16:35

Information and technology law course

LECTURE 3 – 30 SEPTEMBER 2024

FEDERICA CASAROSA – 2024/2025

→ Whenever cyberattacks occurs and we need to regulate we need to think about who we are going to work with
P.A. look at us as consumers or products. Public look at us as citizens.
Public actors want to protect citizens and are accountable for the citizens. They are responsible for their wellbeing.
Private actors are doing something for profit.

Information sharing

The more sophisticated the cyber-attacks the closer the collaboration between private and public actors should be

information sharing mechanisms are fundamental

How private involvement should be framed?

- Security has always been one of the most important prerogatives of a state.
- BUT technical knowledge of the of the field lies mostly in hands of private actors*

Private actors do not have to be transparent about how the system work unlike public actors.
Only some stakeholders may have a closer look. There are different incentives between public and private for info sharing. Info sharing is fundamental: if we know about a vulnerability, sharing can help with prevention.
* Not the state that is pushing knowledge! Legislation is running behind.

We need to make sure that info sharing is addressed.

Information sharing

We will deal with it, but there is a push among institutions and member states.

Regulation 2019/881 (Cybersecurity act)

(6) In light of the increased cybersecurity challenges faced by the Union, there is a need for a comprehensive set of measures that would build on previous Union action and would foster mutually reinforcing objectives. Those objectives include further increasing the capabilities and preparedness of Member States and businesses, as well **as improving cooperation, information sharing and coordination across Member States and Union institutions, bodies, offices and agencies**. Furthermore, given the borderless nature of cyber threats, there is a need to increase capabilities at Union level that could complement the action of Member States, in particular in cases of large-scale cross-border incidents and crises, while taking into account the importance of maintaining and further enhancing the national capabilities to respond to cyber threats of all scales.

Recital *

(29) With a view to stimulating cooperation between the public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, ENISA should support information sharing within and among sectors, in particular the sectors listed in Annex II to Directive (EU) 2016/1148, by providing best practices and guidance on available tools and on procedure, as well as by providing guidance on how to address regulatory issues related to information sharing, for example through facilitating the establishment of sectoral information sharing and analysis centres.

Those are recitals: we explain what we want to do or put the things were not agreed on. They are not binding but help to understand the article.

*We want public and private sector speak to each other and also have companies speak to each other.

Emisa is put as the facilitator of this info sharing.

Information sharing

Across EU, networks and info sec.

Directive 2022/2555 (NIS 2)

41) Member States should be adequately equipped, in terms of both technical and organisational capabilities, to prevent, detect, respond to and mitigate incidents and risks. Member States should, therefore, establish or designate one or more CSIRTs under this Directive and ensure that they have adequate resources and technical capabilities. The CSIRTs should comply with the requirements laid down in this Directive in order to guarantee effective and compatible capabilities to deal with incidents and risks and to ensure efficient cooperation at Union level. Member States should be able to designate existing computer emergency response teams (CERTs) as CSIRTs. In order to enhance the trust relationship between the entities and the CSIRTs, where a CSIRT is part of a competent authority, Member States should be able to consider functional separation between the operational tasks provided by the CSIRTs, in particular in relation to information sharing and assistance provided to the entities, and the supervisory activities of the competent authorities.

119) With cyber threats becoming more complex and sophisticated, good detection of such threats and their prevention measures depend to a large extent on regular threat and vulnerability intelligence sharing between entities. Information sharing contributes to an increased awareness of cyber threats, which, in turn, enhances entities' capacity to prevent such threats from materialising into incidents and enables entities to better contain the effects of incidents and recover more efficiently. In the absence of guidance at Union level, various factors seem to have inhibited such intelligence sharing, in particular uncertainty over the compatibility with competition and liability rules.

The CSIRTs will receive info from other entities and share them.

2 types of communications: incidents or vulnerability disclosure.

1st case is mandatory, 2nd is voluntary.

The CSIRT will have to cooperate with the company to cooperate and solve the vulnerabilities if found.

