Cybersecurity

Main messages

Ransomware

- We need to apply a holistic approach to the global fight against ransomware, allowing law enforcement to jointly investigate ransomware threats, countering illicit finance and the possibility for cyber-criminals to monetise ransoms as well as implementing specific resilience actions for ransomware.
- Moreover, strong internal action should ensure that nations are not cooperative towards cybersecurity criminals, allowing them to operate from their territory.
- On 22 June 2021, [redacted] and Commissioner for Home Affairs Ylva Johansson agreed to create a working group dedicated to ransomware issues focusing on law enforcement. The kick off meeting of took place in November 2021.
- The private sector plays an important role. Public-Private Partnerships (PPPs) to fight cybercrime are essential given the fact that the cyberspace infrastructure is overwhelmingly held by private companies located under different jurisdictions.
- We acknowledge that the private sector needs incentives to improve its own security and to coordinate more effectively with national authorities and with each other. The Commission supports the establishment of PPPs under the Internal Security Fund.

NIS2 – revised Network and Information Security (NIS) Directive:

- Legislative deliberation started in January 2022 and has concluded with the last trilogue on 12 May 2022.
- EU legislators have paid particular attention to the alignment between the NIS2 and the Digital Operation Resilience Act (DORA) proposals.

Resilience of critical entities:

- The Commission proposed a Directive on resilience of critical entities in December 2020, which is currently being negotiated between the Council and Parliament.
- The proposal would set up a new framework to ensure that critical entities in key sectors become more resilient against threats such as accidents, terrorist attacks, floods, fire or droughts. They shall be able to continue providing essential services in, and quickly “bounce back” into operations in case of a disruption or an incident.

Cyber Resilience Act (CRA):

- In the second half of this year, the Commission will propose legislation on common standards for digital products under a new European Cyber Resilience Act.
- The Act will set out horizontal cybersecurity requirements for digital products and ancillary services (hardware, but also ‘intangible’, like non-embedded software).

Joint Cyber Unit:

- In June 2021 we launched the process establishing a Joint Cyber Unit ensuring a coordinated response to incidents and cyber-enabled crises across the Union. The Joint Cyber Unit, once operational, could allow European crisis managers and IT experts to structurally cooperate with the US on crisis management.

- Information sharing and cooperation are key to successfully preventing and combating cybersecurity threats. The proposed Joint Cyber Unit would bring together different EU cybersecurity communities, defence, civilian, law enforcement and diplomacy. As we discovered with the COVID-19 pandemic, in order to respond to a cross-border crisis, we need to rely on all available experts, crisis managers and equipment.

Security Operations Centres (SOCs):

- We believe that Security Operations Centres can play a vital role in the constant and comprehensive supervision of cyber-space, the primary way to detect cyber threats and attacks. By relying on artificial intelligence and machine learning techniques, these Centres can detect the signs of a cyber attack early enough to allow proactive action.
- The Commission has proposed to improve the existing Security Operations Centres and create new ones. Linking them in a network, we will establish an EU cyber shield.
- In 2021-2022, EUR 110 million will be dedicated to SOCs.

Cybersecurity Competence Centre and Network:

- In order to better protect ourselves against cyber-attacks, it is also crucial to increase and better target our strategic public and private investments in cybersecurity. This will be the key task of the Cybersecurity Competence Centre in Bucharest.
- The Centre will establish a strategic agenda for technology development, in close collaboration with industry and the academic community.
- In addition, the Centre is responsible for the implementation of the cybersecurity funds of the Digital Europe and Horizon Europe programmes. This should, with the support of the private sector, generate funding of up to EUR 4.5 billion in cybersecurity by 2027.

EU funding in cybersecurity under EU programmes:

- The Commission is aware of the need for ambitious investments. Funding for cybersecurity in the 2021-2027 EU budget is under the Digital Europe Programme, and for cybersecurity research under Horizon Europe. This amounts to close to EUR 2 billion, which will be complemented by Member States and industry investment.
- Investments in the digital technology supply chain should be at least 20% of the Recovery and Resilience Facility, or EUR 134.5 billion out of EUR 672.5 billion.
- The EU is also stepping up its offer to its partners with major investments in infrastructure development through the EU Global Gateway. Between 2021 and 2027, the EU will mobilise up to EUR 300 billion of investments in digital, climate and energy, transport, health, education and research.
- Under NDICI-Global Europe, with an overall budget of EUR 79 billion, investments in building connections are expected to rise significantly. It has a 35% spending target for climate actions and an additional 10% approximately of the total funding will be dedicated to digital actions.

Background

Ransomware

The European police agency (Europol) is supporting ransomware investigations and, with private sector partners, runs the 'No More Ransom' campaign to increase awareness among companies and supply victims with decryption tools.

Increased threats, accompanied by high profile attacks impacting essential sectors across the Union, has led G7 leaders to commit to action on ransomware last year and the EU to launch a joint initiative with the United States.

Contacts – briefing contribution: [redacted]