CCDCOE

NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

What is a Centre of Excellence?

- Allied Command Transformation (ACT) has overall responsibility for the currently **29 NATO accredited Centres of Excellence (COE)**.
- COEs are nationally or multi-nationally funded. NATO does not directly fund COEs and COEs are **not part of the NATO Command Structure**.
- The COEs cover a **wide variety of areas** such as civil-military operations, cyber defence, military medicine, energy security, naval mine warfare, defence against terrorism, cold weather operations, and counter-IED.
- In addition the European Centre of Excellence for Countering Hybrid Threats (**Hybrid CoE**) in Helsinki focuses on responses to hybrid threats under the auspices of the European Union and NATO.

CCDCOE


ALLIED COMMAND TRANSFORMATION
NOR
4
8
30
EST
LVA
LTU
13
DNK
7
GBR
CAN
3
5
USA
2
6
26
17
NLD
BEL
LUX
DEU
21
23
POL
18
10
14
CZE
SVK
22
15
HUN
HRV
SVN
25
29
FRA
28
1
27
24
ITA
19
PRT
9
ESP
ROU
11
MNE
BGR
20
ALB
MKD
GRC
16
12
TUR
1 Analysis and Simulation Center for Air Operations (AO), Lyon
2 Civil-Military Cooperation (CCOE), The Hague
3 Climate Change and Security (CCAS), Montreal *Under Establishment Process
4 Cold Weather Operations(CWO) Elverum
5 Combined Joint Operations from the Sea (CJOS), Virginia
6 Command & Control (C2), Utrech
7 Operations in Confined and Shallow Waters (CSW), Kiel
8 Cooperative Cyber Defense (CCD), Tallinn
9 Counter-Improvised Explosive Devices (C-IED), Madrid
10 Counter Intelligence (CI), Krakow
11 Crisis Management & Disaster Response (CMDR), Sofia
12 Defence Against Terrorism (CAT), Askara
13 Energy Security (ENSEC), Vilnius
14 Explosive Ordnance Disposal (EOD), Trencin
15 Human Intelligence (HUMINT), Oradea
16 Integrated Air & Missile Defence (IAMD), Chania
17 Joint Air Power Competence Centre (JAPCC), Kalkar
18 Joint Chemical Biological Radiological & Nuclear Defence (JCBRN-D), Vyskov
19 Maritime Geospatial, Meteorological & Oceanographic (MGEOMETOC), Lisbon
20 Maritime Security (MARSEC), Istanbul
21 Military Engineering (MILENG), Ingolstadt
22 Military Medicine (MILMED), Budapest
23 Military Police (MP), Bydgoszcz
24 Modelling & Simulation (M&S), Rome
25 Mountain Warfare (MW), Begunje na Gorenjskem
26 Naval Mine Warfare (NMW), Ostende
27 Security Force Assistance (SFA), Rome
28 Space , Toulouse *Under Establishment Process
29 Stability Policing (SP), Vicenza
30 Strategic Communications (STRATCOM), Riga
NATO CENTRES OF EXCELLENCE
LOCATIONS

NATO Cooperative Cyber Defence Centre of Excellence

- International and multidisciplinary cyber defence hub
- Established in 2008, accredited by NATO
- 32 like-minded nations + 7 joining from NATO and beyond
- Cooperation with nations, NATO, academia, private sector etc
- Evolving to stay relevant and cutting-edge

CCDCOE

Mission

The mission of the NATO CCDCOE is to support **NATO and the Centre's member nations** in the fields of **cyber defence research, training and exercises** by providing **cyber defence expertise** within the focus areas of **technology, strategy, operations and law**.

CCDCOE

Flagship Projects

LOCKED SHIELDS

CROSSED SWORDS

CYCON
INTERNATIONAL CONFERENCE ON CYBER CONFLICT

TALLINN MANUAL
INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

Vision

- NATO CCDCOE maintains its position as
  - an internationally recognised cyber defence hub,
  - a premier subject matter expert and
  - a fundamental resource in strategic, legal, operational and technical aspects of cyber defence.
- The CCDCOE offers
  - thought leadership on the cutting edge of all aspects of cyber defence and
  - provides a 360-degree view of the sector.
- The CCDCOE encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its focus areas of technology, strategy, operations and law.