Both public and private companies inform CSIRT about incidents and vulnerabilities.

- For instance: Pr comp. communicates a vulnerability discovery to CSIRT so they cooperate as fast as possible to produce countermeasures. CSIRT + private company + experts + other CSIRTs... and in that case, the Italian legge sulla Sicurezza forces public companies to adapt to the countermeasures in 30 days (ACN = CSIRT)

Operationalise information sharing

Public authorities er tried to enhance security requesting private companies to share information.

Private actors were reluctant to share voluntarily information related to the activities they carry out

↳ Create possibility to cooperate between private actors and public authorities.
Private-public Partnerships
No more so strong because legislation is pushing info sharing in other ways.

Public-private partnerships

Private-public Partnerships are defined as ‘A long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance’ (World Bank)

- the different group of actors involved in each sector will determine according to the characteristics of their activities, a relationship more or less stringent between private and public actors.
- E.g. actors carrying out activities at the physical infrastructure layer have a marginal relationship with the public sector authorities. Whereas private entities providing services and products to consumers have a stringent relationship with public authorities

"you can receive remuneration but you need to invest in security".
This doesn't include the perspective of citizens pretty much but these collab, will have an impact on society.

ENISA Study on PPP

Cooperative Models for Public Private Partnership (PPP)

- To provide information about PPPs in Europe through collecting information and analysing the current status of PPP and to identify main models of this type of collaboration. (How the info is working in this context)
- To identify current challenges that both the private and public sector face in the process of setting up and developing PPPs.
- To formulate and propose recommendations for the development of PPPs in Europe

ENISA Study on PPP

Memorandum of understanding: this is the objective and we are doing this to achieve it

may be possible to have a contract or cooperation and collab.

A public – private partnership (PPP) is a long – term agreement/ cooperation/ collaboration between two or more public and private sectors and has developed through history in many areas.

PPP is not only about the private-public cooperation. It includes also private-private and public-public relations.

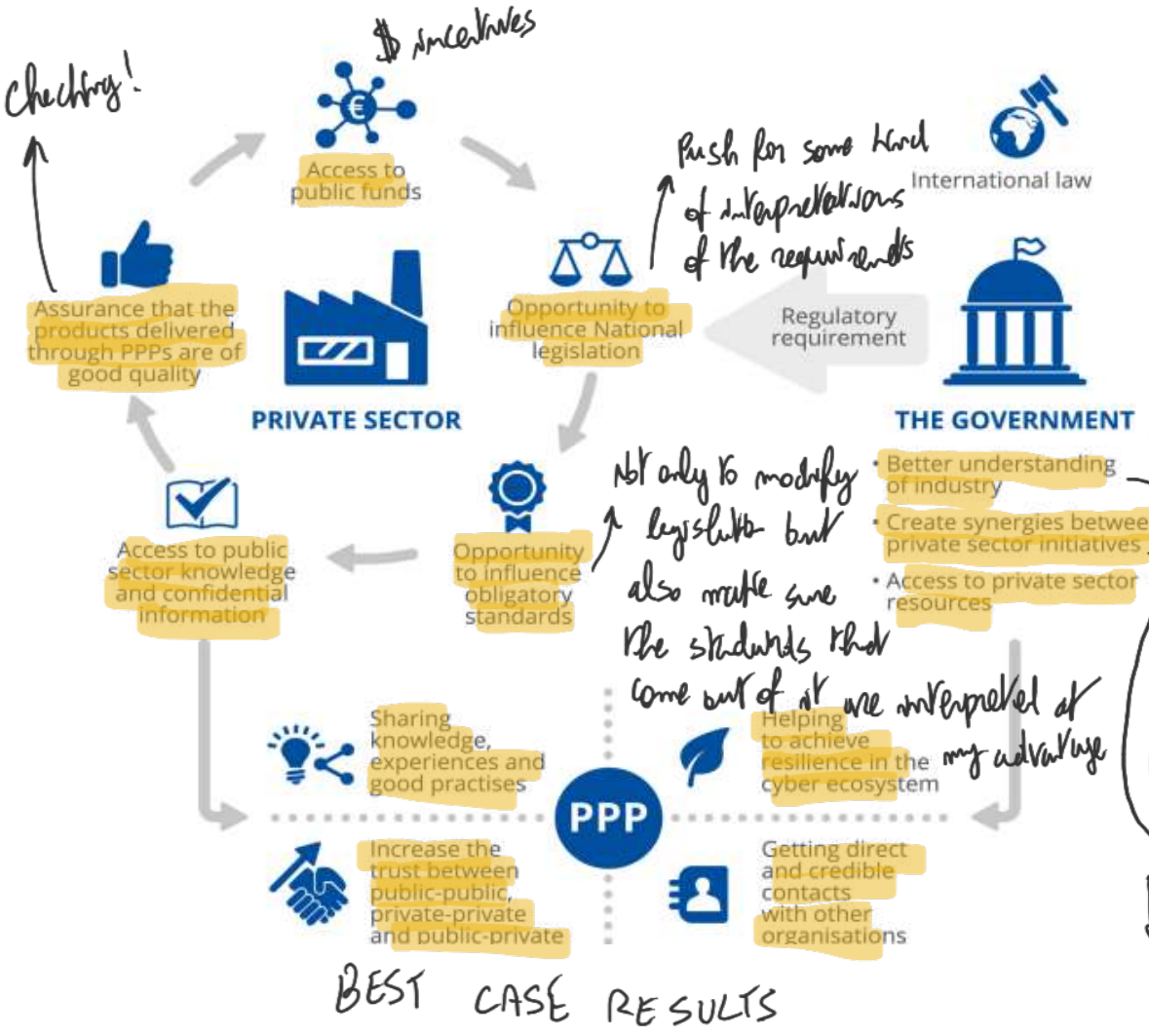
→ But the public is the trigger (gov: "we need this", pvr: "ok")

