Office of the Commissioner of Electronic Communications & Postal Regulation

OCECPR

National Cybersecurity Strategy 2.0

Why, and what will be different this time?

Costas Efthymiou
OCECPR
http://www.ocecpr.org.cy

Digital Security Stakeholders Conference – 25/1/18

Why update the Strategy?

- The current Strategy is almost 5 years old
  - (and was developed 6 years ago!)
- There have been significant changes to the environment that it was based on
  - European Framework and Strategy / Package
  - National-level actions, experiences, knowledge obtained from implementation
  - Developments in other related areas
  - New threats
  - But, the old threats are (still) there
- **Better understanding of existing gaps in CY**

Vision of the National Cybersecurity Strategy

Electricity

Natural Gas/Oil

Water supply

Transport

"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

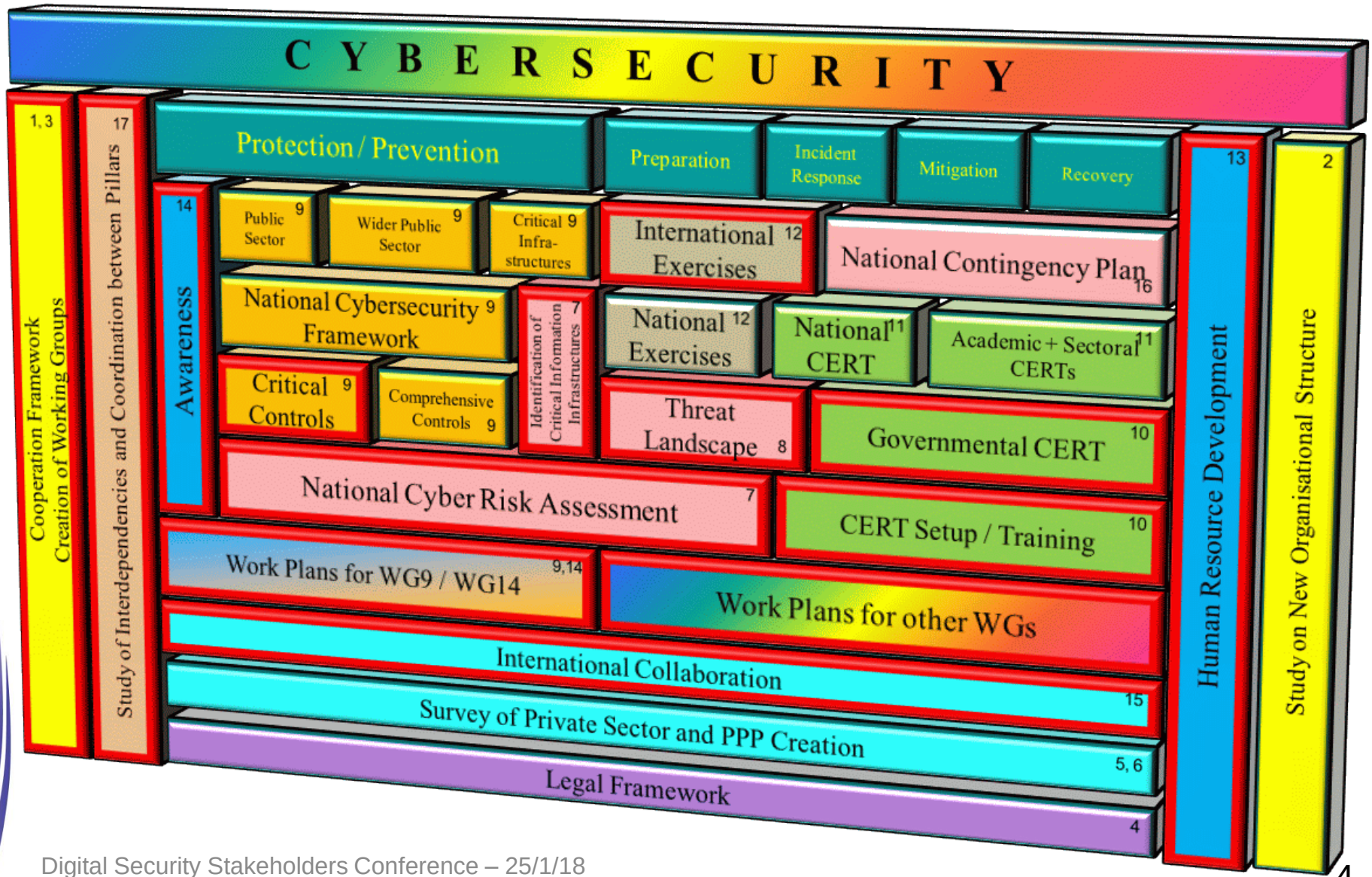
Financial sector

Public sector/security services

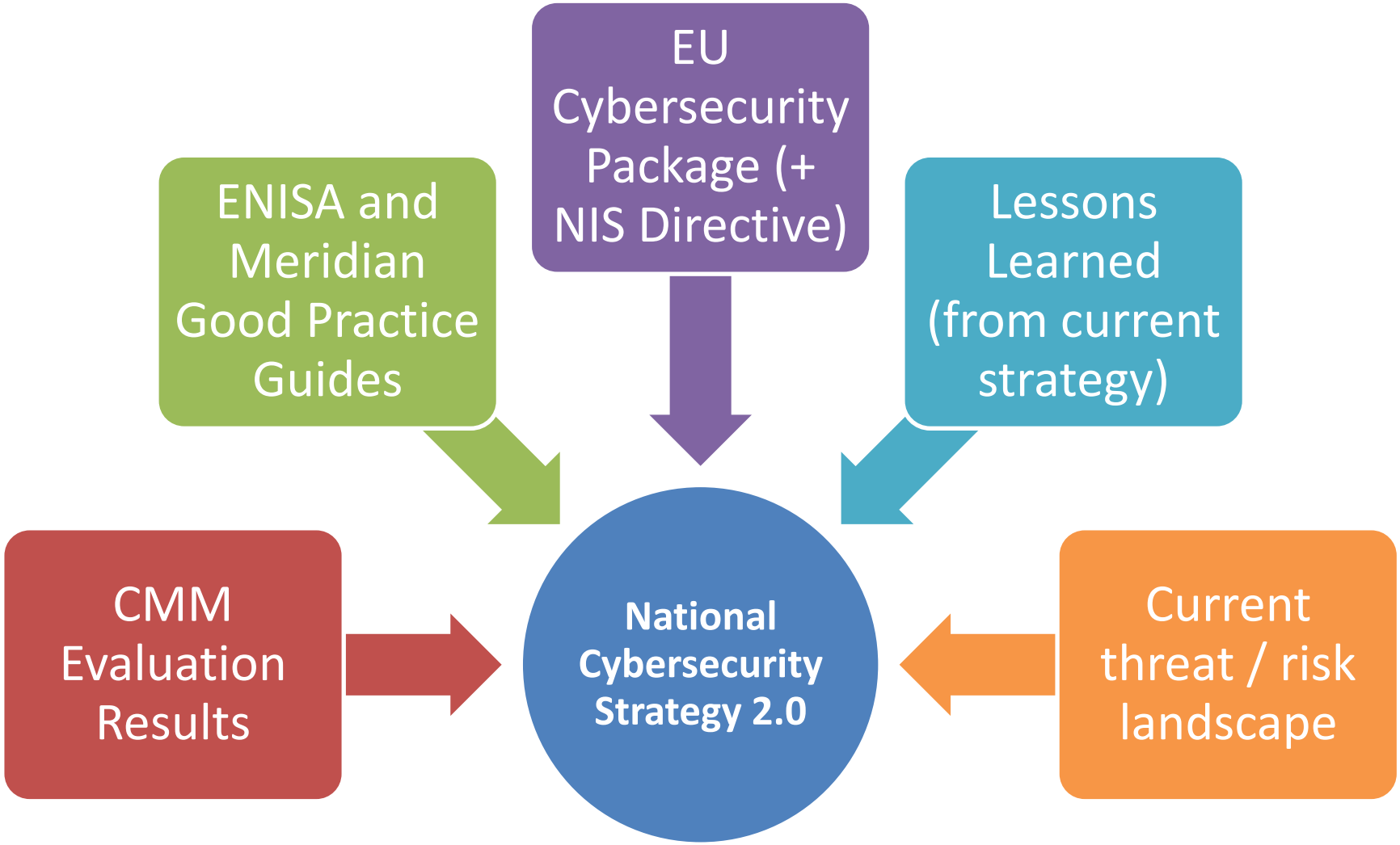
Electronic communications

Education – Training – Awareness – Cooperation – Trust

Cyprus Cybersecurity Strategy - Today



Strategy update inputs



NIS Directive Obligations

National Cybersecurity Strategy

National Collaboration

Cyber Crisis Management

Operational Coordination

NIS Authority

