Digital Security Stakeholders Conference 2018

Current State of Play
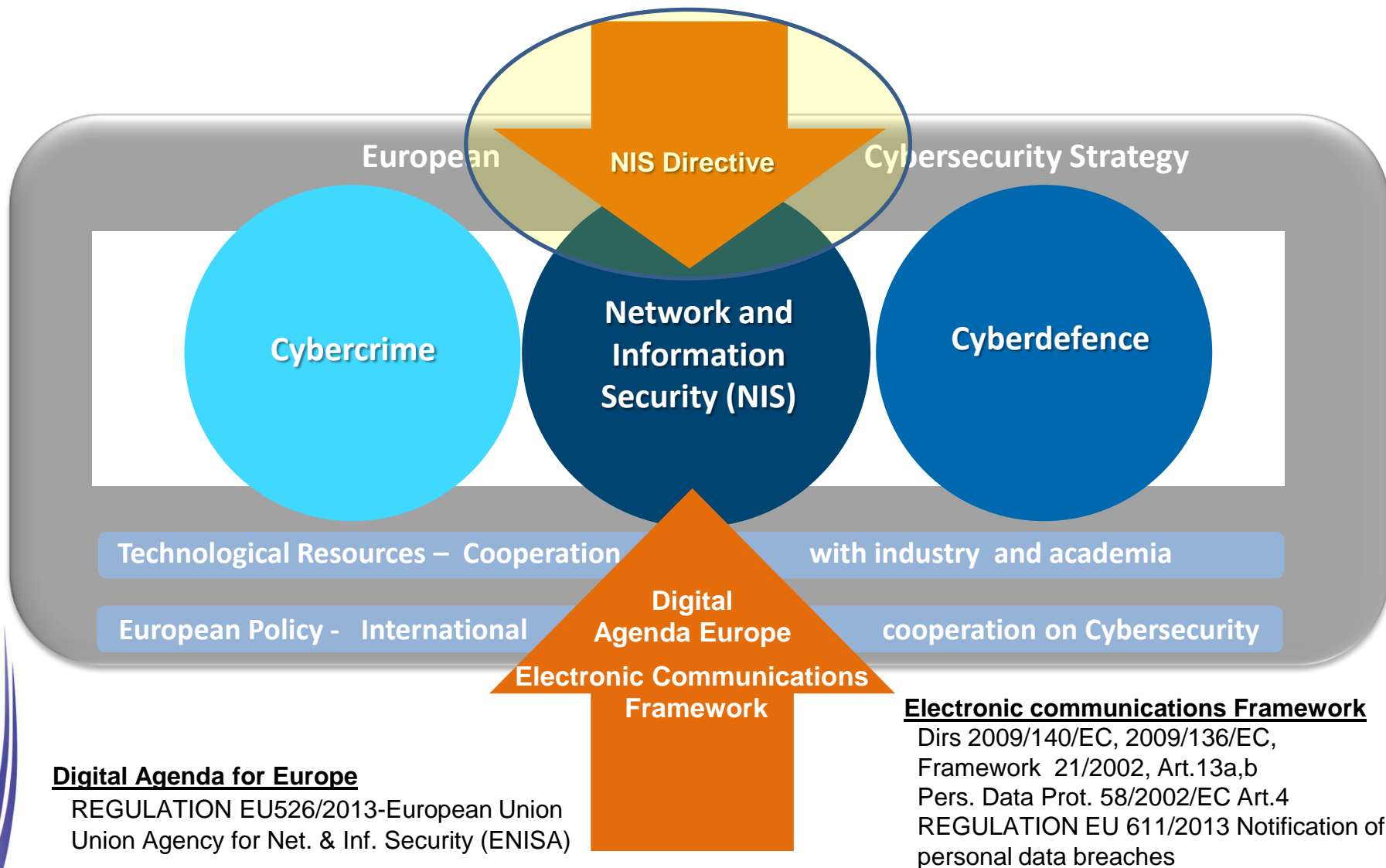
Antonis Antoniades
Office of the Commissioner of Electronic Communications and Postal Regulation
http://www.ocecpr.org.cy

