Information and technology law course

LECTURE 2 – 26 SEPTEMBER 2024

FEDERICA CASAROSA – 2024/2025

To setup this system there were struggles. States didn't want to lose the power over their territory. There was a compromise about the power delegated to the EU.

Power to legislate

EU competence in cybersecurity

We need to understand why EU legislation has an impact to Italy.

Why EU is writing the law? We say Italy is a part of a political institution called EU.
The european community came out after WW2 firstly. We need to get to a part to collaborate in order to start a community.

Through the constitution of the community, we gave citizens the liberty of travelling. The boys was free crossing the border for individuals and org. The first idea is freedom of movement to create an internal market.

EU competence

delegate power

Under the **principle of conferral**, the Union shall only act within the limits of the competences conferred upon it by the Member States in the Treaties, and in order to attain the objectives set out therein.

Art 4 TFEU

if I don't say you have those competences, they're mine.

- 1. In accordance with Article 5, competences not conferred upon the Union in the Treaties remain with the Member States.
- 2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State. […]

Me Belgian is different from others: I don't want to have something imposed against my will.

Germany in particular has struggled a lot with power delegation.
There should be a clear reference in the Treaties. It should be SPECIFICALLY SAID in the Treaties. The objectives have to be clear as well.

* The protection of the state seen through the military lens. BUT It might include cyberthreats! So? Why is EU regulating?

The justification to intervene to protect the european market. We want (the possibility) to have a market to flourish and then each member state has to verify that they comply with the regulation so org. can function correctly.

EU competence

Which is the legal basis for EU cybersecurity legislation?

- Article 114 TFEU - Internal market (in general)
- Article 62 and 53(1) TFEU - right of establishment and freedom of service
  ↱ I have to provide services to other countries
- Articles 127(2), 132(1) TFEU - smooth operation of payment systems
- Article 83(1) TFEU - area of freedom, security, and justice
- And as regards coordination at the EU level – art 74 TFEU

Whatever legislation we have a part of reference which is the legal basis! EU Justifying it has the competence to create legislations about the topic of interest.

EU competence

In areas that do not fall within the exclusive competence of the Union, the principle of subsidiarity must be observed.

Art 5 TFEU

- […] 3. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act **only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States**, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.
- The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol.
- 4. Under the principle of proportionality, **the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties.**
- The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality.

You have:

Competences. Part of them are exclusive, part of them are shared. Member states are free to regulate that but...* . It is possible that some competences become of EU.

Ex: employment, free movement of work; the protection of workers or the recognition of your degree are not the same so you are treated differently. So there is discrimination. In this case national legislations for degree recognitions are different.

But the purpose of EU is to recognise free movement of workers. This objective is not reached through national regulations. If you don't achieve the objective identified in the shared competences EU can intervene.

EU only takes into account the disalignment and work with the least interference possible.

*2 The system is not changed.

① Decision is binding on those to whom it is addressed (EU country or individual company) [Regulation works across all EU]

EU interventions in cybersecurity

They have to define how to interpret some issues.

1992, Council Decision 92/242/EEC in the field of security of information systems

Giving you the guidelines of how to behave. Can be adopted or less.

1995, Council Recommendation 1995/144/EC on common information technology security criteria

- creation of the Senior Officers Information System Security (SOG-IS)

Sets the scene: "I want to do this in the future", not an indication of any kind of behaviour

2001, Communication on Network and Information Security

You will have to follow me

- "policy measures can reinforce the market process and at the same time improve the functioning of the legal framework"

2005, Council Framework Decision 2005/222/JHA27 on attacks against information systems

① → There are attacks against IS. We want to make sure there is a reaction. ☆3

① FD establishes objectives MS have to fulfil. They are free to chose how.

Cybersecurity was not there when EU was born.

* There was the need to take into account the market.

2001 idea: want to make sure that the measures reinforce the market. Was not interested in Member states, private entities the citizens but the bigger companies.

*3 Here I say "I want to have the law enforcement authorities coordinate" better so I'm giving a way for us to understand each other when it comes to criminal offences to understand each other and react.

EU interventions in cybersecurity

1. 2006, 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" COM/2006/0251 final

   2013, Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

2. 2012, 'Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, Security Industrial Policy Action Plan for an innovative and competitive Security Industry' (2012) COM/2012/0417 final

1 and 2 set the direction and find a way to intervene in security.

