# THE CHANGING ROLE OF THE EU IN CYBERSECURITY

# AZ EURÓPAI UNIÓ VÁLTOZÓ KIBERBIZTONSÁG KONCEPCIÓJA

**BELÁZ ANNAMÁRIA**[1]

## ABSTRACT

Cyberspace poses a great challenge to the traditional governance, that is mainly state-centric – it challenges the traditional concepts like security, borders, privacy and sovereignty. Legal discussions about cyberspace governance often focus on international cybercrime arrangements, international standards and national sovereignty. Due to the globalisation and the interconnected nature of cyberspace and the cross-border impacts of attacks, it has been made impossible for any organisation to manage cyberspace and cyber threats without an adequate level of cooperation with various partners and allies. This is especially relevant in certain areas of national security, as well as in the Common Foreign and Security Policy (CFSP) of the European Union.
But what does cybersecurity mean for the European Union and how its viewpoint changed through the past decades? This paper analyses the EU acquis to provide an overview on EU cybersecurity policy and to understand the challenges EU currently facing as a cyber-actor.

**Keywords:** European Union, cybersecurity, Common Foreign and Security Policy (CFSP), governance

## ABSZTRAKT

A kibertér megjelenése kihívást elé állítja a biztonság, határok, magánélet és szuverenitás hagyományos értelmezésén alapuló klasszikus kormányzati modellt. A kibertér kormányzásával kapcsolatos jogi viták és értekezések középpontjában túlnyomórészt a nemzetközi számítógépes bűnözés, nemzetközi jogi

[1] belaz.annamaria@phd.uni-obuda.hu | ORCID: 0000-0002-8222-5283 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

normák és a nemzeti szuverenitás kérdései állnak. Azonban a globalizáció, valamint a kibertámadások határokon átnyúló jellegének köszönhetően egyes országok vagy szervezetek önállóan, más szervezetekkel vagy nemzetekkel való együttműködés nélkül képtelenek leküzdeni a kiberbiztonsági fenyegetéseket. Az együttműködés kérdése kiemelkedően fontos a nemzetbiztonság egyes területein, valamint az Európai Unió közös kül- és biztonságpolitikájában. De mit jelent a kiberbiztonság az Európai Unió számára és hogyan változott a nézőpontja az elmúlt évtizedekben? Jelen tanulmány áttekintést nyújt az uniós jog fejlődéséről, valamint azonosítja az Európai Unió kibertérből fakadó kihívásait

**Kulcsszavak:** Európai Unió, kiberbiztonság, Közös Kül- és Biztonságpolitika, irányítás

## INTRODUCITION

Since the first appearance of personal computers, the development of new technologies and the global digitalization poses a difficult challenge for policymaking experts since the innovative solutions not only appear at the individual but at the governmental level. This challenge requires both regulatory and defence (precisely cyber security and cyber defence) actions. International experiences show that electronic information systems, in particular, governmental and public administration systems, are a constant target of organized cyber-attacks, therefore cybercrime, information warfare, and cyber terrorism are a constant threat to public systems.

In order for the European Union to provide the highest level of security for its citizens, it is essential to tackle down the regulatory and defence challenges. The network and information systems play a crucial role in the cross-border movement of goods, services, and people. The disruption of these systems, regardless of where they occur, can affect the Member States individually, a region or the Union as a whole, therefore, the protection of these systems is vital for the EU.

Based on the EU *acquis communautaire* this paper aims to examine what cybersecurity mean for the EU, how its' viewpoint changed on cyber-related issues in the past decades, and how the current institutional and legal framework support the Union's vision to became a leading actor in the cyber domain.

