Cybersecurity Capacity Maturity Evaluation in Cyprus Findings and Recommendations

Dr. Maria Bada, Senior Researcher
Global Cyber Security Capacity Centre
University of Oxford
Maria.Bada@cs.ox.ac.uk
@MariaBadaOxford

Nicosia 25th January 2018

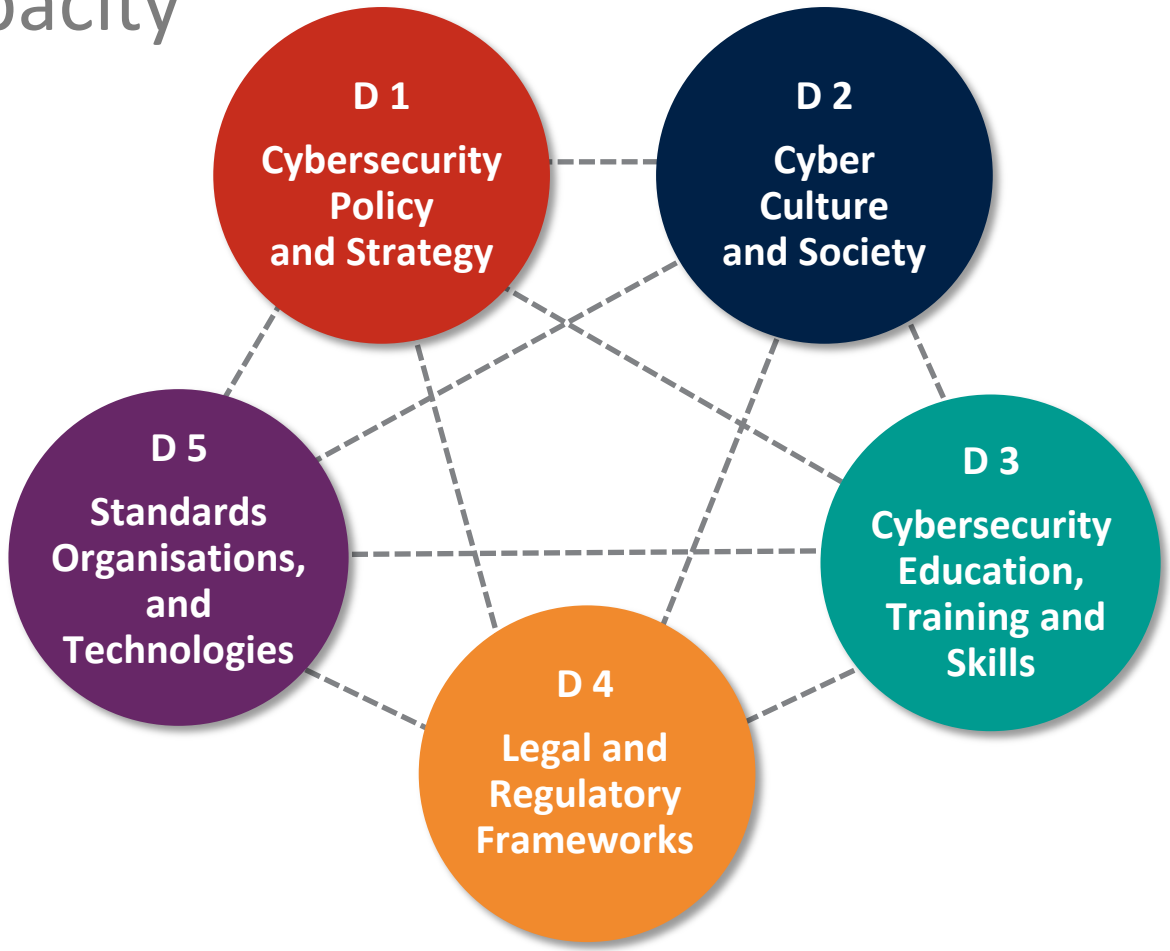
Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Cybersecurity Capacity Maturity Model for Nations (CMM)