National CSIRT

European Cybersecurity Strategy

International Collaboration

Cooperation Group

CSIRT Network

Security Requirements

Incident Reporting

Supervision

Operators of Essential Services (~50)
Energy, Water, Transport, Health, Banking, Financial, Digital Infrastructure

Digital Service Providers (<10)
Cloud Computing Services, Online Marketplaces, Search Engines

What should it look like?

Strategy 2.0 – Main Ideas

- To leverage the strong foundation that has been built and propel us forwards in terms of cybersecurity capability

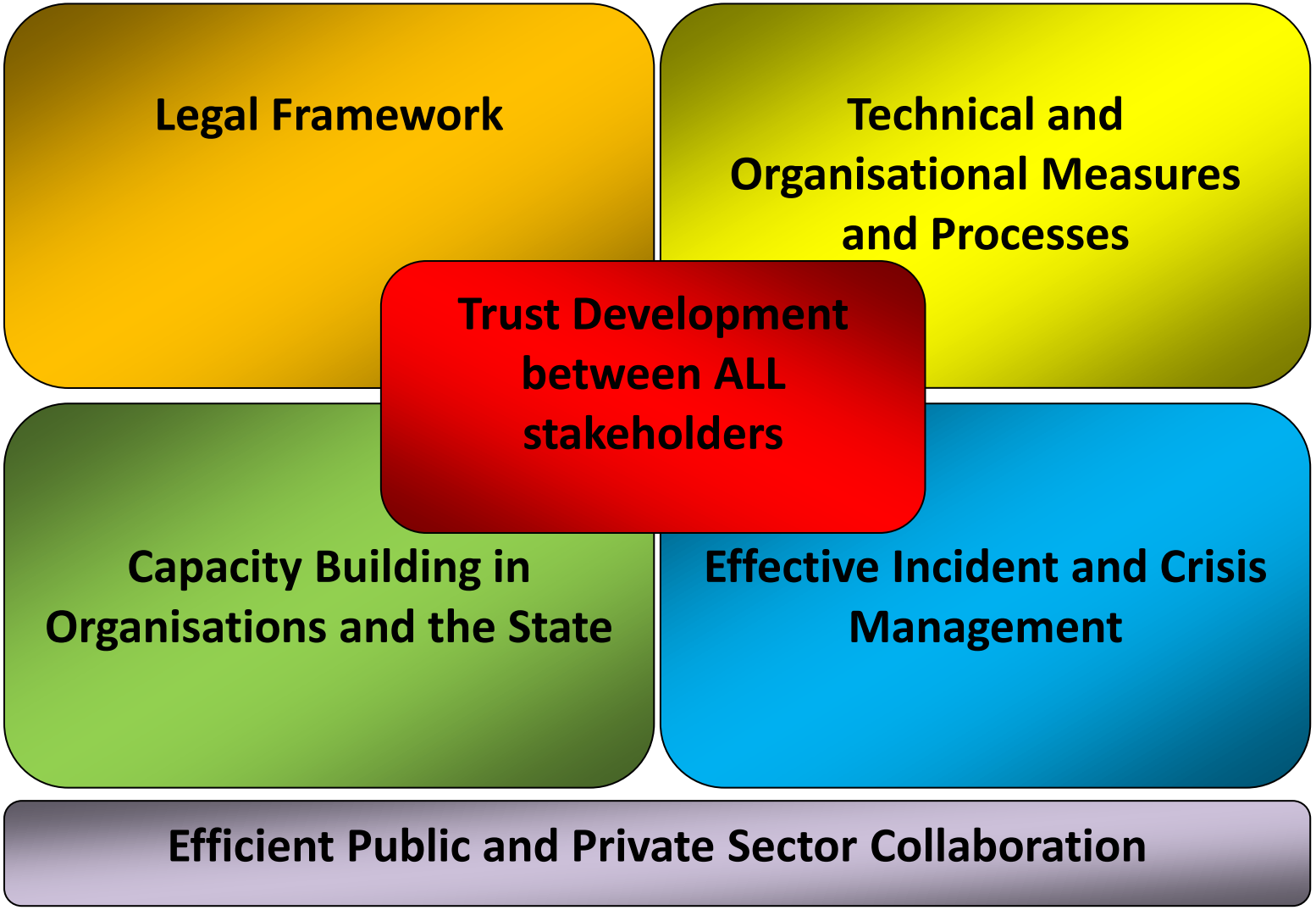
- **Collaboration – Build Together**
  - Security is a team sport!