CCDCOE

We …

… help NATO and nations to understand and utilise cyberspace as a domain of operations

… research, train and exercise cyberspace defence and operations in from all angles

… are the fundamental resource with a 360-degree view on strategic, legal, operational and technical aspects on cyberspace operations and defence

CCDCOE

Member nations

CCDCOE

Research

We conduct interdisciplinary applied research in:

- → Cyber technology
- → Strategic impact of cyberspace
- → Operational planning
- → International law and cyber norms

CCDCOE

Research Areas

- AI and autonomous features of cyber operations
  - Legal
  - Ethical
  - Technical
  - Operational
- Cyber effects in battlefield
- Digital forensics (in military operations)
- Cyber command and control
- Attribution & deterrence
- Critical infrastructure protection
- Approaches of non-Western States to international law & cyber operations
- National cybersecurity strategy & governance

CCDCOE

Research

- Cyber strategy, policy, doctrine & concepts
- International Law & Cyber Operations
- Autonomous features of cyber operations
- 5G security & threats
- Attribution & deterrence
- Critical infrastructure protection
- Cyber operational picture
- National cybersecurity strategy & governance
- Digital forensics (in military operations)
- Cyber dependencies of military mobility
- Cyber physical systems
- Cyber effects in battlefield
- Cyber command and control

CCDCOE

Research projects on 5G

- 1st joint 5G military security workshop hosted by ACT and CCDCOE (Febr 2021)
- Securing 5G networks for military mobility, project funded by USA and Estonia (2021)
- Developing a 5G security testbed to be used at the Centre's cyber defence exercises
- …and others on security aspects of 5G technology

CCDCOE

Cyber Defence Library

- Recent research publications
- INCYDER articles & Recent Cyber Events series
- National cyber strategies and legislation
- Expanded and upgraded Cyber Law Toolkit
- …and much more on:

ccdcoe.org

CCDCOE

Training

CCDCOE promotes continuous learning in cyber security

Our training courses are based on our latest research and cyber defence exercises

CCDCOE

CCDCOE coordinates cyber training within NATO

- → Identify training needs
- → Coordinate education and training solutions across the Alliance
- → Work closely with NATO Allied Command Transformation (ACT)
- → Unconditional quality assurance accreditation from ACT