The **5 DIMENSIONS** of Cybersecurity Capacity

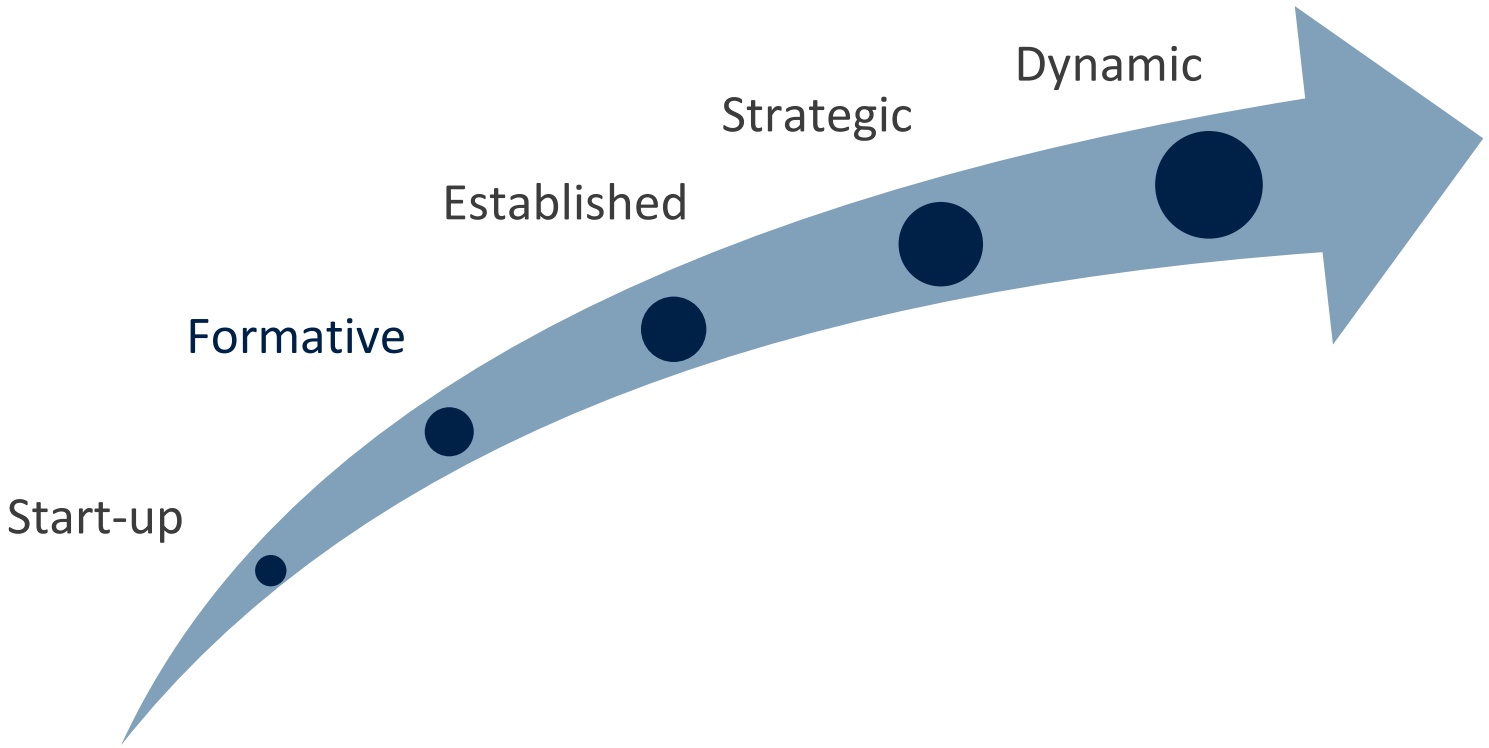


Global Cyber Security Capacity Centre

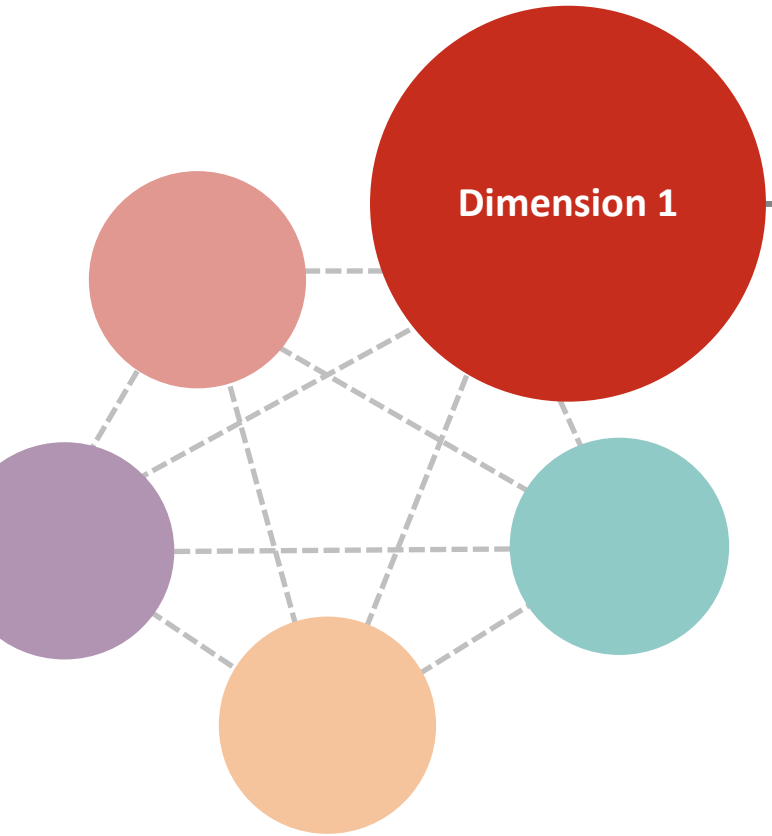
OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Stages of Maturity