Wider perspective

ENISA Study on PPP

Driving forces for the creation of PPP

- Economic interests. for private org.
- Regulatory requirements. implicit obligation by the state
- Social interests. Improving welfare of society, for better presentation of org. to the people
- Public relations. with other private companies in these contracts.
- Other reasons.



There is a common objective for the participation in PPPs, both of the private and the public sector: to raise the level of cybersecurity.

However, there are also a number of different motivations:

ENISA study on PPP

The information about how PPPs are started and how they evolve is valuable in understanding how to develop new partnerships. Different possibilities include:

- Top Down Gov sets the idea and creates it
- Bottom Up Companies see the problem (see the regulatory req. changed) so they can change the ship.
- Fire and Forget Create them (gov sets up) and then go-on without me
- Split or merge Different PPPs already occurring and merge / split

INSTITUTIONAL PPP

- Formed under a legal act linked with the critical infrastructure protection.
- Common means of cooperation are working groups,rapid-response groups and long-term communities.

GOAL-ORIENTED PPP

- Created to build a cybersecurity culture in the MS.
- A platform or a council brings private and public sector together to exchange knowledge and good practices.
- The objective is to focus around one subject or a specific goal.

OUTSOURCING CYBERSECURITY SERVICES

- Created by the government and the private sector.
- Its task is cybersecurity awareness raising.
- Considered as a third party for outsourcing services to address the needs of industry
- Support the government in policy making or implementation.

HYBRID PPP

- CSIRTs operating under a PPP framework.
- Governments' assignment to deliver CSIRT services to the public administration or to the whole country.

ENISA Study on PPP: not really good

Challenges

- Lack of human resources in both the public and private sector.
- Insufficient public sector budget and resources fail to meet the private sector's expectations.
- The establishment of a common level of understanding and dialogue between the public and private sector.
- Promotion of the concept of PPP among SMEs.
- Lack of leadership and legal basis.