CCDCOE

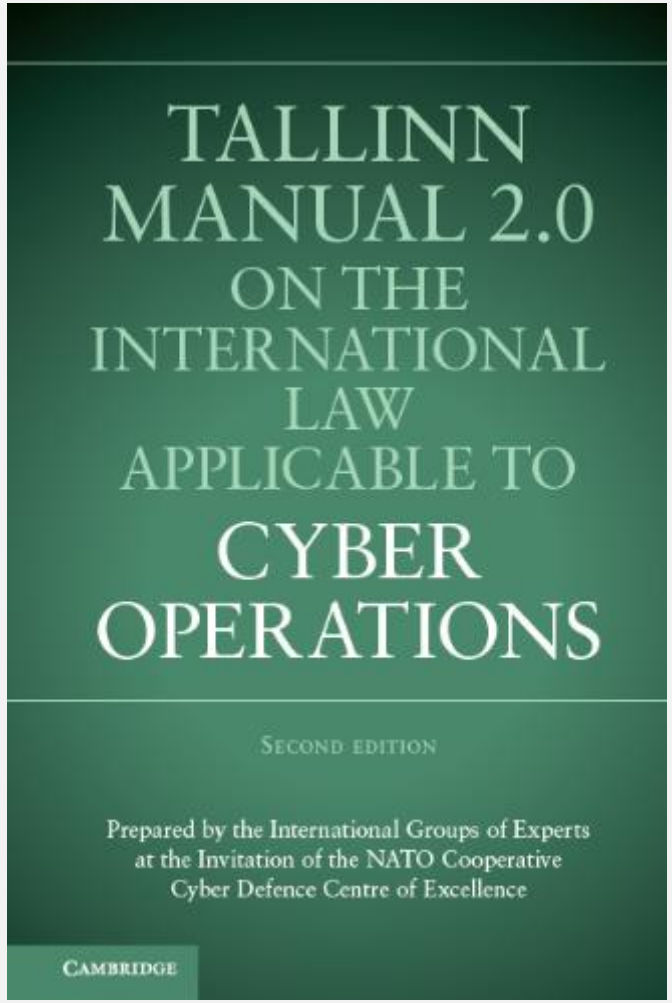
Cyber related Training portfolio

- Senior Leadership Seminar
- Strategic Level Training
- Operational Planning Training
- Training on International Law
- Technical Expert Training

CCDCOE

Strategic, Operational and Legal Training

- **Senior Leadership Training**
  - Executive Cyber Seminar
- **Operational Level Training**
  - Integration of Cyber Considerations into Operational Planning Course
  - Operational Cyber Threat Intelligence Course
  - Critical Information Infrastructure Protection Course
- **Legal Training**
  - International Law of Cyber Operations Course

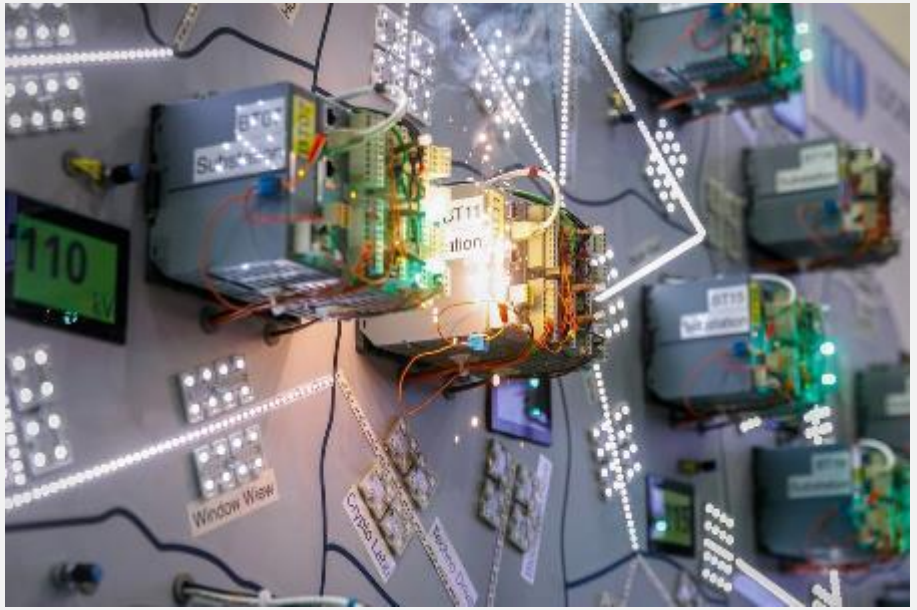


CCDCOE

Technical Training

→ Technical Trainings

- Malware and Exploits Essentials Course
- Cyber Defence Monitoring Course Suite:
  - Module 1: Rule-based Threat Detection Course
  - Module 2: Stream Data Mining Workshop
  - Module 3: Large Scale Packet Capture Analysis Course
- IT Systems Attacks and Defence Course
- Botnet Mitigation Course
- Introductory Digital Forensics Course
- Web Security Essentials Course
- Industrial Control Systems Security Course
- Smartphone Security and Forensics Course



CCDCOE

e-Learning Materials

- The Centre's e-Learning materials are published on the NATO e-Learning website (JADL)
- **General awareness course:** ADL 076 Cyber Defence Awareness (from 2013)
- **Specific Admin Awareness course:** ADL 335 Cyber Awareness course for System Administrators (under update)
- Cyber Awareness Course **Tallinn Manual Module**
- e-Learning materials to support the technical courses

