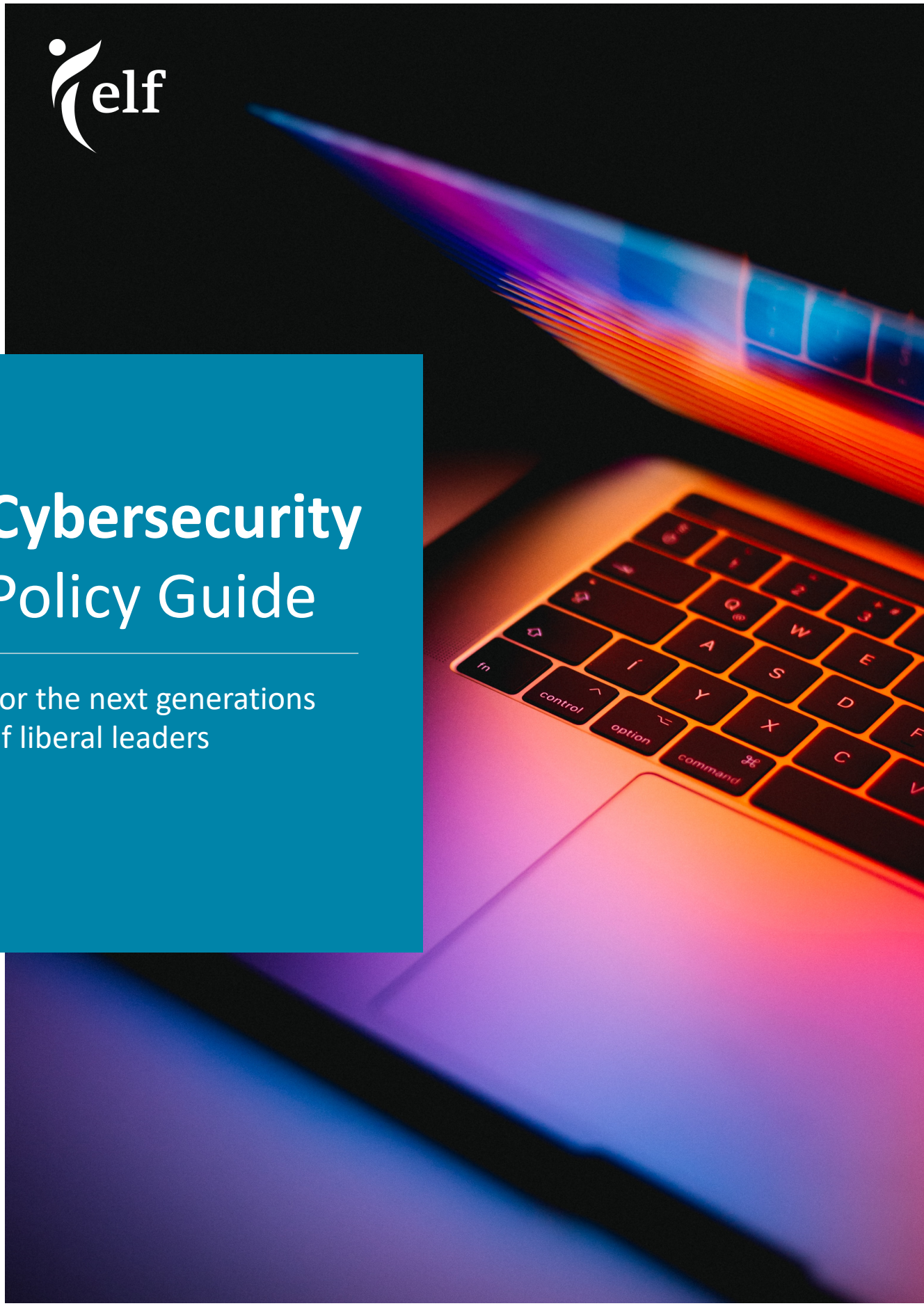
Cybersecurity Policy Guide

For the next generations of liberal leaders



The publishers

The European Liberal Forum (ELF) is the foundation of the European Liberal Democrats, the ALDE Party. ELF consists of several European think tanks, political foundations and institutes and operates as an umbrella organization for them. The foundation issues publications on Liberalism and European public policy issues and offers space for the discussion of European politics. ELF was founded in 2007 to strengthen the liberal and democrat movement in Europe. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European. We bring together a diverse network of national foundations, think tanks and other experts.

