IPS Instituto Politécnico de Setúbal

# Cybersecurity in the EU

Bernardo Augusto - 2814

Miguel Cisneiros - 2674

Professor: COL João Barbas

Curricular Unit: Ethics and Information Security

Barreiro School of Technology – Polytechnic Institute of Setúbal

# Index



# Acronyms and Abbreviations

CERT-EU – Computer Emergency Response Team

EC3 – Europol's European Cybercrime Center

EC – European Commission

ENISA – European Union Agency for Cybersecurity

EU – European Union

ICT – Information and Communication Technologies

# Introduction

Technology is indissociable from life at the 21st century. Individuals, organizations, and states currently depend on it at such level that any failed access to information can result in catastrophic consequences. Cybersecurity incidents, be they intentional or accidental, could disrupt the supply of essential services we take for granted such as water or electricity. Therefore, is necessary to assure safety from attacks to these systems.

This is an important issue to European Union (EU) citizens as 86% of them now believe the risk of falling victim to cybercrime is increasing.

Since the Budapest Convention back in 2001, the EU has used policy, legislation and spending to improve its cyber resilience. Yet, the transposition from European Directives on Cybersecurity only started in 2013, two years after the implementation of National Cybersecurity Strategies by the UK, France, Germany, and several other countries. This inconsistent transposition of EU law among Member States can result in legal and operational incoherence and prevents legislation from reaching its full potential.

With the Treaty of Lisbon, EU's powers were reinforced. Yet, Cybersecurity threats stretch across national and EU borders and impact not only security and stability but also prosperity and democratic order, hence threatening European Values.

In this work we will explore the issues of Cybersecurity in the EU by presenting an overview of the EU's cybersecurity institutions and their roles, overview some of the cybersecurity policies carried by the EU and compiling the present and future challenges of EU's cybersecurity.

# EU's main Cybersecurity institutions and roles

There are many players in the EU's Cybersecurity axis, as seen below in the *EU Cybersecurity Institutional Map* (Figure 1). These various institutions intertwine with each other in their roles and actions specially in the legislative and judiciary levels of the EU.

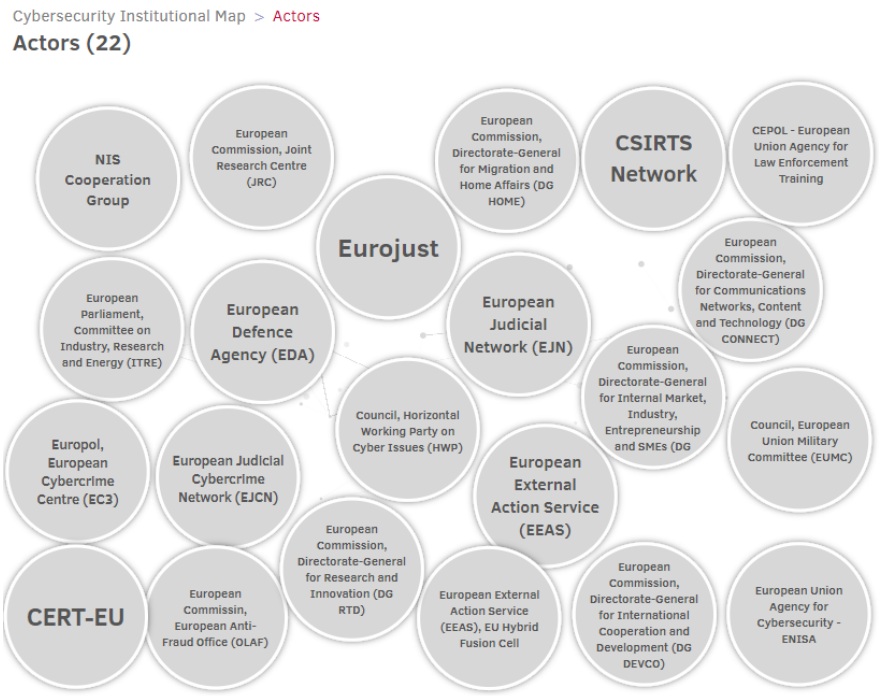


*Figure 1 - EU's Cybersecurity Institutions*

However, there are three institutions that standout:

- European Union Agency for Cybersecurity - ENISA
- Computer Emergency Response Team - CERT-EU
- Europol's European Cybercrime Center – EC3

The European Union Agency for Cybersecurity (ENISA) was founded in 2004 by the Regulation (EC) No 460/2004 of the European Parliament and of the Council and has offices established in Athens and Heraklion (Greece). The annual budget for this agency is around 11 million euros. ENISA's strategic objectives are the following:

- **Expertise** - Anticipate and support Europe in facing emerging network and information security challenges, by collating, analyzing, and making available information and expertise on key NIS issues potentially impacting the EU, taking into account the evolutions of the digital environment.

