AmCham

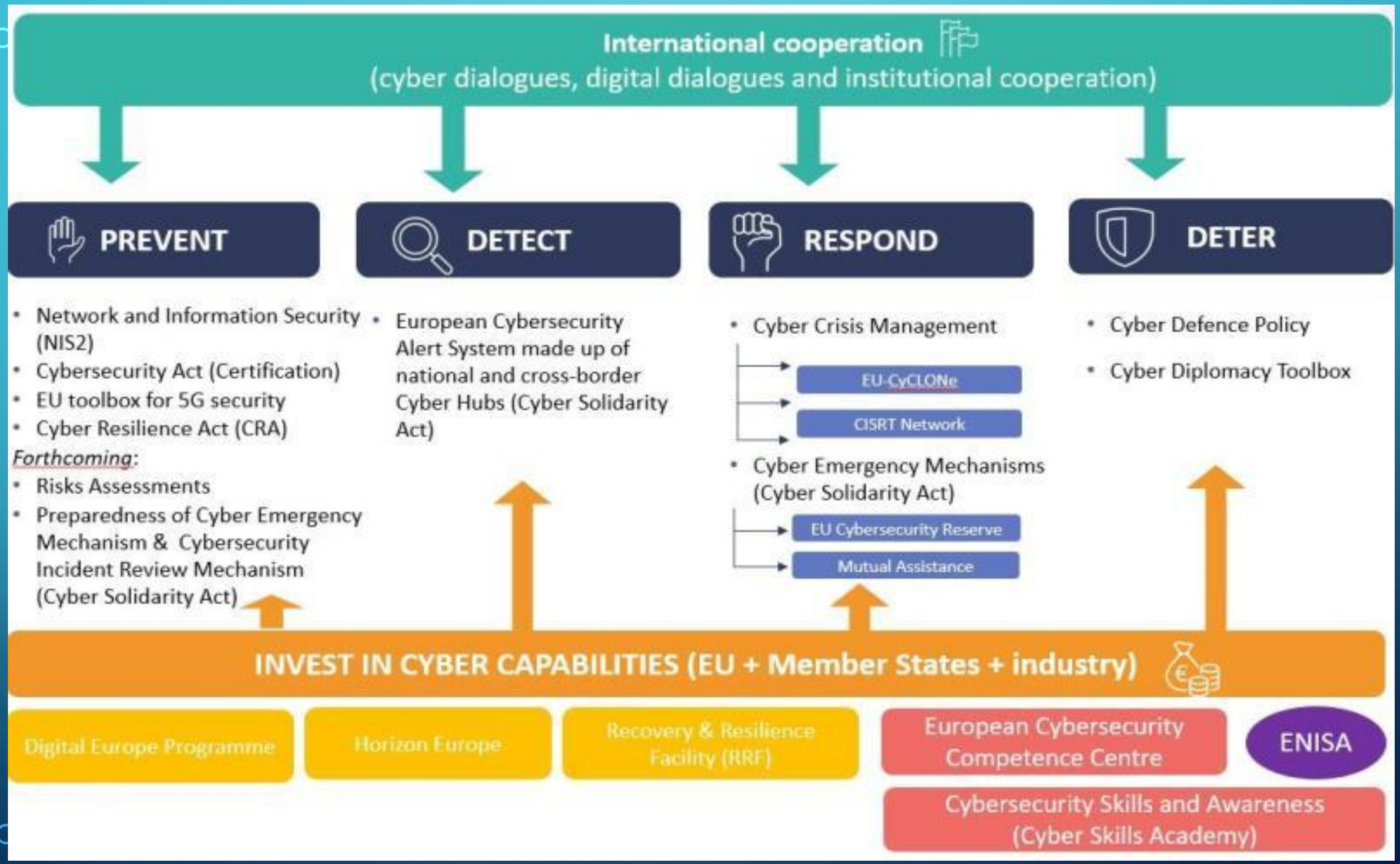
April 10, 2025

Cyber Resilience & EU Policy: What Businesses Need to Know?

Tamara Tafra, Advisor in the Cabinet of the Minister
Ministry of Foreign and European Affairs

THE HITCHHIKER'S GUIDE TO THE CYBER GALAXY

AMCHAM 2025


International cooperation
(cyber dialogues, digital dialogues and institutional cooperation)
PREVENT
DETECT
RESPOND
DETER
Network and Information Security (NIS2)
Cybersecurity Act (Certification)
EU toolbox for 5G security
Cyber Resilience Act (CRA)
Forthcoming:
Risks Assessments
Preparedness of Cyber Emergency Mechanism & Cybersecurity Incident Review Mechanism (Cyber Solidarity Act)
European Cybersecurity Alert System made up of national and cross-border Cyber Hubs (Cyber Solidarity Act)
Cyber Crisis Management
EU-CyCLONe
CISRT Network
Cyber Emergency Mechanisms (Cyber Solidarity Act)
EU Cybersecurity Reserve
Mutual Assistance
Cyber Defence Policy
Cyber Diplomacy Toolbox
INVEST IN CYBER CAPABILITIES (EU + Member States + industry)
Digital Europe Programme
Horizon Europe
Recovery & Resilience Facility (RRF)
European Cybersecurity Competence Centre
ENISA
Cybersecurity Skills and Awareness (Cyber Skills Academy)

EU CYBERSECURITY STRATEGY (2013, 2017 & 2020)

Guidelines for EU cybersecurity policies including legislation

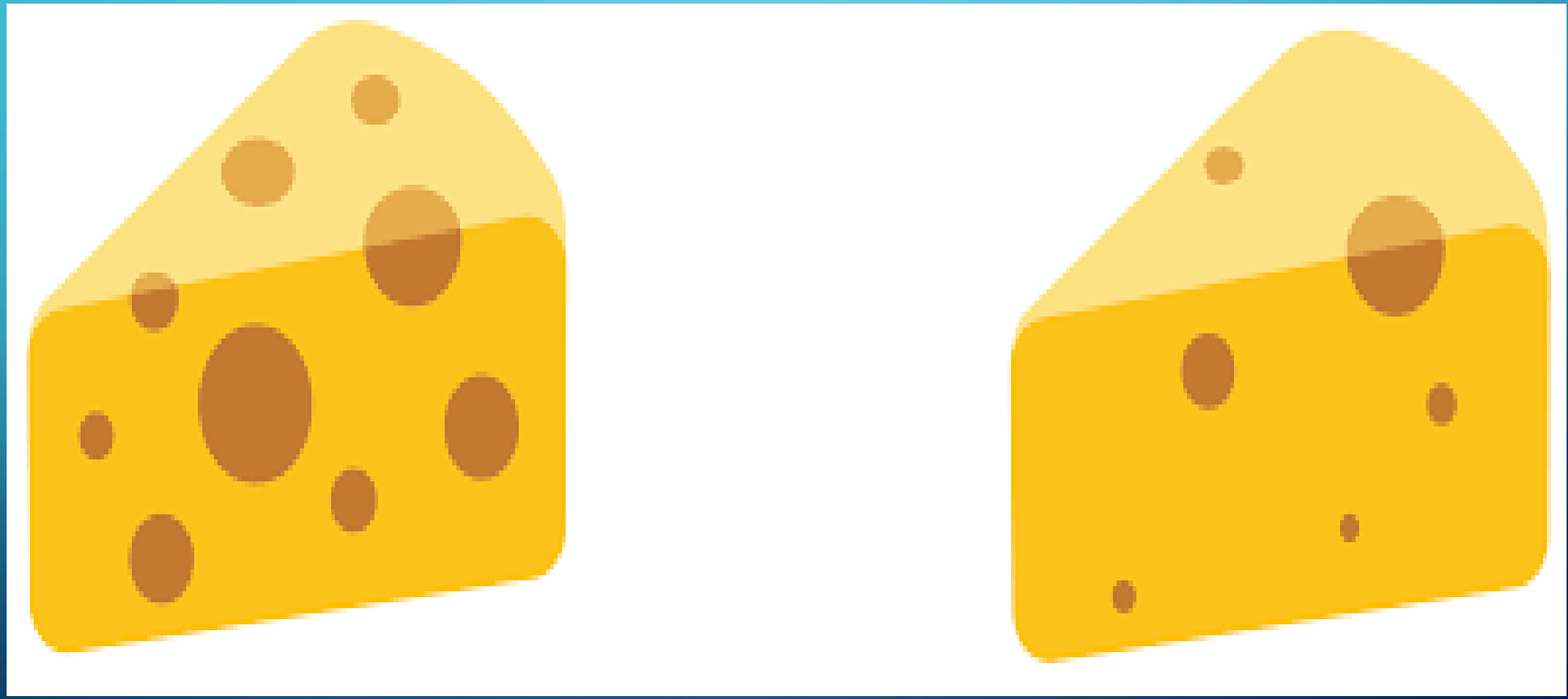
Three areas of action:

1. Resilience, technical sovereignty and leadership;
2. Operational capacities for prevention, deterrence and response;
3. International cooperation

Next strategy – 2025

Additional guidelines: State of the Union (September) + European Commission Work Programme (October)

EU CYBER LEGISLATION



NIS 2 DIRECTIVE

The EU rules on cybersecurity introduced in 2016 (NIS1 Directive) were complemented by the NIS2 Directive, which entered into force in 2023 (transposition deadline: 18/10/2024).

