, including the European Defense Agency (EDA) which works on developing EU cyber defense, the European Network and Information Security Agency (ENISA) which works with relevant stakeholders to develop advice and recommendations on good practice in information security (including cyber crime), and with EU member states in implementing relevant EU legislation to improve the resilience of Europe's critical information infrastructure and networks.

Indeed, whilst creating a comprehensive approach to cyber security within the EU has become a political priority with a renewed sense of urgency around the issue, there is still a lack of clarity on how cyber threats can be regulated and coordinated in governance terms in order to build sustainable and resilient platforms and systems.

Briefly, whilst the EU certainly possesses many tools and mechanisms for addressing the cyber security issue, how it uses them needs to be developed, and the consistency and coherence across the institutions and actors involved need to be improved.

By studying these issues, I have set some central objectives, but there have also been questions arising from the need to find explanations on the evolution of the EU's cyber security governance system, which also provides a deeper analysis (I hope also an understanding) on how the EU can build effective security as resilience (adaptive capacity) in terms of cyber threat issues.

In addition, this analysis may help to provide answers to the central questions that this article seeks to challenge or even provide:

• How can we characterize and understand the EU's evolving ecosystem of cyber security governance?

• To what extent has the EU been able to construct a comprehensive approach to cyber security within the evolving ecosystem, and embed the necessary conditions for effective security as resilience?

• What is the nature of the resilient ecosystem emerging in the EU?

What is at stake within the EU space is significant. If the EU cannot facilitate the construction of the necessary conditions for security as resilience in cyberspace in the near and long term, then there is a danger that trust and confidence in the Internet will be eroded, and that the EU will remain vulnerable to cyber attacks and, importantly, unable to react and recover in an effective way.

Improving the way in which the EU does cyber security is essential for the continued social, economic, financial and cultural benefits that citizens and businesses derive from the Internet and, more broadly, evolving ICTs. Moreover, it is critical if it is to achieve the objectives it has set for itself in the Digital Agenda for Europe (2010), and equally as significant, the driving force of such an agenda, the Europe 2020 strategy.

Fostering trust and security in cyber space then is not an option for the EU; it is a requirement and prerequisite for realizing its own ambitions, promoting its values and (re)defining its identity in a dynamic global order that is increasingly reliant on digital interoperability and connectivity.

In full agreement with the European actions, in February 2015, the National Strategy on the Digital Agenda for Romania 2020 was approved, defining four domains of action, of which only the first domain is mentioned: e-Governance, Interoperability, Security Cybernetics, Cloud Computing and Social Media.

This document has taken on and adapted to the specifics of our country the elements of the Digital Agenda for Europe. The Digital Agenda thus defines the major role that the use of ICT must play in achieving the Europe 2020 objectives.

At EU level, both theoretically and conceptually, work has been dispersed in relation to the cyber security analysis of the emerging (developing) ecosystem made by EUCSS. Cyber security research has been expanded, increasing progressively from one perspective to another, and some authors have provided new insights into the EU through the implementation of cyber power[7] concepts and resilience capability [8].

[7] Alexander KLIMBURG and Heli TIRMAA-KLAAR, (2011), *Cyber War and Cyber Security: Challenges Faced by the EU and Its Member States*, DG for External Policies, Policy Department, European Parliament, April 2011, [http://www.europarl.europa.eu/-RegData/etudes /STUD/2011/ 433828/EXPO-SEDE_ET(2011)433828_EN.pdf], accessed on 04.02.2017.

Another author[9] also compares the EU with the North Atlantic Treaty Organization (NATO) as a benchmark to further understand the limitations and challenges ahead for the EU. Two major factors limit the EU as a cyber security actor: its intergovernmental nature as well as the lack of collective vision of cyber security in the EU and between Member States. To play an important role in shaping cyber space and cyber security, the EU cannot treat the Internet as a simple communication tool or trading platform.