OCECPR

25 January 2018

Overview

- European Framework

- Cybersecurity Strategy of Cyprus

- Political Decisions

- Establishment of new structures

- National CSIRT

Current European Framework

European **NIS Directive** Cybersecurity Strategy

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

New EU Cybersecurity Package

1 Building EU Resilience to cyber attacks

- Reformed ENISA

- EU cybersecurity Certification Framework

- NIS Directive Implementation

- Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund

- Cybersecurity competence network with a European Cybersecurity Research and Competence Centre

- Building strong EU cyber skills base, improving cyber hygiene and awareness

2 Creating effective EU cyber deterrence

- Identifying malicious actors

- Stepping up the law enforcement response

- Stepping up public-private cooperation against cybercrime

- Stepping up political response

- Building cybersecurity deterrence through the Member States' defence capability

3 Strengthening international cooperation on cybersecurity

- Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace

- Strengthening cyber dialogues

- Modernising export controls, including for critical cyber-surveillance technologies

- Continue rights-based capacity building model

- Deepen international cooperation on cybersecurity, hybrid threats and defence

OCECPR

Cyprus Cybersecurity Strategy Structure
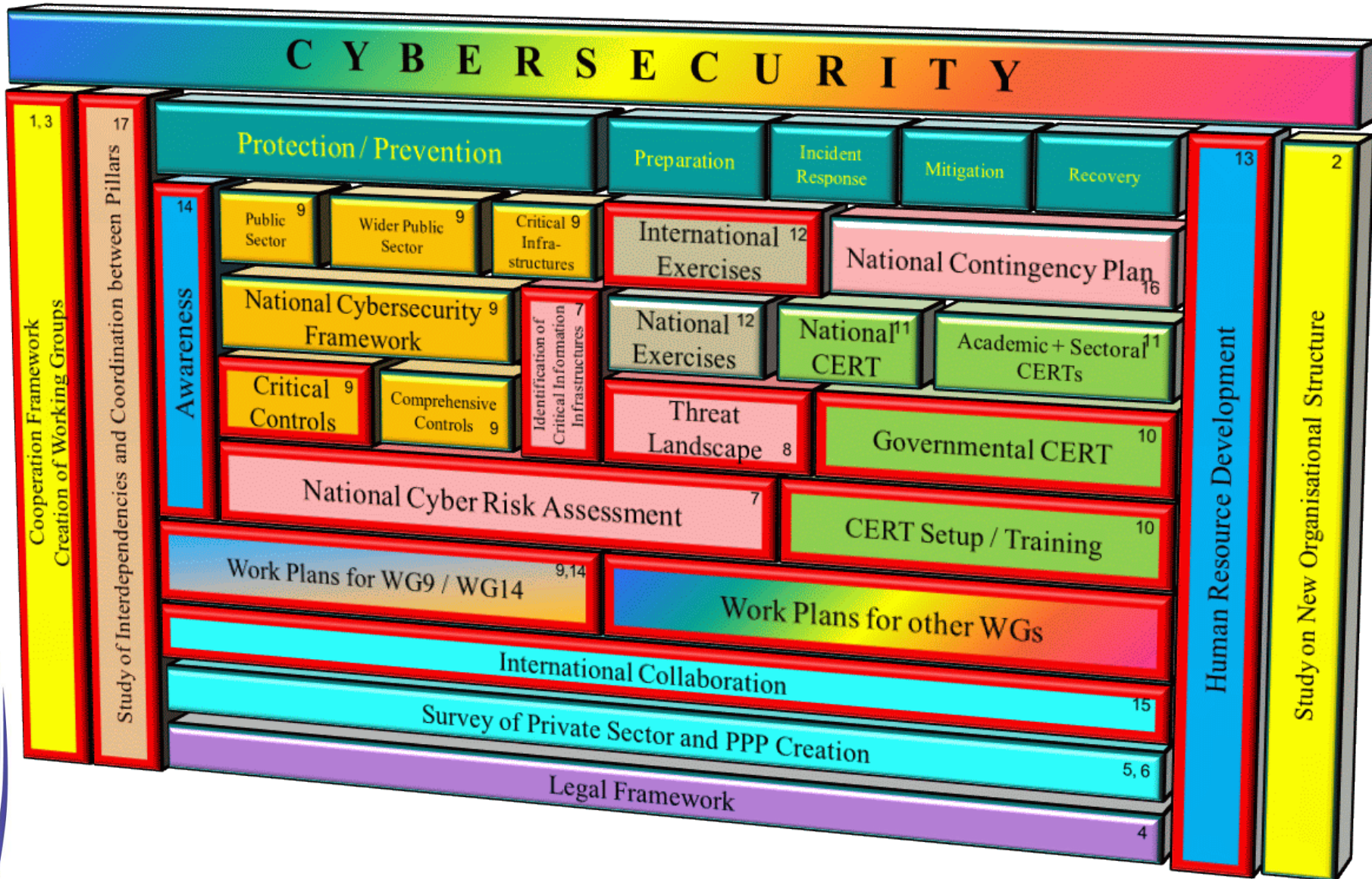
Progress made - Active Groups