## THE CHANGING ROLE OF THE EU IN THE CYBERSECURITY ARENA

Due to the high level of global cybercrime and the increasing number of threats from cyberspace, cybersecurity became a top-level policy in the many states, regions, international organisations and in the European Union. (Carrapico & Barrinha 2018) The policy and debate focus on political measures and behaviour in cyberspace, they searching for an answer how to govern and control the global cyberspace. At the heart of this discussion lie the ***fundamental questions of power and control***. "But how does this play out in the specific

case of the European Union, who is claiming influence as an actor in matters of European and even global cyberspace?" (Cavelty 2018:304) Analysing the relationship between power and governance of the cyberspace is an important step towards understanding that EU's emerging role in the in virtual realm also supports its aspiration to become a leading international security actor. Existing texts and research including those specifically addressing European cyber-power (Klimburg & Tirmaa-Klaar, 2011; Dewar 2017; Christou 2017), are of a primarily policy-oriented nature, there also is a clear dominance of military or strategic voices (Carrapico & Barrinha 2017; Bendiek, 2017b).

In the past few years the idea of ***building a stronger and more resilient internal security by strengthening cyber security policy and institutions*** appeared within the EU. On 19-20 October 2017, the European Council asked for the adoption of a common approach to EU cybersecurity following the proposed ***reform package***[2], calling for 'a common approach to cybersecurity: the digital world requires trust, and trust can only be achieved if we ensure more proactive security by design in all digital policies, provide adequate security certification of products and services, and increase our capacity to prevent, deter, detect and respond to cyberattacks'.[3] But what were the antecedent actions which led to this reform?

Based on previous the research conducted by R. S. Deward (2017) and Molnár (2017) together with the latest legislative reforms, the following part of this paper will examine - in chronological order - the turning points in the EU's existence which led to the development of the current institutional structure. It is not the aim of this section to enter into a lengthy analysis of the EU's history. Such discussions have been conducted in many academic books. However, it is beneficial to briefly consider the key landmarks in the path of cyber policy development.

## The beginnings 1985— 2001

In this time-period four events established particular institutional dynamics which affected the later development of cyber security policy. ***1985 Single Market***: ICT and the Internet itself, were viewed as a great opportunity for social and economic growth - thanks to the free movement of goods, services and people-, and this viewpoint led to the ***commercialisation of the cyber policy***. The economic maximalisation climaxed in the publication of the ***Bangemann Report*** in 1994. The document it contained the conceptual seeds for all elements of the EU's later discourse and "cyber" policy.[4]

After the Union's commercial interest in the ICT sector were articulated, its competences solidified in the Treaty-based codification. The ***Single European Act*** of 1987 and the ***Maastricht Treaty*** of 1992 formalised EU's role in cybersecurity by restricting its competences to "political and economic aspects"[5]. These decisions limited the Union's competence on the "soft" powers, leaving out the "hard" capabilities (meaning a militarized and centralised

[2] Joint Communication to The European Parliament tnd The Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN/2017/0450 final

[3] European Council Conclusions of 19 October 2017.

[4] The Report makes clear that economic factors such as market forces, and the creation of jobs underpin the Union's interest and strategic outlook in ICT. The protection of fundamental rights such as privacy, security and safety are core elements both in the Bangemann Report and later in the European Union Cyber Security Strategy.

[5] European Union, 1987. Single European Act., p. 1049

security governance).[6] Thus, cyber security policy took a non-military, strategic, socio-economic approach.
Under the Treaty of Maastricht, and due to the importance of the internal market info-communication technologies, and so cyber issues fell into the First Pillar. This, in one hand, enabled the EU to initiate legislation and engage proactively in the decision-making process, on the other hand, it strengthened the economical nature of the cyber policy and in the meantime separated it from the cybercriminal issues.
This focus of cyber security initiated the Commission's ***proposal for an information and network security strategy*** in 2001,[7] this is the first document representing an identifiable cyber security policy in the European Union. The document is a milestone in the cybersecurity policy, because it contained a detailed topology of cyber threats, recommended specific technical measures to improve security, defined the network and information systems (this definition was used until 2013), and highlighted the need for reliable warning and information sharing system across Europe.