The European Liberal Youth (LYMEC) is a pan-European youth organization seeking to promote liberal values throughout the EU as the youth organization of the ALDE Party and its parliamentary group in the European Parliament. LYMEC is made up of Member Organisations and Individual Members and it is active across the breadth and diversity of the European continent. LYMEC's central aim is the creation of a liberal and federal Europe.

Author

Irene Rodríguez Ortega. Degree in International Relations at University Complutense of Madrid, with a Master Degree in International Law from the same University. She is currently working on a PhD within the Political Science and International Relations Programme in co-tutorship with the Faculty of Law at the Complutense University of Madrid. Her research is framed in the field of international security and defence. She has worked in big companies in the area of cybersecurity, currently being responsible for the cybersecurity awareness area in a multinational company. As a researcher and expert in cybersecurity, she has participated in several international congresses, conferences and lectures, has conducted workshops and training courses and has published in different specialized publications and has contributed to monographic books.

May 2020. Published by the European Liberal Forum asbl with the support of the European Liberal Youth (LYMEC). Co-funded by the European Parliament.

Cybersecurity context in a digital world

In recent decades, there has been an unprecedented progress in the digitalisation of society, both in professional and personal spheres. This process has had security consequences that continue to represent a challenge today. In a hyper-connected world where technology has disrupted all areas of our lives, exposure to attacks has increased.

In recent years the trend has continued**, increasing the number, type, and severity of attacks** against public sector information systems, companies, and institutions of strategic interest or those with significant intellectual and industrial property assets and, in general, against all types of entities and citizens.

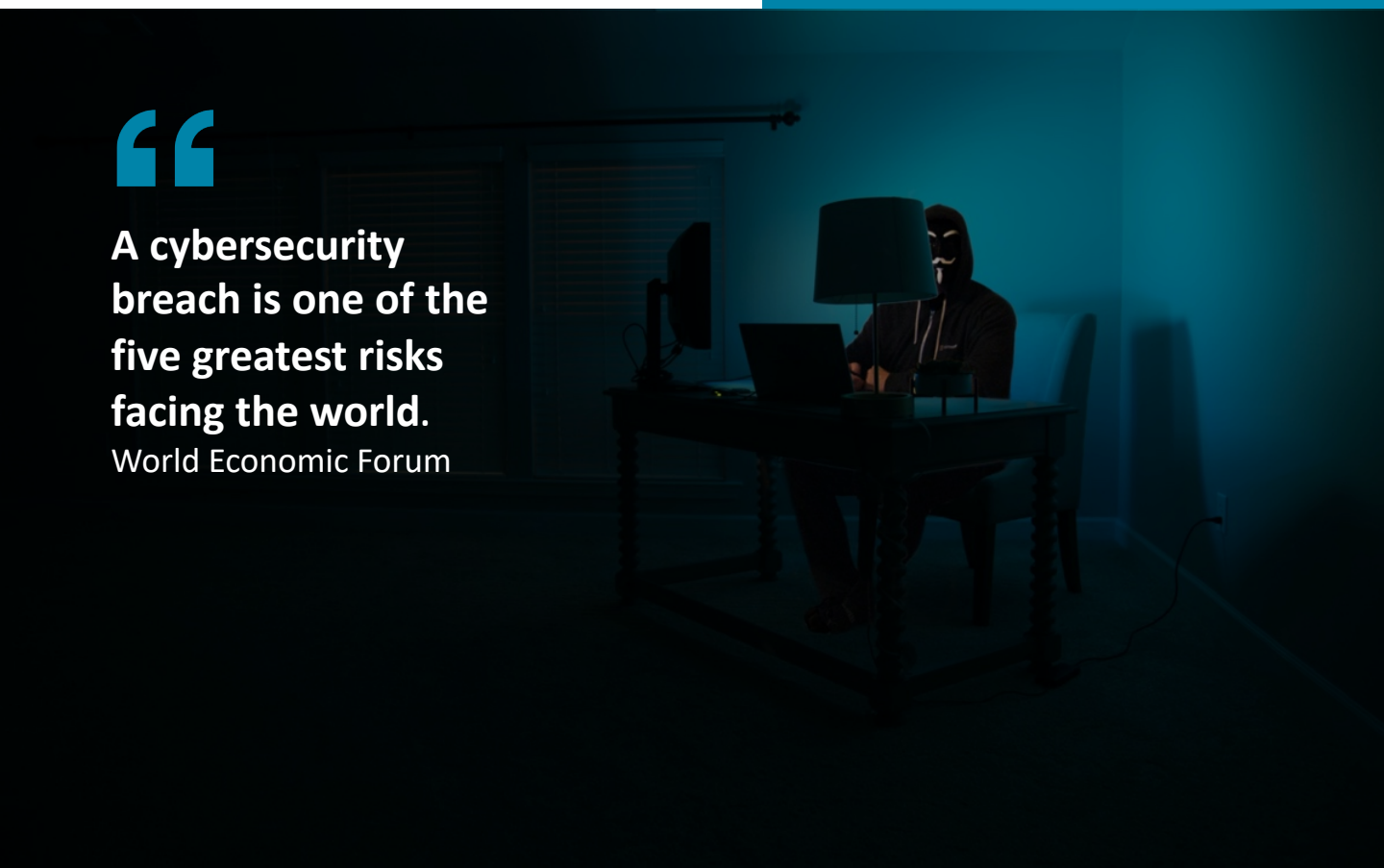
In fact, in recent years, tactics, techniques, and procedures have shown an increasing professionalisation, clearly showing a new type of criminal behaviour, which we could call Cybercrime-as-a-Service. This makes it possible for third parties to develop high-impact cyber-attacks, generally with the aim of obtaining illicit economic benefits.

Worldwide **spending on cybersecurity** is forecasted to reach $133.7 billion in 2022.
Gartner

68 % of business leaders feel their cybersecurity **risks are increasing.**
Varonis

Hackers **attack every 39 seconds**, on average 2,244 times a day.
University of Maryland

Data breaches **exposed 4.1 billion records** in the first half of 2019.
Varonis



A cybersecurity breach is one of the five greatest risks facing the world.
World Economic Forum

Main cyberthreats

In order to develop an efficient security strategy and meet the challenges presented by IT security, it is important to know the main cyberthreats facing institutions and companies.

1 Malware

The concept of malware includes any type of **malicious software that acts with the purpose of compromising the security of systems**. There are many types of malware, the most common being the following:

- Ransomware: Infects the computer by encrypting all files and requesting a rescue in order to recover them.
- Unwanted applications: Such as Adware or Spyware that install additional unwanted software by modifying the home page of browsers or the search provider.
- Trojan: Tricks users by presenting itself as legitimate software while giving at attacker the opportunity to create a back door.
- Botnets: Infected devices may be participating as bots or as Command & Control (C&C) servers in a huge network of infected computers that are involved in conducting DDoS, sending spam, distributing malware, or mining crypto currencies.

92 % of malware is delivered by email.
CSO Online

The average cost of a malware attack on a company is $2.6 million.
Accenture

56 %
of IT decision-makers believe phishing attacks are their top security threat.

32 %
of breaches involved phishing.

2 Phishing

One of the main threats that users, institutions, and companies face daily around the world is phishing. Phishing is a social engineering technique used by cyber criminals to steal confidential information such as passwords, credit card, numbers or bank details. To do this, the cybercriminal impersonates a legitimate person or entity.

Phishing awareness and education are some of the best ways to decrease this risk.

3 Cyber spying

This consists of **cyber attacks sponsored by States** perpetrated by themselves or by other paid actors always with the intention of appropriating sensitive or politically, strategically, security-related or economically valuable information.

71 % of breaches were financially motivated and **25 % were motivated by espionage**.
Verizon

4 Vulnerability exploitation

The objective of cyber attackers is to **nurture vulnerable servers and mobile applications with malicious elements to inject malicious code**. The most common attack is SQL injection and it is often associated with large data breaches around the world.

- SQL Injections: Is a method of infiltrating intrusive code that uses a computer vulnerability present in an application at the input validation level to perform operations on a database.

