2024 REPORT ON THE STATE OF CYBERSECURITY IN THE UNION PANEL SERIES

THE FUTURE OF EU CYBERSECURITY COLLABORATION IN TIMES OF CRISIS- EXPERTS PERSPECTIVES

1. INTRODUCTION

In December 2024, the European Union Agency for Cybersecurity (ENISA) released the 2024 Report on the State of Cybersecurity in the Union, adopted in cooperation with the European Commission and the NIS Cooperation Group, gathering all EU Member States to cooperate on cybersecurity strategic matters. The Report provides an **in-depth analysis of current challenges and opportunities** for strengthening cybersecurity in the European Union. **ENISA is organising a series of policy panels** at key cybersecurity conferences throughout 2025, with the aim to dive deeper into the Report's six key recommendations and foster discussions on the steps required to implement them.

A panel took place on November 27, 2025, at the Cybersecurity Conference of the Danish EU presidency, where experts gathered to exchange insights on EU-wide cyber cooperation in line with the EU Cyber Blueprint.

This paper presents the main discussion points and conclusions from that event.

2. BACKGROUND

In December 2024, ENISA released the 2024 Report on the State of Cybersecurity in the Union. The report offers an in-depth analysis of the current challenges and opportunities for enhancing cybersecurity across the European Union.

The panel provided a forward-looking discussion on strengthening EU-wide cyber cooperation in line with the **EU Cyber Blueprint** (Council recommendation). Topics included:

- Cross-border coordination and lessons learned from past incidents;
- Strengthening public-private partnerships for better situational awareness;
- Actionable strategies to enhance EU-wide digital ecosystem resilience.

The session was anchored in a key ENISA recommendation:

"*As called upon by the Council, **revising the EU Blueprint for coordinated response to large-scale cyber incidents,** while taking into account all the latest EU cybersecurity policy developments. The revised EU Blueprint should **further promote EU cybersecurity harmonization and optimisation, as well as strengthen both national and EU cybersecurity capabilities** for levelled up cybersecurity resilience at national and European level*".

3. THE EXPERT PANEL

Panel Title: The future of EU Cybersecurity collaboration

- **Moderator**: Kia Slæbæk Jensen - Cyber Attaché and chair of the Horizontal Working Party on Cyber Issues (HWPCI), The Danish Permanent Representation to the EU
- **Panellists:**
  - **Jamila Boutemeur** - Head of the Threat Analysis team within the Operations and Situational Awareness Unit, ENISA
  - **Erik Achenbach –** Head of Cyber Situation Centre, Danish Defence Intelligence Service
  - **Andrew Lee** - Vice President Government Affairs & Global CTI Strategist, ESET
  - **Paolo Palumbo** - Vice President, Strategic Threat Intelligence & Research, WithSecure

4. KEY INSIGHTS

Disclaimer: The views and opinions expressed by the panellists are those of the individual experts and do not necessarily reflect the official position of ENISA.

EU Threat Landscape

ENISA gave an overview of the ENISA Threat Landscape, published in October, highlighting some high-level trends:

- Phishing was the dominant intrusion vector, followed by vulnerability exploitation;
- Public Administration was identified as the most targeted sector in the EU, dominated by low-impact DDoS by hacktivists;
- State-aligned activities against EU Member States continued at a steady tempo, with state-nexus cyberespionage activities notably targeting the public administration;
- Ransomware remains the most impactful threat in the EU.

Collaboration between the public and private sector: the importance of trust building and feed-back loops

The ENISA Threat Landscape is an example of collaboration between the public and private sector in several ways. Firstly, it is based on open-source information, also released by actors from the private sector. Secondly, it was reviewed by the members of the **ENISA Cyber Partnership Programme (CPP),** which focuses on cooperation in relation to information exchange and situational awareness with the private sector.

This moved the discussion on how the private sector considers information sharing towards public entities. Panellist stressed the **importance of releasing information to the public sector to contribute to the knowledge of threats and increase the collective capability to defend from them**.

At the same time, several **barriers to information sharing** were identified, such as:

- **Commercial value of information and secrecy**: Intelligence and visibility on the threat landscape are part of companies' competitive advantage. It is a commercial reality that "everyone wants more information, but no-one wants to pay". In addition, some of the victims of incidents can be a company's customers. It is therefore essential to establish collaboration frameworks that enable companies to support affected entities and share relevant information, without exposing victims or compromising their position.
- **Asymmetry of information sharing**: When the private sector gives information to the public, it is not clear what happens next, e.g., which (other) information is being used and how information from different sources is combined into a final analysis. It would be important that the public sector also contributes to the private sector's situational awareness. Feedback between the public and private sectors on what is useful or not can create a virtuous cycle, enabling companies to align their research and capabilities with public-sector priorities.
- **Information sharing modes are not aligned (yet):** Participants highlighted gaps in tooling and interoperability, as different actors rely on different platforms and formats for exchanging data. A common taxonomy is also needed to ensure all parties speak the same language when reporting incidents.

Programs like the CPP are important, as they support **trust building**, both between the private sector and ENISA, and among the partners that trust that information can be shared without it going necessarily public. Still, ENISA noted that asymmetries persist in current information sharing, underscoring the importance of more balanced, two-way exchanges between public and private actors across the EU.

Collaboration in times of crises: the EU blueprint for cyber crisis management in practice

Earlier this year, the EU blueprint for cyber crisis management was adopted. In a nutshell, the blueprint describes who does what in an EU-level cyber crisis.

The discussion pointed out the fact that the blueprint mentions the importance of cooperation with the private sector, but still it has a strong focus on EU-level networks and EU institutions. Yet, handling cross-border incidents requires participation of other actors as well, including from the private sector. The multitude of players can make the response to incidents challenging.

In general, panellists noted that **the private sector is involved in some of the activities of the EU-level networks**. For example, the European Union CSIRTs network (the CSIRTs

Network) is a network composed by Computer Security Incident Response Teams (CSIRTs) appointed by Member States and they are in touch with their local private sector constituency.

Still, panellists agreed that **it is important to focus not on the blueprint document in itself, but its actual implementation.** Simplification of processes are important, but can only be done to a certain extent as cross-border incidents are, by nature, complex.

It is therefore key that we make sure already now that the blueprint will work i*n practice,* to avoid improvisation when a crisis hits. This is already being done with the design and testing of Standard Operating Procedures, as well as multi-level exercises to promote seamless integration of EU-level coordination in national practices.

In this context, the topic of ways to involve the private sector and handling secrecy was raised. Some aspects that were underlined included:

- **Increasingly moving from pro-bono collaboration models to partnerships:** Establishing a privileged relation with EU companies and use partnership contracts to stimulate the EU economy. Even if cybersecurity is in the best interest of all, this could be a way to combine it with market stimulation.
- **Rethinking information classification and distribution:** The modern threat landscape is evolving rapidly, but practices for information classification and distribution have not been followed at the same pace. Information should be shared at the lowest level of classification possible, and, in general, classification and distribution of the same piece of information should change over time if conditions allow. This can help with information sharing to the public, but likely this will not affect real-time information sharing needs in times of crisis.
- **Integrate lessons learnt from on-going conflicts**: The Russian war of aggression against Ukraine has unfortunately raised the issue of information sharing between military and civilian actors. In some Member States, there is legal separation between the military and civil domains and hence legal barriers to sharing. It would be useful to already look at the sharing needs that are emerging in the Ukrainian context.

5. CONCLUSIONS

All panellists agreed that public-private collaboration is ever-more necessary in the current context. We need to assemble information to have visibility on the global context, and make sure that the right information has to be made available to the right parties.

There is the need to break down the siloes among communities that have been built in time of peace, while reminding us that the EU has strong cybersecurity community, and that partnerships can add value to both the public and private sectors.