However, such works were not complete in their approach or conceptual reflection on an emerging ecosystem of resilience within the EU and even in Europe. I cannot argue that such approaches have nothing to offer; in fact, on the contrary, I believe that such works need further applications and further development in order to reach a deeper understanding of how far the EU went in order to achieve effective security as resilience in this evolution of the ecosystem.

The argument of some other authors[10] is that the EU's approach to cyber security should lead to flexible and adaptable resilience through appropriate governance mechanisms and ways to enable it to become an influential actor in cyber space and a leader in good practices in cyber security taking into account its many and different dimensions.

I think some clarifications need to be added and some parameters defined.

The first clarification relates to what kind of role the EU can play in cyber security, in a realistic way, so that some aspects of national sensitivity and security could be achieved.

---

[8] Myriam Dunn Cavelty, *From Cyber-Bombs to Political Fallout-Threat Representations with an Impact in the Cyber-Security Discourse*, Volume: 15, Issue: 1,Pages: 105-122, Publication Year: 2013, [http://www.css.ethz.ch/en/publications/ search/details.html?id=/-f/r/o/m/ from_cyberbombs_to_political_fallout], accessed on 01.03.2017.

[9] Krzysztof Feliks Sliwinski, (2014), *Moving Beyond the European Union's Weakness as Cyber-Security Agent*, Contemporary Security Policy, DOI:10.1080/13523260.2014.-959261 (22 September 2014), [http://repository.hkbu.edu.hk/ cgi/viewcontent.cgi?article=-1007&context=gis_ja], accessed on 14.03.2017.

[10] Alexander KLIMBURG and Heli TIRMAA-KLAAR, *Op.q.*; Myriam Dunn Cavelty, *Op. q.*

The EUCSS acknowledges that *"it is primarily the responsibility of Member States to cope with security challenges in the virtual space"*[11], but also that the EU must play a key role as an actor in itself in this "game".

In the same spirit and approach, the Cyber Security Strategy for the European Union (EUCSS) states that *"cyber security can only be solid and effective if it is based on fundamental rights and freedoms as enshrined in the Charter of Fundamental Rights of the European Union ..."* [12] .

To this end, it is clear that the EU can be a mediator to provide a platform or even a bridge between the different cyber security domains, to create the necessary conditions for an effective implementation of a cyber security culture within the Member States.

The EU could also play a critical role in working with weak or strong member states to build the minimum standards (legal, technical, political, economic, strategic and operational) that are necessary for the EU to develop as an elastic actor in the ecosystem, in terms of cyber security.

Moreover, the EU can act as an effective regional node for the exchange of good practices across the member states – and internationally, through the evolution, promotion and projection of principles and norms for Internet governance, including critical issues of cyber security.

Indeed, given the borderless and transnational nature of cyber security and the external reach and influence of the EU, it has a critical role to play in creating a culture of resilience and cyber security not only in Europe, but also globally.

The second relates to the ongoing debate about how to define cyber security and its various dimensions – cyber security, cyber crime, cyber espionage, cyber terrorism, cyber hacktivism and so on, whilst this has become a topic in and of itself for some researchers[13] (see, for example, Di Camillo and Miranda, 2011), and many regional and international organizations and agencies provide varied definitions.

---

[11] *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, p.4, [http://eeas.europa.eu/ archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf], accessed on 10.03.2017.

[12] *Ibid.*

[13] Federica Di Camillo,Valérie Miranda, *Ambiguous Definitions in the Cyber Domain: Costs, Risks, and the Way Forward*, IAI Working Papers 1126, September 2011[https://www.scribd.com/document/104123830/Di-Camillo-Emiranda-Ambiguous-Definitions-in-the-Cyber-Domain], accessed on 15.02. 2017.

I did not intend to expose here the diversity of concepts and definitions. I do not say that the definitions are not important, but I rather think it would be more appropriate for a central part of the analysis to focus on the emergence (or not) of definitions or common understanding of the various concepts and dimensions of cyber security.

I believe that the starting point can be the definitions adopted by the EU (including the relevant EU agencies) and its Member States. "Cyber security", in this case, is defined by the EU in general terms, with reference to cyber crime (more focused on their nature).

