Information and technology law course

LECTURE 3 – 30 SEPTEMBER 2024

FEDERICA CASAROSA – 2024/2025

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

Information sharing

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.

(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.

Information sharing

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.

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

Private-public Partnerships

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

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.
- 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

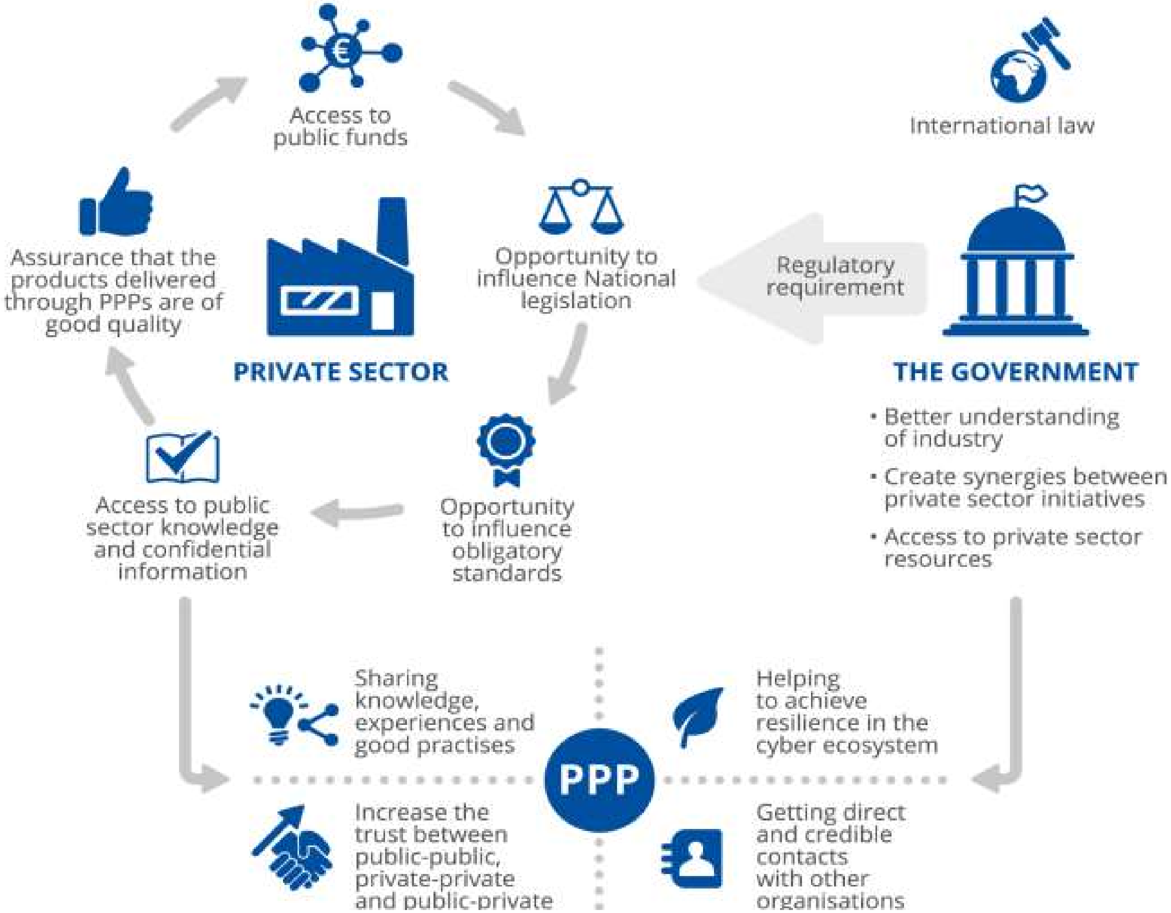
A public – private partnership (PPP) is a long – term agreement/ cooperation/ collaboration between two or more public and private sectors and has developed through history in many areas.

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

ENISA Study on PPP

Driving forces for the creation of PPP

- Economic interests.
- Regulatory requirements.
- Social interests.
- Public relations.
- Other reasons.


Access to public funds
Opportunity to influence National legislation
Assurance that the products delivered through PPPs are of good quality
PRIVATE SECTOR
Access to public sector knowledge and confidential information
Opportunity to influence obligatory standards
International law
Regulatory requirement
THE GOVERNMENT
• Better understanding of industry
• Create synergies between private sector initiatives
• Access to private sector resources
Sharing knowledge, experiences and good practises
Helping to achieve resilience in the cyber ecosystem
PPP
Increase the trust between public-public, private-private and public-private
Getting direct and credible contacts with other organisations

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
- Bottom Up
- Fire and Forget
- Split or merge

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

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.

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

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)

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**.

European Cybersecurity Competence Centre and Network

(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)** …

(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 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

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**.

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.

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.
- procedure for Member States to identify critical entities using common criteria on the basis of a national risk assessment.
- 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.

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 <u>and</u> 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 11 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

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
- 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