Regional Cyber Defence Centre

RCDC

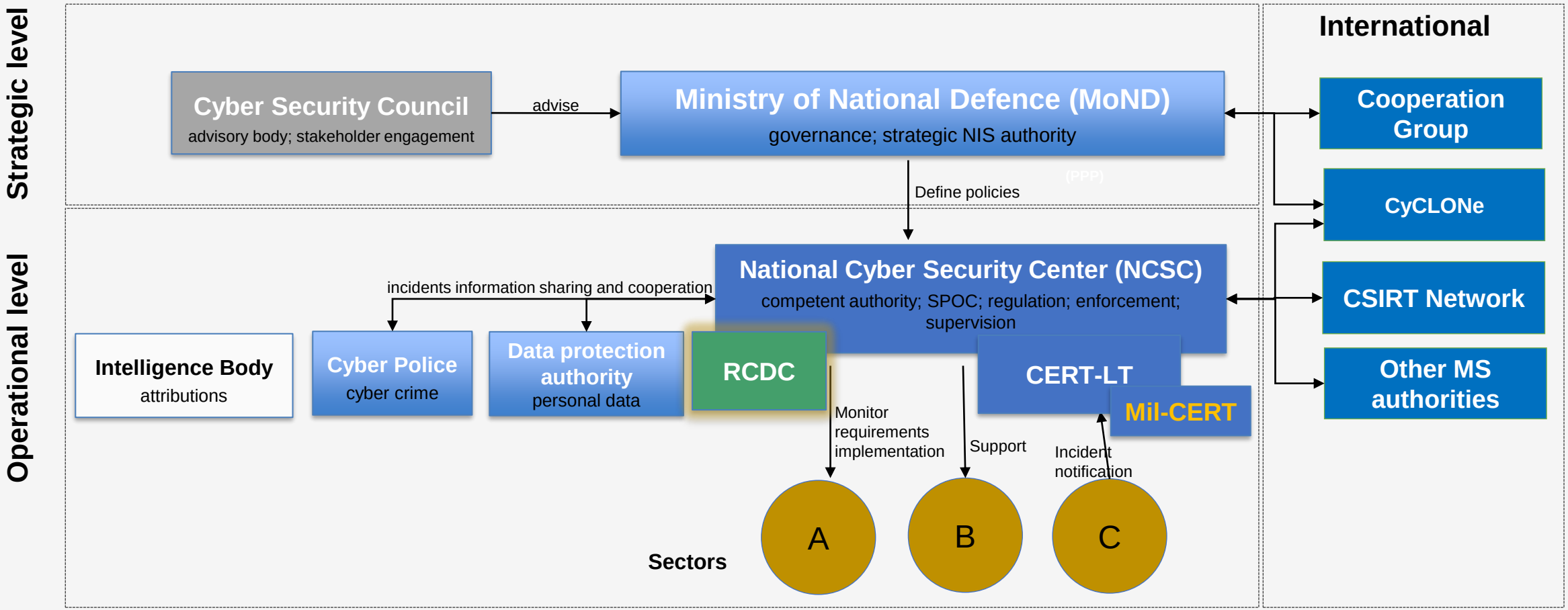
We do cyber security together!