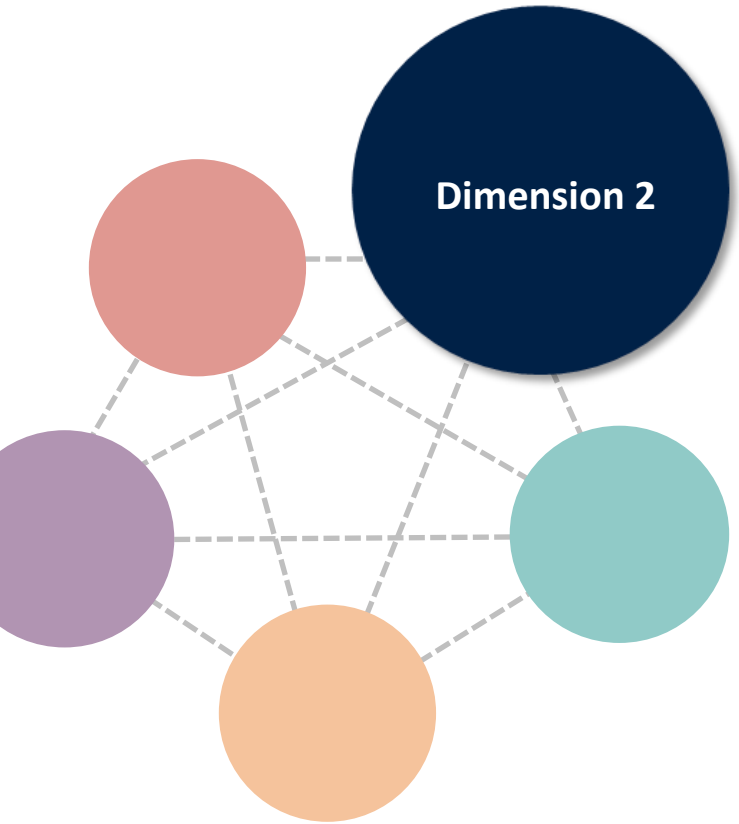


CYBERSECURITY POLICY AND STRATEGY



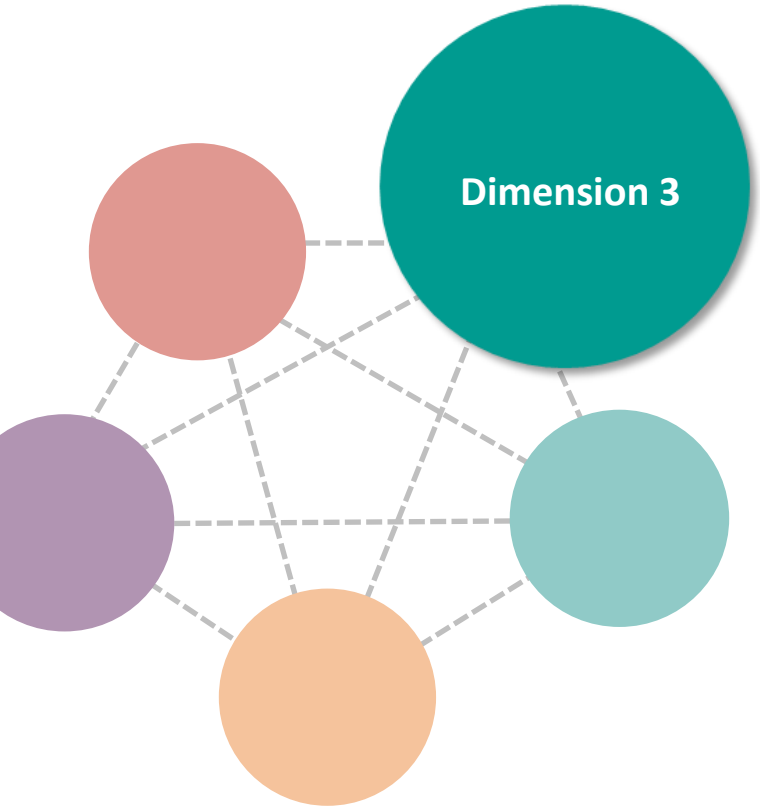
- D1.1 National Cybersecurity Strategy
- D1.2 Incident Response
- D1.3 Critical Infrastructure (CI) Protection
- D1.4 Crisis Management
- D1.5 Cyber Defence Consideration
- D1.6 Communications Redundancy

CYBERSECURITY CULTURE AND SOCIETY



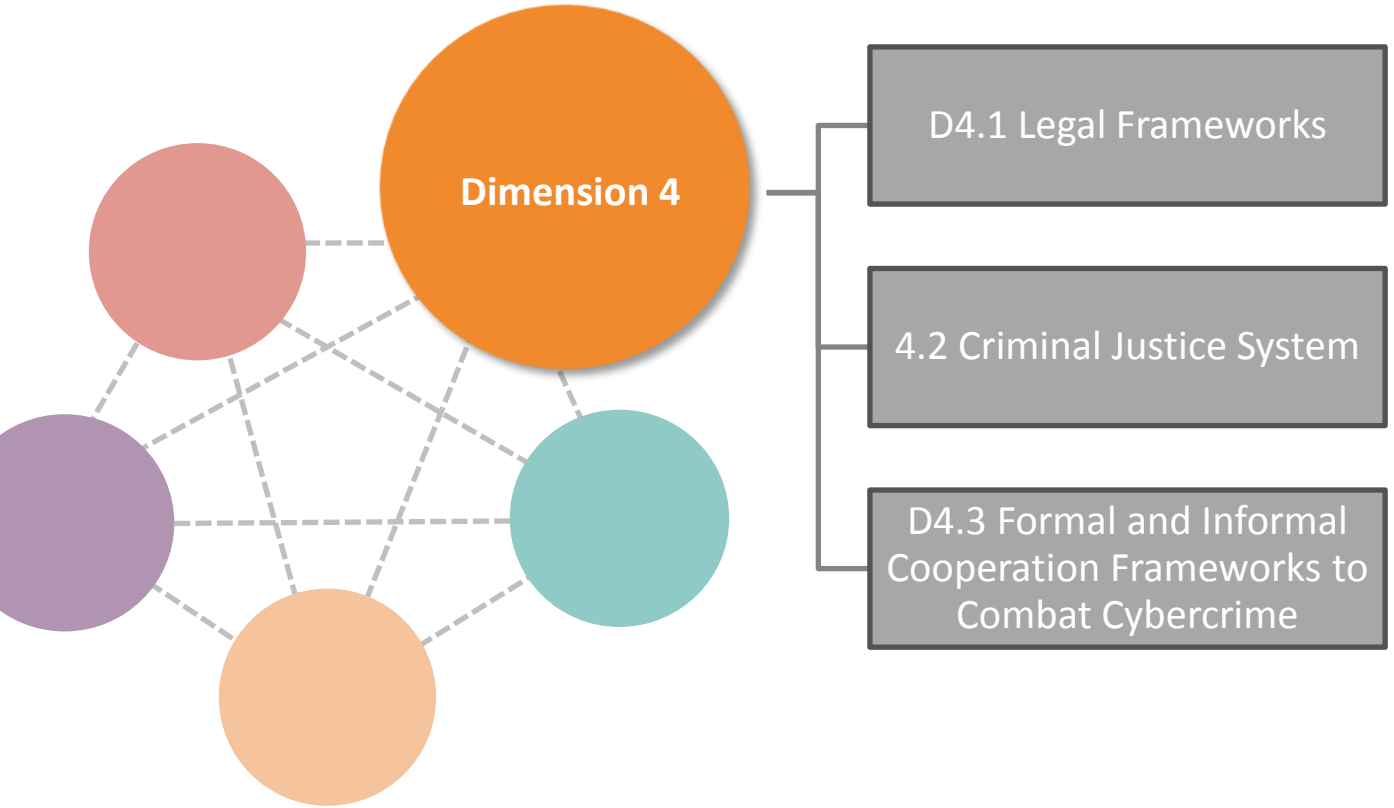
- D2.1 Cybersecurity Mindset
- D2.2 Trust and Confidence on the Internet
- D2.3 User Understanding of Personal Information protection online
- D2.4 Reporting Mechanisms
- D2.5 Media and Social Media

