



Let's cooperate on securing
digital environments!

Cyber security technology consulting, incident response and applied research company with a focus on services for specialized public service providers, finance industry and corporations with high data sensitivity.



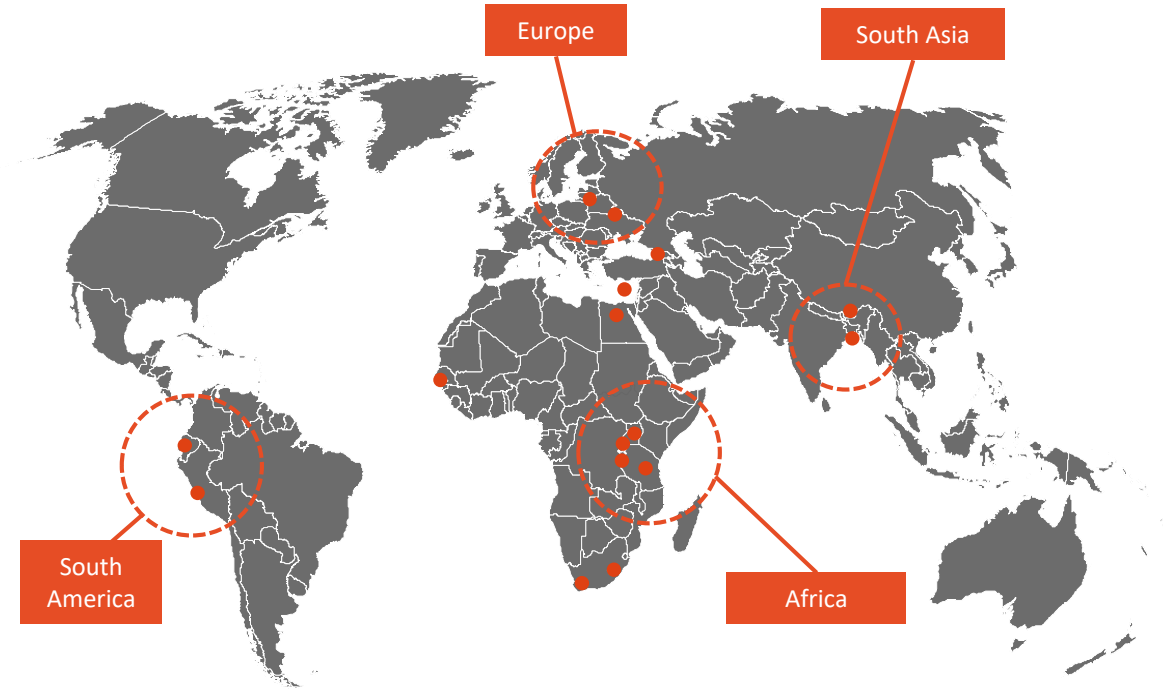
NRDCS.LT

FOCUS

Cybersecurity operation build-out, incident detection and handling, establishment and support of computer security incident response teams (CSIRTs) and cyber capacity enhancement at organizational and national levels

CUSTOMERS

Governments, public and private sector organizations



PARTNERSHIPS AND MEMBERSHIPS



Academia



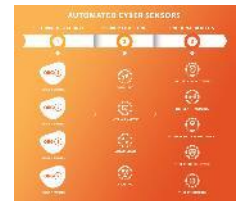
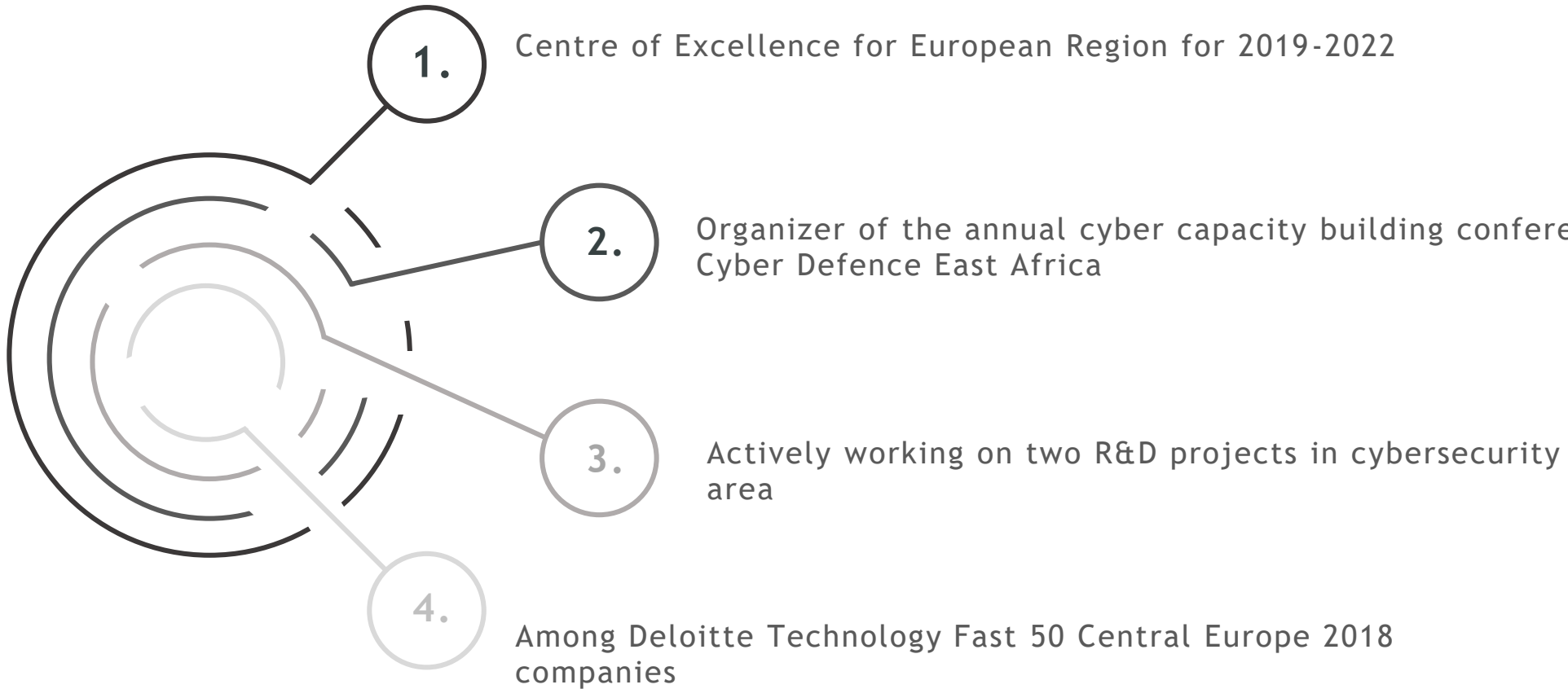
International
community



Associations



QUICK FACTS ABOUT **NRD CYBER SECURITY**



Deloitte



Deloitte Technology
Fast 50 Central Europe 2018

50

WHO I AM



TOMAS MOGODIA

TECHNOLOGY
DEPLOYMENT
MANAGER

- More than 10 years of duty in NATO and Lithuanian armed forces
- NCISG 3rd NSD DCM-D CIS Troop Head
- Deployment to Afghanistan in Sector ISAF
- LTU Armed forces CIS Unit deputy Commander
- LTU Armed forces cyber defence unit Commander

AREAS OF EXPERTISE

- ITIL based service management
- IT project management
- SOC/CSIRT/MilCERT establishment and operations
- Strategic/operational/tactical Cyber Security

Certifications

- CISSP
- ISACA Lithuanian chapter member
- EC Council Certified ethical hacker
- CISCO Cyber Operations certified
- M6-109 Network Vulnerability Assessment & Risk Mitigation course certification
- INFOSEC certified officer
- SIM3 auditor

Collective Cyber Defence: Strategy & Toolkit

NRD Cyber Security
Technology Deployment Manager
Tomas Mogodia

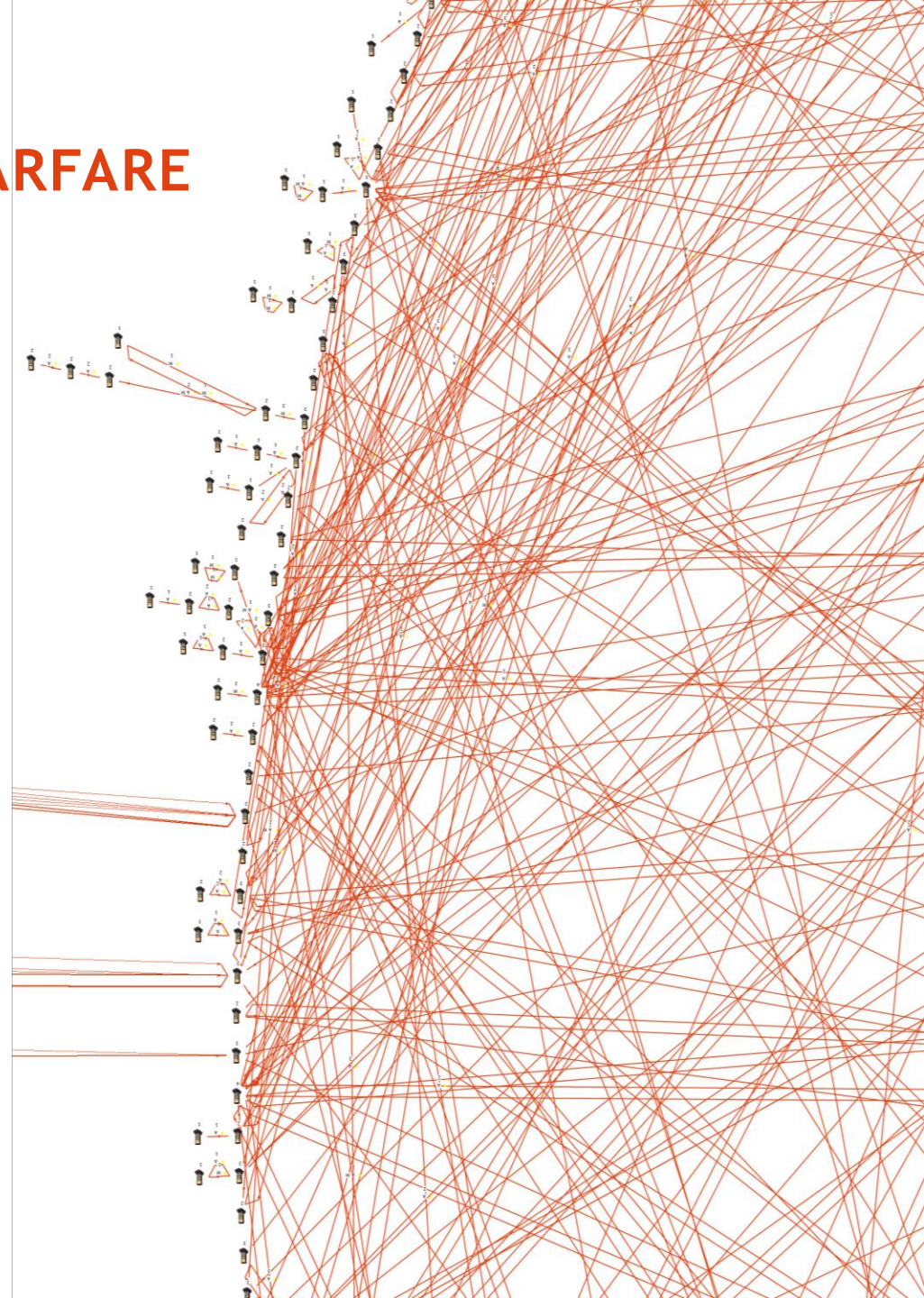
Find us at Lithuanian's stand N10-164!

CONTENT

- Collective cyber defence - what is it?
- What could be the strategy?
- MilCERT as a single point of contact for CyberOPS
- Tactical cyber defense solutions

THE 5th DOMAIN OF WARFARE

Cyberspace is declared as a domain of operations,
just like air, space, land and sea



CYBER OPERATIONS

1. Cyber offensive operations
2. Cyber exploitation operations
3. Cyber defensive operations
4. Global Network Operations

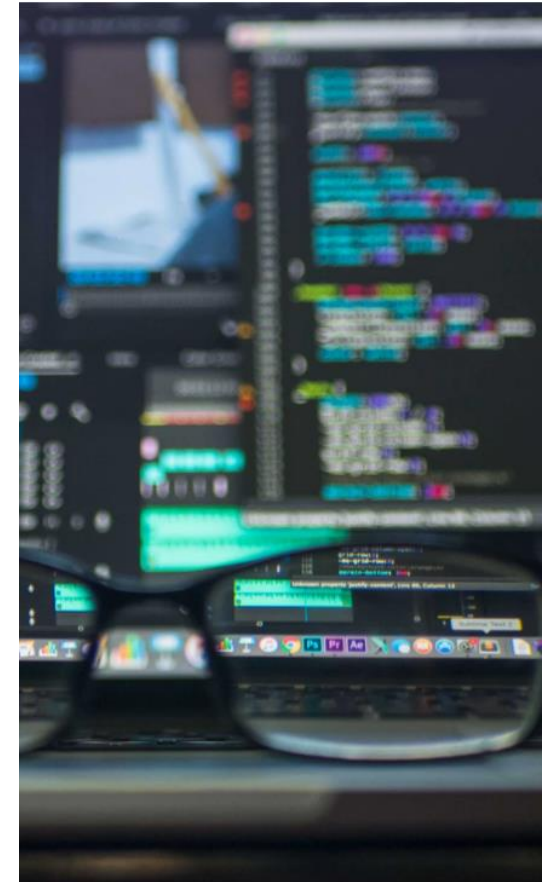
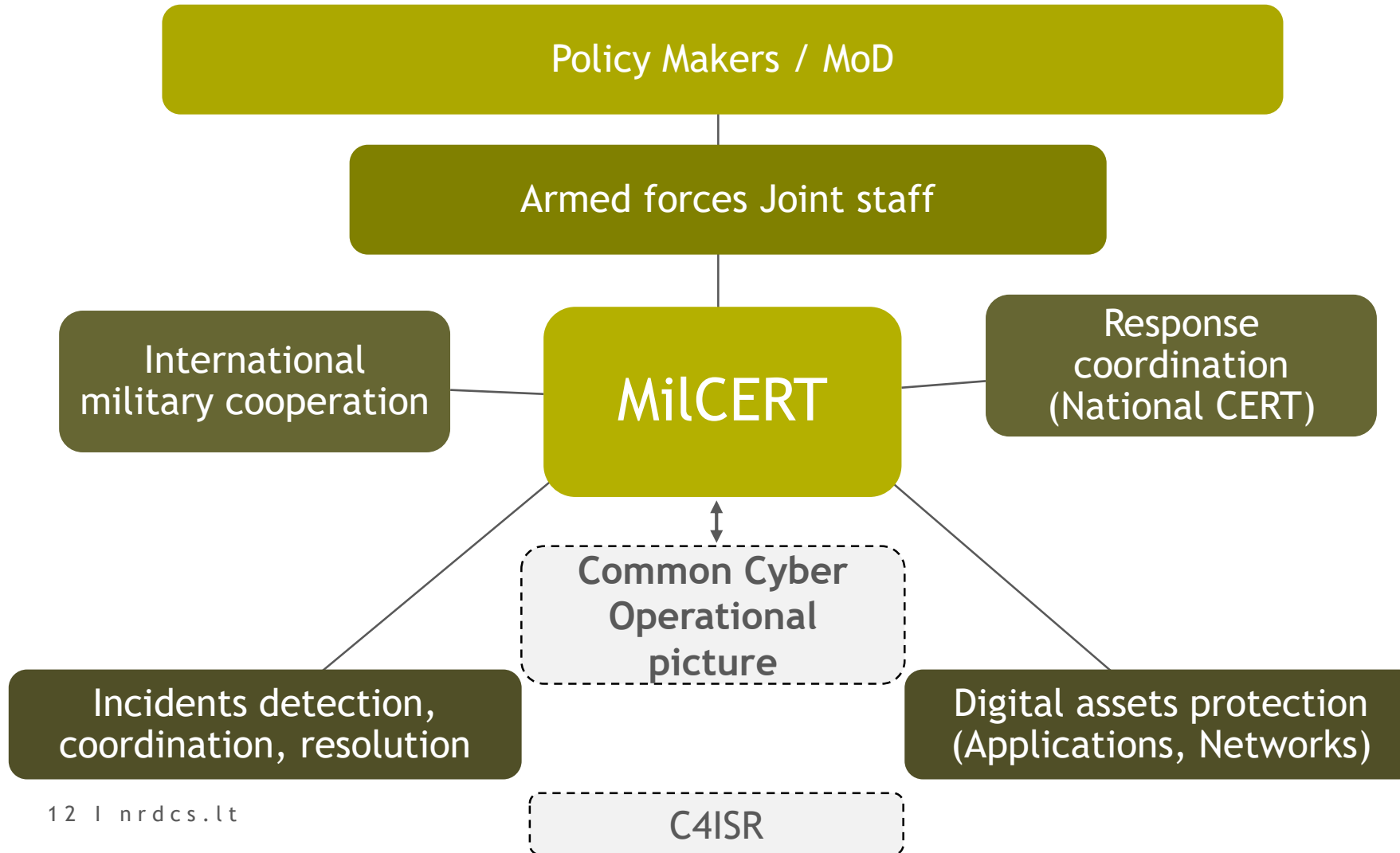
COLLECTIVE CYBER DEFENCE