Col. Romualdas Petkevičius, Director

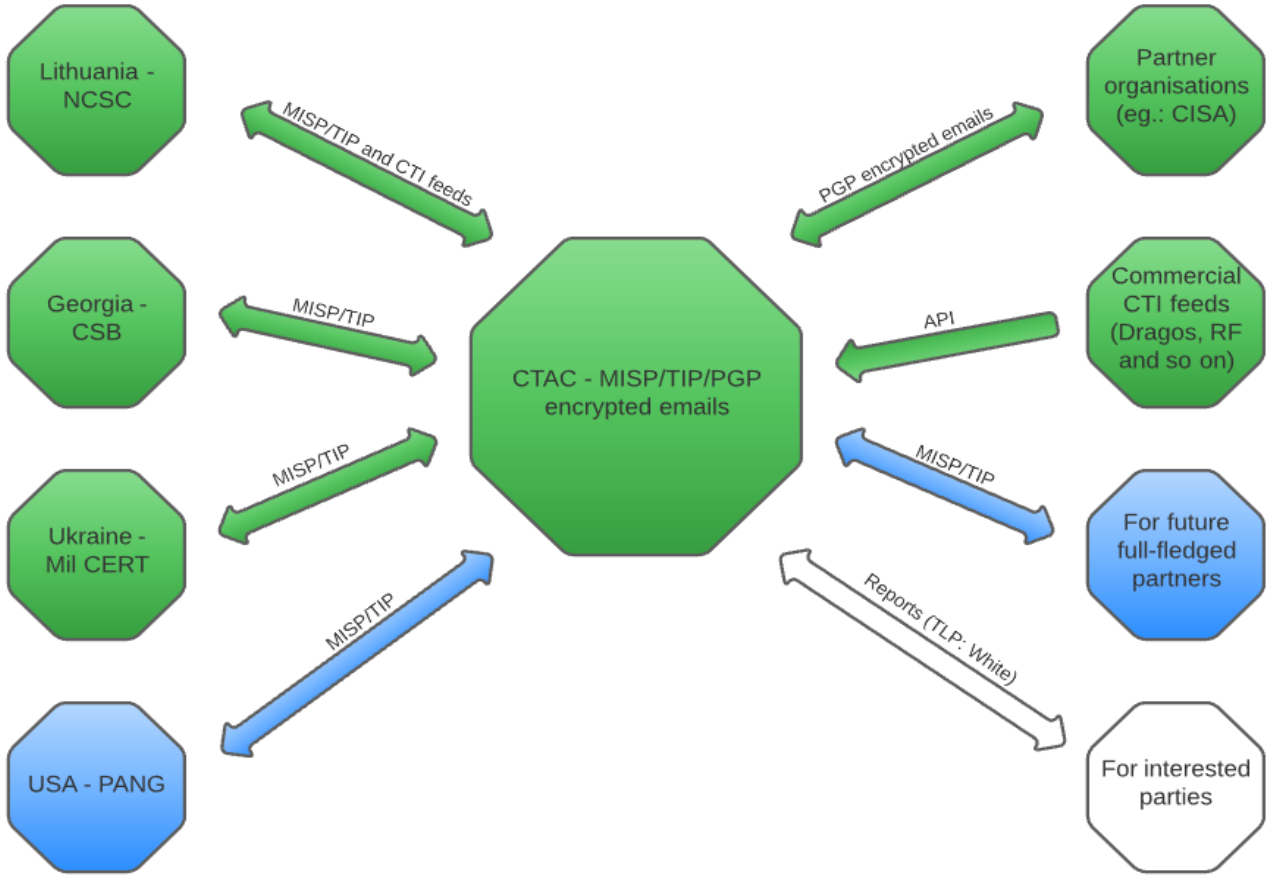
Vision

Collect and analyse information on cyber threats. Prepare and submit actionable information to counter cyber threat units. Organise cyber security exercises and training. Contribute to research related to cyber security.

Lithuania's Approach to Centralised Governance Framework



CTAC – Activity model



Regional Cyber Defence Centre

PPP

In trust we trust!