CYBERSECURITY EDUCATION, TRAINING AND SKILLS

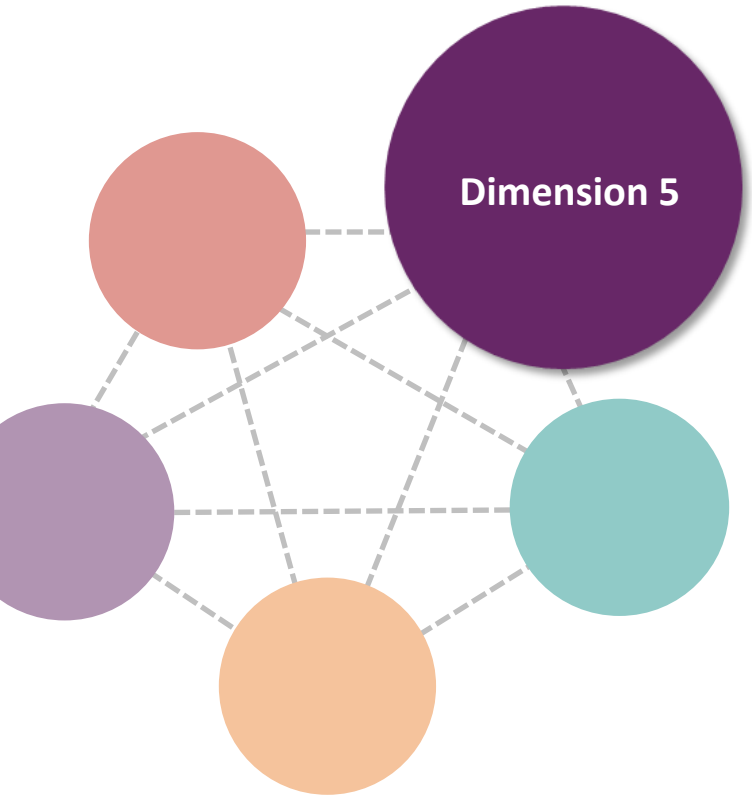


- D3.1 Awareness Raising
- D3.2 Framework for Education
- D3.3 Framework for Professional Training

LEGAL AND REGULATORY FRAMEWORKS



STANDARDS, ORGANISATIONS AND TECHNOLOGIES



- D5.1 Adherence to Standards
- D5.2 Internet Infrastructure Resilience
- D5.3 Software Quality
- D5.4 Technical Security Controls
- D5.5 Cryptographic Controls
- D5.6 Cybersecurity Marketplace
- D5.7 Responsible Disclosure

Cybersecurity Capacity Review
Republic of Cyprus

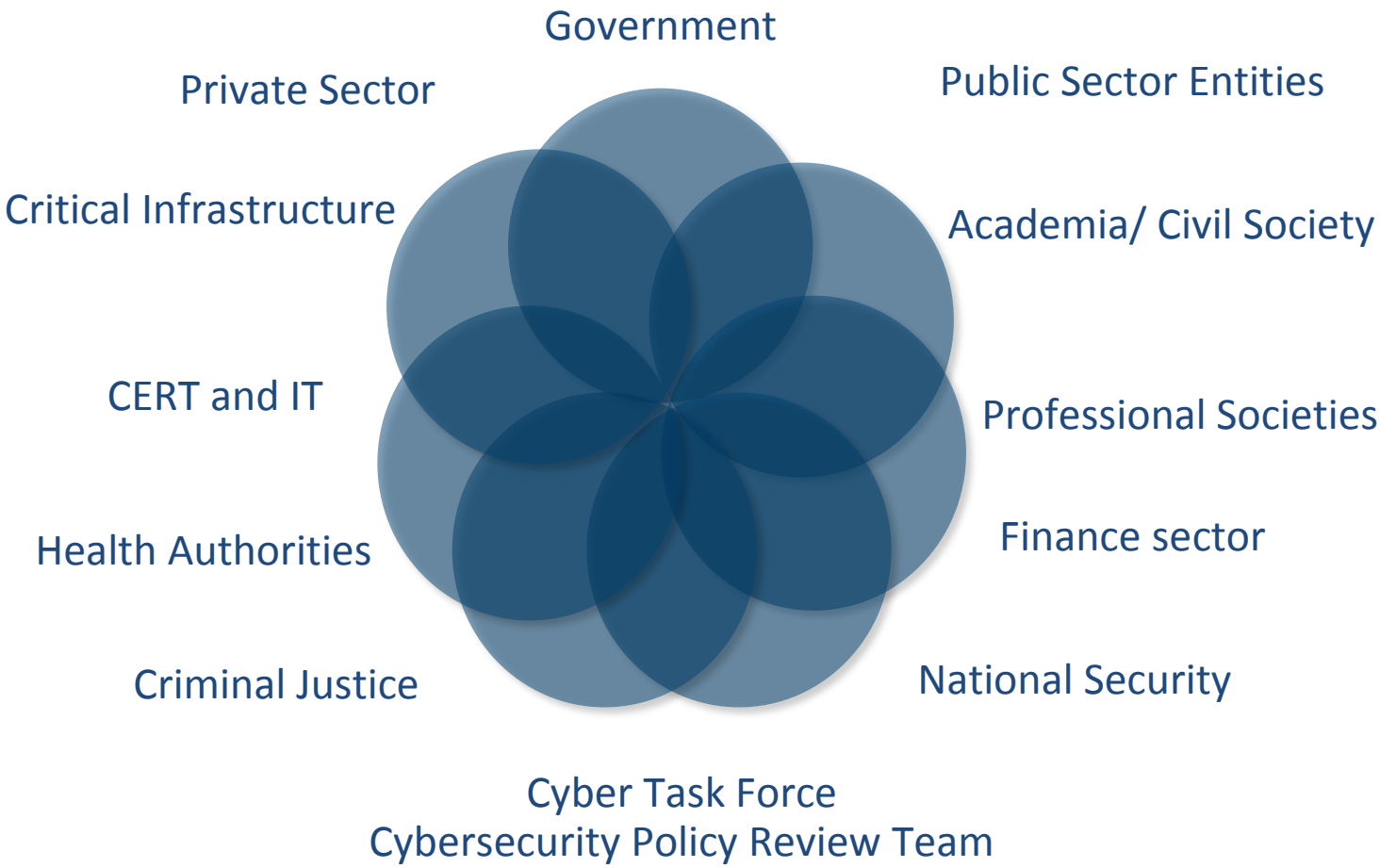
Methodology

Hosted by the Office of the Commissioner of Electronic Communications & Postal Regulation (OCECPR)