## The facilitating role 2002— 2006

The 2001 Proposal laid out the economic dominance of cybersecurity, and highlighted the importance of criminal justice. As a result, two new agencies were established to carry out the policy operations. Within the Europol[8] a new department was established in 2002, called ***"high-tech crime" centre*** (HTCC). The dedicated aim of this centre was tackling computer related criminal activities and online child exploitation, and serve as an intelligence hub for the EU. In this period ***ENISA*** began its operations in 2004 on Heraklion on the island of Crete[9] as a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. The Agency:

- assists the Member States in implementing relevant EU legislation,
- works to improve the resilience of EU's critical information infrastructure and networks,
- supports the development of cross-border communities,
- collates information necessary for risk analysis,
- develops joint methods to prevent security problems whilst following the development of security standards,
- creates its own recommendations, and
- acts as a counsellor for the European Commission.

[6] This viewpoint was also represented in the Petersberg Tasks of 1992, which specified, that any military action under an EU banner would be restricted to peace-making, peacekeeping and rescue. In that day this restriction seemed logical and acceptable, however, this attitude limited the EU from developing a holistic approach of cybersecurity including offensive cyber-attack capabilities.
[7] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach /* COM/2001/0298 final */
[8] The organisation responsible for coordinating Member States' police forces with the goal to combat international crime, terrorism, drug and human trafficking. It became operational in 1999.
[9] The European Network and Information Security Agency was established following a regulation passed on 10 March 2004 by the European Parliament and the Council (460/2004/EC). This was modified in 2008 and again in 2011. In 2013, the new basic regulation of 526/2013 references the agency as European Union Agency for Network and Information Security (ENISA).

During this period ***EU started to shape its role*** in the cyber domain ***by becoming a facilitator*** rather than a policy leader. It was visible from the language the EU documents used. For example, the Member States instead of being *instructed* to do something, in the new documents they were *encouraged* or *invited* to take certain actions. Above all, detailed technological measures and best practices disappeared from the *acquis*. With the publication of the Strategy for a Secure Information Society[10], this new role was made official.

**The awakening 2007— mid-2016**

Due to the complexity, influence, and the high level of risks these major cyber-attacks beginning with those targeted at Estonia in 2007 caused, the Union interest in cybersecurity significantly transformed. As the consequence between 2007 and 2013, ***73 of the total 143 legal documents accepted relates to cybersecurity in some extent***. The attacks against Estonia were considered as a threat to the internal market, hence EU was able to initiate legislation and undertake the fortification of digital security measures.[11]
The European Union started cybersecurity regulations in the area of ***critical infrastructure protection*** in March 2009.[12] The CIIP action plan was based on five pillars:

1. preparedness and prevention,
2. detection and response,
3. mitigation and recovery,
4. international cooperation and
5. criteria for European Critical Infrastructures in the field of ICT.

The Commission decided to follow the CIIP plan, and [13]strengthen its intention to build a ***coherent approach to cybersecurity***, although it put the ***national interests and practices into the first place***. In the same year, the Council of the European Union highlighted the need for the development of resilient and secure ICT systems and the necessity to upgrade Europe's ***technical competences***. Two Ministerial Conferences were held (Tallinn, 2009 and Balatonfüred, 2011) which led to the adoption of the European Parliament Resolution on Critical Information Infrastructure Protection,[14] the establishment of the European Forum for Member States and of the European Public-Private Partnership for Resilience; two pan-European exercise (Cyber Europe 2010 and 2012); policy recommendation by ENISA

[10] Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" {SEC(2006) 656} /* COM/2006/0251 final */
[11] As Deward (2017:171) argues: "Economic threats are issues where the EU can act. Direct threats to national security, by contrast, are sectors where Union action is severely restricted… It needed to address, or at least acknowledge, the threat of state-sponsored aggression against national communications infrastructures and the potential impact of such incidents on the EU's financial and economic viability."
[12] Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe From Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience" {Sec(2009) 399} {Sec(2009) 400}
[13] European Commission, Brussels, 31.3.2011 COM(2011) 163 final
[14] European Parliament resolution of 12 June 2012 on critical information infrastructure protection – achievements and next steps: towards global cyber-security (2011/2284(INI))

on a minimum set of baseline capabilities and services; and recommendations on the functioning of national CERTs (Computer Emergency Response Teams).[15]