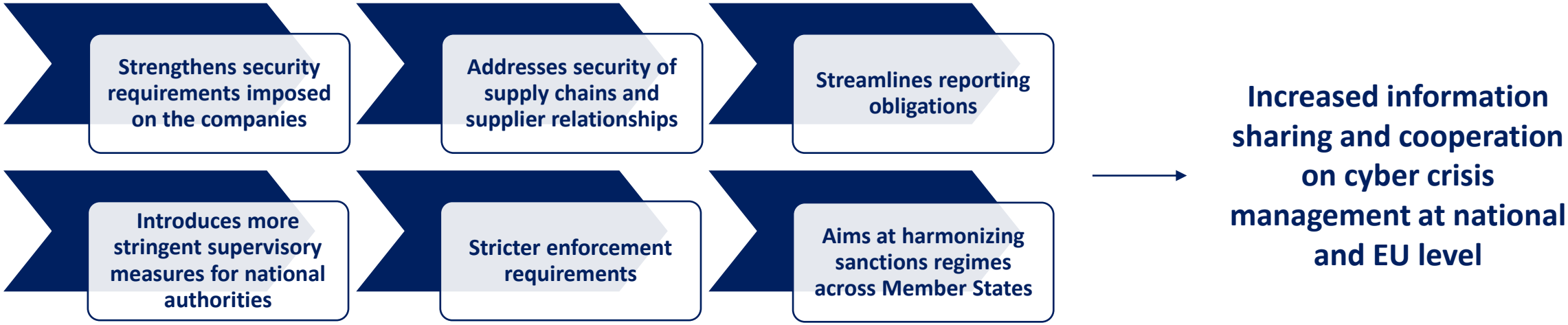
Incentives and regulations

PPP EU Approach: why set up a PPP?

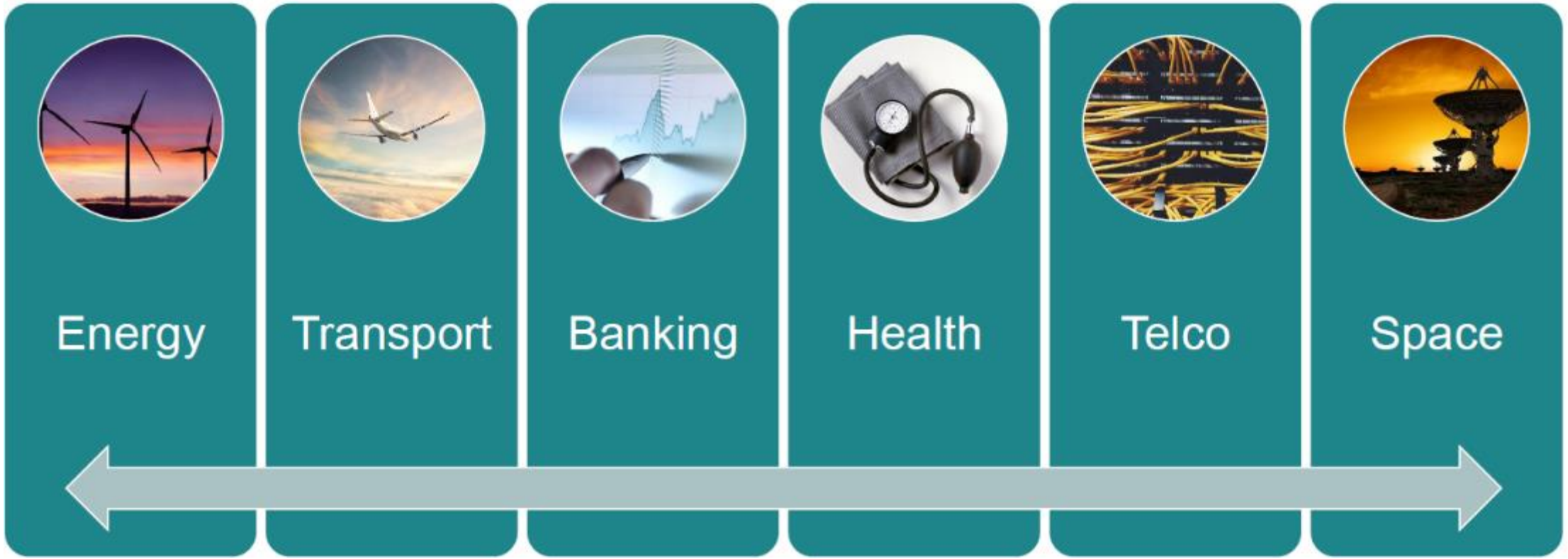
PRIVATE SECTOR REASONS TO PARTICIPATE IN A PPP	PUBLIC SECTOR REASONS TO PARTICIPATE IN A PPP
Access to public funds	Better understanding of Critical Infrastructure Information Protection and industry in general
Opportunity to influence national legislation and obligatory standards	Possibility to create synergies between different initiatives of private sector
Access to public sector knowledge and confidential information (EU legislation, fighting cybercrime)	Access to private sector resources (e.g. experts) which makes it easier to set up standards and good practices
Assurance that the products delivered through PPP are of good quality, as it is guaranteed by the government	
Sharing knowledge, experiences and good practices	
Helping achieve resilience in the cyber ecosystem	
Increased trust between the public-public, private-private and public-private – PPP allows to expand the network and have better information, communication and proactive attitude in case of a crisis	
Acquiring direct and credible network	

Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2')

Covers medium and large entities based on their criticality for the economy and society. At the same time, it leaves some flexibility for Member States to identify smaller entities with a high security risk profile.



Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or ‘NIS 2') identified sectors:



Partner Approach

Trust and mutual respect

Code of conduct

Industry 100

Trust Principles for the PPP

- Exchange of information and cooperation in cybersecurity requires **trust**
- Trust requires involvement and engagement of every member of the PPP
- Certain principles need to be followed in order to achieve mutual trust:
  - **Openness**: only if everybody decides to be open, everyone can benefit
  - **Give and take**: active participation is expected; only if everyone contributes, everybody can take something out
  - **Sensitivity & confidentiality**: every information received in the PPP is treated with sensitivity and confidentiality; the Traffic Light Protocol is respected in any case
  - **No exploitation**: no information received in the PPP, irrespective of the source, is used for exploitation of a personal or professional business advantage
  - **Non-commercialism**: the PPP is not used for advertisement or promotion of products and services

UK NCSC Industry 100

- Industry 100 (i100) is the principal initiative from the NCSC to facilitate close collaboration with the best and most diverse minds in UK industry
- i100 brings together public and private sector talent to challenge thinking, test innovative ideas and enable greater understanding of cyber security – one of the most important issues of our time
- i100 secondees work across a wide range of placements on a part time basis, ranging from one day a week to one day a month

CYBER4DE
Cyber Rapid Response Toolbox for Defence Use

CYBER4DE

CONSORTIUM

BPTI · NRD Cyber Security · LEONARDO · AIRBUS · THALES · asseco · TALGEN · infigo · poslovna inteligencija · comCERT · CY4GATE

Rapid response to cyber-attacks is one of the main interests of European Defence as it strongly affects stability in Europe and outside Europe and wealth and safety of the society.

Launched under European Defence Industrial Development Programme in December 2021, the project “Cyber Rapid Response Toolbox for Defence Use” (CYBER4DE) takes on the challenge to develop an easily deployable, modular, and scalable cyber rapid response toolbox to manage cyber incidents in different complex national and international scenarios.

CYBER4DE stems from the needs of the project “Cyber Rapid Response Teams and Mutual Assistance in Cyber Security” under the Permanent Structured Cooperation (PESCO) framework, which seeks to ensure a higher level of cyber resilience and collective response to cyber incidents among the Union.

Cyber Information Sharing and Collaboration program (CISCP)