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). Formation of working groups (Done) Development of new structures (In Progress).

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

Action 15

Action 17

Action 14

Action 7,8: National Risk Assesment

Actions 10, 11

Actions 1,2,3

Action 9

Action 7, 16

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

Action 10: Establishment of Government CSIRT (Done). Accreditation of Cyprus gov CSIRT (Pending). **Action 11:** Establishment of National CSIRT (Done). Accreditation of National CSIRT (In Progress).

Action 14: Development of a comprehensive National Awareness Programme for Cybersecurity (In Progress). Establishment of National Strategy on Cyber safety (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).

NCS - What is next

NCS 2.0

Establishment of the National Cybersecurity Strategy 2.0
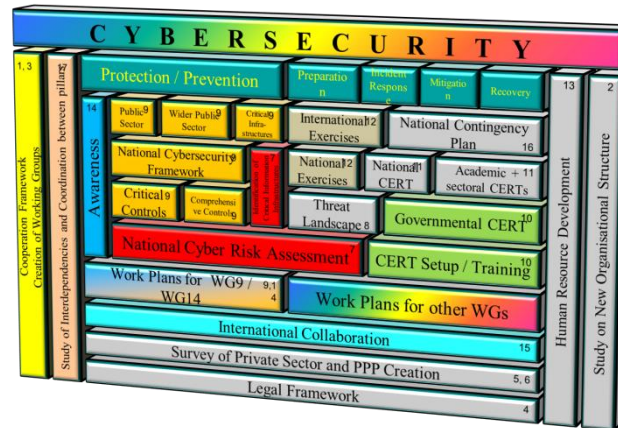
NIS Directive

Transposition/Implementation of the new NIS Directive

Action 2

Establishment of the new structures DSA /national CSIRT/National governance of Cybersecurity in Cyprus

Action 11

Establishment and accreditation of National CSIRT

Action 17

Evaluation of Interdependencies between stakeholders and Revission of Cybersecurity Strategy