As Deward (2017:181) points out, as a response for ***2008's financial crisis***: "certain industrial sectors were identified where stimuli would be established to increase economic growth and employment. In a move of striking similarity to that of 1985, the digital domain was specifically earmarked for attention. As a result, a ***"Digital Agenda for Europe"*** was initiated. This was a programme intended to increase uptake of digital technology in all sectors of society – political, social and economic – and transform the EU into a knowledge-based economy." The ***Treaty of Lisbon***, which entered into force in 2009[16] codified the effects of the Estonian cyber-attacks and the financial crisis. The Treaty's core was, to improve the coherence and effectiveness of the policy-making, and policy implementing structure, with the abolition of the pillar structure, and the codification of the exclusive, shared and supporting competences of the Union. In the fields of foreign affairs and security, the role of the High Representative of the Union for Foreign Affairs and Security Policy was extended. The High Representative was to be assisted in the fulfilment of the Common Foreign and Security Policy (CFSP) and the Common Security and Defence Policy (CSDP), by the new European External Action Service (EEAS) and the European Defence Agency (EDA).
The Lisbon Treaty shows the importance of cybersecurity, by specifically mentioning (Article 69 (b)) as an ***area requiring cooperation*** to support the stability of the internal market. Thanks to the abolition of the pillar structure a more holistic approach to cybersecurity became possible. Activities related to policies and jurisdiction of cyber-crime where joined up, thus the Commission gained the ability to officially support the ***Europol EC3*** (previously established high-tech centre which later transformed to the European Cybercrime Centre) and supervise the implementation of cyber-crime related regulations.
The policy-making and changing processes started in the beginning of 2007, strengthened by the Lisbon Treaty culminated in the development of the ***European Union Cyber Security Strategy*** (EUCSS) -following a long controversial negotiation process[17]-, published in 2013[18]. The vision of the EUCSS was, to build a resilient cybersecurity to maintain the global status quo, and in the same time being adaptive to new challenges. The strategy emphasises the unity of public authorities and the private sector, and the development of cyber capacities, resources and efficiency (Kovács 2018).
To achieve this goal EU level prevention, detection and management system was needed. The following actions were taken:

- ENISA's task to fortify European cyber resilience by
  - establishing minimum requirements and
  - creation of ***CERT network***

[15] For more information on CIIP policy, read: https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip
[16] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, (2007/C 306/01)
[17] The proposal for the strategy was published in two parts from 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 has later become known as a package for the NIS Directive.
[18] EU cybersecurity strategy: an open, safe and secure cyberspace - European Parliament resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP))

- the Member States adopted national cybersecurity strategies
- Launch of the ***European Cyber Security Month*** (ECSM) series in 2013
- Establishment of the ***Safer Internet Programme*** (SIP),
- Initial cybersecurity training started for public servants.

Finally, the EUCSS calls for an ***international policy,*** the 46th point reads "there is no need at present for the creation of new legal instruments at international level; welcomes, however, international cooperation to develop norms of behaviour for cyberspace, supporting the rule of law in cyberspace; considers that the updating of existing legal instruments to reflect advancements in technology should be considered and holds the view that jurisdictional issues require a thorough discussion on the subject of judicial cooperation and prosecution in transnational criminal cases." This objective includes the EUs intention to make cyberspace issues the part of its CFSP.
Although the multitude of adopted regulation during this period, the modus operandi of the EU in cyberspace remained the same: high-level information sharing and political cooperation platform. As Swilinski (2014:13) reasons "behind this state of affairs is the lack of a truly pan-European vision of the role of the EU as an agent of cyber-security on the part of particular member states as well as the whole institution. What limits the European Union most in cyber-security is its inter-governmental character and the corresponding lack of collective vision on the part of member states." But this role was about to change. How?

