CYBER4Dev

Building Cyber Resilience for Development

ENISA Cyber Skills Conference
21/22 September 2023,

Dr Enrico Calandro

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Funded by the European Union

Who we are

EU Funded project, implemented by NI-CO in partnership with:

- RIA (Republic of Estonia, Information System Authority)
- UK Foreign, Commonwealth and Development Office
- Ministry of Foreign Affairs of the Netherlands

Team of experts coming from a range of disciplines. This enabled Cyber4Dev to provide a holistic and comprehensive mentoring approach.

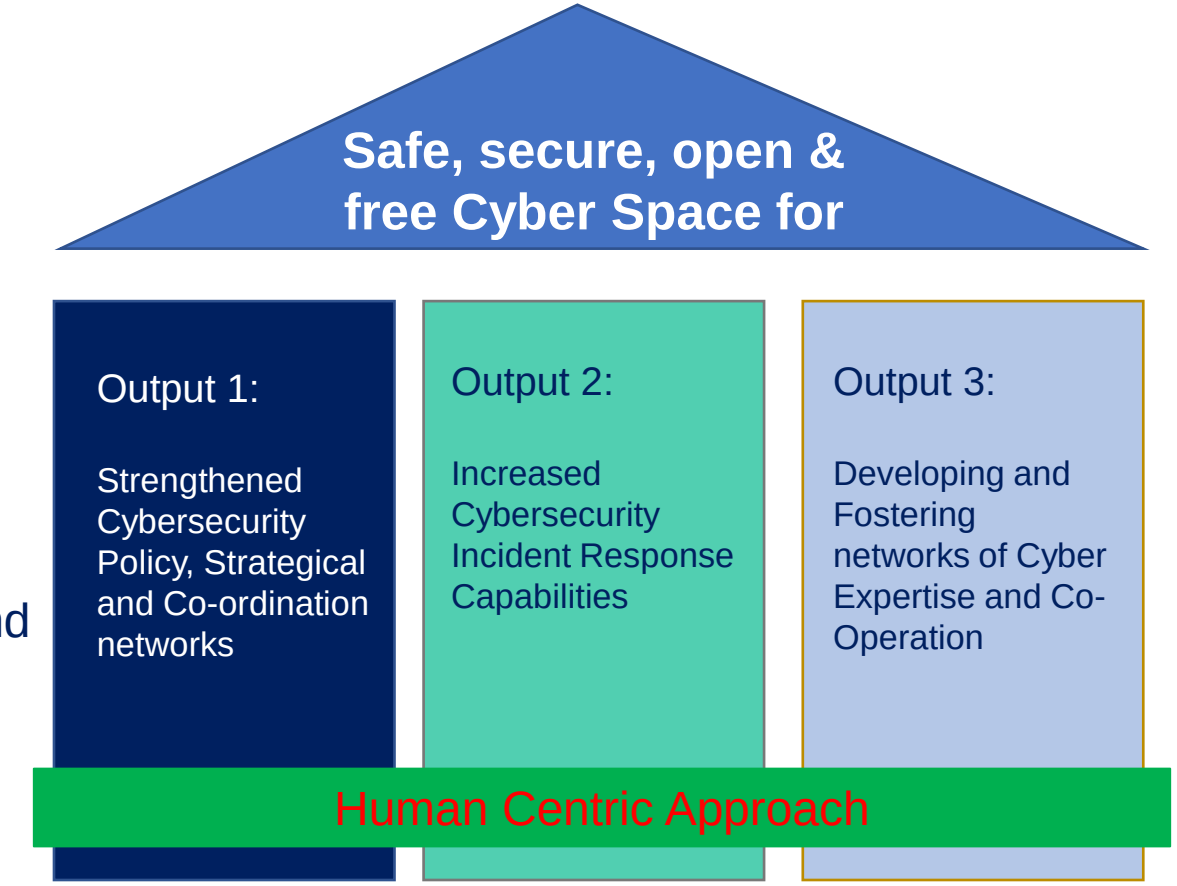
Funded by the European Union

Our priority countries - 2022

Cyber4Dev's Objectives

We support countries to build cyber resilience by:

- Supporting the development of national cyber security strategies and the implementation of detailed action plans
- Establishing, training and empowering Computer Emergency Response Teams
- Building early warning, information sharing and analysis capabilities