Over the period 12-14 July 2017

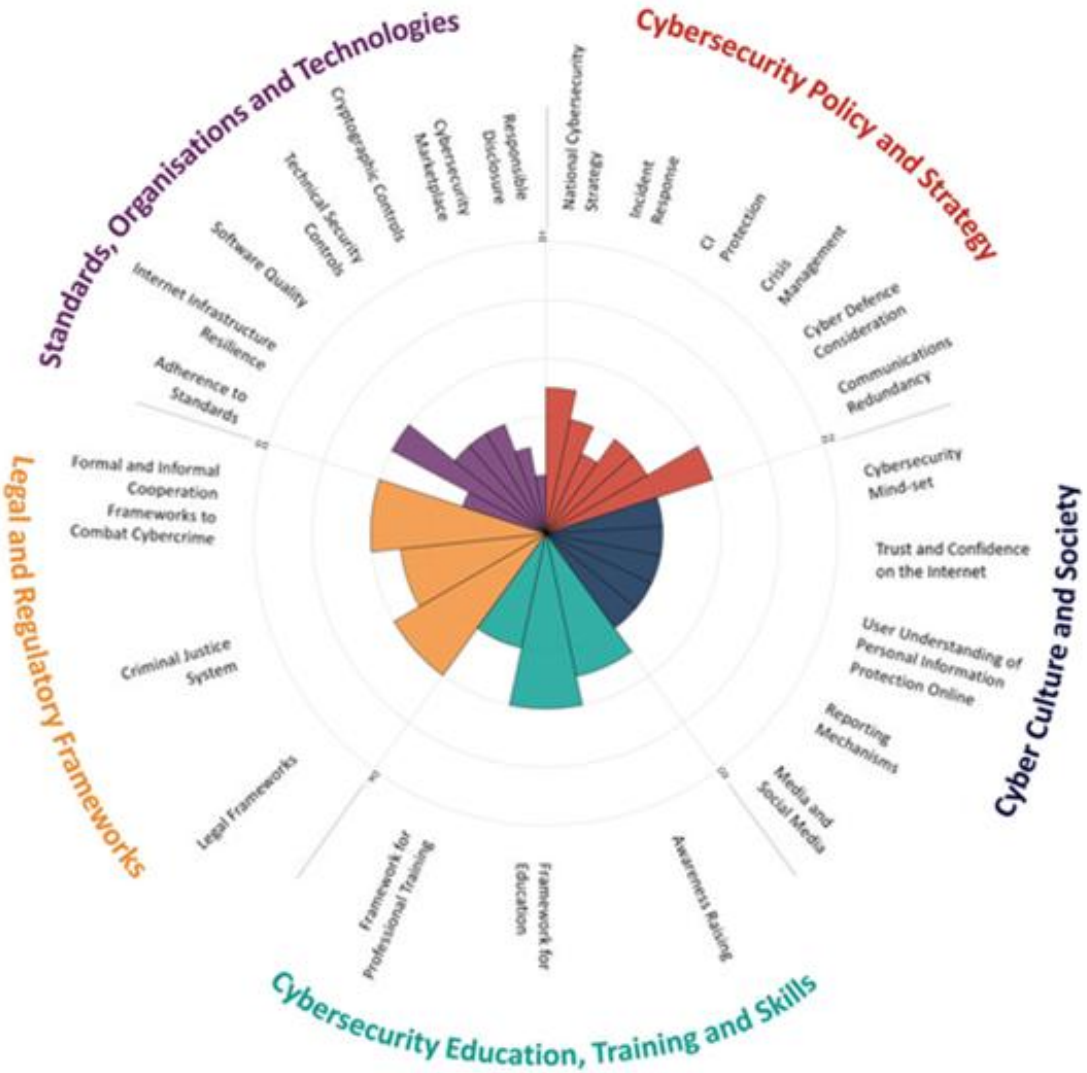
- In-country focus group discussions with key stakeholders from all sectors
- 9 sessions over 3 days
- Research team from the GCSCC

Stakeholder Clusters



CMM Review in Cyprus
Findings

Overall representation of the cybersecurity capacity in the Republic of Cyprus



Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

Cybersecurity Policy and Strategy

- Cyprus is in the process of revising the National Cyber Security Strategy, under the OCECPR while implementing the NISD and GDPR
- A National CERT has been established to act as a central point of contact
- A national level cyber risk assessment methodology developed
- CII asset list developed but not disseminated to all stakeholders
- Formal vulnerability disclosure for CII, Government and Telecoms

Cybersecurity Policy and Strategy

- Risk assessment exercises conducted every 2 years not necessarily including all CII stakeholders
- The National Defence Strategy considers elementary cybersecurity issues but no official cyber defence document developed
- Plans for a Cyber Defence Strategy under way based on the National Cybersecurity Strategy and the OCECPR cyber risk assessment plan
- The Ministry of Defence seeks collaboration with the government and the National CERT as well as other countries
- Emergency response assets in place

CYBERSECURITY CULTURE AND SOCIETY

- Recognition of cybersecurity across government with mandatory password update
- High levels of ''blind'' trust online
- E-government & E-commerce services established
- General knowledge on privacy and protection of personal information online
- Some reporting mechanisms exist on incidents online
- Ad-hoc media coverage of cybersecurity and incidents online