**Repositioning EU in the cyber sector mid2016—nowadays**

On the 6th of July 2016 the first piece of EU-wide cyber legislation was adopted by the Parliament. The proposal on the ***Directive on security of network and information systems*** (NIS Directive)[19] was introduced. Yet three more years were needed to finalise the document, and further shape EU's role in the cyberspace. The NIS Directive set up a new legal and institutional framework to boost the overall level of cybersecurity in the EU. It includes the following criterions:

- The Member States are required to appoint a national NIS authority and a CERT (or Computer Security Incident Response Team -CSIRT)
- Setting up an information exchange network between the Member States, and the network of national CSIRTs, to promote swift and effective operational cooperation
- Building a culture of security across every sector which are vital for the economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure
    - Businesses in these sectors that are identified by the Member States as operators of essential services (OES) will have to take appropriate security measures and to notify serious incidents to the relevant national authority.
    - Key digital service providers (DSPs -search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

[19] 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

The NIS Directive is a cornerstone of the EU's response to the growing cyber threats and challenges which accompany the digitalisation of the economic and societal life. To support the implementation of the NIS Directive, the Commission released a Communication[20] which urged the Member States to harmonise their national legislations and policy with the NIS Directive as quickly as possible[21].

During 2016 other significant communications were released, like: launch of public-private partnership on cybersecurity, strengthening cyber resilience system and innovative cyber-security industry.[22] Furthermore, the Commission announced that it would bring forward the evaluation and review of Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning ENISA and repealing Regulation (EC) No 460/2004 ("ENISA Regulation"). The goal of the evaluation is the reform of the ENISA by enhancing its capabilities and capacities to support Member States, and strengthening its central, operational role in the cyber field.

According to the NIS Directive a cooperation group ("***NIS Cooperation Group***") has been established, to promote cooperation and exchange of information. The Cooperation Group is supported by the work of the network of Computer Security Incident Response Teams (***the CSIRT s Network***). Its' members are the representatives of the Member States, the Commission and the ENISA.

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". The Commission and the EU High Representative proposed a reform package, which envisions EU's new, leading position in the cyberspace.[23]The ***reform package*** includes the following six proposal as shown in Fig. 1.

- Establishing a stronger ***European Union Cybersecurity Agency*** built on the Agency for Network and Information Security (ENISA), to assist Member States in dealing with cyber-attacks. (Proposal of the ***Cybersecurity Act***)
- Creating an EU-wide ***cybersecurity certification scheme*** that will increase the cybersecurity of products and services in the digital world.
- A Blueprint for how to respond quickly, operationally and in unison when a large-scale cyber-attack strikes.
- A network of competence centres in the Member States and a ***European Cybersecurity Research and Competence Centre*** that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.

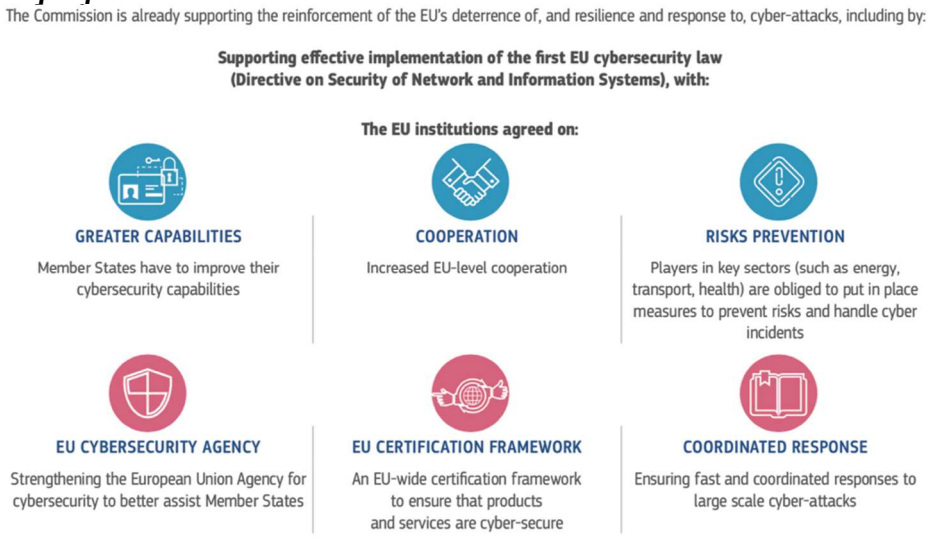
[20] Communication from The Commission to The European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. COM/2017/0476 final

[21] Although the NIS Directive should have been implemented by May 9th 2018 in every Member State, most of them failed to succeed by the given deadline.