- **Policy** - Promote network and information security as an EU policy priority, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS.
- **Capacity** - Support Europe maintaining state-of-the-art network and information security capacities, by assisting the Member States and European Union bodies in reinforcing their NIS capacities.
- **Community** - Foster the emerging European network and information security community, by reinforcing cooperation at EU level among Member States, European Union bodies and relevant NIS stakeholders, including the private sector.
- **Enabling** - Reinforce ENISA's impact, by improving the management of its resources and engaging more efficiently with its stakeholders, including Member States and Union Institutions, as well as at international level.

The Computer Emergency Response Team for the EU institutions, bodies, and agencies (CERT-EU) was permanently established in 2012 after a one-year pilot phase. CERT-EU runs on an annual budget of about 2.5 million euros.

It is the first responder in any information security incident that concerns several institutions yet does not operate on a 24/7 basis. Its team is composed by 30 IT security experts coming from across Europe who work closely with EU national/governmental CERTs, the internal IT security teams of the different constituents, industry partners and entities like NATO and ENISA.

CERT-EU's mission is to contribute to the security of the Information and Communication Technologies (ICT) infrastructure of all Union institutions, bodies and agencies by helping to prevent, detect, mitigate and respond to cyber-attacks and by acting as the cyber-security information exchange and incident response coordination hub for the constituents. The scope of CERT-EU's activities covers prevention, detection, response, and recovery. It also provides EU institutions, bodies and agencies with reports and briefings regarding cyber threats targeted at them.

At last, the European Cybercrime Center (EC3) was established in 2013 by Europol with an initial budget of 7 million euros to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. It is currently headquartered in the Netherlands.

EC3 is focused on cybercrimes as cyber-dependent crime, online child sexual exploitation and payment fraud.

This center has established a series of advisory groups with private sector operators, EU institutions and agencies, and other international organizations to improve collaboration through

networking, strategic intelligence-sharing, and cooperation. Some of EC3's mission objectives include:

- serving as the central hub for criminal information and intelligence.
- supporting operations and investigations by Member States by offering operational analysis, coordination, and its considerable expertise.
- providing a variety of strategic-analysis products that enable informed decision-making at the tactical and strategic levels on combating and preventing cybercrime.
- providing a comprehensive outreach function connecting law-enforcement authorities tackling cybercrime with the private sector, academia, and other non-law enforcement partners.
- supporting training and capacity-building, for the relevant authorities in Member States.
- providing highly specialized technical and digital forensic support capabilities to investigations and operations.
- representing the EU law-enforcement community in areas of common interest (research-and-development requirements, internet governance and policy development).

# Cybersecurity policies carried by the EU

The 2013 *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* was a game-changer by proposing measures to improve the Union's performance through a joint intervention of European institutions, Member States, and industry. This strategy had five core objectives: increase cyber resilience, reduce cybercrime, develop cyber defense policies and capacities, promote the development of industrial and technological cybersecurity resources, and establish an international cyberspace policy aligned with core EU values.

This strategy was accompanied by a proposal for a Network and Information Security (NIS) Directive, namely measures for a high common level of security of network and information systems across the Union. This Directive was later adopted in 2016 and became the first piece of EU-wide legislation on cybersecurity. Member States had 21 months to transpose the NIS Directive into their national laws and an additional period of 6 months to identify operators of essential services.

The 2013 Cybersecurity Strategy connects with three subsequently adopted strategies:

- The European Agenda on Security's (2015): improving the law enforcement and the judicial response to cybercrime, mainly by renewing updating existing policies and legislation.
- The Digital Single Market Strategy (2015): creating better access to digital goods and services by creating the right conditions in which to maximize the digital economy's growth potential.
- The European Union Global Strategy (2016) aims to boost the EU's role in the world. It replaces the European Security Strategy of 2003. Cybersecurity forms a core pillar through a renewed commitment to cyber issues, cooperation with key partners, and a resolve to address cyber issues across all policy areas, including the rebuttal of disinformation through strategic communication.

A Cyber Defense Policy Framework was adopted in 2014 and updated in 2018. The 2018 updates identified six priorities, including the development of cyber defense capabilities and the protection of the EU Common Security and Defense Policy (CSDP) communication and information networks.

In 2017 the European Commission presented a new cybersecurity package more known as EU's Cybersecurity Act. This package revamps and strengthens the ENISA, establishes an EU-wide cybersecurity certification framework for digital products, services and processes and complements the NIS Directive.

In the context of the SARS-CoV-2 pandemic, the European Commission issued the *Europe's moment: Repair and Prepare for the Next Generation* communication (May 27th 2020) where it proposes a new Cybersecurity Strategy to boost EU-level cooperation, knowledge, and capacity.