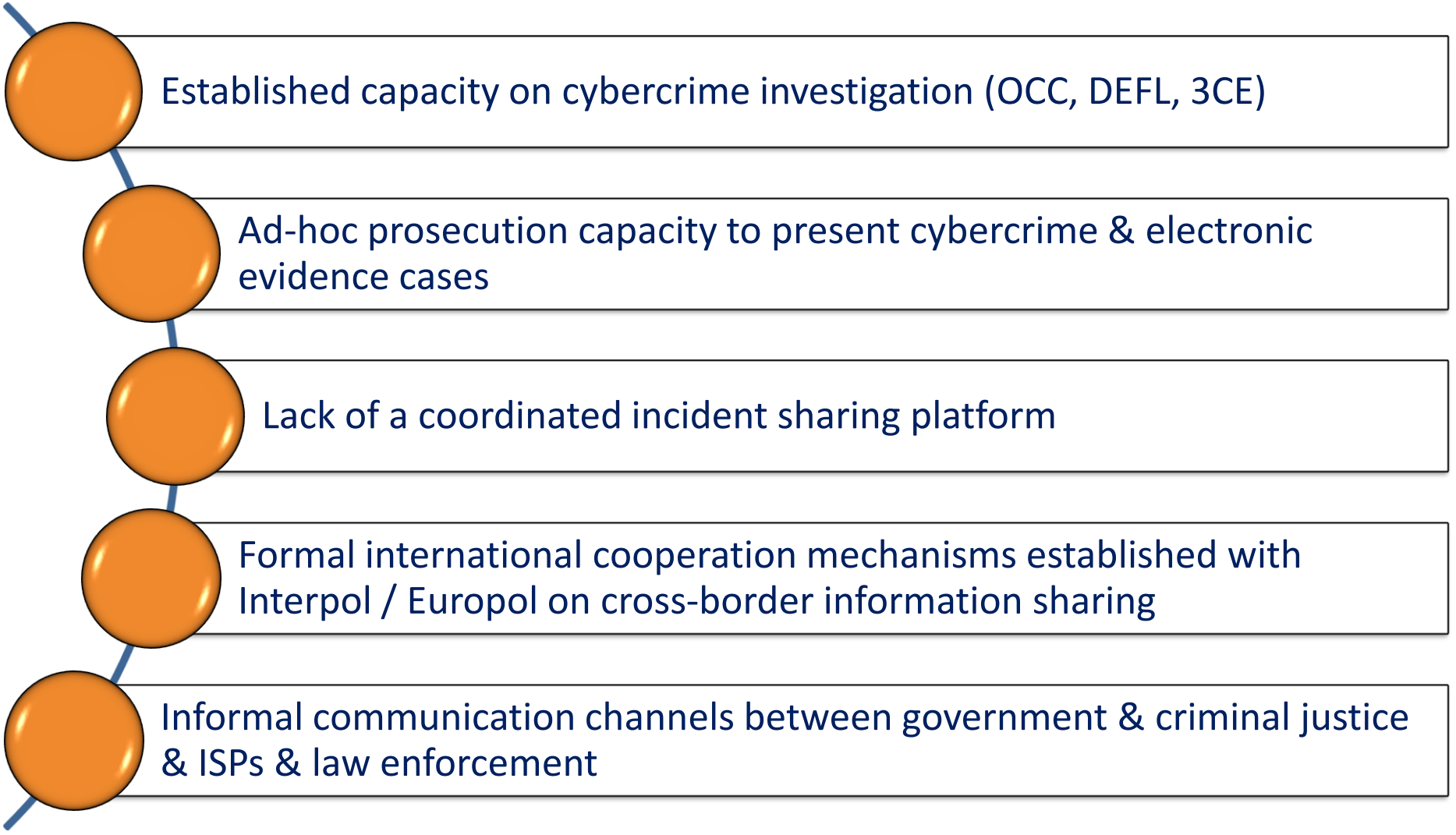
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

- Awareness-raising initiatives developed but no national level programme – Action 14 of NCS speaks on a national awareness & education strategy
- General executive knowledge of cybersecurity issues
- University level courses in cybersecurity offered
- ICT professional certification available
- Need for training professionals in cybersecurity
- Ad-hoc provision of courses for CEOs in cybersecurity and risk management

LEGAL AND REGULATORY FRAMEWORKS

- Provisions on cybersecurity in ICT legislative and regulatory frameworks
- Work underway towards the implementation of NIS Directive and GDPR
- Fundamental human rights recognised in Law (freedom of speech, freedom of information etc.)
- Adopted Child Protection legislation
- Substantive cybercrime legal provisions in criminal law (Budapest Convention)

LEGAL AND REGULATORY FRAMEWORKS



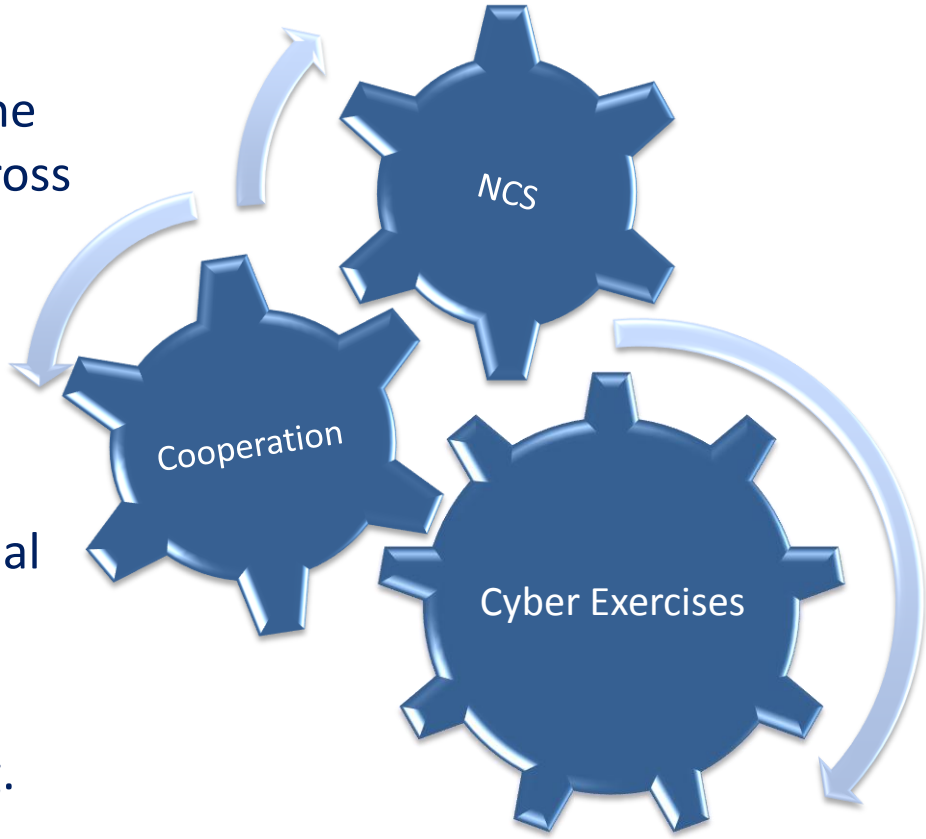
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

- ICT security standards and good practise adopted in public & private sector
- Ad-hoc software quality assessment
- Varying adoption of technical security & cryptographic controls
- Lack of understanding of such controls by general public
- Limited market provisions of cybersecurity and cyber insurance products
- No official vulnerability disclosure framework at place