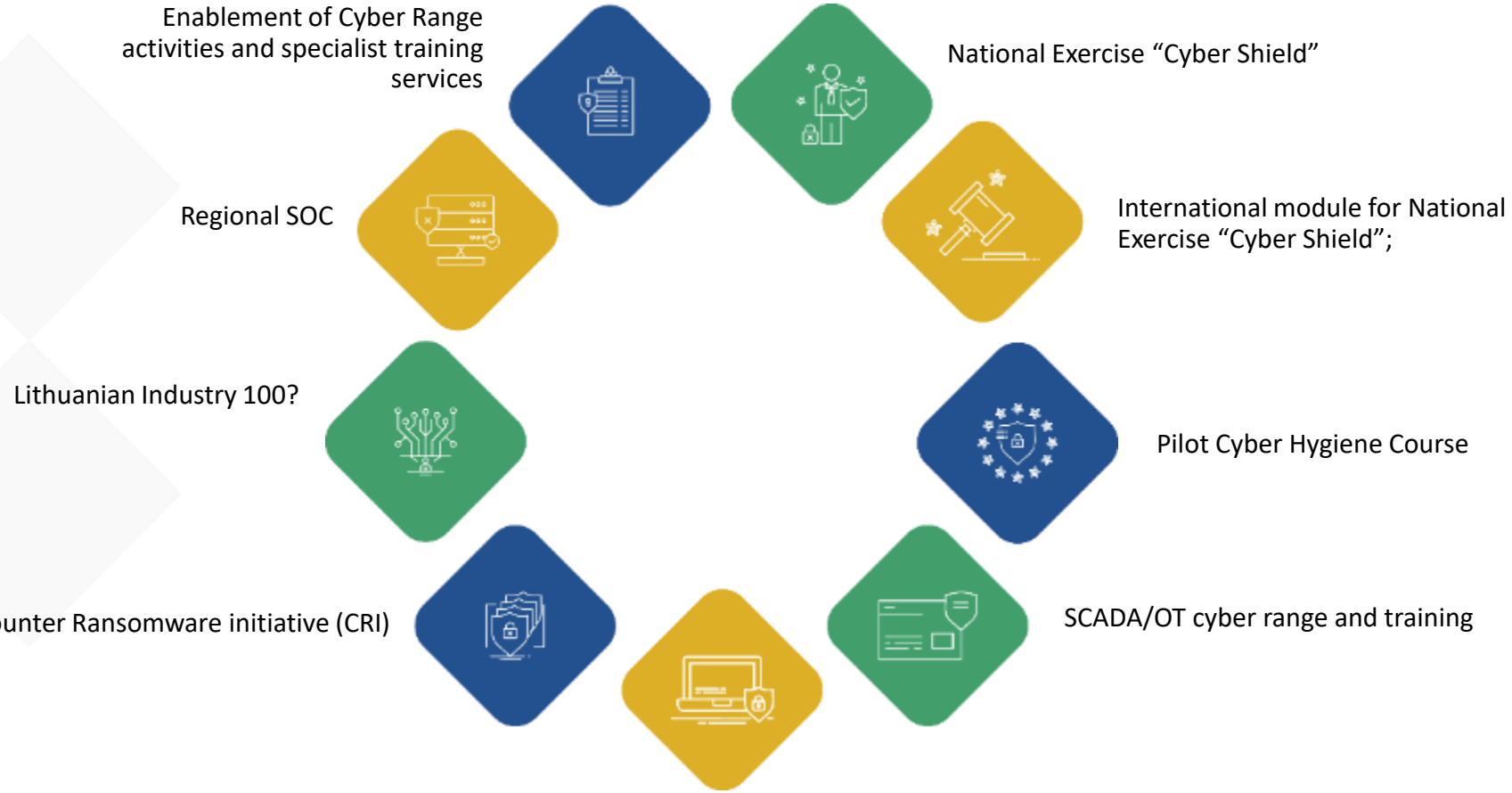
The U.S. Department of Homeland Security (DHS) Cyber Information Sharing and Collaboration Program (CISCP) **enables actionable, relevant, and timely unclassified information exchange through trusted public-private partnerships across all critical infrastructure (CI) sectors.** CISCP fosters this collaboration by leveraging the depth and breadth of DHS cybersecurity capabilities within a focused operational context. Through analyst-to-analyst sharing of threat and vulnerability information, CISCP helps partners manage cybersecurity risks and enhances our collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. CISCP's overall objective is to build cybersecurity resiliency and to harden the defenses of the United States and its strategic partners.