SO: NOT THE BEST SOLUTION

EXAMPLE

European Cyber Security Organisation

- The ECSO is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.
- It was created in order to act as the Commission's counterpart in a contractual public-private partnership covering Horizon 2020 in the years 2016 to 2020.
- The majority of ECSO's 250 members belong either to the cybersecurity industry or to research and academic institutions in the field. To a lesser degree, ECSO's members also comprise public sector actors and demand-side industries.
- Besides making recommendations on Horizon 2020, ECSO carries out various activities aiming at community building and industrial development at European level.
- https://ecs-org.eu/about

An example of (European) PPP

EU legislative framework

NOW THE RULES

EU Cybersecurity legislation

Directive on Resilience of critical infrastructures (2008) - Resilience of Critical Entities (2022)

NIS Directive (2016) - NIS 2 Directive (2022)

Cybersecurity Act (2018)

Regulation on European Cybersecurity Competence Centre and Network (2021)

Cyber Solidarity Act (2023)

Cyber-resilience Act (2024)

Artificial Intelligence Act (2024)

European Health Data space (2024)

Connected with PPP and info sharing.
Try to figure out how to make collect and info sharing.

Legally binding laws that must be applied in their entirety
Directives set goals to be achieved but leave freedom in how to.

European Cybersecurity Competence Centre and Network

Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

- The **European Cybersecurity Competence Centre** (ECCC), together with the **Network of National Coordination Centres** (NCCs), is Europe's new framework to support innovation and industrial policy in cybersecurity.
- The ECCC, which will be located in Bucharest, will develop and implement, with Member States, industry and the cybersecurity technology Community, a common agenda for technology development and for its wide deployment in areas of public interest and in businesses, in particular SMEs.
- The Centre and the Network together will enhance our **technological sovereignty through joint investment in strategic cybersecurity projects**.

↳ keep the cybersec. tech in the hands of EU

It's some sort of duplication of ENISA: Create a Centre additional to ENISA (cert. training, info sharing, collect vuln. disclosure) but they

& based on EU systems to compete with third parties that have different frameworks. I want to create my own systems that provide cybersecurity. Sov. underlines making sure that EU is the point of reference for member states

"I don't want to rely on technology that comes from outside". We make sure that what's happening in EU is competitive enough.

European Cybersecurity Competence Centre and Network

Not taking work of CSIRTs

Recital

(16) **The Competence Centre should not carry out operational cybersecurity tasks, such as tasks associated with Computer Security Incident Response Teams (CSIRTs), including the monitoring and handling of cybersecurity incidents.** However, the Competence Centre should be able to facilitate the development of ICT infrastructures at the service of industries, in particular SMEs, research communities, civil society and the public sector, consistently with the mission and objectives laid down in this Regulation. Where CSIRTs and other stakeholders seek to promote the reporting and disclosing of vulnerabilities, the Competence Centre and members of the Cybersecurity Competence Community (the 'Community') **should be able to support those stakeholders at their request within the limits of their respective tasks and while avoiding any duplication with the European Union Agency for Cybersecurity (ENISA)** …

additional expertise provided

(17) The Competence Centre, the Community and the Network are intended to **benefit from the experience and the broad representation of relevant stakeholders built through the contractual public-private partnership on cybersecurity between the Commission and the European Cyber Security Organisation (ECSO)** for the duration of Horizon 2020 …, from the lessons learnt from four pilot projects launched in early 2019 under Horizon 2020, namely CONCORDIA, ECHO, SPARTA and CyberSec4Europe, and from the pilot project and the preparatory action on Free and Open Source Software Audits (EU FOSSA), for the management of the Community and the representation of the Community in the Competence Centre.

(European projects and partnerships)

We are figuring out a way to collaborate

Duplicating!

European Cybersecurity Competence Centre and Network

The Competence Centre should facilitate and coordinate the work of the **Network**.

- The Network should be made up of one national coordination centre from each Member State.
- National coordination centres which have been recognised by the Commission as having the necessary capacity to manage funds to fulfil the mission and objectives laid down in this Regulation should receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out their activities in relation to this Regulation.
- National coordination centres should be public sector entities, or entities with a majority of public participation, performing public administrative functions under national law, including by means of delegation, and they should be selected by Member States.
- National coordination centres should have the necessary administrative capacity, should possess or have access to cybersecurity industrial, technological and research expertise and should be in a position to effectively engage and coordinate with the industry, the public sector and the research community.