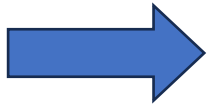
Cyber4Dev as a learning and service provider

Cyber4Dev Services Portfolio Draft v2.0 20 Dec 2022		Cyber4Dev Service Areas		
		Service Area A **Advisory Services**	**Service Area B** **Executive Seminars (ES)** **& Workshops (WS)**	**Service Area C** **Training Courses**
Cyber4Dev Main Outcomes	**Pillar 1** **(policy)**	1. National Strategy: 1.1 - Planning & development 1.2 - Implementation support 2. Organisational & national cyber maturity: 2.1 Roles & responsibilities 2.2 Cross-government & multi-stakeholder communication 2.3 Awareness raising campaigns 2.4 Change management 2.5 Monitoring & measuring progress 2.6 Crisis management 3. Regulatory & policy reviews 4. Multi-stakeholder outreach & cooperation 5. Critical information infrastructure protection (CIIP) 6. National & sectoral CSIRT development 7. International outreach & collaboration: 7.1 For Cyber4Dev beneficiary countries 7.2 Liaisons with ENISA, FIRST, GFCE, AU, OAS, APCERT etc.	1.1 National Strategy Development & Review (ES) 1.2 CIIP Definition & Planning (ES) 1.3 Decision-maker exercises (ES) 1.4 (n)CSIRT Relationship with Public Stakeholders (WS) 1.5 Digital Transformation & Cyber Security (WS) 1.6 Cyber Security Hygiene (WS)	1.1 Cyber Security Strategy Development 1.2 Information Security Standards 1.3 Critical Information Infrastructure Protection (CIIP) 1.4 Cyber Emergency Preparedness & Crisis Management 1.5 Development & Use of Cyber Security Exercises: strategic/tactical 1.6 Planning and Executing IT Security Assessments *[1.6] not Policy but Operational* 1.7 Establishing Organisational information Security Structures for CISOs 1.8 IT Risk Assessment
	Pillar 2 **(operational)**		2.1 (n)CSIRT: How to Communicate Prevention (WS) 2.2 SIM3 Assessment (WS) 2.3 MISP (WS) 2.4 Open Source Tooling (WS)	2.1 SIM3 Introduction (assessment preparation) 2.2 Essential CSIRT Training 2.3 Advanced CSIRT Management Training 2.4 Advanced CSIRT Technical Training* 2.5 Understanding Exploits I : Overview & Analysis* 2.6 Understanding Exploits II : Defence* 2.7 Detecting Compromise* *2.8* Secure Logging *2.9* Secure Industrial Control Systems (ICS/SCADA)*
	Pillar 3 **(engagement)**		3.1 International Cyber Security Engagement (ES/WS) 3.2 Communication Strategy (WS) 3.3 Trainer & Presenter Skills (WS)	3.1 Programme Management 3.2 Media Training
		Pillar 3 - Services across all Areas * Regional Meetings & Conferences * South-south cooperation * Hub activities		

CYBER4Dev

Recommendations

1. **Project Design:** Integrate the ECSF into various CCB activities in third countries
   - Workforce & skills development, lifelong learning
   - Set M&E indicators
2. **Project Implementation:** Develop& Review curricula, training modules, advisory services by using the ECSF (in terms of skills, knowledge, competence)
3. **Project Output:** Prioritise human to build institutional, operational and technical capacities
4. Increase forms of collaboration between projects on CCB in third countries and ENISA on cyber skills development



- Common language on cyber skills dev between projects
- Sustainability
- Long term impact/Lifelong learning
- Support ambition of EU not only as a regulatory super-power but also global reference body on cyber skills dev & standards

NI·CO
Republic of Estonia Information System Authority
Foreign, Commonwealth & Development Office
Ministry of Foreign Affairs of the Netherlands
Funded by the European Union

CYBER4Dev

www.cyber4dev.eu

Twitter/X @Cyber4Dev
@EnricoCalandro
LinkedIn @Cyber4Dev

NI·CO
Republic of Estonia
Information System Authority
Foreign, Commonwealth & Development Office
Ministry of Foreign Affairs of the Netherlands
Funded by the European Union