CCDCOE

e-Learning materials to support the technical courses

- ADL 344 Digital Forensics and Digital Evidence (Pre-study material for Introductory Digital Forensics Course)
- ADL 345 Network and Log Monitoring (Pre-study material for Cyber Defence Monitoring Course)
- ADL 346 Web Application Security (Pre-study material for Web Applications Attack and Defence Course)
- ADL 347 Critical Infrastructure and Industrial Control Systems (Pre-study material for Industrial Control Systems Security Course)

CCDCOE

e-Learning materials to support the technical courses

- ADL 348 Fighting a Botnet Attack: a Case Study (Pre-study material for Botnet Mitigation Course)
- ADL 349 Systematic Approaches to the Mitigation of Cyber Threats (Pre-study material for Botnet Mitigation Course)
- ADL 343 Information Security Management System

CCDCOE

Exercises

CCDCOE organizes and contributes to exercises targeting technical experts and decision-makers in member nations and within NATO

CCDCOE

Exercises and exercise support

- CCDCOE develops and organizes Cyber exercises **Locked Shields** and **Crossed Swords**
- Support to NATO Cyber Defense Exercise **Cyber Coalition**
- Support to NATO military exercises for evaluation and certification (e.g. **TRIDENT Juncture**)
- Cyber related scenarios and injects
- Cyber operations **inject database**

CCDCOE

Flagship Projects

LOCKED SHIELDS

CROSSED SWORDS

CYCON
INTERNATIONAL CONFERENCE ON CYBER CONFLICT

TALLINN MANUAL
INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

LOCKED SHIELDS

CROSSED SWORDS

CROSSED
SWORDS

Exercise Crossed Swords (XS)

- Developed and conducted since 2014
- Exercises essential aspects of cyber operation
- Complex scenario integrating cyber and conventional elements
  - Integrates innovative technologies, tactics, techniques and procedures
- Exercises Command & Control (C2) to include intelligence in conflict situation

CCDCOE

Crossed Swords 2021

Offensive Cyber Operations, Digital Forensics, Cyber Command HQ, kinetic operations with battlefield forensics

CROSSED SWORDS

- **400** Virtual Machines
- **108** participants from more than 21 countries
- **200** Offensive Cyber Operations target systems
- **150** Offensive Cyber Operations machines attack infrastructure and testing
- Windows, Linux, Siemens Spectrum and many more