## Present and future challenges of EU's Cybersecurity

The process of digitalization turns European societies and economies more efficient. Over the last few years, the Internet has reshaped the structure and functioning of a lot of sectors like media, energy sector, finance, agriculture, etc. Technologies can bring plenty of opportunities and advantages. However, this dependency on automation and exponential growth of digitalization in our lives bring new challenges and vulnerabilities to every entity. In the present, this dependency on automation and exponential growth of digitalization open new doors for cyber-attacks. Cyber-attacks have become one of the main concerns in terms of security for the EU and its member states, which confirm the danger of technologies and the digitalization process in all sectors. And according to the EU's cybersecurity factsheet, published in 2018, cyber incidents and attacks are reportedly on the rise.

Since 2016, the number of daily ransomware (a type of malicious software designed to block access to a computer system until a sum of money is paid) has surpassed 4000 and this number has increased by 300% since 2015. As the European Commission President Jean-Claude Juncker highlighted "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks […] Cyber-attacks know no borders, and no one is immune". For this reason, the EU and member states have been vigorous in terms of the responses to the cybersecurity challenges. They have created numerous EU bodies and agencies, adopted new frameworks and other initiatives. For example, soon, the EU plans to establish the Network of National Coordination Centers (NCC), a Cybersecurity Competence Community, and a European Cybersecurity Industrial, Technology, and Research Competence Center (Dominika Giantas, 2019).

Some of the EU member states have defined the cooperation at the European Union level to reach greater cybersecurity. The best example is Spain. One of the six objectives of its national cybersecurity strategy is "to contribute to improving cybersecurity, supporting the development of coordinated cybersecurity policy in the EU and international organizations, and to collaborate in the capacity building of States that so require through the development cooperation policy". It is also spotlighted that "the Cyber Security Policy will be aligned with the initiatives similar to those of the countries in our neighborhood and with the European and International organizations with responsibilities in this area, particularly in the EU Cyber Security Strategy".

As we saw in this section the concern of the EU in the cybersecurity field is growing. The EU and its member states still have a big number of future challenges in this area but they are going on a

good path with the creation of new initiatives and institutions to protect this new assent that is present everywhere nowadays.

# Conclusion

Nowadays, Cybersecurity is one of the most important assents for the population, organizations, and states. The grown of the digital world has been exponential. Our lives are now inseparable from the cyberspace and technologies. Technology is everywhere. It is on economies, medicine, and national security. Data moves the world. With the evolution of technology, there is also a continuous growth of opportunities and challenges.

As the European Commission former President Jean-Claude Juncker highlighted "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks […] Cyber-attacks know no borders, and no one is immune". The EU is not immune to these threats and becomes a new focal point for cybercrime, industrial espionage, and cyberattacks. The EU has large security gaps and because of that, the EU has been the target of many cyber incidents. For this reason, the need for solutions is colossal.

As referred on this research work, some policies and institutions were created to counter cybercrime. This resulted in a good improvement over the years and EU's cyberspace is becoming a safer place every day.

# References

(2019, March). Challenges to effective EU cybersecurity policy, p. 74.

Barbas, J., & Sancho, C. (2018). Cibersegurança e Políticas Públicas: Análise comparada dos casos chileno e português. Lisboa: Instituto da Defesa Nacional (IDN).

Carrapiço, H., & Barrinha, A. (2017, May 10). The EU as a Coherent (Cyber)Security Actor? Journal of Common Market Studies, pp. 1254-1272.

CERT-EU. (n.d.). About us. Retrieved from CERT-EU: https://cert.europa.eu/cert/plainedition/en/cert_about.html

Council of the European Union. (2020, March 6). Cybersecurity in Europe: stronger rules and better protection. Retrieved from Council of the European Union: https://www.consilium.europa.eu/en/policies/cybersecurity/

Dominika Giantas, D. A. (2019, September). CyberSecurity in the EU: Threats, Frameworks and future prespectives .

ENISA. (n.d.). About ENISA. Retrieved from ENISA: https://www.enisa.europa.eu/about-enisa

ENISA. (n.d.). Mission and Objectives. Retrieved from ENISA: https://www.enisa.europa.eu/about-enisa/mission-and-objectives

European Commission. (2017, January). Cybersecurity Factsheet.

European Commission. (2020, May 28). Cybersecurity. Retrieved from European Commission: https://ec.europa.eu/digital-single-market/en/cyber-security

European Union Agency For Cybersecurity . (2020, February 10). Retrieved from Do you know who is who in EU cybersecurity?: https://www.enisa.europa.eu/news/enisa-news/do-you-know-who-is-who-in-eu-cybersecurity

European Union Agency for CyberSecurity. (2020). Retrieved from Cybersecurity Institutional Map: https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=actors

Europol. (n.d.). European Cybercrime Centre - EC3. Retrieved from Europol: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Giantas, D., & Liaropoulos, A. (2019). Cybersecurity in the EU: Threats, frameworks and future perspectives.

The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. (2011).

Touhill, G. J. (2014). Cybersecurity for Executives: A practical guide. Wiley-AIChE.