- **Build a strong cybersecurity ecosystem**

High-Level Features

- Cover all NIS Directive obligations, and bring all related cybersecurity activities under a single comprehensive umbrella
- Emphasis on measurable capabilities (use of Oxford CMM for targeting activities and strategy evaluation)
- Structures – beyond DSA and CSIRT-CY
  - Formal cooperation between DSA, cybercrime, cyberdefence, related external affairs
  - National Risk and Crisis Management structures
- **Risk management approach**

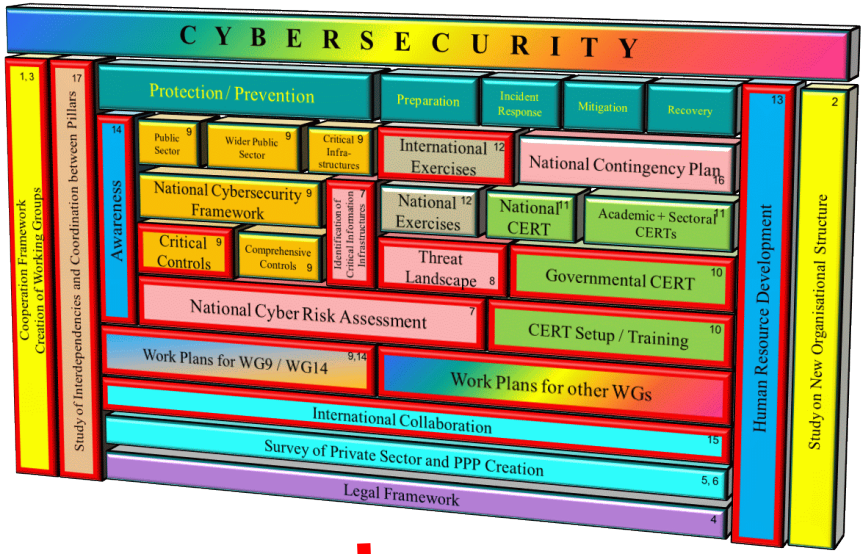
Strategy Priorities

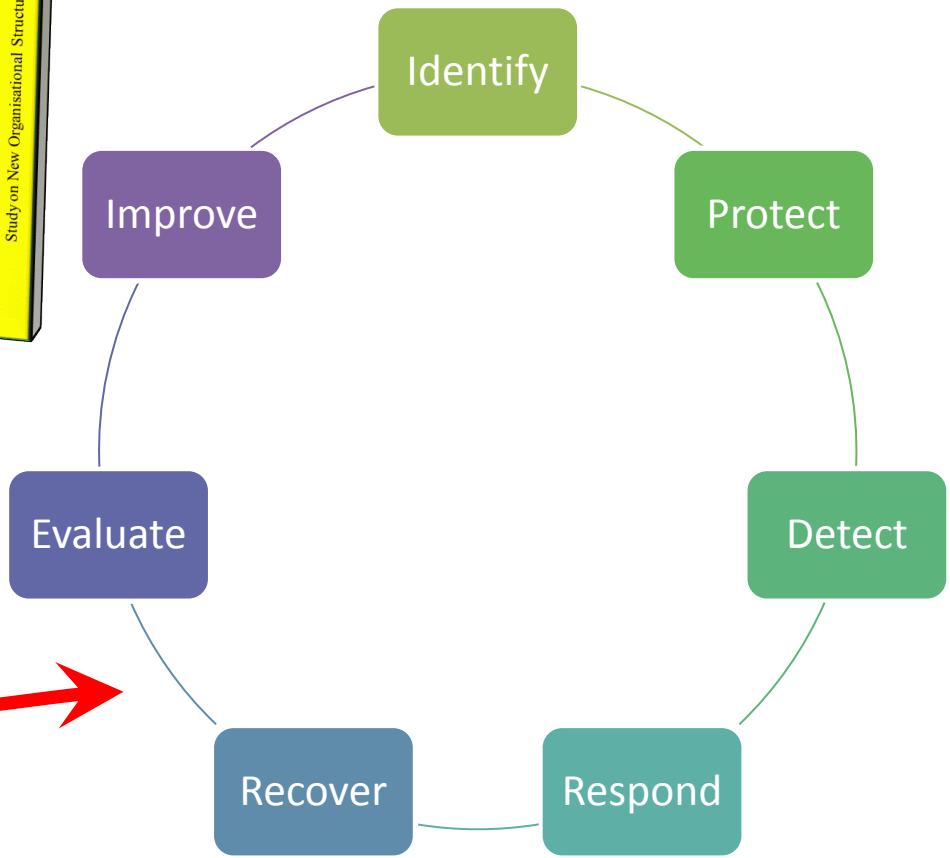


Strategy Content (1)

- **Introduction of new Actions** to cover gaps (see Strategy 2.0 inputs)
- **Improvement of existing Actions** (where necessary)
- **Continue important Actions** that can still be developed further
- Emphasis on **information sharing and situational awareness**
- **COLLABORATION!**
  - Stronger involvement of the private sector

Placement of Actions on the ‘Spectrum’