* The idea is having info internalised

① ② All these interventions, ① there was serious talk about the necessity to implement security measures for network and information security.

"We want to make sure that there dialogue in the issue of secure information society, then with the industry. The EU is trying to find a way to intervene in the security and it has found a way to do so, in 2016 we had the network & information security directive, the culmination of this process. It was not a general info regarding prevention: there is reaction to offenses, but not doing anything to enforce rules in order to prevent negligence. No criminal offence. You have to make sure that this is something internalised by the citizens and companies instead of looking only at attacks.

EU interventions in cybersecurity

2020, Joint Communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final

- The strategy has three areas of action:
  - resilience, technical sovereignty and leadership; *
    - (1) Cybersecurity shield Protection
    - Internet of Secure Things
    - DNS4EU (There is a structure for the IP allocation which is mainly controlled by US) *
  - operational capacity to prevent, deter and respond;
    - Joint cybersecurity Unit * (2)
  - cooperation to advance global and open cyberspace.

make sure that we do not rely on 3rd countries.

Before Ukraine war. Was a communication. We want to make a resilience...*

① Network of security operation center that will construct a shield able to detect attacks and respond.
Idea is we want to create a system of centers at national levels that collaborate and share info to react and be resilient.
There is an ongoing process to increase intervention in Cybersecurity.

* We want a system that is able to compete.

The strategy covers the period from 2020 to 2025 and focuses on priority areas where the EU can help Member States in fostering security for all those living in Europe, while respecting our European values and principles.

https://commission.europa.eu/publications/fifth-progress-report-eu-security-union-strategy_en

EU governance structure

We don't have a single person representing EU.

EU governance structure (cyber context)

Decentralised structure (No need to have each area working together)

- Allocation to the three different areas of cybersecurity: Network and information security, cybercrime, and cyber defense

Where national security speaks to eu defense and try to collaborate.

EU governance structure

Network and information security

- ENISA is the one that becomes the point of reference.
  - Established in 2004, received a new permanent mandate in 2019 by the EU Cybersecurity act → at first was not permanent, it was renewed every 5 years.
  - raise awareness and assist the EU, Member States, and public and private stakeholders develop and improve cyber resilience and response capacities
  - responsible for the preparation of European cybersecurity certification schemes, which will serve as the basis for certification of ICT products, processes, and services
- CERT-EU, CSIRTs, Cooperation Group, CSIRTs Network and FIRST

→ only have one, EUCC (common criteria), there is one for Cloud Computing too in the chamber.

Enisa is an agency, is in charge of raising awareness. It's a support and tutor for nations to build their strategy and EU.
Doesn't work as a regulator.

*2 Comp-System Incident Response Teams. They are the point of reference if an attack happen.
They will be experts and give guidelines.
↓
it is national and so we have a network.

- Cert-EU, response team at the european level. (COMP. EMERGENCY RESPONSE TEAM)
- Cooperation group: facilitate exchange of information and strategic cooperation and includes representative of the member states, the European Commission and ENISA. Develops best practices, share experiences.

↳ other face of the CSIRTs. Those are the response team, they will be understanding the overall situation and get back to CSIRT, and they can provide guidelines.

The cooperation group may set priorities and provide high-level recommendations that CSIRTs can apply in their day-2-day operations.
The information sharing in CSIRT network is more technical.

No line crossing - EU supports and coordinates but it's a hub for analysis and provides expertise

EU governance structure

Cybercrime

→ part of europol

- European Cybercrime center (EC3)
  - operational support and training to the Member States and has become the first hub for expertise on cybercrime operations.