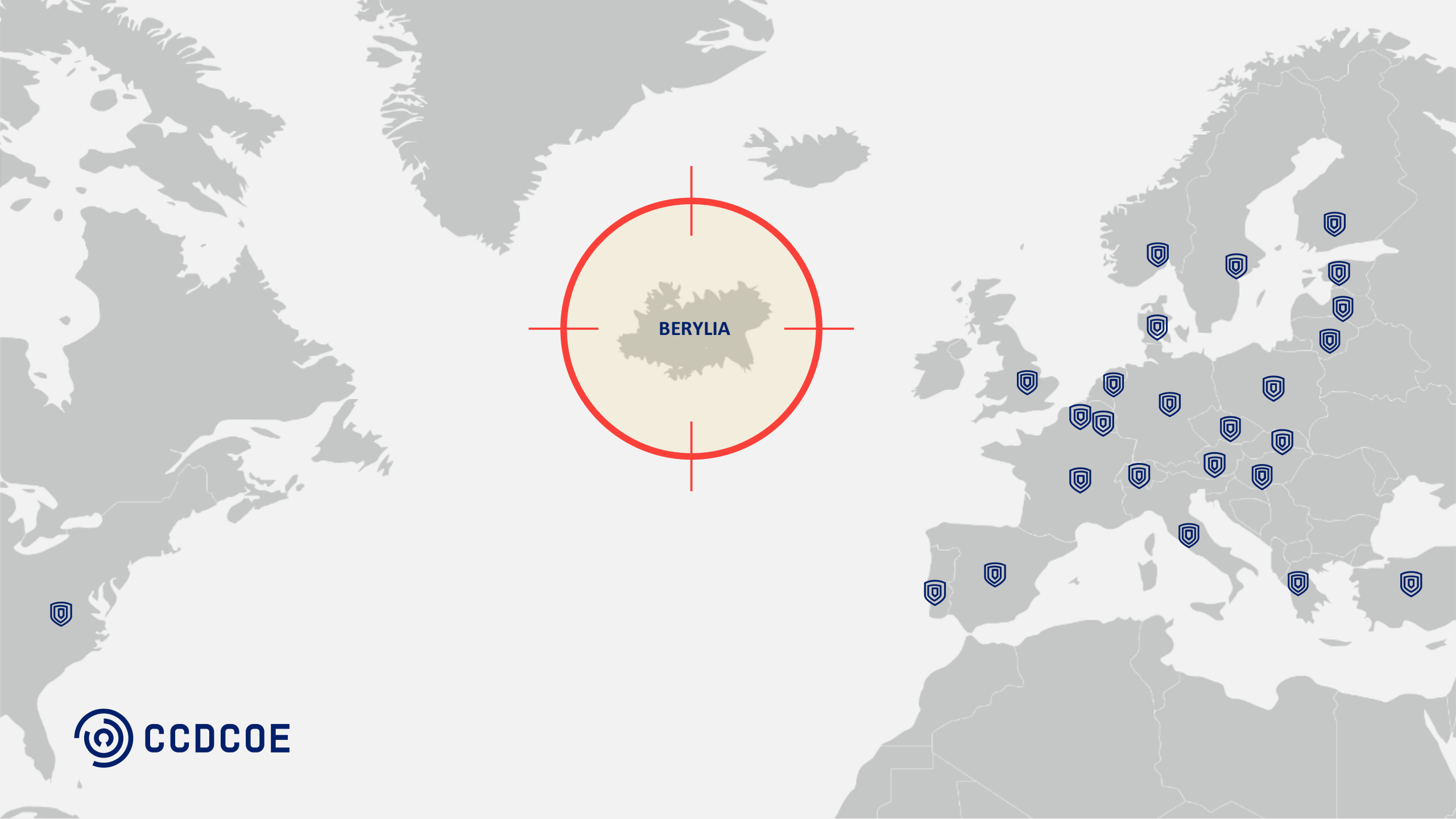
CCDCOE

LOCKED
SHIELDS

Locked Shields is unique

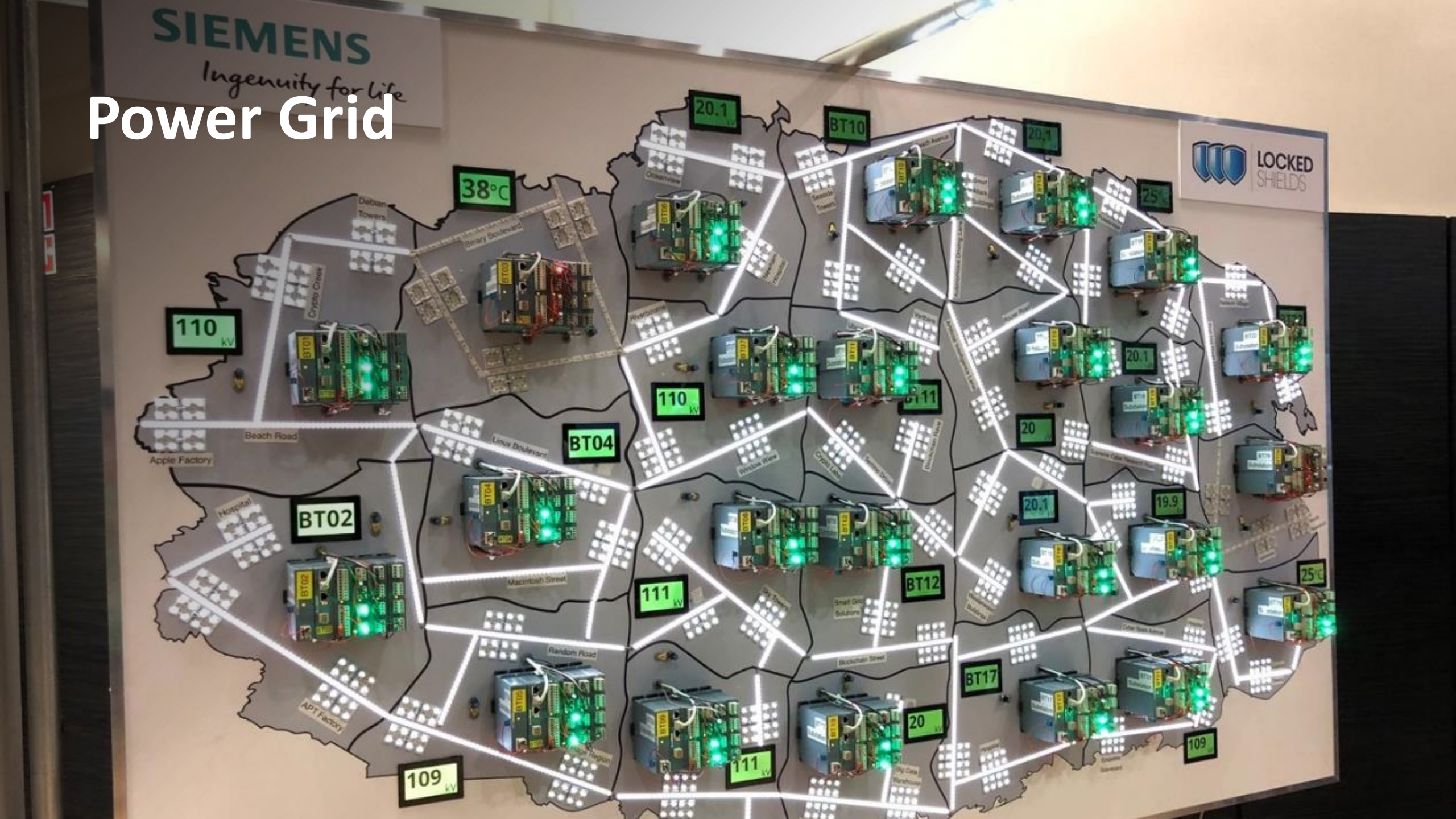
- → International
- → Technical & Strategic
- → Live Fire
- → Red ↔ Blue
- → Game Based
- → Complex, including ICS/SCADA
- → Innovative
- → Cyber Range Environment
- → Defense Oriented
- → Cooperation & information sharing

CCDCOE



CCDCOE

Power Grid


SIEMENS
Ingenuity for life
LOCKED SHIELDS
38°C
110 kV
110 kV
BT04
BT02
111 kV
BT12
BT17
20 kV
109 kV
111 kV
BT10
BT11
20
19.9
25°C
Beach Road
Apple Factory
Linux Boulevard
Macintosh Street
Random Road
Blockchain Street
Debian Towers
Crypto Creek
Hospital
APT Factory