War in Ukraine

- Ukrainian government **went to major** U.S. **information technology and cybersecurity companies**, like Google, Microsoft, Amazon.com and CrowdStrike, and asked them for help and to be part of their cyber defense efforts
- The Ukrainian government managed to realize this whole idea of an **international hacker army** with both defensive and offensive capabilities by integrating the Ukrainian and partner governments, Ukrainian infrastructure operators and IT experts, together with multinational IT and cybersecurity companies outside Ukraine.

  Starlink played an important role in the rapid restoration of communication in critical places and de-occupied territories. “To hell with it… while Starlink is still losing money and other companies are getting billions of taxpayer dollars, we’ll just keep funding the Ukrainian government for free”, - Musk tweeted.

Let’s keep Trusting!



OPTION I

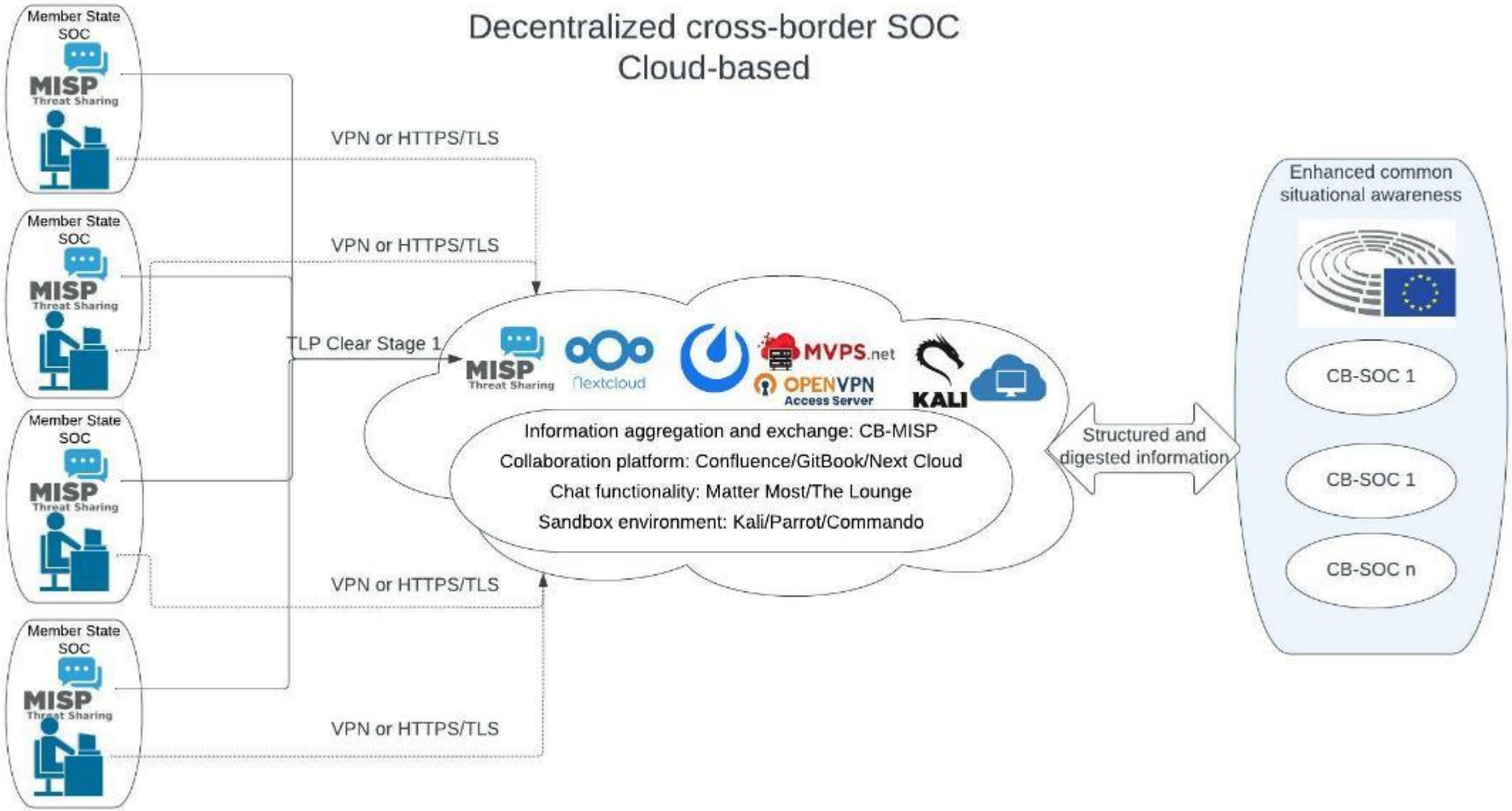
“SCADA Cyber Security Course”