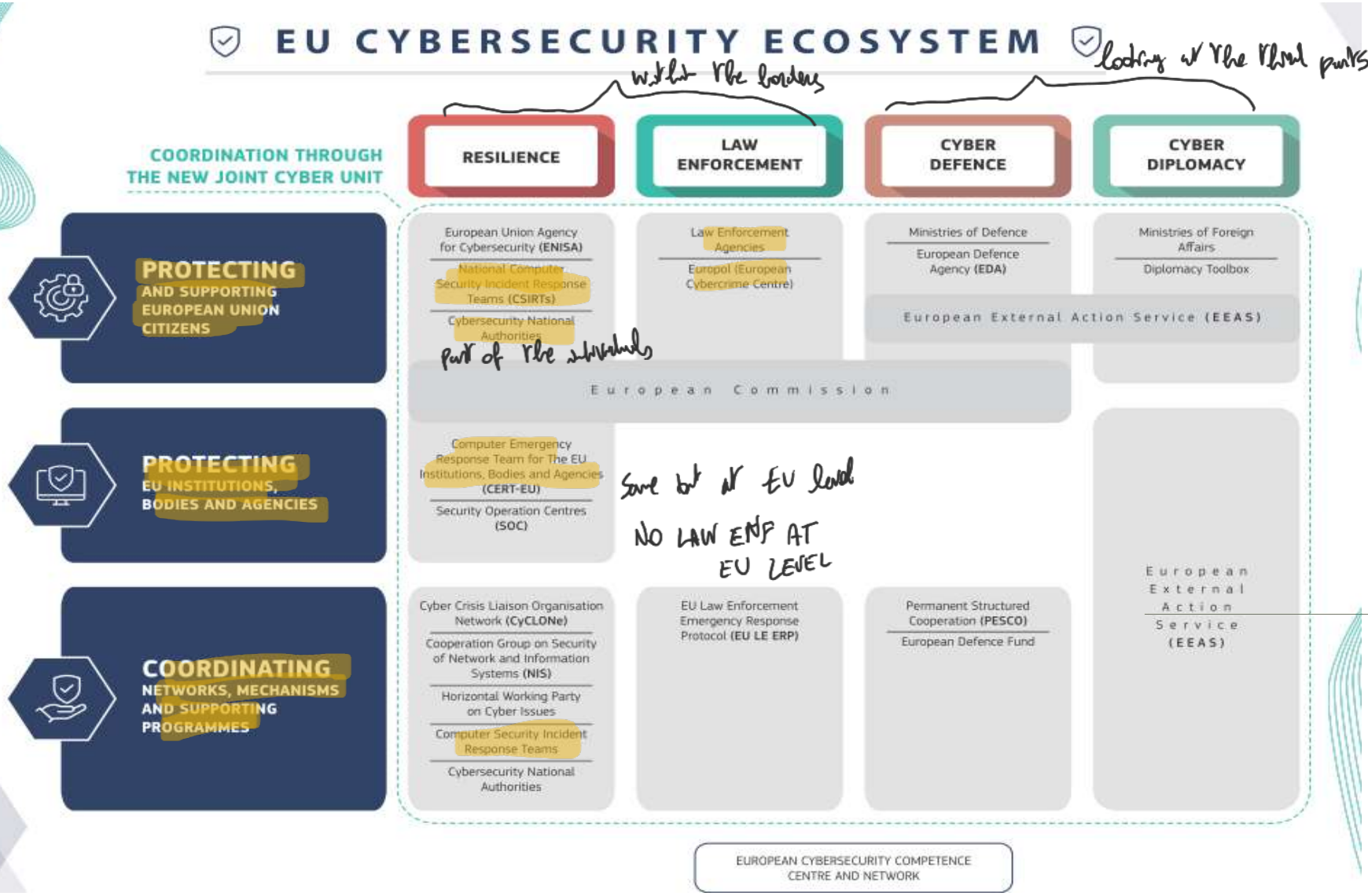
↳ Created in 2013

It was the only one where law enforcement could look upon for help but run as understaffed.

EU governance structure

Cyberdefence

- European Defence Agency (EDA) and EU Military Staff
  - advisory function, leaving the operational and strategic realities of defense to the Member States.



IDEA IS TO CREATE AN ATTENTION UNIT AT EU LEVEL

Joint Cyber Unit

The Joint Cyber Unit will support participants to:

Create **an inventory** of operational and technical capabilities available in the EU;

Systems where you can look upon info and people about field

Produce **integrated EU cybersecurity situation reports**, including information and intelligence about threats and incidents;

Replicate ENISA

Deliver the **EU Cybersecurity Incident and Crisis Response Plan**, based on national plans proposed in the revised NIS Directive (NIS2);

Conclude **memoranda of understanding** for cooperation and mutual assistance;

Establish and mobilise EU **Cybersecurity Rapid Reaction Teams**;

Share information and conclude operational cooperation agreements

MY's an agreement relying for cooperation

There has been a process bringing us from "we don't know" to

* We have a process that has created a system that has become an important part of the EU skill within the EU authority. We have a framework. Now decentralization doesn't work anymore.