CMM Review in Cyprus
Recommendations

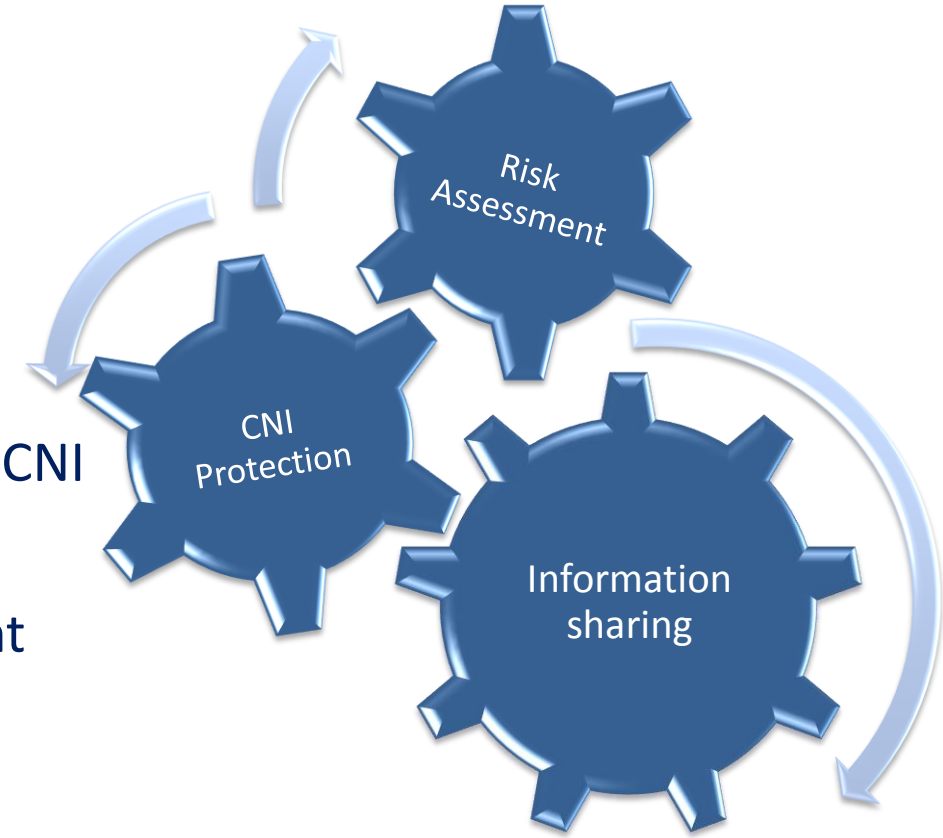
CYBERSECURITY POLICY AND STRATEGY
Recommendations

- Encourage the implementation of the National Cyber Security Strategy across government and other sectors.
- Conduct regular scenario cyber exercises that provide a picture of national cyber resilience.
- Develop a central registry for national level incidents.
- Promote cooperation with other EU CERTs for threat intelligence sharing.



CYBERSECURITY POLICY AND STRATEGY
Recommendations

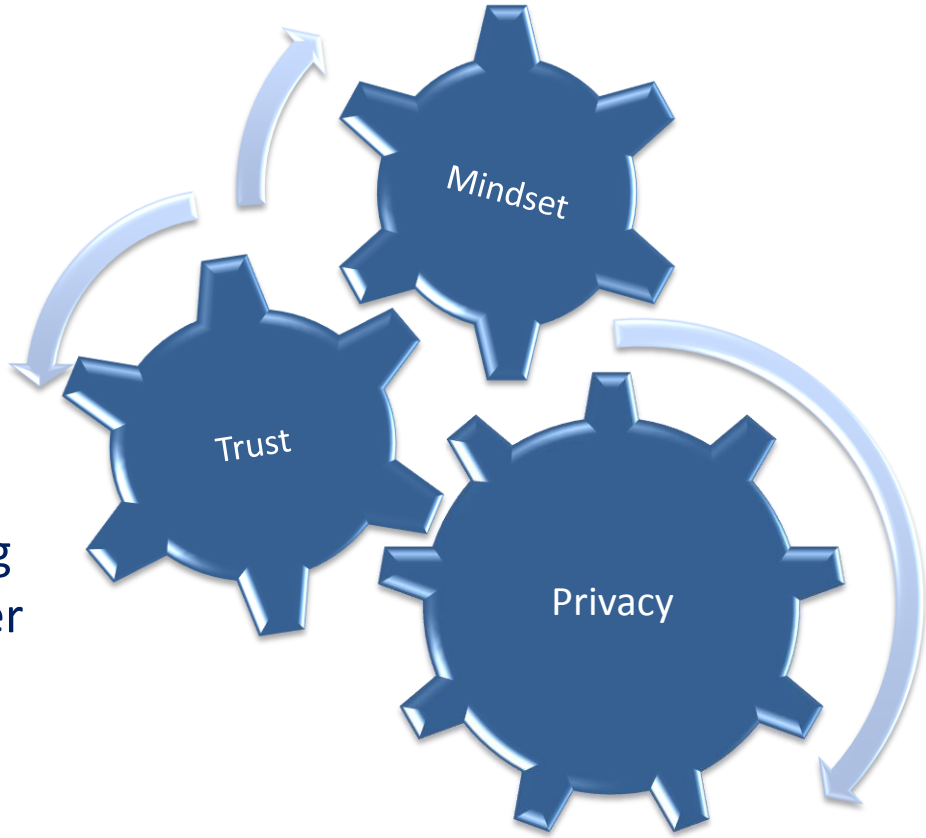
- Strengthen formal coordination regarding CNI protection.
- Promote information sharing between public - private sector & CNI owners.
- Develop a national risk assessment plan for defence.



