EEF.DEL/13/19
29 January 2019

ENGLISH only

The Updated Cyber Landspace in the European Union *for the Trusted Digital Single Market*

Radoslav Repa

Permanent Representation of the Slovak Republic
to the European Union in Brussels

January 2019

PAST STRATEGIES – 2013 & 2015

EU Cyber Security Strategy (2013)
outlined the principles which guided the EU action in 5 priorities:

1. increasing cyber resilience;
2. reducing cybercrime;
3. extending EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
2. developing the industrial and technological resources for cybersecurity;
3. establishing a coherent international cyber policy of the EU and promoting core EU values

Main objectives:
- Increasing cybersecurity capabilities and cooperation
- Making the EU a strong player in cybersecurity
- Mainstreaming cybersecurity in EU policies

European Agenda on Security (2015)
focusing mainly on fight against the **cybercrime** through fostering implementation of **existing policies on cybersecurity**, focusing on **attacks against information systems and** combating **child sexual exploitation**.

- reviewing legislation on **combatting fraud and counterfeiting of non-cash means of payments** *against fraudulent use of credit card details or other electronic means of payment (the directive was politically approved in 12/2018);*
- reviewing **obstacles to criminal investigations** on cybercrime, notably *on issues of competent jurisdiction and rules on* ***access to evidence*** *(new draft legislation issued in 4/2018, under discussion);*
- **enhancing cyber capacity building**

Key deliverable:

Directive on security of network and information systems (NIS Directive)

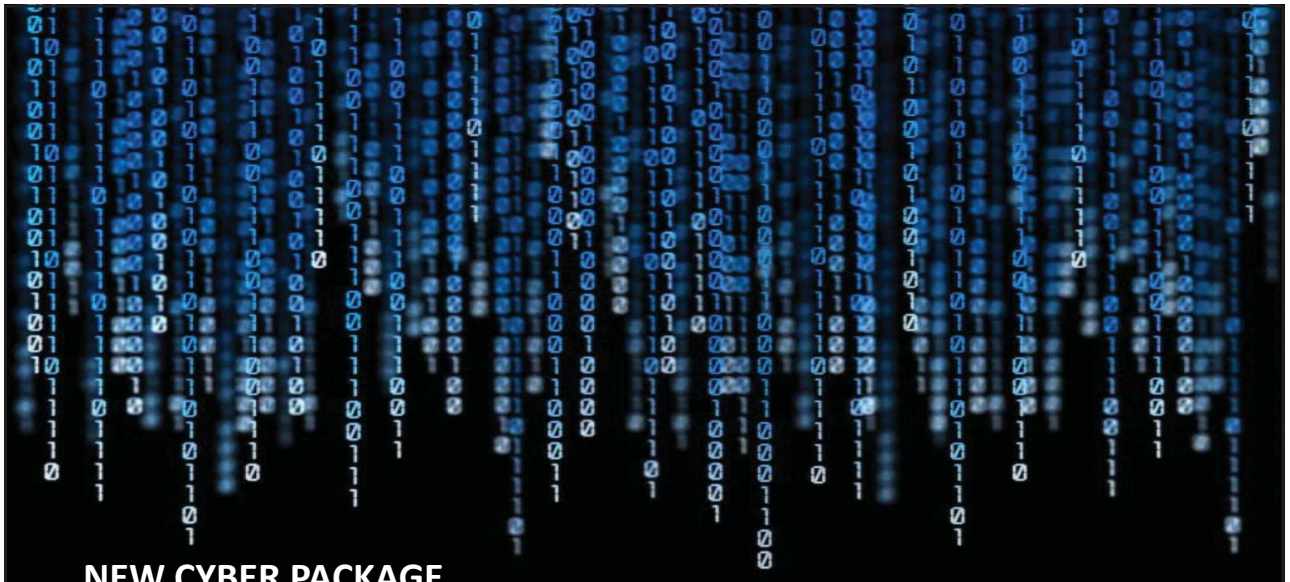
The first EU-wide law aiming at ensuring a high common level of cybersecurity in the EU was adopted in 2016. By 5/2018 Member States should have transposed it into their national laws.

Other **important pieces of legislation:**

- **Directive on attacks against information systems** *(2013) aims to tackle large-scale cyber attacks by obliging Member States to strengthten their national cybercrime laws and introduce more effective criminal sanctions;*
- **Payment Services Directive (PSD2)** *from 2015 seeks to improve the existing EU rules for electronic payments. It takes into account emerging and innovative payment services, such as internet and mobile payments (in force from 1/2018);*
- **General Data Protection Regulation (GDPR)** *from 2016* ***d****eals with the personal data protection while setting the highest possible standards (in force from 5/2018);*

Digital Single Market Strategy (DSM) from 2015 and 2017 (revision)

- Completing a Digital Single Market could contribute **€ 415 billion per year** to Europe's economy, create jobs and transform our public services to digital era;
- An inclusive DSM offers opportunities for citizens, as enhanced use of digital technologies can improve their access to information and content, better undertaking or improve their job opportunities. It can promote modern open government. Proper digital skills are needed!
- More than 44 proposals where 24 are legislative ones *(almost accomplished and delivered);*
- **3 Pillars:**
  - **Better access for consumers and businesses to digital goods and services across Europe;**
  - **Creating the right conditions for digital networks and innovative services to flourish;**
  - **Maximising the growth potential of the digital economy;**
- In order to ensure a fair, open and secure digital environment, the revised 2017 DSM focused on **online platforms, European Data Economy** *(Free Flow of Data, Platforms to Business)* and on **cybersecurity assets of Europe** (a new CyberSecurity Act and Strategy)



NEW CYBER PACKAGE
FOR THE UPDATED CYBERSECURITY LANDSPACE IN EU 9/2017

THE EU REGULATORY FRAMEWORK IN CYBER? WHY?

- Aims to increase the **cybersecurity capabilities and resilience** on the level of Member States;
- Aims to optimize and broaden the **cyber cooperation** and collaboration among MS;
- Aims to establish the EU as a **strong, trustworthy player** in the global cyberspace;
- Aims to establish the „Security by Design“ approach in all policies and programmes;

- Cross-border character of the cyber attacks and incidents
- More data and services available through the electronic communication networks
- More interdependencies and interrelations of the digital infrastructures
- **Dependence on foreign security technologies developed outside the Union**
- European critical infrastructures protection based on risk
- The **national „silo“** approach of Member States to the cybersecurity is not sufficient and in the EU internal market may be considered as the weakest link in a chain

A REVISED CYBERSECURITY STRATEGY (2017)

BUILDING STRONG CYBERSECURITY FOR THE EU:
RESILIENCE (I), DETERRENCE (II) AND DEFENCE (III)

I.) Building EU Resilience to cyber attacks

- **NIS Directive (2016) implementation** *(no. 1 objective in the Council Conclusions in 11/2017)*
- **Reinforced and restructured ENISA** *(a new EU Cybersecurity Act politically agreed in 12/2018)*
- **Established joint EU cybersecurity certification framework** *(a part of EU Cybersecurity Act, improving trust in the internal market and „quality label“)*
- **Rapid emergency response and crisis management** *(reinforced tools and a new emergency fund)*
- **European Cybersecurity Competence Centre and the Network of National Coordination Centres** *(draft regulation introduced in 9/2018, under discussion. Helping the EU retain and develop the cybersecurity technological and industrial capacities necessary to secure its DSM. Increasing the competitiveness of the EU's cybersecurity industry by 2 bil. EUR)*

BUILDING STRONG CYBERSECURITY FOR THE EU: RESILIENCE (I), DETERRENCE (II) AND DEFENCE (III)

II.) Creating effective EU cyber deterrence

- **Identifying malicious actors** *(capacity to identify perpetrators, uptake of IPv6)*
- **Strenghtening the law enforcement response** *(cybercrime´s effective investigation and prosecution, cross-border access to electronic evidence, traceability and attribution, common standards, an improved forensic capability of Europol, role of encyption)*
- **Stepping up the public-private cooperation against cybercrime** *(e.g. between financial institutions and law enforcement bodies against online frauds)*
- **Strenghtening the EU political response** *(a framework for a joint EU diplomatic response to malicious cyber activities – a part of Common Foreign and Security Policy, restrictive measures may be applied, a major issue - attribution)*
- **Improving Member States deterrence and defense capabilities** *(synergies between military and civilian efforts to cyber defense and cybersecurity approaches, PESCO, encouraging the EU strategic autonomy – a part of Common Security and Defense Policy)*

BUILDING STRONG CYBERSECURITY FOR THE EU: RESILIENCE (I), DETERRENCE (II) AND DEFENCE (III)

III.) Strengthening international cooperation on cybersecurity

Fueled with the EU core values and fundamental rights (freedom of expression, right to privacy and protection of personal data, promotion of the open, free, stable and secure cyberspace). International law in cyberspace.

- **Cybersecurity in external relations** *(prevention and deterrence of cyber-attacks, strategic framework for conflict prevention and stability in cyberspace, cyber dialogues with the third countries, CBM)*
- **External cybersecurity capacity building** *(help for training, policy, legislation development efforts, CERTS and cybercrime units, development cooperation – D4D approach, setting up of a EU Cyber Capacity Building guidelines)*
- **EU-NATO Cooperation** *(coordinated exercises, interoperability of cybersec standards)*

EU CYBERSECURITY CERTIFICATION NETWORK

If we want our joint cybersecurity market to flourish in the EU, we need to increase trust in digital products, services and systems.

- Current European system (no single model) lacks mutual recognition, it´s widely fragmented resulting in the limited use of cross-border market potential *(several isolated systems between some Member states have been built so far, hard to compare);*
- The idea is to build one joint system (framework) where the ICT products and services certified by one country will be valid across the whole EU *(certificates would remain voluntary with a possibility to introduce mandatory certification schemes if necessary; more cyber resilience, more product/service information on security, more trust in the market);*
- Cybersecurity certification schemes should be adopted by the European Commission based on the prepared candidate scheme by ENISA in cooperation with Member States *(after consulting stakeholders)*

DIGITAL EUROPE PROGRAMME 2021-2027

5 key policy areas: **High-performance Computing, Cybersecurity, Artificial Intelligence, Advanced Digital Skills** and best use of **Digital Capacities** and **Interoperability**

Total (draft) budget of 9.2 bil. EUR where **for cybersecurity = 2 bil. EUR**

Now a draft proposal of legislation – a subject of the joint EU´s future budget agreement

- EU's cybersecurity **capacity** is going to be reinforced to gain the necessary capacities to protect its citizens and businesses from cyber threats. Consumers will be protected when using **connected products that can be hacked and their safety compromised.**
- **Trust is a prerequisite for the Digital Single Market to work well.** Cybersecurity technologies such as digital identities, cryptography or intrusion detection, and their application in areas such as finance, industry 4.0, energy, transportation, healthcare, or e-government are **essential to safeguard the security and trust of online activity and transactions by both citizens, public administrations, and companies.**

WHAT WILL BE SUPPORTED?

- The best use and deployment of **cybersecurity knowledge, capacities, culture and skills** for **public admnistrations** and for **industries**;
- Wide deployment of the latest **effective state of the art cybersecurity solutions** including advanced **cybersecurity equipment, tools** and **data infrastructures** *(i.a. quantum facilities, IoT, data, situational awareness, etc.*)
- Certification of products and services that reinforce cybersecurity and trust within the DSM. *This includes **strengthening** security and safety for products**, from their design to their commercialisation**.*
- Closing the **cybersecurity skills gap** by aligning cybersecurity skills programmes to specific sectorial needs and facilitating access to targeted specialised training courses

Thank you for your attention

Any questions?

radoslav.repa@mzv.sk