- https://cybersecurity-centre.europa.eu/nccs_en

Resilience of critical entities directive: requires implementation at national level

Directive (EU) 2022/2557 on the resilience of critical entities

Predecessor: European Critical Infrastructure (ECI) Directive in 2008.

- applies only to the energy and transport sectors,
- provides a procedure for identifying and designating ECIs, the disruption or destruction of which would have significant cross-border impacts in at least two Member States.
- sets out specific protection requirements on ECI operators and competent Member State authorities
- To date, 94 ECIs have been designated, two-thirds of which are located in three Member States in Central and Eastern Europe (3 in the transport and all the others in energy)

However,

- the scope of EU action on critical infrastructure resilience extends beyond these measures and **includes sectoral and cross-sectoral measures on inter alia climate proofing, civil protection, foreign direct investment and cybersecurity**
- **Member States themselves have taken measures of their own in this area in ways that diverge from one another.**

* 1 What happens in my Member State can have an impact to other member states and at least 2: idea is make very stringent rules in order to be applied. So only 2 sectors and has to have big consequences, so we can impose some obligations on them.

* Critical infrastructures are subject to a wide area of attack.

Directive on the resilience of critical entities

Different setting:

- the risk landscape is more complex than in 2008, involving today natural hazards (in many cases exacerbated by climate change), state-sponsored hybrid actions, terrorism, insider threats, pandemics, and accidents (such as industrial accidents). *
- operators are confronted with challenges in integrating new technologies such as 5G and unmanned vehicles into their operations, while at the same time addressing the vulnerabilities that such technologies could potentially create.
- these technologies and other trends make operators increasingly reliant on one another: a disruption affecting the service provision by one operator in one sector has the potential to generate cascading effects on service provision in other sectors, and also potentially in other Member States or across the entire Union.

Ex: Nn a hospital ENEL won't provide energy anymore. We have to open up the system for sectors that can become critical.

* Those critical infrastructure have to be safeguarded from the cybersec. POV.
The risk hazards do not look at cybersec. but cybersec attacks can cause or worsen those hazards. Directive wants critical entities to be protected.

Directive on the resilience of critical entities

- wider sectoral scope, covering ten sectors: energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, and space. (only at the moment perceived as critical)*
- procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment. So now there is no cross-border elements ecc., there can still be a disrupt. of services.
- obligations on Member States and the critical entities that they identify, including ones with particular European significance, i.e. critical entities that provide essential services to or in more than one third of Member States that would be subject to specific oversight.

CI
=
EE/IE Essential entities or important entities in NIS2. For the cybersec perspective we need to take this measure (NIS2)

Directive on the resilience of critical entities

Main changes :

- from protection to resilience
  - *Protection* is based on ex ante approach and risk assessment (with the objective of avoiding the unwanted event) v *Resilience* is based on ex ante and ex post analysis (with the certainty that the unwanted event will occur)
  - No standard upon which evaluate the resilience

- From European Critical infrastructures to Critical entities
  - Not synonyms
  - Bottom-up and agent-based approach

- wider number of critical infrastructure sectors
  - From energy and transport to 10 sectors (coordination with NIS 2 directive)
  - Interdependencies and between sectors, countries and physical-digital interfaces
    - Dependencies or interdependencies?

- from terrorism as priority to all-hazards approach

They are complementary. The operators that have risks related to cybersec look at NIS 2. For the fields they look at Resilience directive.