Cyber defense is not defined in EU documents, given the sensitivity of the Member States to this issue and the reluctance of some Member States to participate in this action, given their own cyber defense strategies.

That is why cyber defense, unlike cyber crime and NIS (Network and Information Security), is under the intergovernmental mandate of the Common Security and Defense Policy (CSDP) and not under the exclusive or shared EU competence.

I present some definitions of the main concepts in the field, in a European vision:

Cyber security usually refers to: *"safeguards and actions that can be used to protect the cyber domain, both in civilian and military environments, from those threats that are associated with, or which may affect, its interdependent networks and information infrastructure"*[14]

Cyber security strives to maintain the availability and integrity of networks and infrastructure and the confidentiality of the information contained therein.

Computer crime is very broadly defined as *"a wide range of different criminal activities, involving computer and computer systems, either as a primary tool or as a primary target"* [15].

In the same approach, ***computer crime*** is considered to include*: "traditional offenses (e.g. fraud, forgery and identity theft), other cyber crime (e.g. the online distribution of child pornography or inciting racial hatred) and single offenses against computer and information systems (for*

[14]*Cybersecurity Strategy of the European Union, Brussels, Op. q*., p.3.
[15] *Ibid.*

example, attacks against information systems, denial of service or malware) [16].

Third, while recognizing and accepting that cyber security analysis within any domain must be interdisciplinary in order for the presentation to be as comprehensive as possible - that is to say, equal weight to all levels: the "physical level" (hardware), "logical level" (software and protocol) and its content or "social level" (culture, human contact, ideas and policies) [17].

In Romania, the general framework for cooperation bringing together those authorities and public institutions with responsibilities and competences in the field of cyber security is represented by the National Cyber Security System (SNSC). SNSC's activity is coordinated at strategic level by the Supreme Defense Council of the Country.

The unitary coordination of SNSC elements is ensured by the Cyber Security Operational Council (COSC). This council includes, as permanent members, representatives of the main ministries and services that have responsibilities and competencies in the field of national security and defense. The technical coordination of COSC is provided by the Romanian Intelligence Service.

Depending on the specific competencies in the field of national security and defense, each of the institutions represented in the COSC cooperates with the international bodies of the EU, NATO, OSCE, etc.

The Government of Romania, through the National Cybersecurity Response Center - CERT-RO[18] - ensures, according to its competence, the elaboration and the promulgation of the public policies for prevention and counteraction of the incidents within the national cyber infrastructures.

In 2013, GD no. 271 was issued, approving the Cyber Security Strategy of Romania and the National Action Plan on the Implementation of the National Cyber Security System.

This strategy comprises a separate chapter in which it presents the concepts, definitions and terms specific to cyber security. In a national approach, the concepts I have referred to above are presented as follows: *"Cyber security is the state of normality resulting from the application of a*

[16] *Ibid.*

[17] Yochai Benkler, (1998), *The Commons as a Neglected Factor of Information Policy*, [www.benkler.org/commons.pdf], accessed on 20.03.2017.

[18] *Government Decision no. 494/2011* regarding setting up the National Cybersecurity Response Center - CERT-RO.

set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public and private resources and services in cyber space. Proactive and reactive measures can include security policies, concepts, standards and guides, risk management, training and awareness-raising activities, implementation of cyber-protection technical solutions, identity management, consequences management" [19].

Cyber crime - *"all the facts provided by criminal law or other special laws that pose social hazards and are committed intentionally through cyber-based infrastructures"* [20].

The rapid evolution of the nature of cyber threats also required the adoption by the North Atlantic Organization of a new concept and new policy in the field of cyber defense. In this respect, NATO has redefined its role and its field of action and has developed an action plan to develop capabilities to protect its own cyber infrastructures, as well as mechanisms for consulting Member States and providing assistance in case of major cyber attacks.

As a national specific element, in the sense of Cyber Security Strategy of Romania, **cyber defense** is defined as: *"cybernetic actions in order to protect, monitor, analyze, detect, counteract aggressions and provide a timely response against threats to specific cybernetic infrastructures of national defense"*[21].