[22] Commission Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM/2016/0410 final. -15 November 2016.

[23] Joint Communication to The European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN/2017/0450 final

- A Framework for a ***Joint EU Diplomatic Response to Malicious Cyber Activities*** and measures to strengthen international cooperation on cybersecurity, including deepening of the cooperation between the EU and NATO.
- Skills development for civilian and military professionals through providing solutions for national efforts and the set-up of a ***cyber defence training and education platform.***




**1. Figure The cybersecurity reform package recommendations (source EU Commission)**

The European Economic and Social Committee stated the following in its opinion on the "Cybersecurity Act": "So far, ***no legal framework has been able to cope with the pace of digital innovation,*** and a number of legal texts are contributing item by item to establishing an appropriate framework: the revision of the Telecoms Code, the GDPR, the NIS Directive, the e-IDAS Regulation, the EU-US Privacy Shield, the Directive on non-cash payment frauds, and so on." This means that ***the reform package 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." (Kovács (2018)

Obviously, the Union's previous vision on its role in the cyber field as an information sharing platform, and the perception of cyber and ICT development in general as an economic issue failed. In order to reach the full spectrum of cybersecurity the Union has to adopt several new regulations, and it has to scrutinise the implementation in every Member State. The EU took a major step towards stabilisation of its new role on the 10th December 2018, when the European Parliament, the Council of the European Union, and the European Commission have reached a political agreement on the "Cybersecurity Act" [24]. ENISA's new Regulation requires a formal approval by the European Parliament and the Council of the European Union. The approval is expected in the following weeks, and after its publication in the EU Official Journal, the "Cybersecurity Act" will immediately enter into force.

The Act will replace ENISA's limited mandate to a permanent mandate and provides more resources to the agency. It establishes an EU framework for cybersecurity certification,

[24] Agreement on the „Cybersecurity Act" – European Commission Press release http://europa.eu/rapid/press-release_IP-18-6759_en.htm

boosting the cybersecurity of online services and consumer devices. This new approach is clearly a paradigm shift towards a more centralised policy-making and governance. (Bendiek 2017a)

## Cooperation with the Member States

In the previous part of this paper we examined how EU's viewpoint on cybersecurity policy changed through the past few decades. In this part, we will examine the cooperation between centralised EU level and the Member States.

The Treaty of Lisbon specifically mentions the area of cybersecurity whereas cooperation between EU and Member States is needed. Though the EU's explicit goal is, to strengthen its cyber-power, the perception on cybersecurity remains economic and not security based as it should be. It is generally accepted, that cybersecurity is a multilateral field, therefore the origin of the policy initiation is irrespective, until it promotes resilience and high level of preparedness. EU's main focus in the coherent cybersecurity policy is directed to cybercrime, critical information infrastructure protection and cyber defence. Regarding to the security approach institutional cooperation and mutual understanding of security are the most important "pillars". Institutional co-operation is understood as being particularly important given that ***the European governance of cybersecurity is rather decentralized***, with relevant bodies to be found in the public and private sectors and national and international levels.

As Carrapico & Barrinha (2017:1264) highlights: "***There are co-ordination problems*** between, but also within institutions, which are related to the historical evolution of the different cybersecurity areas, as well as the perception that each area still experiences different separate challenges. It is not unusual to find projects whose objectives clash with those of other institutions. Furthermore, states, via the Council, seem to be more reluctant than other institutions (such as the European Parliament) to enhance EU powers in this area…as a consequence, ***the allocated resources are often extremely low when compared with other security areas and other parts of the world***."