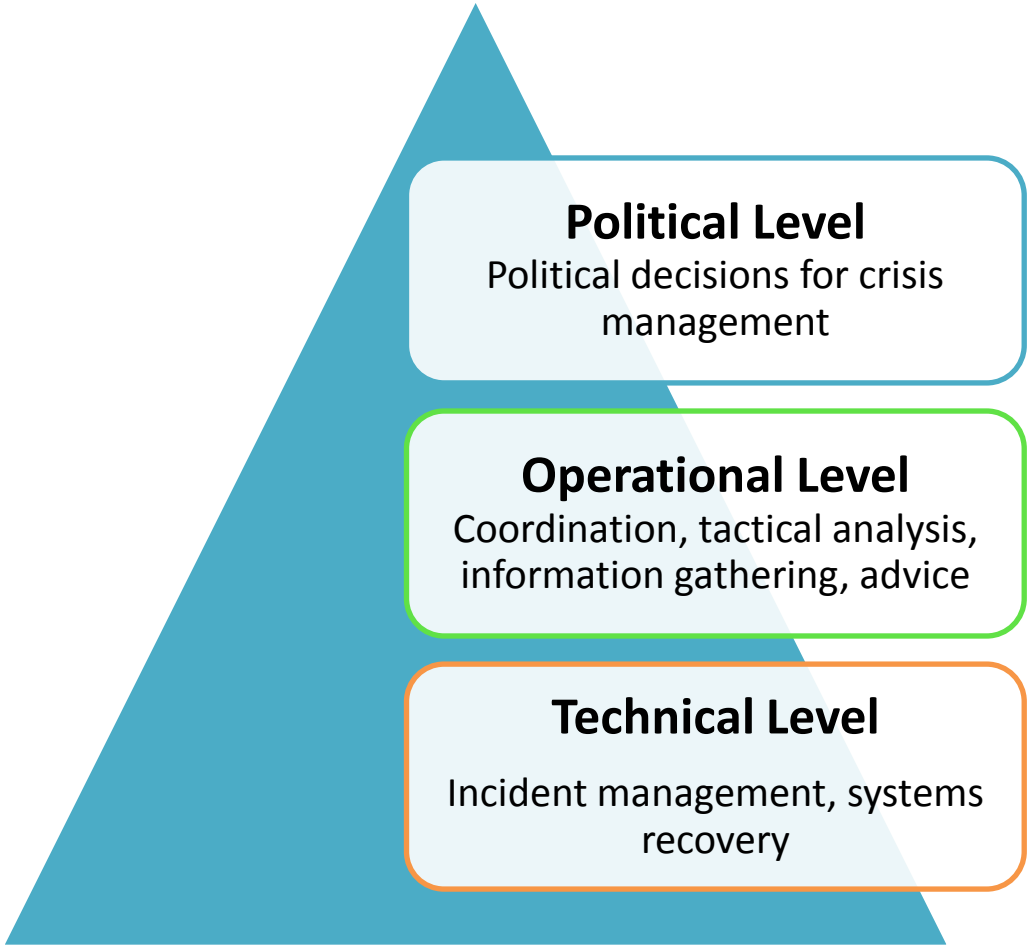


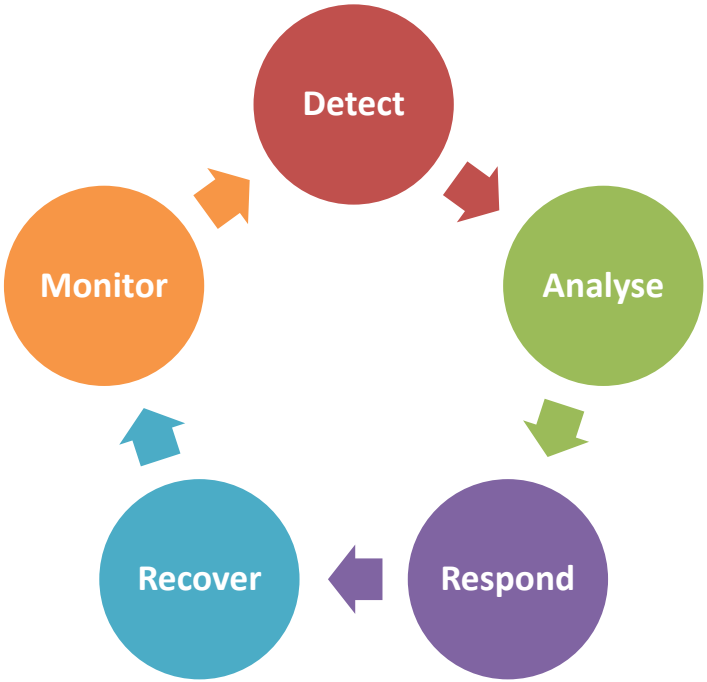


Strategy Content (2)

- **Leverage academic capabilities and expertise**
  - There is much activity in local universities, both at the teaching and research levels for cybersecurity
  - We should take advantage of all available funding opportunities – e.g. Collaborative projects (win-win!), that could even be used to implement some parts of the new Strategy
- **Leverage new structures**
  - E.g. Comprehensive Crisis Management (see next slide)

Crisis Managment – Response Levels





Strategy 2.0 is Coming...

Στρατηγική Κυβερνοασφάλειας της Κυπριακής Δημοκρατίας 2018

Ασφάλεια Δικτύων και Πληροφοριών και Προστασία Κρίσιμων Υποδομών Πληροφορίας

Thank you

Costas Efthymiou
OCECPR
http://www.ocecpr.org.cy

Digital Security Stakeholders Conference – 25/1/18