Action 9

Complete National Cybersecurity Framework with comprehensive controls – to cover Public and wider public sectors, as well as national Critical Infrastructures
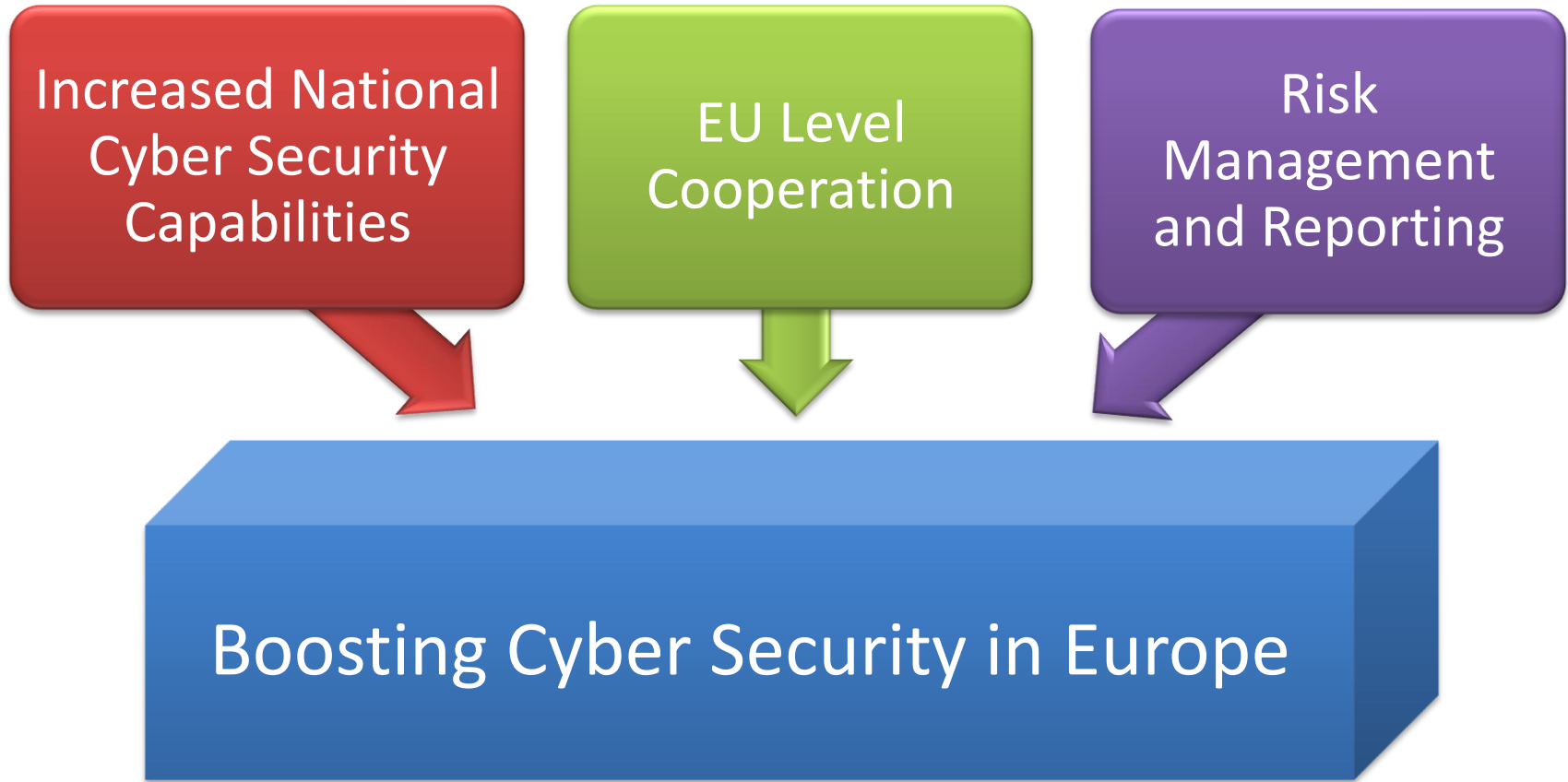
Action 14

Further developments in the field of awareness to cover the public and private sectors
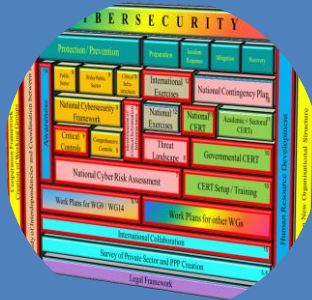
Cybercrime & Cyberdefence

Further Developments in the fields of Cybercrime and Cyberdefence by the competent Ministries and government authorities

OCECPR

The Objective

Increased National Cyber Security Capabilities

EU Level Cooperation

Risk Management and Reporting

Boosting Cyber Security in Europe

OCECPR

Capability Requirements

National NIS / Cybersecurity Strategy

NIS Competent National Authority

National CSIRT

National NIS Capability

Establishment of the Digital Security Authority and the National CSIRT

Council of Ministers Decisions on the establishment and operation of the Digital Security Authority and the National CSIRT:

a) Decision to establish the National CSIRT (Decision No. 81/477, dated 22/10/16) (based on Article 9 of the NIS Directive).

b) Decision on the identification of critical information infrastructures in the Republic of Cyprus for cyber-security purposes (Decision No. 82/518, dated 3/5/2017).

c) Decisions with No. 82.518, dated 20/6/2017 and No. 82/898 dated 28/6/2017 by which:

   i.   The Commissioner is designated as the National Competent Authority under Article 8 of the NIS Directive; and

   ii. A structure is created, under the Commissioner, to act as a national Competent Authority and as the single point of contact.

CIIs/Essential Services

Electricity

Natural Gas/Oil

Water supply

Transport

Public Health

Financial Sector

Public Sector/Security Services

Electronic Communications

"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"

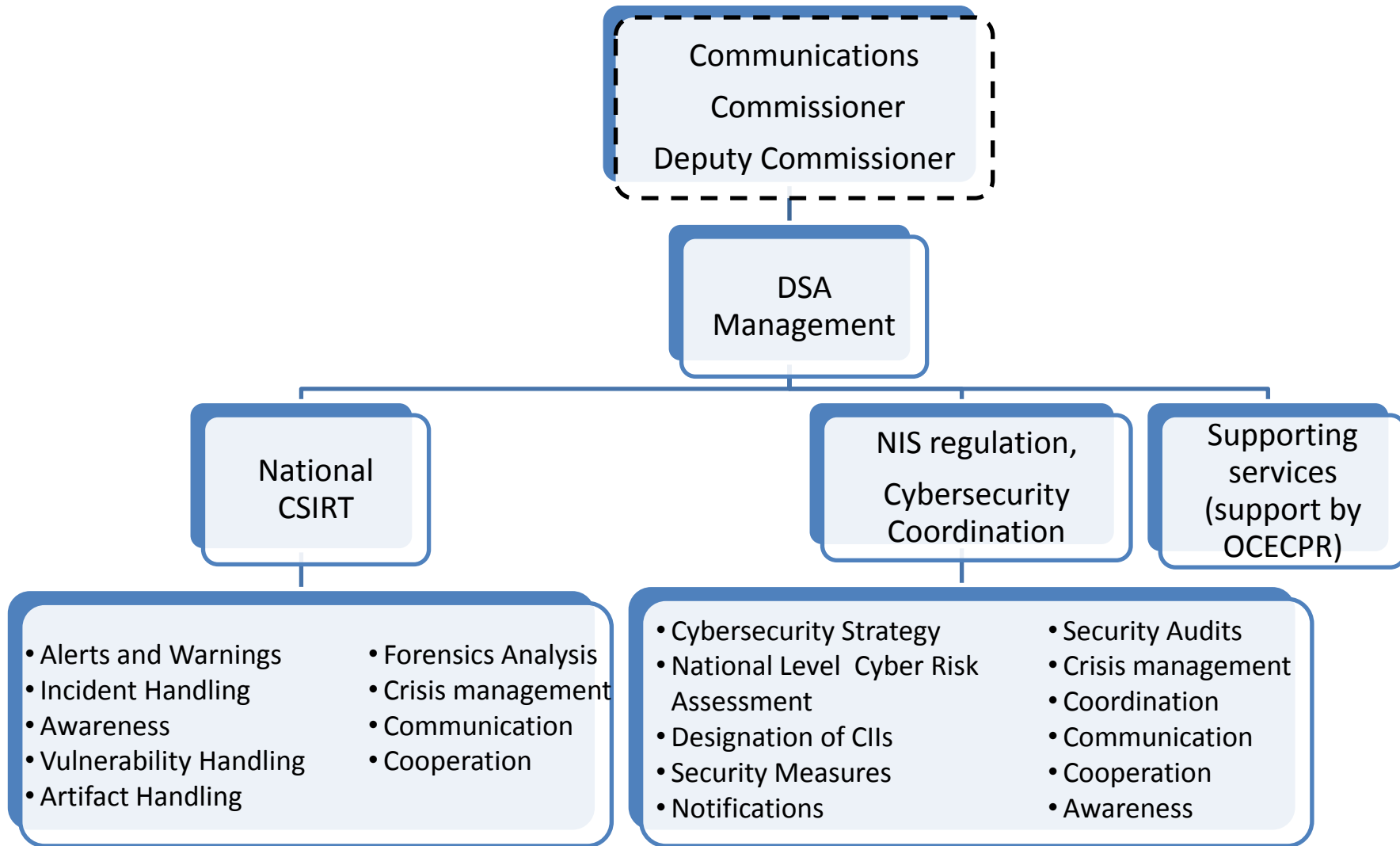**Cyprus National Cybersecurity Strategy Vision**

OCECPR

New Legislation

- New legislation submitted to the House of Representatives, provides that:

  – All powers of OCECPR on Network and Information Security are transferred to the Digital Security Authority (DSA) which is under the supervision of the Commissioner,

  – DSA is defined as the competent authority for the implementation of the NIS Directive in the Republic of Cyprus and the coordination of the implementation of the National Cybersecurity Strategy, and

  – The National CSIRT will operate under the structure of the DSA.

Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

Digital Security Agency - National CSIRT

Communications Commissioner
Deputy Commissioner

DSA Management

National CSIRT

- Alerts and Warnings
- Incident Handling
- Awareness
- Vulnerability Handling
- Artifact Handling
- Forensics Analysis
- Crisis management
- Communication
- Cooperation

NIS regulation, Cybersecurity Coordination

- Cybersecurity Strategy
- National Level Cyber Risk Assessment
- Designation of CIIs
- Security Measures
- Notifications
- Security Audits
- Crisis management
- Coordination
- Communication
- Cooperation
- Awareness

Supporting services (support by OCECPR)

Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

National CSIRT - Mandate

- Commissioner is mandated by decision of the Council of Ministers in order to undertake and coordinate work leading to the establishment and accreditation of a National CSIRT in Cyprus.

- **CY National CSIRT:** independent entity from OCECPR, under the new NIS structure (DSA), with activity and operations supervised by the Commissioner.

- **CY National CSIRT:** to share building facilities with OCECPR.

- 12 people in total to engage in CSIRT provision of services to constituents

OCECPR

National CSIRT - Mandate

- **Services to be provided to constituents**
  - Basic Services: Reactive services, Proactive services
  - Advanced Services (to be offered at a later stage)

- **CY National CSIRT Constituency:**
  - Cyprus Internet Users
  - Private Sector Cybersecurity/Network Security experts/Community in Cyprus
  - Electronic Communications Network and Service Providers in Cyprus including ISPs
  - Cyprus Police Force- Cybercrime Unit
  - Critical Infrastructure Owners/Admins (NIS directive)
  - Academic CSIRT
  - Cy Gov CSIRT

National CSIRT – Areas of activities

Communication Awareness

- Early warning, alerts, announcements, etc.
- General awreness regarding incidents (public/media) etc.

Incident Handling

- Incident Monitoring
- Incident Response
- Incident Analysis
- EC awareness on incident handling process etc.

NATIONAL CSIRT-CY

Cooperation

- Cooperation with NIS Authority
- Mutual assistance with other national/european CSIRTs
- Exchange non-classified information
- Participation in exercises etc.

National CSIRT – Recent activities

- CSIRT-CY equipped with basic infrastructure and tools
- Team has received a holistic basic training on CSIRT functions and operation, by ITU
- Team participation in the ALERT Cyber Drill for Europe and the CIS regions in Moldova
  - Information on the community of national CSIRTs and the importance of the exchange of information
  - Presentation of tools for infected files analysis
  - Contest between 25 countries with Cyprus finishing 6th
  - October 2018: A similar event will be hosted in Cyprus
- National CSIRT – CY has participate at the event organized by CIRCL.lu in Luxemburg regarding MISP platform
  - The National CSIRT – CY has registered in MISP platform and since 16th of January the National CSIRT-CY is a member of the MISP family
- CSIRT-CY listed with the TI community
- Accreditation and certification with FIRST and TI communities is in progress
- CIRT-CY CEF Project 2016-CY-IA-0129 is in progress

National CSIRT – Portal

National CSIRT – Portal

CSIRT-CY Contact Information

National Computer Security Incident Response Team - *CSIRT-CY*

HOTLINE number: 1490

email: info@csirt.cy

Website: http://www.csirt.cy

Tel.: +357 22693094, +357 22693095

Fax: +357 22683096

Address: Ilioupoleos 8, Nicosia 1101, Cyprus

OCECPR

Thank you!

OCECPR