The following table summarize the EU institutions currently appointed to certain particular cybersecurity related tasks:

**1. Table: EU institutions dealing with cybersecurity issues**

| Organisation | Missions, tasks |
|---|---|
| ENISA | Issues of cybersecurity, cybercrime, network and information security |
| DG HOME | Development of policies, trainings and fostering cross border investigations in the area of organised cybercrime, encryption. |
| Europol EC3 | Central hub for criminal information and intelligence; supports operations and investigations, provides highly specialised technical and digital forensic capabilities, and offers strategic analysis and training.<br>Focuses on: cyber-dependent crime; online child sexual exploitation; payment fraud |
| CERT-EU | The team is made up of IT security experts from the main EU Institutions (European Commission, General Secretariat of the Council, European Parliament, Committee of the Regions, Economic and Social Committee). It cooperates closely with other CERTs in the Member States and beyond as well as with specialised IT security companies. |
| EU INTCEN (Intelligence and Situation Centre) | Cybercrime, cyber defence - providing intelligence analysis, early warning and situational awareness to the High Representative and to the European External Action Service |
| eu-LISA (European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice) | The Agency is currently managing Eurodac, the second-generation Schengen Information System (SIS II) and the Visa Information System (VIS). The agency's core mission is to be dedicated to continuously add value to Member States, supporting through technology their efforts for a safer Europe. |
| ECSO<br>(the European Cyber Security Organisation)<br>A self-financed non-for-profit organisation under the Belgian law, established in June 2016. | Collaborate with the Commission to promote (R&I) in cybersecurity; foster market development and investments.<br>Support the widest and best market uptake of innovative cybersecurity technologies and services<br>Promote and assist in the definition and implementation of a European cybersecurity industrial policy and support the development and the interests of the entire cybersecurity and ICT security ecosystem. |
| EDA (the EU Defence Agency) | Supporting the development of defence capabilities and military cooperation among the European Union Member States; stimulating defence R&T and strengthening the European defence industry; acting as a military interface to EU policies. |

The ***adequate level of cooperation between national and EU level is hard to determine***. Although mandatory institutional regulations have been set up by the NIS Directive, cybersecurity in many countries still considered a sensitive issue, where sharing of information does not come naturally. Meanwhile some Member States (like France, the Netherlands and Germany) promote deeper cooperation throughout the EU, others foster cooperation on a

more regional, sub-regional level.[25] Furthermore, all EU Member States differ in their institutional systems, political preferences, cybersecurity governance models and ideologies and cyber-defence capabilities.

The Member States must establish and provide for (financial, technical, human resources) the national institutions determined by the NIS Directive. These are the:

- Competent Authority (CA): Every Member State appoint one at least, with the role to monitor the application of the Directive at a national level. The CA is to be notified in case of an incident.[26]
- Single Point of Contact (SPC): This institution exercises a liaison function to ensure cross-border cooperation. (in case of an incident, SPC is responsible to notify the other affected Member States)
- CSIRT: Institution which reside inside the CA, responsible for monitoring incidents, providing early threat warnings, responding to incidents, and cooperating with the private sector. Concrete tasks of CSIRTs have to be clearly defined and supported by national policy.

Despite the centralisation efforts, and EU's vision, that cybersecurity is a complex and transnational issue, where cooperation is crucial, the ***policy remains mostly an exclusive national prerogative*** (Renard 2014:13). Carrapico & Barrinha (2017:1266) summarises the EU and Member State level cooperation on cybersecurity with the following remarks: "Brussels often has difficulty convincing Member States of the importance of furthering integration in this area, often resorting to projects 'á la carte' where national participation is voluntary as is the case of EDA projects. The problem, however, does not stem only from the national level. The NIS Directive is a specific example which could lead to co-ordination problems and a lack of coherence, particularly regarding the division between network information infrastructure bodies and law enforcement ones, as EC3 plays a very limited role in the directive."

## CONCLUSIONS

Cybersecurity is an activity, ability or capability to protect information and communications systems and the data/information contained therein. Based on this paper, in contrary with nation-states where cybersecurity is a crucial part of the national security policy, for the European Union, cybersecurity has always had an economic perception as the part of the digital single market. Cyber-related questions arise in the Common Foreign and Security Policy as well in the Common Security and Defence Policy – main areas of action are: cybercrime, critical information infrastructure protection and cyber defence

The cyber domain is a multilateral field where institutional cooperation and mutual understanding of security are the most important "pillars". Institutional co-operation is understood as being vital given that the European governance of cybersecurity is rather decentralized, with relevant bodies to be found in the public and private sectors and national and international levels.

[25] As an example the Visegrad Group + Austria founded the Central European Cyber Security Platform in 2013 to promote the cooperation and sharing of information between their CERTs/CSIRTs

[26] Article 8, par. 6 NIS-Directive.

There are several bodies and agencies in the EU at the central level, national bodies and organisations at every Member State and transnational, international organisations at the global level.
The new "Europe of security" concept is clearly a conflicting idea with the vision of multilateralism. The cybersecurity reform package proposals prefer civilian police and military defensive instruments to protect information technology infrastructures, it fosters the secure development of digital market and supports the interoperability of systems, procedures, technologies. Though, the proposals package and especially the Cybersecurity Act was accepted by the main EU bodies, the effectiveness of this reform requires a deeper engagement from the Member States. The Union as a whole, can be conceptualised as an emerging soft power in cybersecurity, underpinned with the aim to secure cyberspace through development of resilience and preparedness for large-scale cyber-attacks. Hence, it is still a question whether the Member States are willing to engage, and if yes to what extent in the new cybersecurity ecosystem. That is why the greatest challenge is the trusting relationship between all participants.

## BIBLIOGRAPHY

Bendiek, A. (2017a) *A Paradigm Shift in the EU's Common Foreign and Security Policy: From Transformation to Resilience*. SWP Research Paper 2017/RP 11, October, p. 1-30

Bendiek, A. Bossong, R. and Schulze M. (2017b) *The EU's Revised Cybersecurity Strategy, Half-Hearted Progress on Far-Reaching Challenges.* SWP Comments 47, November, p. 1-7

Carrapico, H., Barrinha, A. (2017) *The EU as a Coherent (Cyber)Security Actor?* Journal of Common Market Studies 2017 Vol. 55., No. 6. p. 1254–1272.

Cavelty, M. D. (2018) *Europe's cyber-power*. European Politics And Society, Vol. 19, No. 3, p. 304–320

Christou, G. (2017) *The EU's Approach to Cybersecurity*. University of Essex Online paper series, Spring/Summer 2017

Dewar, R. S. (2017) The European Union and Cybersecurity: A Historiography of an Emerging Actor's Response to a Global Security Concern. In: O'Neill, M. Swinton, K. Eds*.: Challenges and Critiques of the EU Internal Security Strategy*. Cambridge Scholars Publishing, p. 113 - 148

Feliks Sliwinski, K. (2014): *Moving beyond the European Union's Weakness as a Cyber-Security Agent*, Contemporary Security Policy, p. 1-19.

Klimburg, A., Tiirmaa-Klaar, H. (2011) '*Cyber war and Cyber security: challenges faced by the EU and its Member States*', DG for External Policies, Policy Department, European Parliament, April.

Kovács L. (2018) *Cyber security policy and strategy in the European Union and NATO*. Land Forces Academy Review Vol. XXIII, No 1(89)

Molnár D. (2017) *Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése*. Hadmérnök. vol. 12, no. 1, p. 255-267.

Renard, T. (2014) '*The Rise of Cyber-Diplomacy: The EU, Its Strategic Partners and Cyber- Security*', ESPO Working Paper No. 7, European Strategic Partnership Observatory.

Sliwinski, Krzysztof Feliks (2014): *Moving beyond the European Union's Weakness as a Cyber-Security Agent*, Contemporary Security Policy