- Technical
- Military and civilian
- OT/ICS Range used for practice
- On RCDC premises
- Up to 30 participants

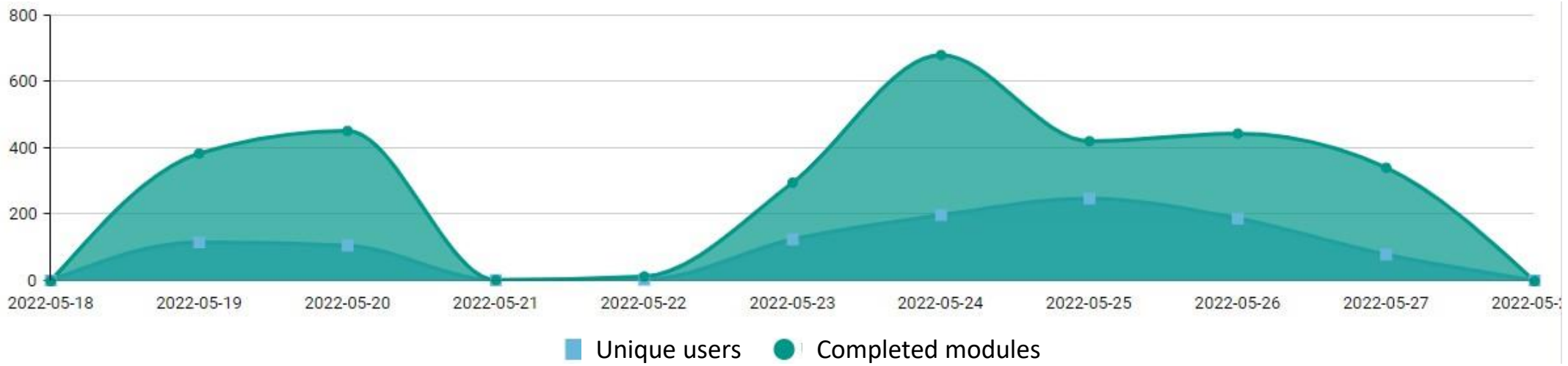
OPTION II

“Cyber Threat Intelligence course”

- Technical
- Military and civilian
- MISP/Eclectic IQ/other used for practice
- On RCDC premises
- Up to 30 participants


Decentralized cross-border SOC
Cloud-based
Member State SOC
MISP Threat Sharing
Member State SOC
MISP Threat Sharing
Member State SOC
MISP Threat Sharing
Member State SOC
MISP Threat Sharing
VPN or HTTPS/TLS
VPN or HTTPS/TLS
TLP Clear Stage 1
VPN or HTTPS/TLS
VPN or HTTPS/TLS
MISP Threat Sharing
Nextcloud
MVPS.net
OPENVPN Access Server
KALI
Information aggregation and exchange: CB-MISP
Collaboration platform: Confluence/GitBook/Next Cloud
Chat functionality: Matter Most/The Lounge
Sandbox environment: Kali/Parrot/Commando
Structured and digested information
Enhanced common situational awareness
CB-SOC 1
CB-SOC 1
CB-SOC n

National and International Cyber Hygiene Course



First group of users finished last week.
Invited: 464; Completed at least one module: 358; Completed the whole course: 304

Regional Cyber Defence Centre

Thank You