It contains key elements that all businesses must address or implement as part of the measures they take, including incident handling, supply chain security, vulnerability handling and vulnerability detection, use of cryptography.

NIS2 COMPLIANCE ROADMAP

17.10.2024 first implementing rules on cybersecurity of critical entities and networks under the NIS2 Directive - cybersecurity risk management measures, as well as cases in which an incident should be considered significant and companies providing digital infrastructures and services should report it to national authorities (*DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, trust service providers*)

CROATIA – IMPLEMENTATION OF NIS2

- Croatian Cybersecurity Act – entered into force 15 February 2024
- Regulation on Cybersecurity – November 2024
- 13 cybersecurity risk-management measures (technical, administrative, procedural and human)

- criteria for the classification of essential and important entities;
- cybersecurity requirements for essential and important entities;
- implementation of cybersecurity audits and cybersecurity self-assessments;
- voluntary cyber protection mechanisms;
- strategic planning and decision-making framework, as well as national frameworks for managing large-scale cybersecurity incidents and crises;
- expert supervision over the implementation of cybersecurity requirements and infringement provisions

CYBER RESILIENCE ACT (CRA)

DECEMBER 2024

Target:

- ensure that manufacturers improve the safety of products with digital elements from the design and development phase and throughout their life cycle;

- ensure a consistent cybersecurity framework that facilitates compliance for hardware and software manufacturers;

- increase the transparency of the safety features of products with digital elements and enable businesses and consumers to use products with digital elements safely.

- introduces mandatory cybersecurity requirements at EU level for the design, development, manufacture and maintenance of hardware and software products;
- The Regulation applies to products with digital elements that have been made available on the market and that are therefore supplied for distribution or use on the Union market in the course of a commercial activity;
- software and hardware products will bear the CE mark to indicate that they comply with the requirements of the Regulation

CYBER SOLIDARITY ACT (CSOA)

FEBRUARY 2025

Objective - to strengthen the EU's capacity to detect, prepare for and respond to significant cybersecurity threats and large-scale attacks through:

- the establishment of a European Cybersecurity Alert System, consisting of a network of national and cross-border cyber centres;

- the establishment of an Emergency Mechanism that will improve preparedness and response capacity to major and large-scale cyber incidents (coordinated testing, reserve and mutual support);

- the establishment of a Cybersecurity Incident Review Mechanism with a view to assess and review specific cybersecurity incidents and make recommendations to improve the EU's cybersecurity posture.

CYBER SECURITY ACT (CSA & CSA+)

JUNE 2019 & JANUARY 2025

- a new mandate for ENISA (the EU Agency for Cybersecurity);
- establishing a framework for (voluntary) cybersecurity certification of ICT products, services and processes at EU level. The certification framework will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures.

The planned revision of the CSA will be in 2025.

CSA+

Possibility to adopt European certification schemes for managed security services covering areas such as incident response, penetration testing, security audits and consultancy. This will help provide a framework for the establishment of trusted service providers in the EU Cybersecurity Reserve under the Cyber Solidarity Act.

CERTIFICATION

- EUCC - Common Criteria-based cybersecurity certification scheme
- EUCS -European Certification Scheme for Cloud Services
- EU5G - European Cybersecurity Certification Scheme for 5G

Planned – Scheme for *Managed Security Services*

In consideration - Scheme for AI

EUROPEAN CYBERSECURITY COMPETENCE CENTER FOR INDUSTRY, TECHNOLOGY AND RESEARCH (ECCC)

MAY 2021

- facilitate the development of cyber infrastructures at the service of the economy, in particular SMEs, research communities, civil society and the public;
- the Union's main instrument for pooling investments in cybersecurity research, technology and industrial development, as well as for the implementation of relevant projects and initiatives, together with the Network of National Coordination Centres;
- manage financial support for cybersecurity from Horizon and Digital Europe (DEP).

FUNDING

- Digital Europe Programme (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital)
- Horizon Europe
- https://cybersecurity-centre.europa.eu/funding-opportunities_en
- https://nks.hr/natjecaji/

EU & USA

- Regular cyber dialogues
- Cooperation between DG CNECT, ENISA and CISA
- Joint CyberSafe Products Action Plan (*mutual recognition of cybersecurity labelling programs and regulations for IoT devices*)
- Counter Ransomware Initiative

THANK YOU!

tamara.tafra@mvep.hr