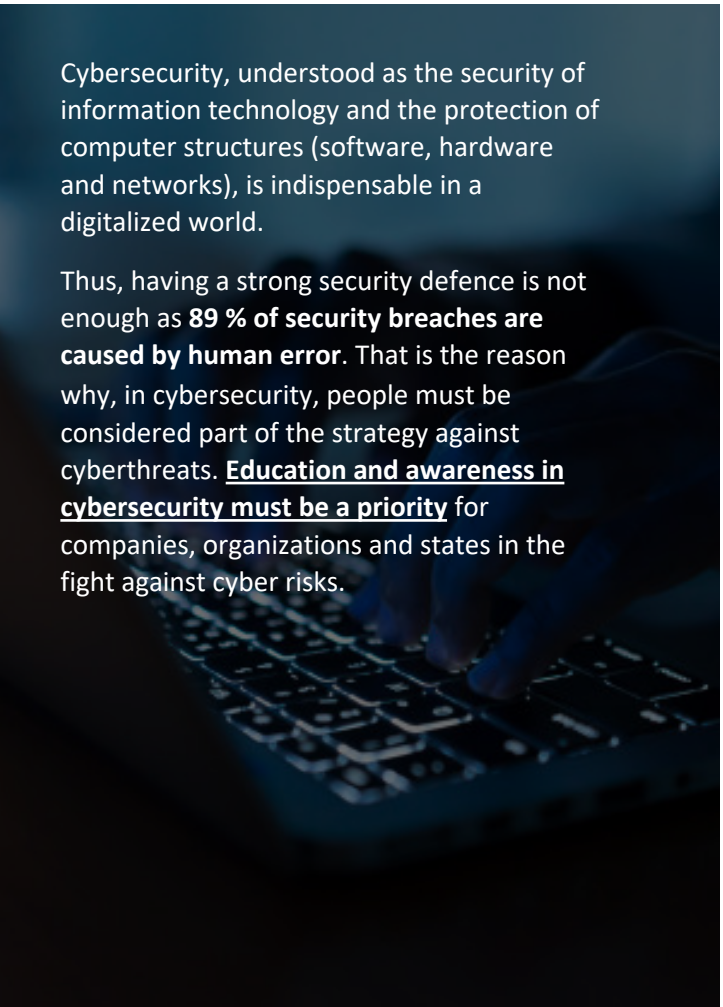
51 % of businesses experienced denial of service attacks in 2018. *Varonis*

As users we must check the configuration of our routers and firewalls to detect invalid or false IP's coming from possible attackers.

5 DoS/DDoS attack

A denial of service attack aims to disable the use of a system, application or machine in order to block the service for which it is intended. Web servers have the ability to resolve a number of user requests or connections simultaneously. This type of attack generates a massive amount of requests to the service with the aim of blocking the service.

There are two techniques for this type of attack: denial of service (DoS) and distributed denial of service (DDoS). The difference between the two is the number of computers or IPs that carry out the attack.



Cybersecurity, understood as the security of information technology and the protection of computer structures (software, hardware and networks), is indispensable in a digitalized world.

Thus, having a strong security defence is not enough as **89 % of security breaches are caused by human error**. That is the reason why, in cybersecurity, people must be considered part of the strategy against cyberthreats. **Education and awareness in cybersecurity must be a priority** for companies, organizations and states in the fight against cyber risks.

Main cyberthreats

As users, **how can we deal with cyberthreats** such as those described previously?

1. Have **antivirus** and **antispyware** software and maintain it regularly updated.
2. Use **strong passwords**, change them periodically and do not write them down or save them in the browser.
3. **Download** files and programs only from **certified websites.**
4. When browsing the Internet, check that the pages use **secure HTTPS** and clear the browser history.
5. Do not click on links in suspicious emails, always **check the sende**r and pass the cursor over the link to verify the legitimacy.
6. Keep your **computer and software updated.**
7. Make regular backups to protect your information.
8. Keep your **social networks private** and be careful not to publish personal information on the Internet.

Cybersecurity policy

Today is more necessary than ever to address the challenges and threats presented by cybersecurity at the international level in order to prevent these incidents and mitigate their impact. Simply "adequate" security is not enough.

Defending against these threats requires an equally sophisticated strategy to provide permanent security for people, processes, and technology.

- Organisations need to strengthen the most basic aspects of security in order to build on a solid foundation and protect themselves against more advanced threats.
- Align information security as part of the risk management framework.
- Define and update security procedures.

Implementing security involves planning for and taking into account the following elements:

- **Risk Analysis**. Study the possible risks and evaluate the consequences of these on the assets. (Information and service).
- **Risk Management.** Evaluate the different protection measures and decide which solutions best suits the entity. (Determination of the residual risk).
- **Governance.** Adapt the entity's usual operations to the security measures.
- **Surveillance.** Continuous observation of the security measures, as well as their adaptation to the appearance of new technologies.
- **Contingency Plans and Resilience.** Determination of the measures to be adopted in the event of a security incident.