Directive on the resilience of critical entities

Coordination issues as regards cybersecurity :

- synergies with the NIS 2 Directive (enhancing all- hazards information and communication technology (ICT) resilience on the part of 'essential entities' and 'important entities' meeting specific thresholds in a large number of sectors)
- Competent authorities designated under the directive and those designated under the NIS 2 Directive take **complementary measures and exchange information as necessary regarding cyber and non-cyber resilience**, and (there will be interplay and communication)
- critical entities in the sectors considered to be 'essential' per the NIS 2 Directive are also subject to more general resilience- enhancing obligations to address non-cyber risks.
- The physical security of network and information systems of entities in the digital infrastructure sector is addressed comprehensively in the NIS 2 Directive as part of those entities' cybersecurity risk management and reporting obligations

* the same

* Measures related to cybersec are related to other risks.

RECAP

The more sophisticated an attack is, the closer the collaboration between private and public actors should be.

The problem? Public and private actors have different interests: while public actors are generally more oriented towards transparency and they are responsible for our well being (they see us as citizens), private actors are profit oriented and treat us as customers or worst case as product.

Cooperation is not easy, especially when ensuring security, which is a top priority of a state, requires technical knowledge in the hands of private actors, most of the time only accessible by specific stakeholders.

The focus on cooperation and information sharing goes way back, with many EU interventions focusing on making different parties communicate. In the "Cybersecurity Act", the 2019 Regulation (legally binding laws that must be applied in the entirety across all member states), we can see in the 6th recital the focus the act has on increasing capabilities and preparedness of Member States and businesses and increasing cooperation, information sharing and coordination across Member States and Union institutions, agencies and bodies. The 29th recital also puts the attention on the importance of stimulating cooperation between public and private sector and within the private sector, with ENISA designated as the facilitator of this information sharing process, in order to support the protection of critical infrastructures.

(Recitals serve as introductory statements that explain the purposes and reasons behind an act).

Similarly, we saw with the NIS 2 directive (intervention that sets goals that all EU members have to achieve, but each country decides how) the focus on ensuring member states having the adequate technical and organizational capabilities for prevention, detection and response and for risks and incidents mitigation through the designation of CSIRTs. Under the NIS2 directive, stricter rules were established for reporting to CSIRTs: an organization victim of an attack must report it to the national response team and in case of a new vulnerability being discovered, has the possibility to report it to coordinate efforts (also between other experts or CSIRTs) for the production of a countermeasure.

In general, public authorities were always interested in private companies information to enhance security. Private organizations on the other hand didn't want to share info related to their activities. That's why Private-Public Partnerships were born (not used a lot today though: legislation is pushing for info sharing through other means).

PPPs can be seen as "A long term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance" (World Bank)
The relationship can be more or less strong between the parties depending on the characteristics of their activities.

Of great interest in this context is the Enisa study on PPPs. Its focus was on providing info about PPPs in Europe through collecting info and analysing the current status of PPPs to identify models of this type of collaboration. The interest was also on the challenges that both sectors faced in order to propose recommendations for the development of PPPs in EU.

For this purpose, the ENISA definition of a PPP offers a wider perspective: a PPP is any long-term agreement, cooperation or collaboration between two or more public and private sectors. It has developed through history in many areas.
PPP does not only focus on private-public cooperation, but even public-public and private-private relations (ignited by the public sector).

What are the driving forces for the creation of PPPs? For private entities the access to public funds, the opportunity to influence and shape interpretations of National legislation and the obligatory standards that may follow, the access to public sector knowledge and confidential info, the guarantee of the good quality of products produced under PPPs, but also the possibility of being seen in a better light by the people for improving welfare of society or the chance of establishing relations between the other companies involved in PPPs.

The main interest for governments and public actors is the possibility of better understanding the industry by accessing to the resources of a private sector and being able to encourage synergies and private sectors initiatives that would otherwise be scarce.
The best case results are increased trust between parties, sharing of knowledge and experience, helping to achieve resilience in the cyber ecosystem and creating synergies with different organizations.

But how are PPPs started? Enisa showed different possibilities: Top Down refers to when the government is the one that makes the first step; similarly, when companies are the one to show interest (for example when new regulations need to be put out) we have a Bottom Up approach; Fire and Forget means that the government sets up the PPP and lets it evolve without its intervention while split or merge refers to the way PPPs start and end with the splitting and merging of other PPPs.

What are the different PPPs and their purpose? In general, institutional PPPs are formed under legal acts and tackle the protection of critical infrastructure. Good-oriented PPPs are created to foster exchange of knowledge in a specific area to achieve better results. Some PPPs are created as a way for the government (which may lack in expertise and skills) to outsource cybersecurity services to private sectors. In other situations, we can have a hybrid PPP with multiple purposes.

But PPP is not the solution to all our problems. The ENISA study reported different main challenges in establishing and maintaining PPPs: firstly, PPPs require to create a system of collaboration, and there might be lack of human resources in both parties to achieve that. This makes it particularly difficult to collaborate with SME, which are the ones that would benefit from it the most. In addition, most of the times the public sector budget and measures fail to meet the private sector's expectations. There's also the possible absence of a common ground between the parties, which might facilitate a problem in very different ways. Finally, a lack of leadership and loyal teams makes it hard to cooperate when a specific agreement doesn't exist.

On the second page of information sharing, there was a new attempt by the Union in a 2021 Regulation that established the European Cybersecurity Competence Centre together with the Network of National Coordination Centres. The organs have the main purpose of pushing for the development of a common agenda for tech development and innovation with the member states in order to enhance technological sovereignty through investments in strategic cybersecurity projects. The EU purpose is to become a point of reference for cyber security for the Member States to gain independence from any third party.

As stated in the 16th recital, the Competence Centre should not carry operational tasks associated with other organs like CSIRTs, like the monitoring and handling of cybersec. incidents, but can offer help in raising awareness in vulnerabilities discovery and reporting if asked by CSIRTS and other stakeholders, as long as this does not cause duplications with the work of ENISA.
The Centre focus is also on fostering collaboration and promoting knowledge acquired through european projects and partnerships. Basically a lot of what the new organs do has a very high chance to cause duplications.

On another note, we introduce now the efforts made by the EU regarding critical entities protection and resilience, starting with the EUROPEAN CRITICAL INFRASTRUCTURE DIRECTIVE (2008). This directive focused on identifying Critical Infrastructures in the energy and transport sectors, the disruption or obstruction of which would have significant cross-border impacts in at least two Member States. The directive set out specific requirements for the operators. The main problem was that with such limiting requirements, only 94 ECIs were designed (2/3 in just 3 member states) and the measures taken by the Member States were so diverse that they weren't compatible, causing mess rather than harmony.

This problem was partially solved in the Directive on the resilience of critical entities, tackling a more complex risk landscape which included possible natural hazards, terrorism, insider threats, pandemics and accidents. The directive kept into account the fact that operators were challenged with interplaying new technologies which also addressing the vulnerabilities that they might create.
Those technologies made operators linked more than ever, with possible disruption in one sector causing a chain reaction with possible consequences in other Member States or across the entire Union.

The directive focused on a wider sectoral scope, covering ten sectors including energy, transport, banking, health, drinking water, waste water...
The procedure for the identification of critical entities was based on national risk assessment criteria, with obligations on the entities identified and special attention on entities that provided services to at least 1/3 of the Member States.

The main changes were a shift from protection to resilience (when that adverse events will occur and be able to tackle the unexpected) even though there is no clear standard for resilience evaluation; there was also a shift from Critical Infrastructures to Critical Entities, probably for comparison with the Essential Entities defined in the NIS 2 directive; lastly, one big difference was the shift from revision as a priority to a wider hazard approach.

Let's keep in mind that there are several synergies between the resilience directive and the NIS 2, starting from the same definition of Critical Entities, called Important or Essential Entities in NIS 2 and the focus on taking complementary measures and exchange information between the competent authorities designed for both directives.
Keep in mind that essential entities that were also recognised as critical under the resilience directive had to follow additional obligations to enhance more general resilience, and in a similar way, the measures described by the NIS 2 directive also included a related focus on a more general physical security of network and information systems for those that were identified as essential entities.