Information and technology law course

LECTURE 2 – 26 SEPTEMBER 2024

FEDERICA CASAROSA – 2024/2025

EU competence in cybersecurity

EU competence

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

- 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. […]

EU competence

Which is the legal basis for EU cybersecurity legislation?

- Article 114 TFEU - Internal market
- Article 62 and 53(1) TFEU - right of establishment and freedom of service
- 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

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.

EU interventions in cybersecurity

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

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

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

2001, Communication on Network and Information Security

- "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

EU interventions in cybersecurity

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

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

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;
    - Cybersecurity shield
    - Internet of Secure Things
    - DNS4EU
  - operational capacity to prevent, deter and respond;
    - Joint cybersecurity Unit *
  - cooperation to advance global and open cyberspace.

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

EU governance structure

Decentralised structure

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

EU governance structure

Network and information security

- ENISA
  - Established in 2004, received a new permanent mandate in 2019 by the EU Cybersecurity act
  - 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

EU governance structure

Cybercrime

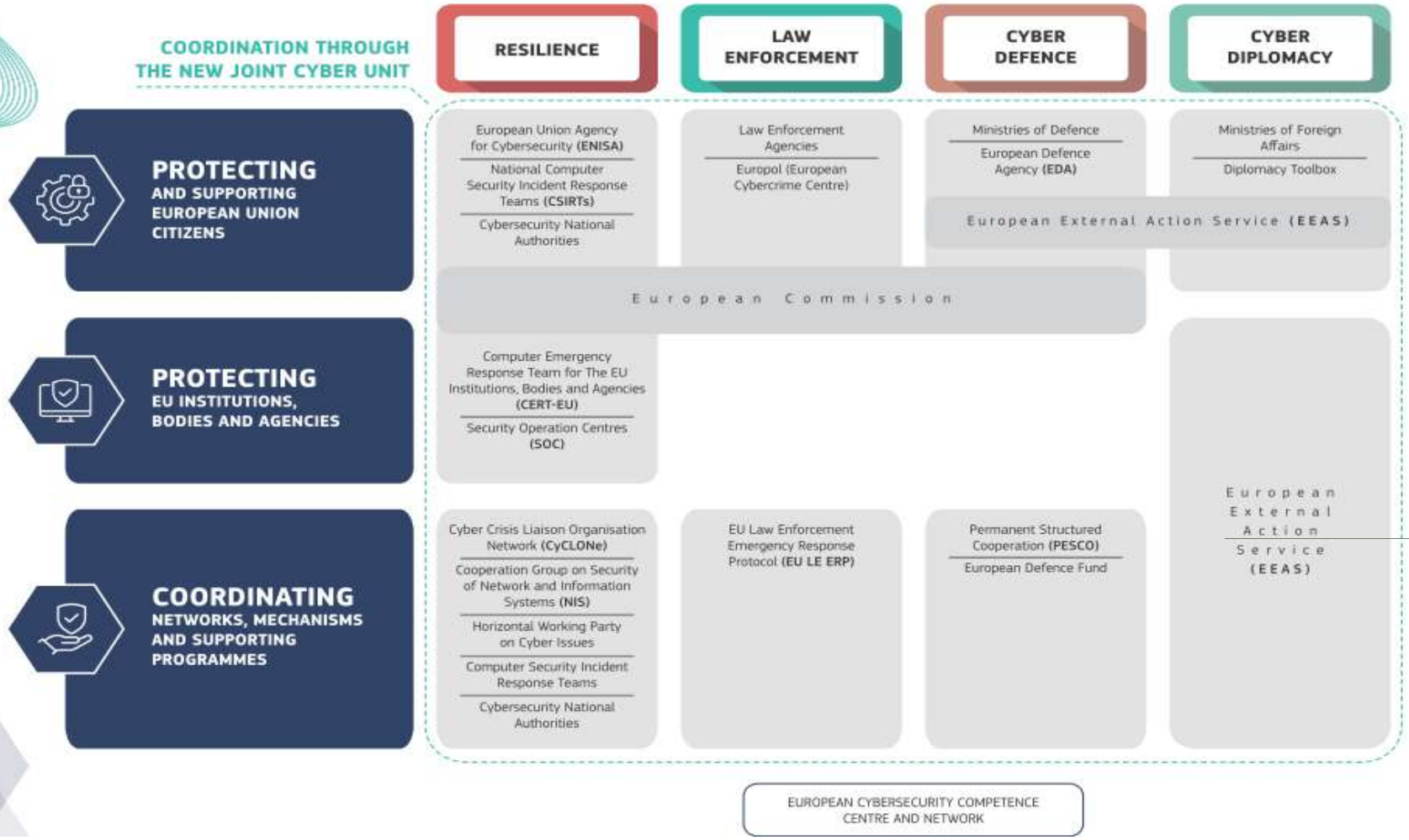
- European Cybercrime center (EC3)
  - operational support and training to the Member States and has become the first hub for expertise on cybercrime operations.

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.

EU CYBERSECURITY ECOSYSTEM



The Joint Cyber Unit will support participants to:

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

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

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

Joint Cyber Unit