It is worth highlighting that, in this area of cyber security, the Romanian approaches are in full agreement with the European ones but also with the NATO requirements.

Fourth, while this presentation of ideas provides sufficient coverage of the main pillars of the EUCSS, there are still many important EU issues and European cyber security that could not be covered. In addition, the priorities highlighted in the EUCSS (2013), such as the development of cyber security industrial and technological resources and the establishment

[19] *HG no. 271/2013* for approving *Romanian Cyber Security Strategy* and its Action Plan on national level regarding the implementation of the National Cyber Security System, Appendix no.1 to Romanian Cyber Security Strategy, p.7.
[20] *HG nr. 271/2013, Op.q.*
[21] *HG nr. 271/2013, Op.q.*

of a coherent international virtual space policy for the EU, are briefly presented in this approach.

Beyond this, there would be other aspects, such as cloud computing security, smart technologies (cities, environment, devices, etc.) and IT - activating industrial control systems to name just a few that are not covered. The "Brexit" phenomenon compels us to recognize that not all cyber problems affecting Europe, the EU and its Member States could be clarified in a single such exploration.

Finally, there is one note of caution that needs to be added given the dynamic nature of developments in ICT and cyber security policy and practice more broadly, and the formative nature of many of the EU's initiatives stemming from its Cyber Security Strategy (EUCSS 2013).

The topic addressed can cause, within the various structures, at least a conversation on the relationship between the political, cultural and technical challenges of building an elastic cyber security ecosystem in Europe and beyond. After all, technical solutions are only possible if there is a proper legal and political environment to implement them effectively.

BIBLIOGRAPHY

*** *HG nr. 494/2011* regarding setting up the National Cybersecurity Response Center - CERT-RO.

*** *HG nr. 271/2013 Romanian Cyber Security Strategy* and its Action Plan on national level regarding the implementation of the National Cyber Security System, Appendix no.1 to Romanian Cyber Security Strategy.

*** *HG nr. 245/7 apr. 2015* approving *National Strategy regarding Digital Agenda for Romania 2020.*

*** *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, [http://eeas.europa.eu/ archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf].

BENKLER Y., *The Commons as a Neglected Factor of Information Policy*, 1998, [www.benkler.org/commons.pdf].

CAVELTY M.D., *From Cyber-Bombs to Political Fallout-Threat Representations with an Impact in the Cyber-Security*, Discourse, Volume: 15, Issue: 1, Publication Year: 2013, [http://www. css.ethz.ch/en/publications/ search/details.html?id =/f/r/o/m/ from_cyberbombs_to_political_fallout].

CHRISTOU G., *CYBERSECURITY IN THE EUROPEAN UNION-Resilience and Adaptability in Governance Policy*, New Security Challenges Series, Macmillan Publishers Limited, London, 2016.

FEDERICA Di Camillo, MIRANDA V., *Ambiguous Definitions in the Cyber Domain: Costs, Risks, and the Way Forward*, IAI Working Papers 1126, September 2011, [https://www.scribd.com/document/104123830/Di-Camillo-Emiranda-Ambiguous-Definitions-in-the-Cyber-Domain].

KLIMBURG A., TIRMAA-KLAAR H., *Cyber War and Cyber Security: Challenges Faced by the EU and Its Member States*, DG for External Policies, Policy Department, European Parliament, April 2011, [http://www.europarl.europa.eu/RegData/etudes /STUD/2011/ 433828/EXPO-SEDE_ET(2011)433828_EN.pdf].

MAIOR G.C., *Un Război al Minții. Intelligence, servicii de informații și cunoaștere strategică în secolul XXI*, Editura RAO, București, 2010.

SLIWINSKI K.F., *Moving Beyond the European Union's Weakness as Cyber-Security Agent*, Contemporary Security Policy, DOI:10.1080/ 13523260. 2014.959261 (22 September 2014), [http://repository.hkbu.edu.hk/cgi/viewcontent.cgi?article =1007 & context=gis_ja].