Speaking points (~5min / 718 words)

- Members of the Houses of the Oireachtas[1], a chairde[2], I am very honoured to join you today at this meeting of the Joint Committee on European Union Affairs to speak to you about the European Union Cybersecurity Strategy and the European Commission's view on current and future challenges in the area of Cybersecurity.

- As President von der Leyen expressed in her 2021 State of the Union address on 15 September: "If everything is connected, everything can be hacked." Recent events have once again shown and reminded us that Europe, and more generally the world, remains vulnerable to cyber -attacks.

- This included, amongst others, the hacking of the Colonial Pipeline in the US, the Solarwinds incident as well as the ransomware attack on the IT-supplier Kaseya. And of course, as you all are well aware, the massive cyber-attack on the Irish Health Service Executive which hit critical parts of the healthcare system in midst of fighting a worldwide pandemic.

- We were following the developments closely with the Member States via our incident response teams and of course in particular with the Irish authorities.

- I would like to emphasize that, despite the severity of the attack, the coordination system at EU level seems to have worked well. The Irish authorities sought and received valuable support from the European Computer Security Incident Response Team CSIRT Network.

- According to the European Union Agency for Cyber Security, ENISA, attacks on our supply chains will increase fourfold in 2021 compared to last year. And attacks on cloud infrastructure have increased fivefold in one year.

---

[1] Irish name of the Parliamanet, pronunctiation: ERR-uhk-tuhss (-err as in merry)

[2] Irish for „dear friends", pronunciation: uh KHAHR-dyuh

- For exactly these reasons, the European Commission is firmly committed to ensure that all European citizens and businesses are well protected, both online and offline, against increasing cyber threats and incidents.

- Honourable members, digital transformation cannot succeed without cybersecurity. This is why, on 16 December 2020, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy, together with a revised Directive on measures for a high common level of cybersecurity across the Union, the so-called NIS-2 proposal.

- The EU Cybersecurity Strategy provides a fresh EU vision and plan for cybersecurity that is urgently required for the challenges of the digital age ahead of us.

- It aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies.

- Building upon the achievements of the past months and years, the strategy contains concrete proposals for regulatory, investment and policy initiatives in three main areas of EU action:

    1. Resilience, technological sovereignty and leadership
    2. Building operational capacity to prevent, deter and respond
    3. Advancing a global and open cyberspace through increased cooperation

- Each of these three pillars of EU activity is supported by concrete actions including new initiatives. I already mentioned the Commission's proposal for a revised NIS 2 Directive which is currently being negotiated in the European Parliament and the Council of the EU. We expect the Trilogues to start at the end of this or the beginning of next year.

- The NIS2 proposal raises the EU common level of ambition on cybersecurity through a wider scope, clearer rules and stronger supervision tools.

- The strategy also describes the role of a future Joint Cyber Unit, a hub potentially for all cyber communities to share information and coordinate collective response to major crises and incidents.

- Furthermore, the strategy sets out the establishment of new horizontal rules – i.e. common European cybersecurity standards for products and associated services placed on the internal market. As announced by President von der Leyen, this could also be achieved through legislation on common standards under a new European Cyber Resilience Act.

- Honourable members, Ireland is stronger in the Union and the EU is stronger with Ireland. I would therefore like to express my gratitude for the constructive and cooperative role Ireland has played so far in the various discussions we had on advancing cybersecurity across the EU.

- We will continue to listen carefully to the opinions expressed on this matter by the members of the Houses of the Oireachtas, the Irish Members of the European Parliament and the Irish representatives in the Council of the European Union.

- I have been honoured by your invitation to this meeting today and am looking forward to the discussions in the future.

- Thank you.