CyBureau
The Cyber Empowerment Center

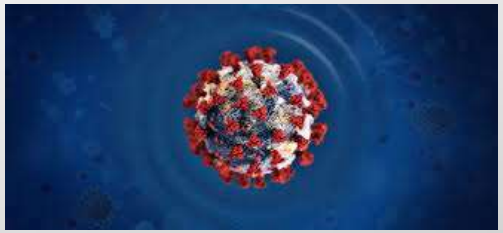
Cybersecurity Policies addressing new cybersecurity challenges

Associate Professor Nineta Polemi
University of Piraeus, Dept. of Informatics

Disclaimer: The views in this presentation represent ONLY the presenter

COVID: THE BIGGEST CYBERSECURITY THREAT IN HISTORY - REVEALED OUR VULNERABILITIES

- INCREASE OF E-TRANSACTIONS (PAYMENT CERTIFICATION, SECURE RECONCILIATION, ANTI MONEY LAUNDERING, FRAUD PROTECTION, PII PROTECTION)
- CONTINUOUS TELECONFERENCING (PII PROTECTION, CONFIDENTIALITY, SECURE AUTOMATED MINUTES EXTRACTION AND STORAGE, RELIABLE VIDEO STREAMING, VIDEO/AUDIO QUALITY BOOST)
- USAGE OF COLLABORATION PLATFORMS (LUCK OF TRACKING TOOLS)
- E- ENTERTAINMENT (VIDEO/MUSIC STREAMING, ONLINE GAMING)

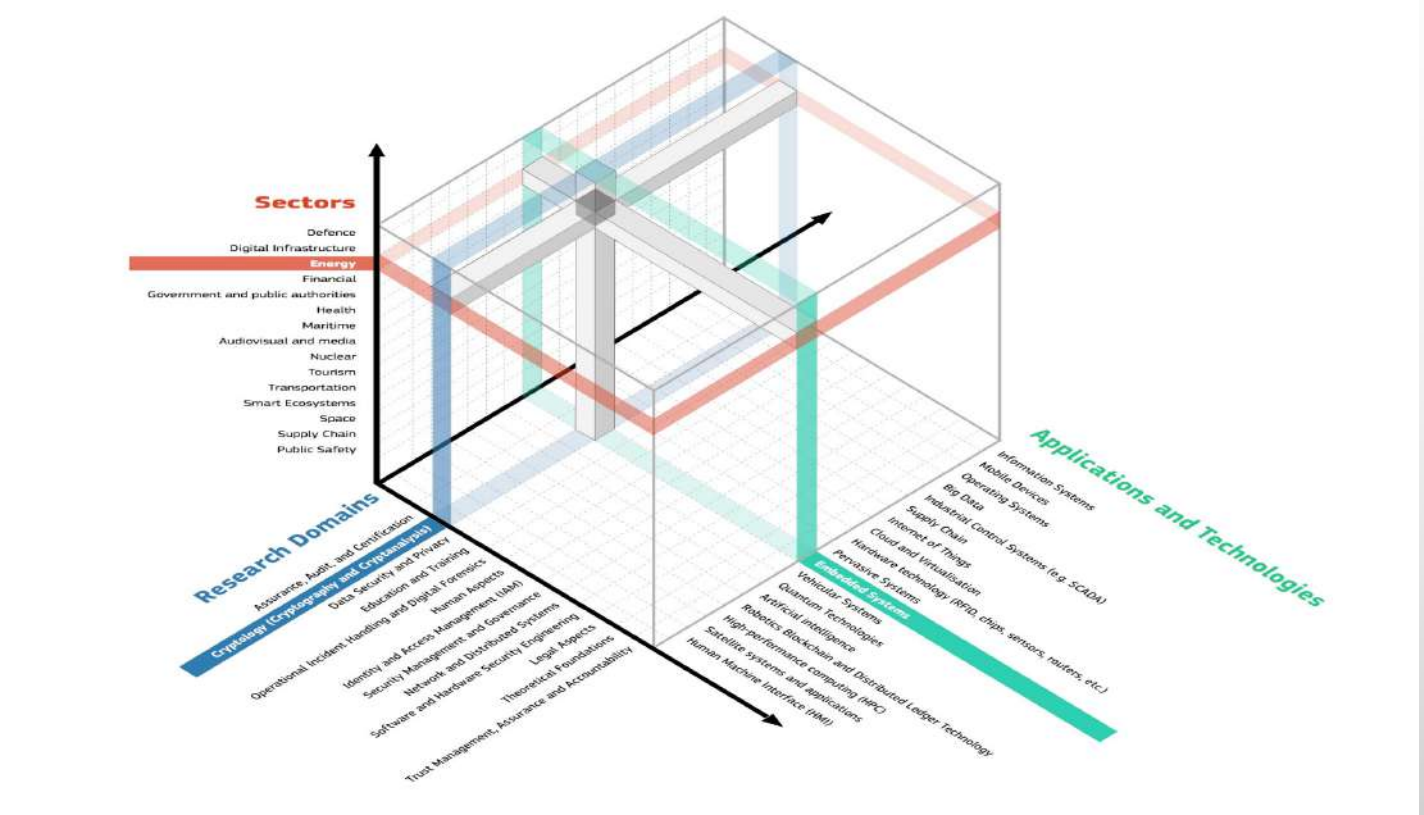


238% rise in attacks on banks 630% rise in cloud services, Phishing attempts rose 600% (Fintech news)

A SYSTEMATIC APPROACH

i. IDENTIFY **GOALS** & OBJECTIVES (RESEARCH, POLICY, TECHNOLOGICAL, INDUSTRIAL, SOCIETAL,…)

I. ADOPT A **TAXONOMY** FOR CYBERSECURITY DIMENSIONS (E.G. DOMAINS, SECTORS, TECHNOLOGIES)



I. IDENTIFY **CYBERSECURITY CHALLENGES** THAT ARE STUMBLING BLOCKS FOR REACHING THE GOALS

CHALLENGE I: SECURE CRITICAL INFORMATION INFRASTRUCTURES (CII)

NIS DIRECTIVE

GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

- NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIS-RT)
- NATIONAL NIS STRATEGY
- NATIONAL NIS AUTHORITY

COOPERATION

Increased EU-level cooperation

- EU MEMBER STATES COOPERATION GROUP (STRATEGIC)
  - EU MEMBER STATES; EUROPEAN COMMISSION; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY
- EMERGENCY TEAMS (CSIRTS) NETWORK (OPERATIONAL)
  - EU MEMBER STATES; CERT-EU; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

- SECURITY MEASURES
- NOTIFICATION OF MAJOR INCIDENTS

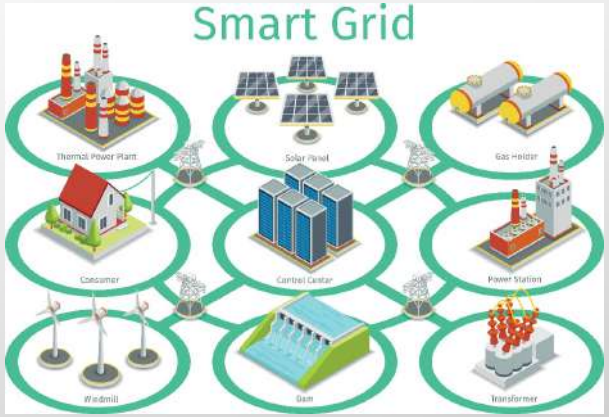
SECTORAL CYBERSECURITY POLICIES

Space Strategy for Europe 2016/2325(INI

EU Maritime Security Strategy (EUMSS)

Common Security and Defence Policy –CSDP-, Decision No 541/2014/EU)EC

EC recommendation of cybersecurity of 5G networks



EC recommendation on cybersecurity in the energy sector COM(2019)

Challenge II: Digital sovereignty

Bureau
yber Empowerment Center

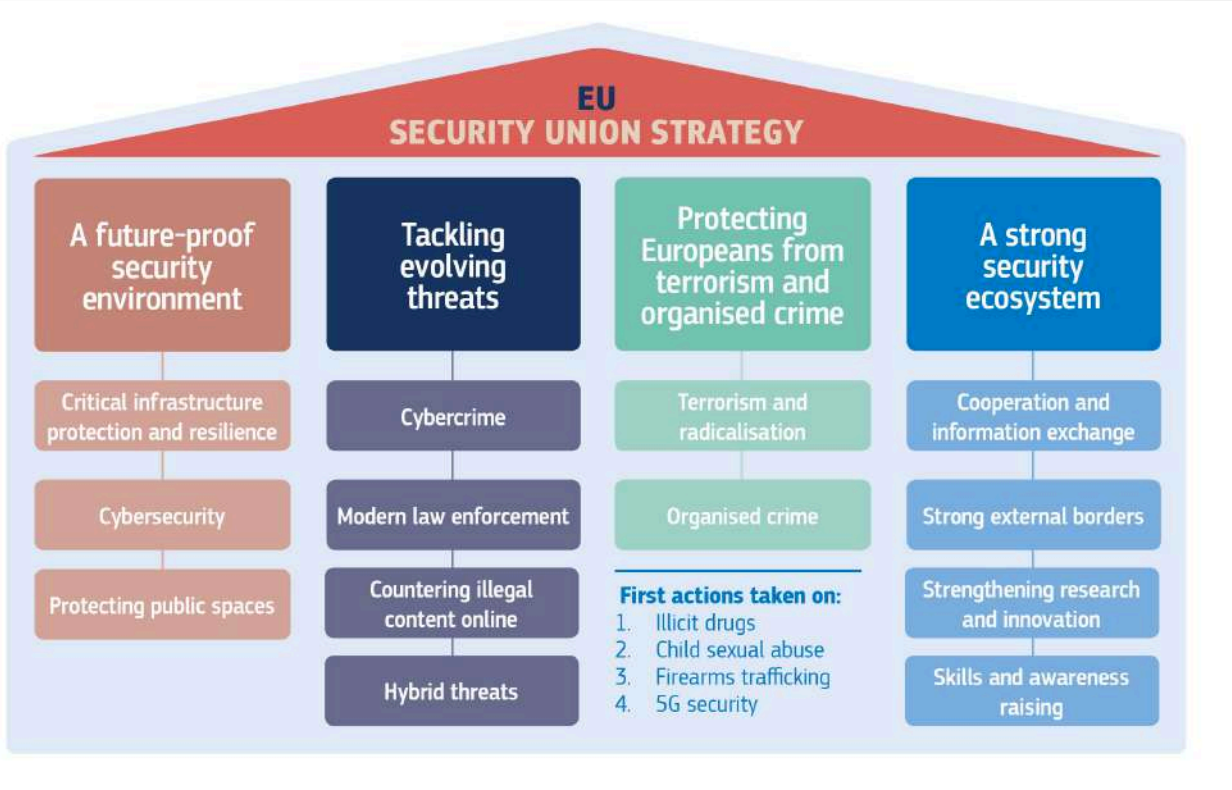
- Security/Privacy
- Accountability
- Duty of Care
- Trustworthy supply-chains

GDPR (General Data Protection Regulation) states that data is also vulnerable to accidental or unlawful destruction, loss or disclosure

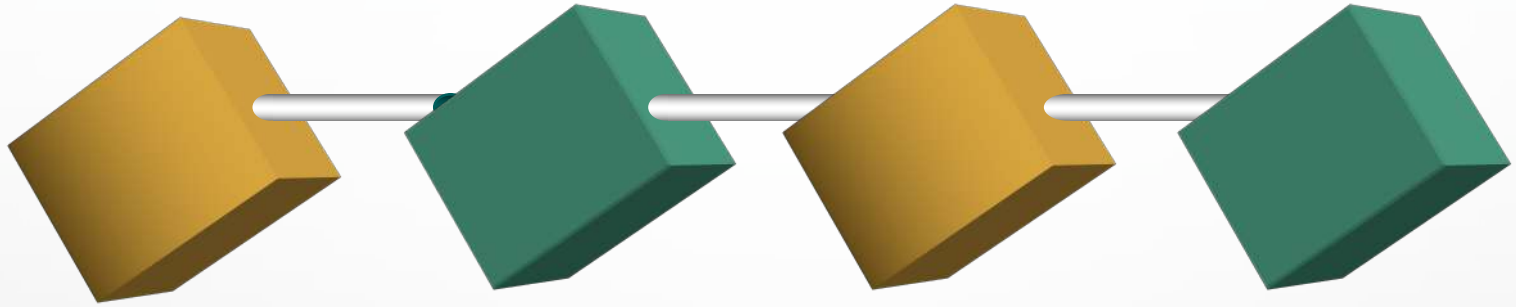
Liability for defective products Directive 85/374- Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics

On EU Security Union Strategy 2020

NIS II (under way)



CHALLENGE III: TRUSTWORTHY EU CYBERSECURITY TECHNOLOGIES



- ✓ Privacy
- ✓ Security
- ✓ Accountability

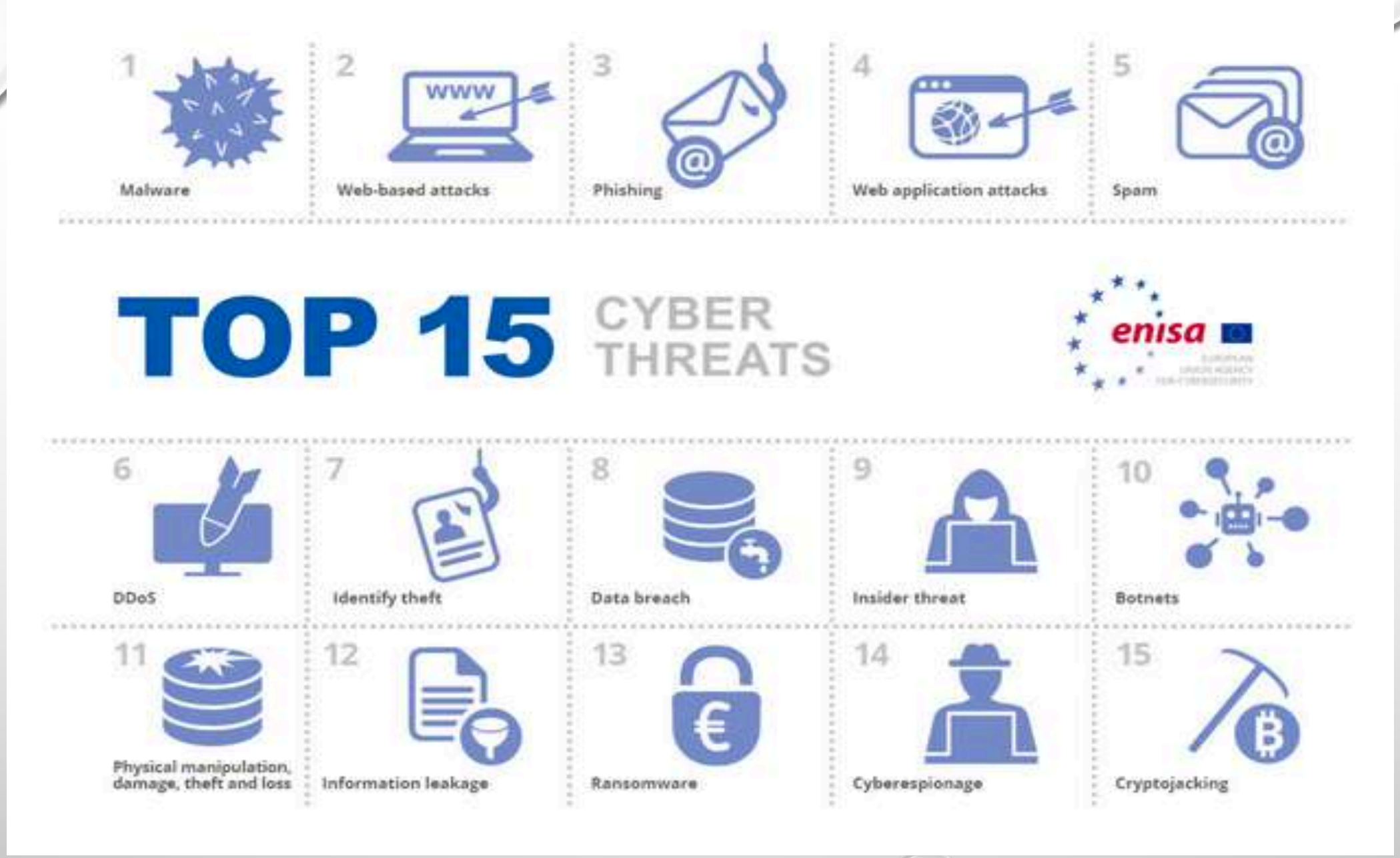
by design

- ✓ Robust
- ✓ Dynamic
- ✓ Resilient
- ✓ Autonomous

(independent of non EU components)

- ✓ Ethical,
- ✓ non bias
- ✓ human centric
- ✓ democratic

Self-
- ✓ healing
- ✓ management
- ✓ recovery



Sources:

ENISA Threat Landscape 2020

ENISA Sectroral thematic threat analysis, 2020

EUROPEAN
COMMISSION

Brussels, 13.9.2017
COM(2017) 477 final

2017/0225 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

(Text with EEA relevance)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

- ENISA Reform
- An **EU Agency for Cybersecurity**
- Stronger Mandate
- Permanent Status
- Adequate Resources

EU Cybersecurity Certification Framework

- One framework, many schemes
- Certificates valid across all MS
- Roles for MS and ENISA
- Voluntary and risk-based approach; any need for mandatory schemes to be identified

TECHNOLOGY RELATED SECURITY POLICIES

EU COORDINATED PLAN IN ARTIFICIAL INTELLIGENCE

EU REPORT ON THE SAFETY AND LIABILITY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE, THE INTERNET OF THINGS AND ROBOTICS, COM(2020)

ENISA GOOD PRACTICES FOR IOT AND SMART INFRASTRUCTURES TOOL

…..

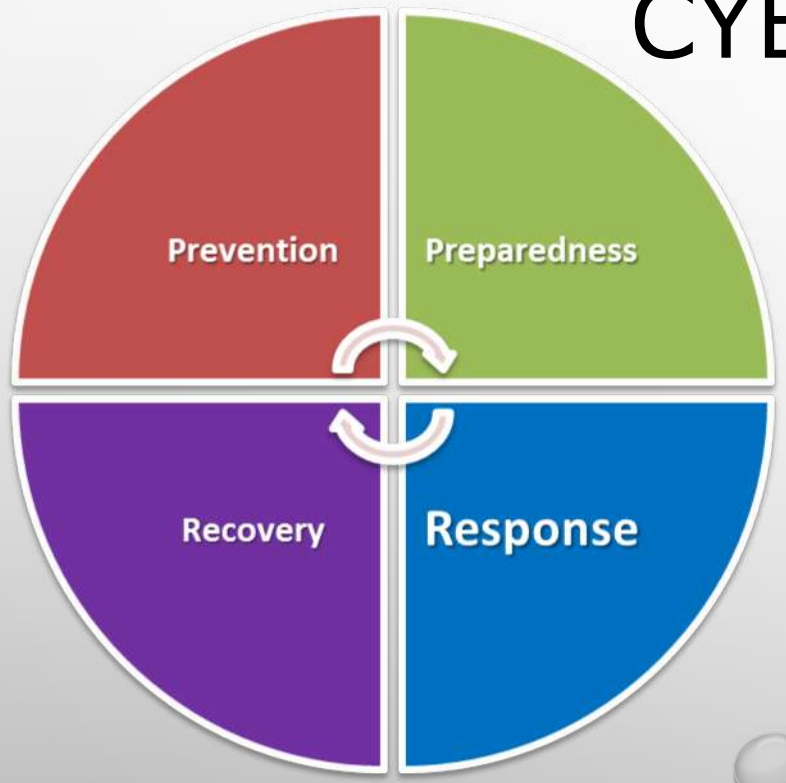
Challenge IV: Enhancement of skills- Faster deployment

CyBureau
The Cyber Empowerment Center

- ✓ Close the gap between cybersecurity education and EU industrial, business, operational needs; create a cybersecurity business culture;
- ✓ Upgrade cybersecurity training with new means (e.g. cyber ranges, AI simulation platforms, HPCs, Cloud resources, Big Data centers, innovation hubs);
- ✓ Align academic & certification programmes;
- ✓ Adopt a multidisciplinary approach to cyber security training;
- ✓ Utilise all expertise (military, industrial, law enforcement, financial, governmental);
- ✓ Match cybersecurity skills and workforce-Prepare people!

CyBureau
The Cyber Empowerment Center

BLUEPRINT - COORDINATED RESPONSE TO LARGE-SCALE CYBERSECURITY INCIDENTS AND CRISES



THE CYBERSECURITY COMPETENCE CENTRE AND NETWORK (CCCN)

BRUSSELS, **12.9.2018** COM(2018) 630 FINAL

2018/0328 (COD) REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL **ESTABLISHING THE EUROPEAN CYBERSECURITY INDUSTRIAL, TECHNOLOGY AND RESEARCH COMPETENCE CENTRE AND THE NETWORK OF NATIONAL COORDINATION CENTRES**

EUROPEAN CYBERSECURITY INDUSTRIAL TECHNOLOGY AND RESEARCH COMPETENCE CENTRE

Centre's Role:

- Network coordination and support
- Research programming and implementation
- Procurement
- Ensuring synergies between civilian and defence spheres

Horizon 2020 cybersecurity pilot projects

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners: **46**

EU Member States involved: **14**

Cyber Security for Europe

Partners: **43**

EU Member States involved: **20**

ECHO

Partners: **30**

EU Member States involved: **15**

SPARTA

Partners: **44**

EU Member States involved: **14**

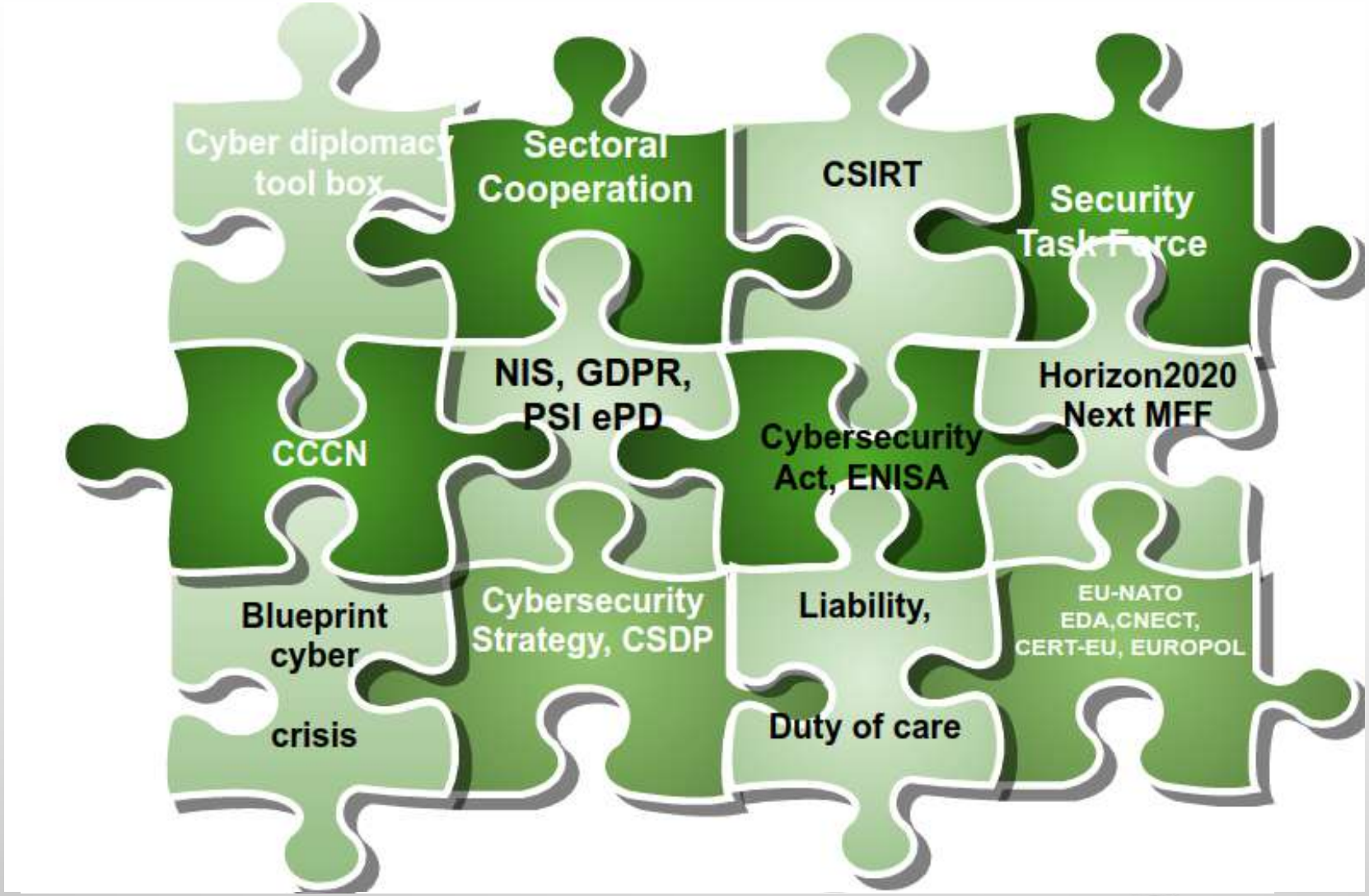
European Commission

#H2020 #CyberSecurity

CHALLENGE V: INFORMATION SHARING

- INFORMATION SHARING AND ANALYSIS CENTERS (ISACS
- CSIRT NETWORK
- EUROPOL-EDA-EC-CERT-EU
- EU-NATO AGREEMENT

CSIRTs NETWORK


Cyber diplomacy tool box
Sectoral Cooperation
CSIRT
Security Task Force
NIS, GDPR, PSI ePD
Horizon2020 Next MFF
CCCN
Cybersecurity Act, ENISA
Blueprint cyber
Cybersecurity Strategy, CSDP
Liability,
EU-NATO EDA,CNECT, CERT-EU, EUROPOL
crisis
Duty of care

THANK YOU FOR YOUR ATTENTION

ASSOCIATE PROFESSOR NINETA POLEMI

UNIVERSITY OF PIRAEUS, DPT. OF INFORMATICS, CYBERSECURITY LAB

KARAOLI & DIMITRIOU 80, PIRAEUS, 18534, GREECE

DPOLEMI@GMAIL.COM, *DPOLEMI@UNIPI.GR*

SKYPE: NINETA.POLEMI ,

LINKEDIN: HTTPS://WWW.LINKEDIN.COM/IN/NINETAPOLEMI/HTTPS://SECLAB.CS.UNIPI.GR/