Most infections could be prevented or resolved by the establishment of basic IT policies.

The **design of a security strategy** will depend on the context, however, in general, some basic steps can be considered when developing a strategy:

- Create a Security Policy.
- Conduct a Risk Analysis.
- Apply the corresponding safeguards.
- And especially, raise user awareness.

Cybersecurity is increasingly a determining factor in the strategies and agenda of leaders in all sectors. **What are the keys to leadership in a cybersecurity strategy?**

1. Build and practice strong cyber hygiene
2. Protect access to mission-critical assets
3. Protect your email against phishing
4. Apply a zero-trust approach to securing your supply chain
5. Prevent, monitor, and respond to cyber threats
6. Develop and practice comprehensive crisis management plan
7. Build a robust disaster-recovery plan for cyberattacks
8. Create a cybersecurity culture

The role of the EU

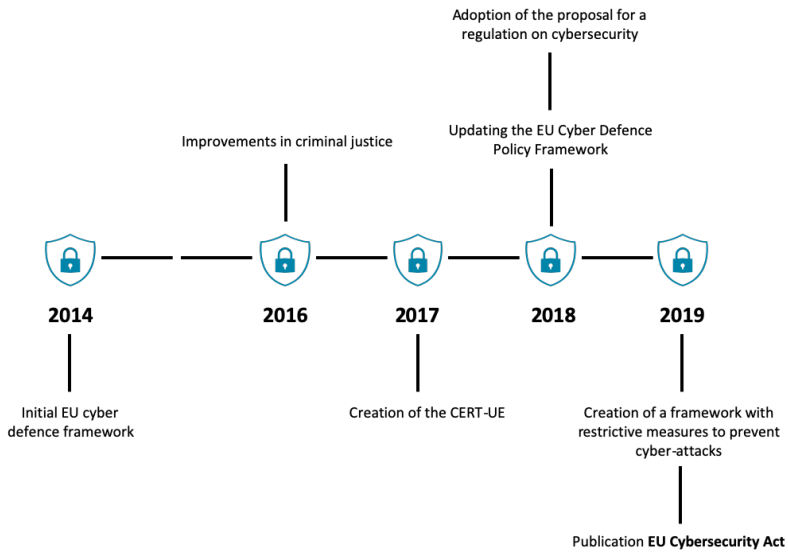
Aware of the cybersecurity challenges for the EU, an initial EU cyber defence framework was created in 2014. In 2017, a plan was launched to provide companies and institutions with the necessary mechanisms for both prevention and rapid response to any incident affecting their computers and the data they store on their servers.

This plan has resulted in the entry into force of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 (Cybersecurity Act), in which the following measures should be highlighted:

- The **creation of a common certification framework at European level**, with the aim of ensuring an adequate level of cybersecurity for ICT products, services and processes in the EU, avoiding the fragmentation of the internal market.
- The **ENISA** (European Agency for Cybersecurity, now renamed the European Union Agency for Cybersecurity) **is to play a more relevant role** in the field of cybersecurity.

According to a Eurobarometer, 87 % of Europeans consider cyber attacks to be a serious challenge to the EU's internal security, and most are concerned about becoming victims of such attacks.

Also in 2019, on May 17, the European Council established **a framework allowing the EU to impose specific restrictive measures** to deter and counteract cyber attacks that represent an external threat to the EU or its Member States, in particular those perpetrated against third States or international organisations.



The EU institutions are also promoting legislation that will establish the European Industrial, Technological and Research Centre for Cybersecurity, supported by a Network of National Coordination Centres.

Pending issues and future challenges include the increase in the number of attacks on critical infrastructures in the EU (electricity, communications, water, etc.), as well as the increase in IoT devices and the mistrust of users towards the security and privacy of their devices.

References

- ENISA, “Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity”, December 2018.
- European Commission, “Joint communication to the European parliament and the council. Resilience, deterrence and defence: Building strong cybersecurity for the UE”, Brussels, 13/9/2017.
- European Council, “Cybersecurity in Europe: stronger rules and better protection”, last reviewed on 6 march 2020. https://www.consilium.europa.eu/en/policies/cybersecurity/
- World Economic Forum, “The Cybersecurity Guide for Leaders in Today’s Digital World”, October 2019.

EUROPEAN LIBERAL YOUTH
LYMEC