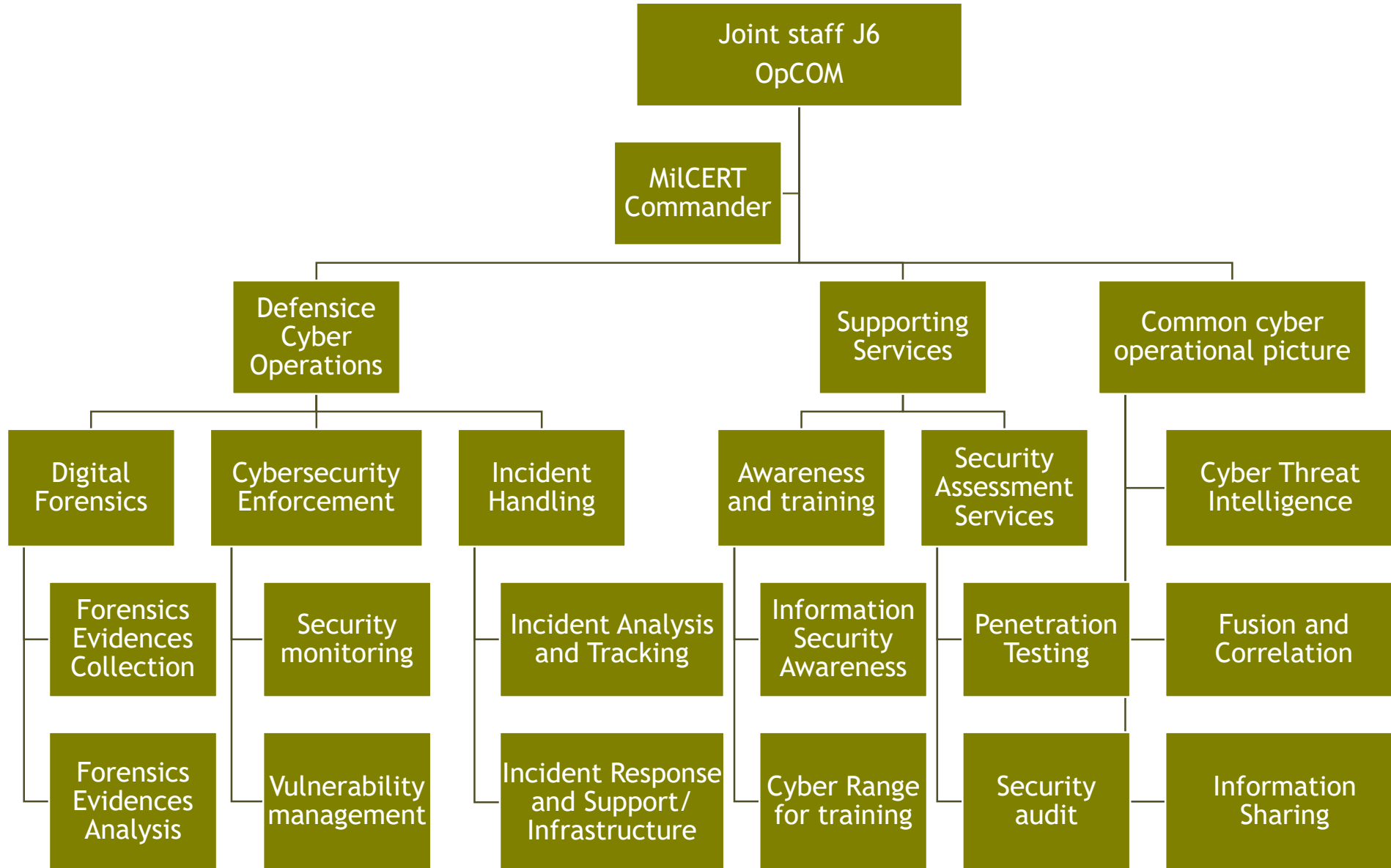
MILCERT AS AN OWNER OF CCOP

1. Single point of contact for all cyber operations
2. Rapid reaction capability in cyber domain
3. Timely exchange of information among involved parties
4. Operational and tactical solutions for cyber defense and IT visibility
5. Common cyber operational picture for cyber and cyber-kinetic situational awareness

MILCERT AS SPOC



MILCERT STRUCTURE



OUR WAY OF DEPLOYING

NRD Cyber Security CSIRT/SOC Stack Options	Mini	Basic	Effective	Full Scale
Governance 	<ul style="list-style-type: none"> ✓ Operational control definition ✓ SOP ✓ Roadmap & Strategy 	<ul style="list-style-type: none"> ✓ Operational control definition ✓ SOP ✓ Roadmap & Strategy 	<ul style="list-style-type: none"> ✓ Operational control definition ✓ SOP ✓ Roadmap & Strategy ✓ Orgchart buildout 	<ul style="list-style-type: none"> ✓ Operational control definition ✓ SOP ✓ Roadmap & Strategy ✓ Orgchart buildout
People 	<ul style="list-style-type: none"> ✓ Featured MILCERT training ✓ Limited remote support 	<ul style="list-style-type: none"> ✓ Relevant MILCERT training ✓ Remote support ✓ SOPs ✓ Study mission tours 	<ul style="list-style-type: none"> ✓ Relevant MILCERT training ✓ Remote support ✓ SOPs ✓ Study mission tours 	<ul style="list-style-type: none"> ✓ Relevant MILCERT training ✓ On-site and remote support ✓ SOPs ✓ Study mission tours
Processes and services 	<ul style="list-style-type: none"> ✓ Defensive Cyber Operations ✓ Incident handling service ✓ Incident handling process 	<ul style="list-style-type: none"> ✓ Defensive Cyber Operations ✓ Incident handling and outreach ✓ Infrastructure support ✓ Standard reporting 	<ul style="list-style-type: none"> ✓ Defensive Cyber Operations ✓ Incident handling, outreach, digital forensics, vulnerability management ✓ Process automation ✓ Infrastructure support ✓ Standard reporting 	<ul style="list-style-type: none"> ✓ Defensive Cyber Operations ✓ Full scale MILCERT/SOC services ✓ Process automation ✓ Automated custom reporting ✓ Maturity progress assessment ✓ Infrastructure support
Measurements 	<ul style="list-style-type: none"> ✓ A few KPIs ✓ No SLAs 	<ul style="list-style-type: none"> ✓ Basic KPIs ✓ SLAs for processes 	<ul style="list-style-type: none"> ✓ KPIs system ✓ SLAs for processes ✓ SIM3 audit 	<ul style="list-style-type: none"> ✓ KPIs system ✓ SLAs for services and automation ✓ Annual reviews, SOC-CMM L3 C1.5
Technological Capability 	<ul style="list-style-type: none"> ✓ Incident registration and handling ✓ Encrypted data communication solution 	<ul style="list-style-type: none"> ✓ Incident registration and handling ✓ Outreach and visualization portal ✓ Internal support ✓ Vulnerability management ✓ Encrypted data communication solution 	<ul style="list-style-type: none"> ✓ Incident detection and handling ✓ Outreach and visualization portal ✓ Internal support, PGP ✓ Vulnerability management ✓ Operations centre establishment ✓ Cyber Threat intelligence ✓ Digital forensics ✓ Integrations deployment ✓ Building Cyber Operational picture ✓ Encrypted data communication solution 	<ul style="list-style-type: none"> ✓ Incident detection and handling ✓ Outreach and visualization portal ✓ Internal support, PGP ✓ Vulnerability assessment ✓ Operations centre establishment ✓ Cyber Threat intelligence ✓ Digital Forensics ✓ Integration with existing tooling ✓ Cyber operational picture ✓ Multi-site sensing ✓ Encrypted data communication solution
Local resources	❖ 2-5 people	❖ 5-10 people	❖ 7-15 people	❖ 15-45 people
Duration	❖ 6 months	❖ 9 months	❖ 12 months	❖ 12-18 months

TACTICAL SOLUTIONS FOR CYBER VISIBILITY



CollectiveSight platform

Collective sight platform can be used as an operational/tactical cybersecurity solution for:

1. Military operations
2. Forward operating bases
3. Both classified and unclassified networks
4. Static and deployable CIS

Cyber visibility allows timely detection, mitigation, and response coordination to cyber-attacks in CII at national and CII's levels.

LET'S HAVE A CHAT!

Find us at DSEI'19: we are part of Lithuanian's stand N10-164!

Visit us in Lithuania!

- www.nrdcs.lt
- Tomas Mogodia tm@nrdcs.lt