CYBERSECURITY CULTURE AND SOCIETY

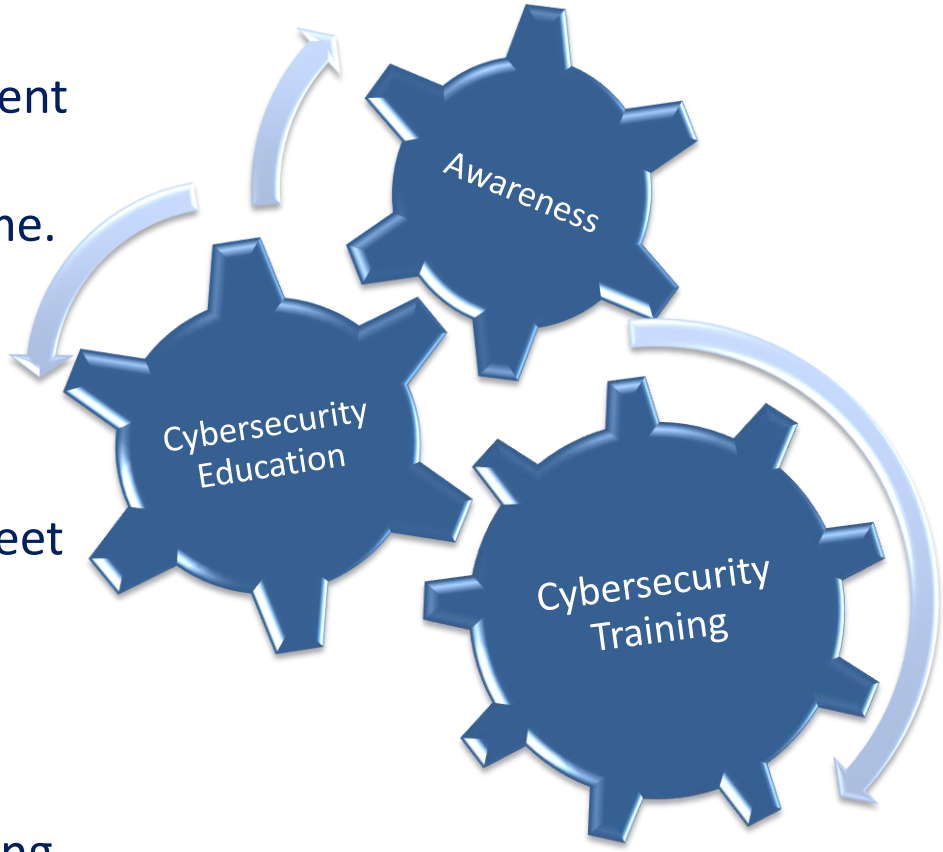
Recommendations

- Promote a cybersecurity mindset.
- Promote the understanding of data protection online.
- Apply security measures to establish trust in e-government and e-commerce services.
- Promote the use of existing reporting mechanisms on child abuse and other online incidents.
- Encourage discussions about cybersecurity on social media.



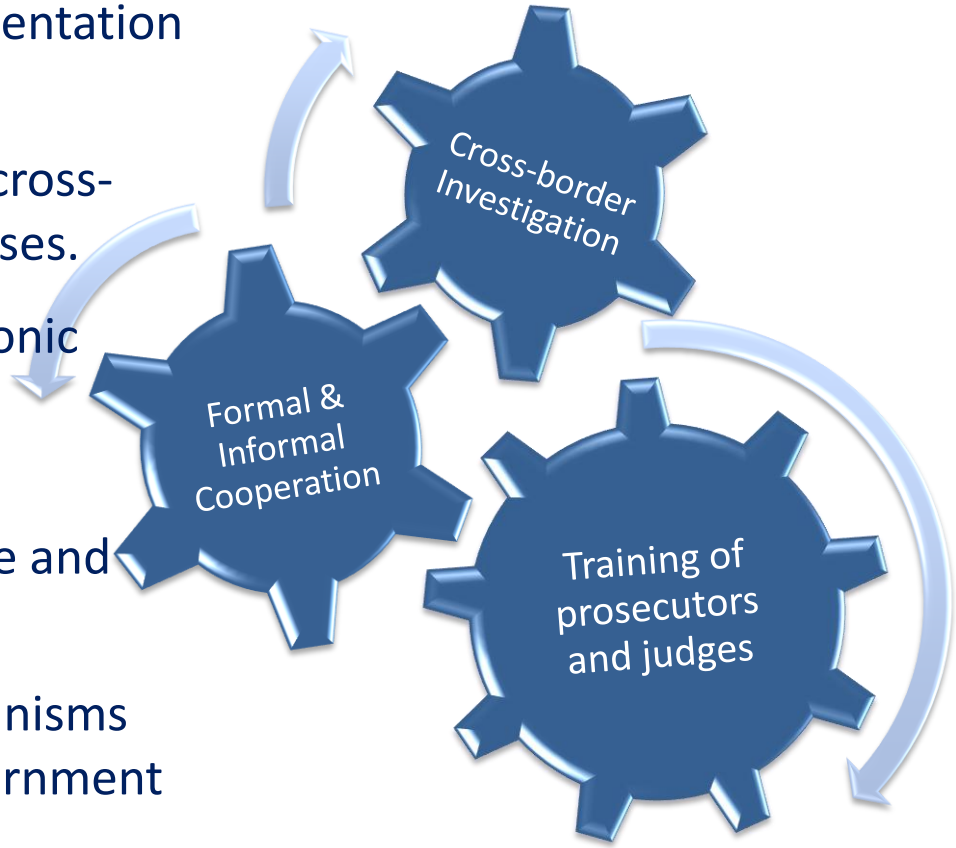
CYBERSECURITY EDUCATION, TRAINING AND SKILLS
Recommendations

- Continue working on the development and implementation of a National Cybersecurity Awareness programme.
- Create cybersecurity education programmes.
- Establish cooperation agreements between academia & industry to meet market demand.
- Establish cybersecurity training programmes for professionals.
- Develop a central platform for sharing training information for experts.



LEGAL AND REGULATORY FRAMEWORKS
Recommendations

- Coordinate work towards the implementation of NIS Directive and GDPR.
- Ensure procedural law provisions on cross-border investigation of cybercrime cases.
- Develop a platform for sharing electronic evidence.
- Enhance training and education of prosecutors and judges on cybercrime and data protection.
- Enhance informal cooperation mechanisms between ISPs, law enforcement, government & criminal justice.



STANDARDS, ORGANISATIONS AND TECHNOLOGIES
Recommendations

- Promote cybersecurity standard adoption in all sectors.
- Conduct regular assessments of processes on national information infrastructure security & critical services.
- Promote understanding of deployment of security controls across all sectors.
- Develop a responsible vulnerability disclosure framework with all stakeholders involved.

Thank you!

Dr Maria Bada, Senior Researcher
Global Cyber Security Capacity Centre
University of Oxford
Maria.Bada@cs.ox.ac.uk

@MariaBadaOxford

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD