Oireachtas Joint Committee on EU Affairs - EU Digital Strategy. Speaking notes (5 minutes).

A chaothairligh, members of the Oireachtas Joint Committee on EU Affairs. I would like to thank you for your invitation to speak in front of you today. My name is Ciarán Cuffe and I am a Member of the European Parliament. As an MEP, I sit on the Parliament's Committee on Industry, Telecoms, Research and Energy which is the Committee that deals with issues relating to Cybersecurity. I will present you with a brief overview of the EU's recent Cybersecurity Strategy as well as touch upon some other topics which might be relevant. We've just come to the end of European *Cybersecurity Month*; the European Union's annual campaign dedicated to promoting cybersecurity among EU citizens and organisations.

EU Cybersecurity Strategy

In December 2020, the European Commission published a joint communication on the EU's cybersecurity strategy for the digital decade. The strategy aims to bolster Europe's collective resilience against cyber-threats, and ensure that all citizens and businesses can fully benefit from trustworthy and reliable services and digital tools. The Strategy included a proposal for the revision of the Directive on measures for high common level of cybersecurity across the Union (the Network and Information Security Directive or 'NIS 2') and a proposal for a new directive on the resilience of critical entities.

The original directive dating from 2016 has three parts which were aimed at promoting:

1. **National capabilities**: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT (Cyber Security Incident Response Team), perform cyber exercises, etc.

2. **Cross-border collaboration**: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT (EU Cyber Security Incident Response Team) network, the strategic NIS cooperation group, etc.

3. **National supervision of critical sectors**: EU Member states have to supervise the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure and finance sector), ex-post supervision for critical digital service providers (online market places, cloud and online search engines)

However, Member States were slow to fully implement this Directive and therefore the Commission proposed a revision in December 2020.

NIS 2 aims to strengthen EU cybersecurity capabilities, with proposals for information sharing and cooperation on cyber-crisis management at national and EU level. The directive on the resilience of critical entities provides for an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist and recover from disruptive incidents whatever their source. In fact, last Thursday I voted in the ITRE Committee in support of the revised Cybersecurity legislation. Within my group, the Greens EFA, we have supported topics such as promoting cybersecurity skills and pushing for an increased participation of women in the industry, but have also identified measures that could limit cyber-threats.

State of play in Europe

From January 2019 to April 2020, the EU's cybersecurity agency ENISA (EU Network and Information Security Agenda) reported 230,000 new malware infections every day, while this year, Europol highlighted a 'notable' increase in the number of ransomware attacks on public institutions and large companies. Europol's Internet Organised Crime Threat Unit stated that targeting such institutions allows cyber-criminals to increase the ransom amount and has noted a significant increase in attacks on governments, such as their healthcare and education, energy and transport systems. These cyber-attacks have targeted EU institutions and bodies, as well as Member States' critical infrastructure.

In May 2021, Ireland's HSE fell victim to a 'catastrophic' ransomware attack, which led to a shutdown of its ICT (Information and Communication Technology) system, with widespread cancellation of patient services. In the same month in Belgium there were two large scale cyberattacks against public service organisations. The first concerned Belnet, the network which serves third level institutions and research centres, as well as hospitals and federal ministries. The Federal Internal Affairs Department was subjected to a cyber-attack of such a scale that it has raised suspicions of the involvement of a foreign state.

In March 2021, the European Council adopted the cybersecurity strategy, highlighting a number of areas for action in the coming years, including the design of a network of security operational centres (SOCs) across the EU to monitor and anticipate signals of attacks on Member States, and a common cyber unit to provide clear focus to the EU's cybersecurity crisis management framework. The strategy also promotes the development of strong encryption standards, while also permitting law enforcement and judicial authorities to exercise their powers both online and offline with a view to preventing and countering cyber-attacks.

So what's in the new legislation?

The proposed revised NIS Directive has increased the EU national cybersecurity capabilities, requiring Member States to create a National Cybersecurity strategy, to establish Computer Security Incident Response Teams (CSIRTs) and to appoint national competent authorities for Cybersecurity. It also aims to improve the cyber resilience of public and private entities in specific sectors and across digital services. In order to respond to the growing threats due to the increase in cyberattacks, the proposed revised Directive broadens its old scope, aiming to:

- strengthen the security requirements of Member States
- Address the security of supply chains
- streamlining reporting obligations,
- introducing more stringent supervisory measures and stricter enforcement requirements including harmonised sanctions regimes across Member States.
- It also includes proposals for information sharing and cooperation on cyber crisis management at national and EU level.

Cybersecurity and consumers

A lot of burden is put on the users of electronic devices but they lack sufficient information about their own cybersecurity. We tell our children not to get into a car with a stranger, but we need to ensure we don't click on a link that we don't recognise. Basic cybersecurity practices are not yet part of the educational establishments curricula. In NIS2, the Greens/EFA have pushed for increasing this at Member State and EU level.

The assessment of security of devices is especially important since many security incidents happen because of insufficient security measures being built into devices. We have repeatedly pointed out that things connected toys, connected cameras, and many other consumer connected devices sometimes lack basic security features like a password or encrypted communication. This makes them easy targets in denial of service attacks that can bring down health systems or other essential entities. To that regard we have called for minimal cybersecurity requirements for goods to be checked before they are put on the market.

Cybersecurity and enhancing privacy:

It must be noted that many in the security industry see the secret of communication and privacy as mere obstacles in the way of their research and activities. The Greens/EFA have argued that encryption is a necessary tool to enhance privacy, thus preserving a fundamental right, but also a barrier for attackers trying to steal data, therefore it brings additional economic and security benefits. As a consequence in the NIS 2 revision, we promoted the implementation of security by design and by default and enhanced encryption use together with including encryption requirements and the use of open source cybersecurity products.

As a general rule when it comes to Cybersecurity, we are only as strong as the weakest link. And speaking of weakest link, without naming and shaming some member states, we need to recognise that the investments in cybersecurity are uneven and so are the measures that are being implemented. If cyber-criminals were able to attack an essential infrastructure as important as our health system, it means that they could attack our energy supply or our national telecommunications framework. Now is the time to invest in our National Cyber Security Centre and increase our cooperation with other EU Member States to ensure we are prepared for the next cyberattack.

Links

Explainer on the NIS2

Improving the common level of cybersecurity across the EU

PR: European Commission New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient