Cybersecurity Strategy of the Republic of Cyprus

George Michaelides
Commissioner of Electronic Communications and Postal Regulation
http://www.ocecpr.org.cy

12th February 2016

Overview

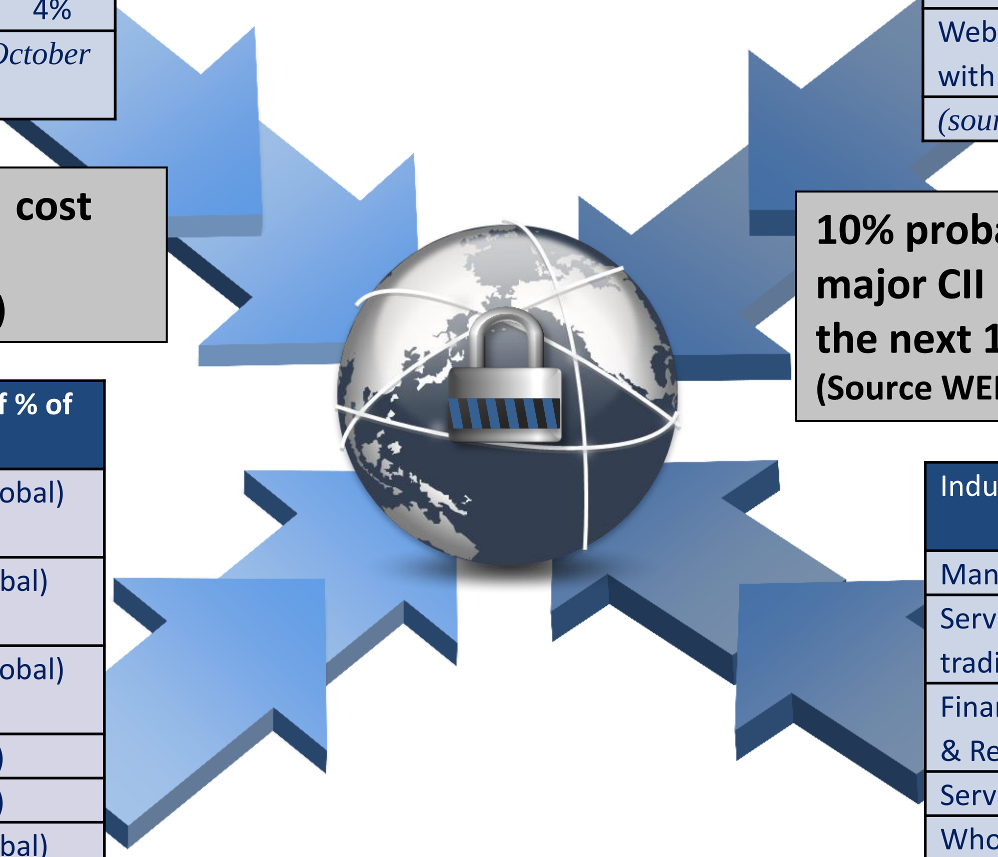
- Cybersecurity facts
- Cybersecurity Strategy
  a. European strategy
  b. NIS
  c. Strategy pillars
- OCECPR responsibilities
  - o Open Internet
- National Cybersecurity Strategy
  - Priority areas
  - Collaboration framework
  - Progress made
  - What is next
- Important messages

Office of the Commissioner of Electronic Communications & Postal Regulation

Cybersecurity facts

Percentage cost for external consequences	
Information loss	39%
Business disruption	35%
Revenue loss	22%
Equipment damages	4%
(source Ponemon Institute October 2014)	

Vulnerabilities	● 2014 ● 2013
Scanned Websites with Vulnerabilities	76% 77%
Percentage of Which Were Critical	20% 16%
New Vulnerabilities	6,549 6,787
Web Attacks Blocked per Day	496,657 568,734
Websites Found with Malware	1 in 1,126 1 in 566
(source Symantec 2015)	



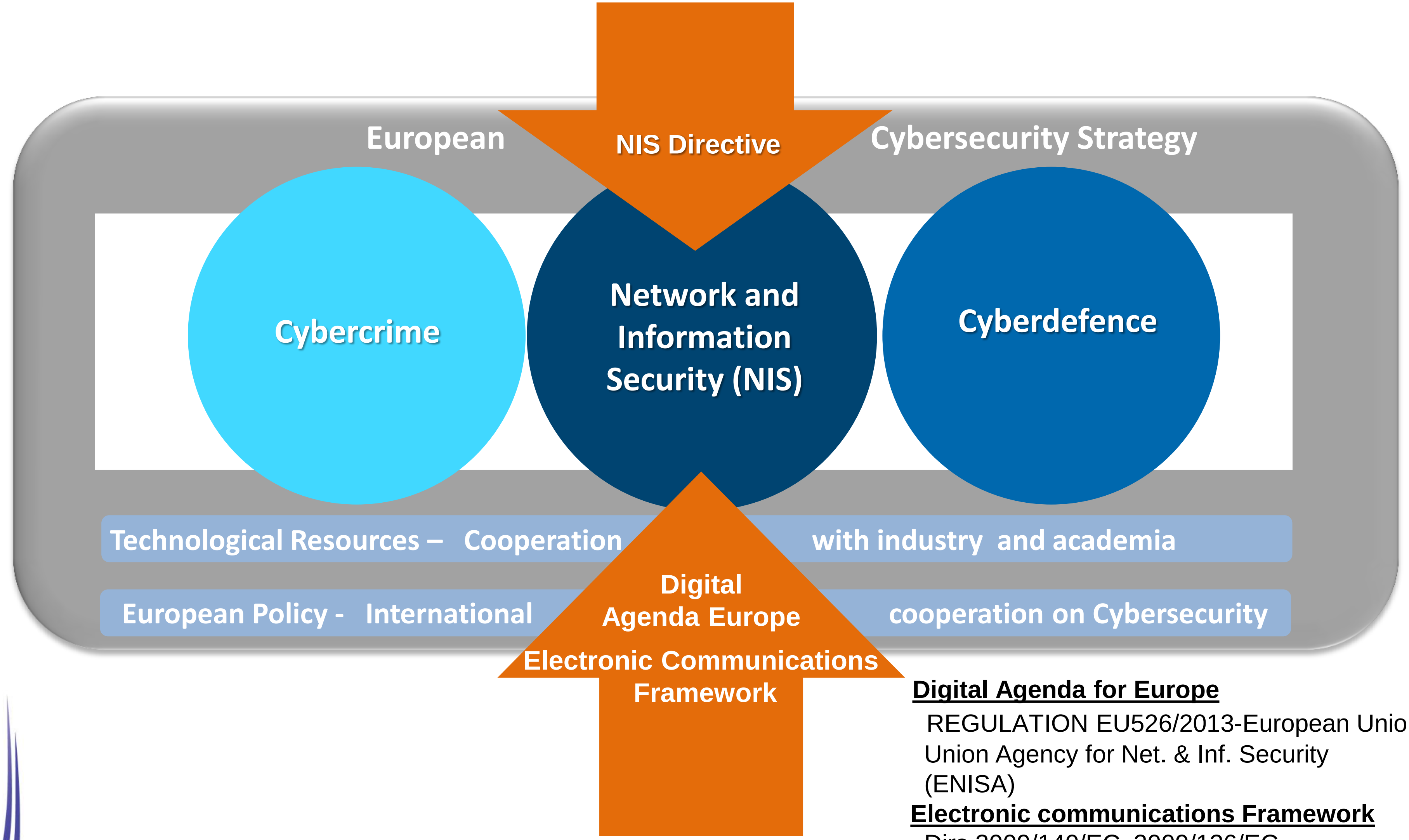
Global economic cost of over $445B
(Source Mcafee 2014)

10% probability of a major CII breakdown in the next 10 years
(Source WEF)

Activity	Cost as of % of GDP
Maritime Piracy	0.02% (global)
Transnational crime	1.2% (global)
Counterfeiting /Piracy	0.89% (global)
Pilferage	1.5% (US)
Car crashes	1.0% (US)
Narcotics	0.9% (global)
Cybercrime	0.8% (global)
(source Mcafee June 2014)	

Industry	● 2014 ● 2013
Manufacturing	20% 13%
Services-Non-traditional	20% 14%
Finance, Insurance & Real Estate	18% 13%
Services- Professional	11% 15%
Wholesale	10% 5%
Top 10 Industries Targeted in Spear-Phishing Attacks	
(source Symantec 2015)	

European Cybersecurity Strategy


European Cybersecurity Strategy
NIS Directive
Cybercrime
Network and Information Security (NIS)
Cyberdefence
Technological Resources – Cooperation with industry and academia
European Policy - International cooperation on Cybersecurity
Digital Agenda Europe
Electronic Communications Framework

Digital Agenda for Europe

REGULATION EU526/2013-European Union Union Agency for Net. & Inf. Security (ENISA)

Electronic communications Framework

Dirs 2009/140/EC, 2009/136/EC,
Framework 21/2002, Art.13a,b
Pers. Data Prot. 58/2002/EC Art.4
REGULATION EU 611/2013 Notification of personal data breaches

NIS Directive

To whom does it apply?

The NIS Directive applies to operators of "essential services" in "critical sectors" :

- Energy
- Transport
- Banking
- Financial market infrastructures
- Health
- Drinking water supply and distribution

as well as to "digital service providers":

- Digital infrastructure
- Online marketplace
- Online search engine
- Cloud computing service

NIS Directive

Subject matter and Scope

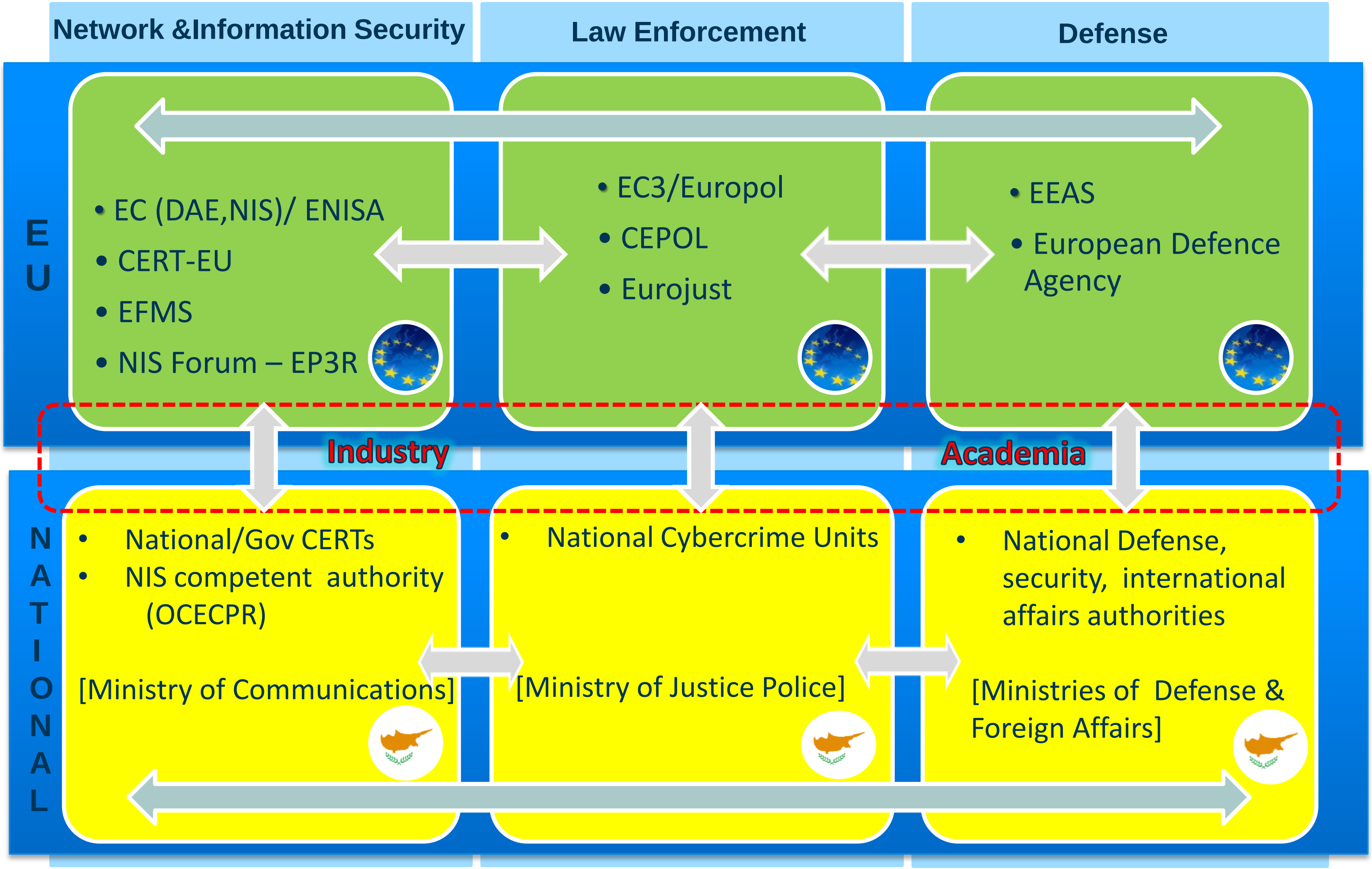
The NIS Directive aims to ensure a uniform level of cybersecurity across the EU. Within the scope of the directive, MS, ENISA and the Commission should ensure:

- NIS Strategy and Cooperation plan in all MS
- Computer Security Incident Response Team (CSIRT) in all MS
- Establishment of a cooperation group at EU level
- Establishment of a CSIRTs network at EU level
- Security requirements and Incident Notifications mechanism
- Identification of operators of essential services at national level
- Encourage Standardization

Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

European Cybersecurity Strategy - Pillars



Network &Information Security

Law Enforcement

Defense

EU

- EC (DAE,NIS)/ ENISA
- CERT-EU
- EFMS
- NIS Forum – EP3R

- EC3/Europol
- CEPOL
- Eurojust

- EEAS
- European Defence Agency

Industry

Academia

NATIONAL

- National/Gov CERTs
- NIS competent authority (OCECPR)

[Ministry of Communications]

- National Cybercrime Units

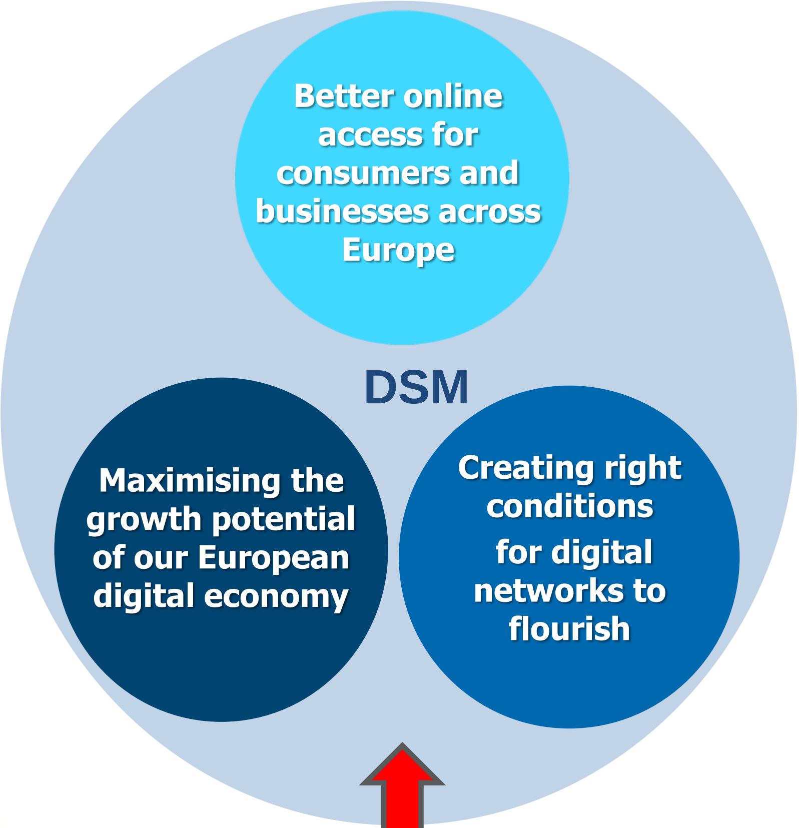
[Ministry of Justice Police]

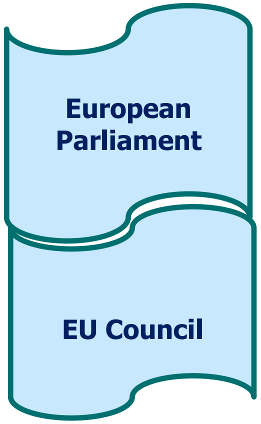
- National Defense, security, international affairs authorities

[Ministries of Defense & Foreign Affairs]

EU, ITU, ICANN vs OCECPR responsibilities

EC Vision: Delivering the Digital Single Market (DSM)

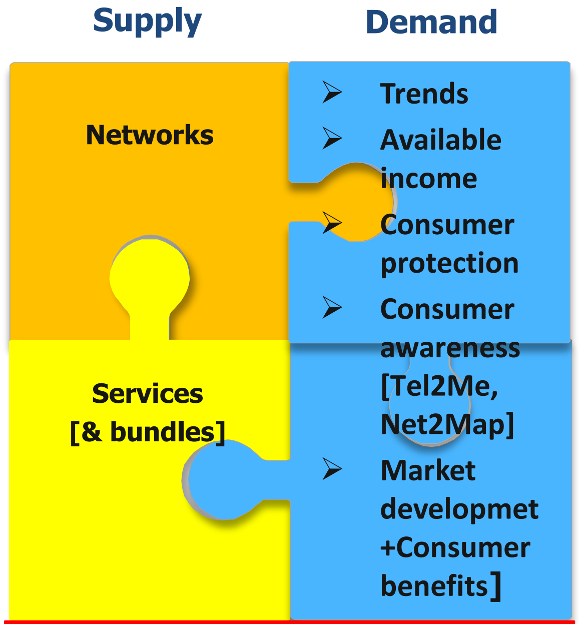

Better online access for consumers and businesses across Europe
DSM
Maximising the growth potential of our European digital economy
Creating right conditions for digital networks to flourish



Legislation / Regulation

CY: Information Society

[OCECPR Responsibilities]



- Trends
- Available income
- Consumer protection
- Consumer awareness [Tel2Me, Net2Map]
- Market developmet +Consumer benefits]

Legislation / Regulation

Network neutrality [2B2T – Mlab]
NIS Directive

EU: ENISA, FoP Cyber, HLIG

World: ITU, ICANN

Open Internet

EU Cybersecurity Strategy [NIS, Cybercrime]

EU position on Internet Governance [GAC-ICANN, IANA]

Open Internet

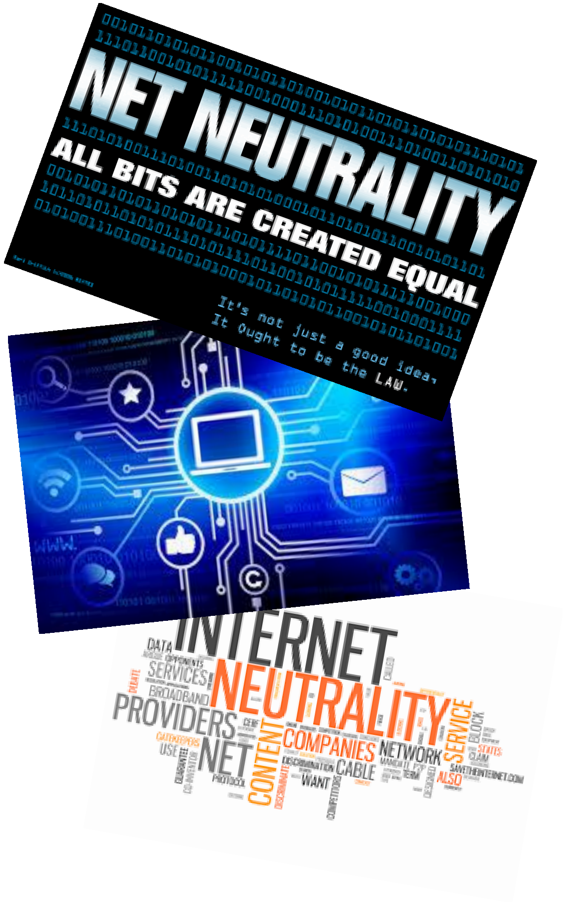
CY Cybersecurity Strategy [NIS, CERT, Risk Assessment, Awareness, Interdependencies]

CY position on Internet Governance [GAC-ICANN, IANA], .cy, .кп

Open Internet - Net neutrality Regulation (EU) 2015/2120

Subject matter and Scope

- Adoption of measures on ensuring access to the open Internet
- Establishment of common rules to ensure:
  - equitable and non-discriminatory traffic management, in the provision of internet access services,
  - the rights of end users
- Users have the right to access and to distribute information and content, to use and to provide applications and services and use terminal equipment of their choice



Vision of the Cybersecurity Strategy of the Cyprus Government

Electricity

Natural Gas/oil

Water supply

Transports

“The protection of all critical information infrastructures of the state and the operation of information and communication technologies with the necessary levels of security, for the benefit of every citizen, the economy and the country”

Public Health

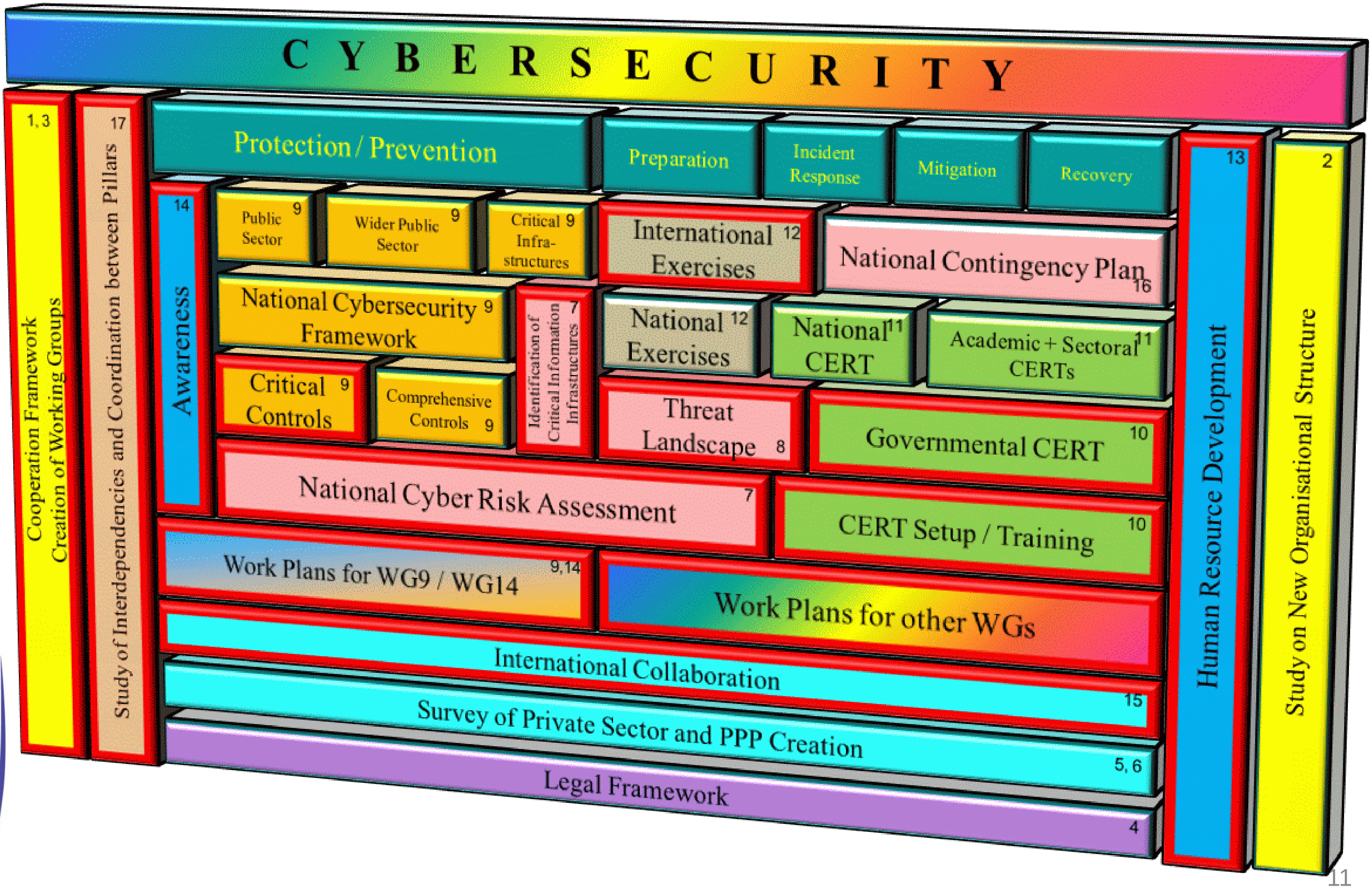
Financial sector

Public sector/security services

Electronic communications

Education – Training – Awareness – Cooperation – Trust

Cyprus Cybersecurity Strategy Building blocks



CYBERSECURITY

Cooperation Framework
Creation of Working Groups 1, 3

Study of Interdependencies and Coordination between Pillars 17

Protection / Prevention

Preparation

Incident Response

Mitigation

Recovery

Awareness 14

Public Sector 9

Wider Public Sector 9

Critical Infra-structures 9

International Exercises 12

National Contingency Plan 16

National Cybersecurity Framework 9

Identification of Critical Information Infrastructures 7

National Exercises 12

National CERT 11

Academic + Sectoral CERTs 11

Critical Controls 9

Comprehensive Controls 9

Threat Landscape 8

Governmental CERT 10

National Cyber Risk Assessment 7

CERT Setup / Training 10

Work Plans for WG9 / WG14 9,14

Work Plans for other WGs

International Collaboration 15

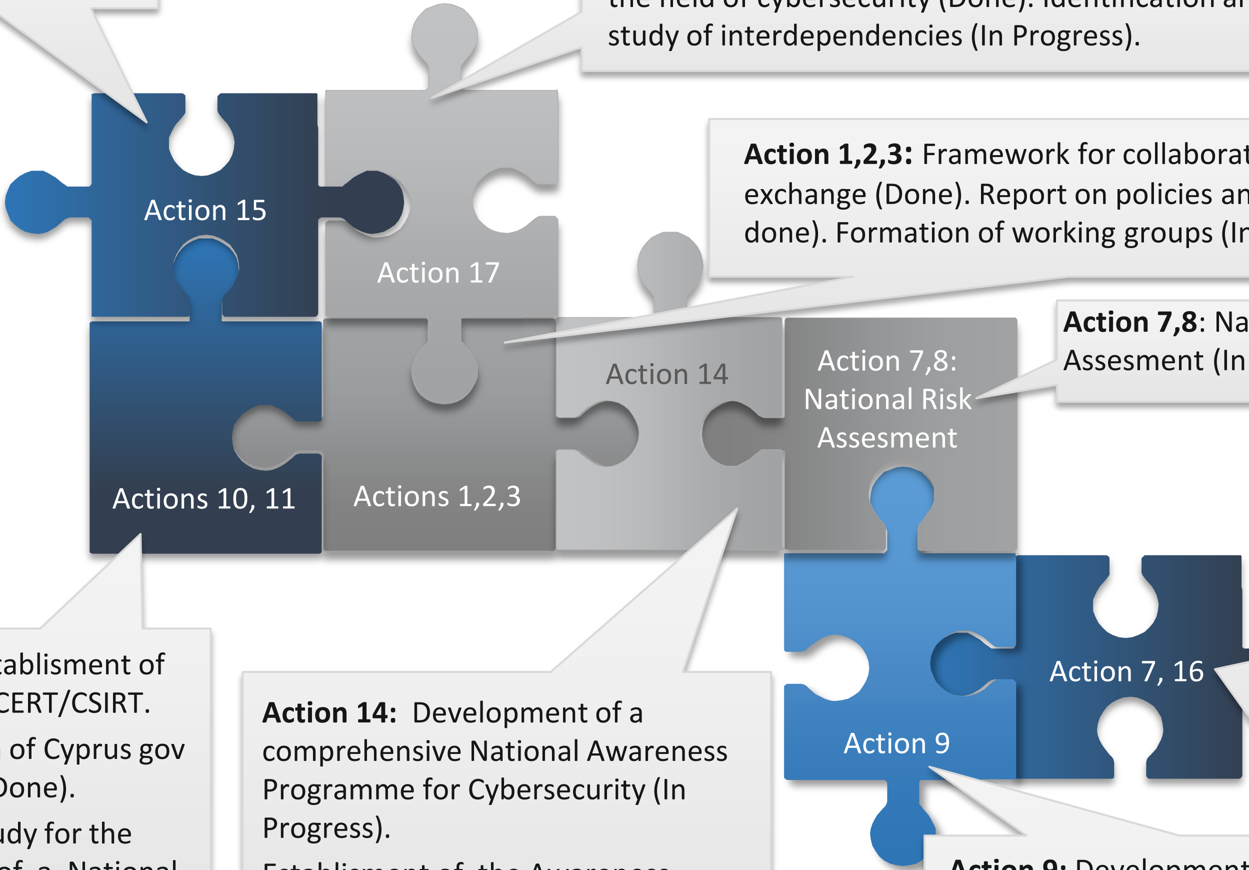
Survey of Private Sector and PPP Creation 5, 6

Legal Framework 4

Human Resource Development 13

Study on New Organisational Structure 2

Progress made - Active Groups



Action 15: International cooperation activities

Action 17: Guidance and coordination on operations in the field of cybersecurity (Done). Identification and study of interdependencies (In Progress).

Action 1,2,3: Framework for collaboration and information exchange (Done). Report on policies and structures (To be done). Formation of working groups (In Progress)

Action 7,8: National Level Cyber Risk Assesment (In Progress)

Actions 7, 16: Identification and assessment of the Critical Information Infrastr. (In Progress) (Development of National Conting. Plan. (In Progress)

Action 10: Establishment of Government CERT/CSIRT.

Accredidation of Cyprus gov CERT/CSIRT (Done).

Action 11: Study for the Establisment of a National CERT/CSIRT (To be done)).

Action 14: Development of a comprehensive National Awareness Programme for Cybersecurity (In Progress).

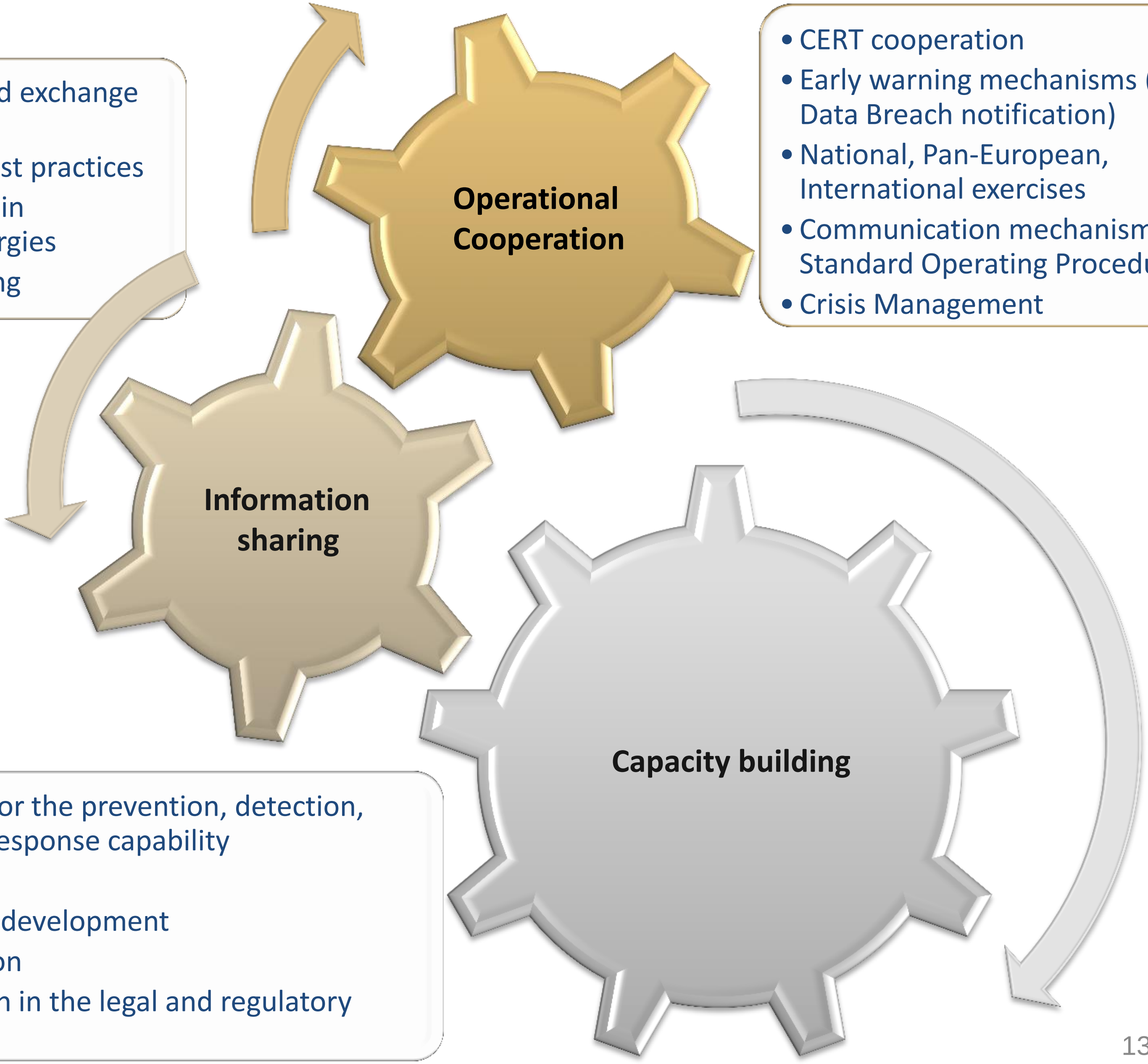
Establisment of the Awareness subgroup for students/ teachers/ Kids/parens (Done).

Action 9: Development of a National Cybersecurity Framework for the critical information infrastructures in Cyprus, as well as the government sector (In Progress).

Initialised with the development of Critical controls (Done).

Fields of further Cooperation

- Development and exchange of Know-how
- Exchanging of best practices
- Providing advice in Developing Synergies
- Awareness Raising



- CERT cooperation
- Early warning mechanisms (e.g Data Breach notification)
- National, Pan-European, International exercises
- Communication mechanisms – Standard Operating Procedures
- Crisis Management

- Cooperation for the prevention, detection, analysis and response capability
- Training
- Research and development
- Standardization
- Harmonization in the legal and regulatory framework

Important messages

1 Cybersecurity - A complex task - Great responsibility to the relevant bodies,

2 Cooperation - Absolutely necessary, at National, European and International level,

3 Cooperation and collaboration between public and private sector is essential,

4 Multi-stakeholder approach to the implementation of the Strategy,

5 Trust between stakeholders - the key to the successful implementation of the Strategy,

6 Awareness raising at the highest level,

Thank you