Critical Infrastructure Protection

Critical Infrastructure Protection

Locked Shields in numbers

24
Blue Teams

32
Nations

8000
Attacks

2600
People involved

5.500
Virtual Machines

~100.000
Manhours for preparation

CCDCOE

Cyber exercises for strategic level

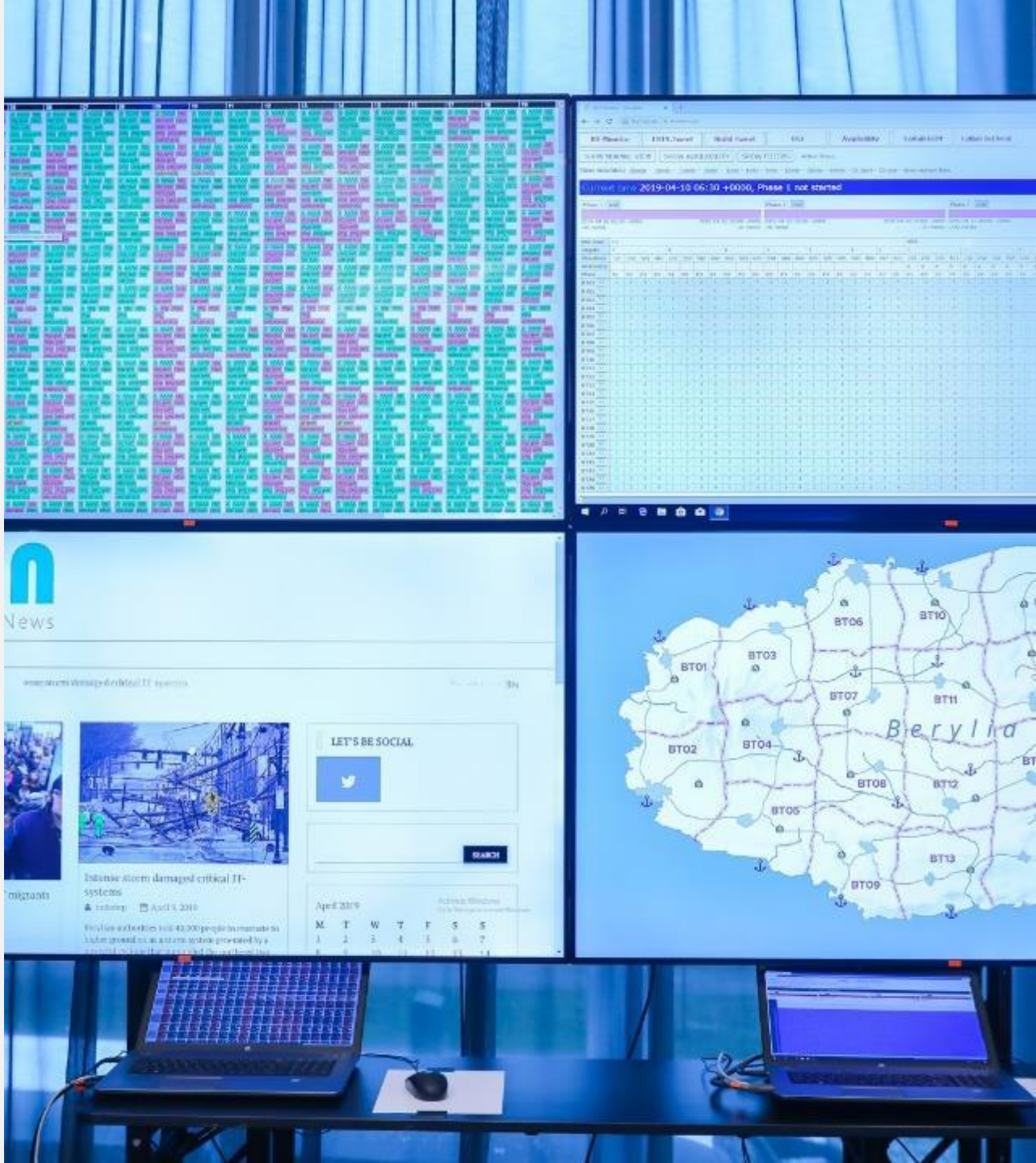
We must continue emphasising the need for training on strategic decision-making level. The Locked Shields also offers national senior-level decision-makers the chance to test their readiness to manage a crisis.

Kaja Kallas, Prime Minister of Estonia,
at Locked Shields 2021

CCDCOE

Strategic decision making - goals

- Translate technical incidents into strategic decisions as outlined by National Cyber strategies
- Reporting and information sharing, command and control functionality
- Understand the coordination and decision making process during a cyber event - both domestically and internationally



CCDCOE

Decision-making during a cyber event

- Who has the authority to make decisions
- How long does it take to effectuate the decision
- How the information used to make the decision should be classified
- How transparent is the process; and
- Wether mechanisms to share information between agencies, the private sector and partners are available

CCDCOE

Evaluation of Cyber Strategies

→ The strategic element of Locked Shields allows senior leadership to:

- practice processes and procedures as outlined by National Cyber strategies
- understand the coordination and decision making process during a cyber event - both domestically and internationally
- understand cyber interdependencies not just between public and private institutions but also among like-minded nations

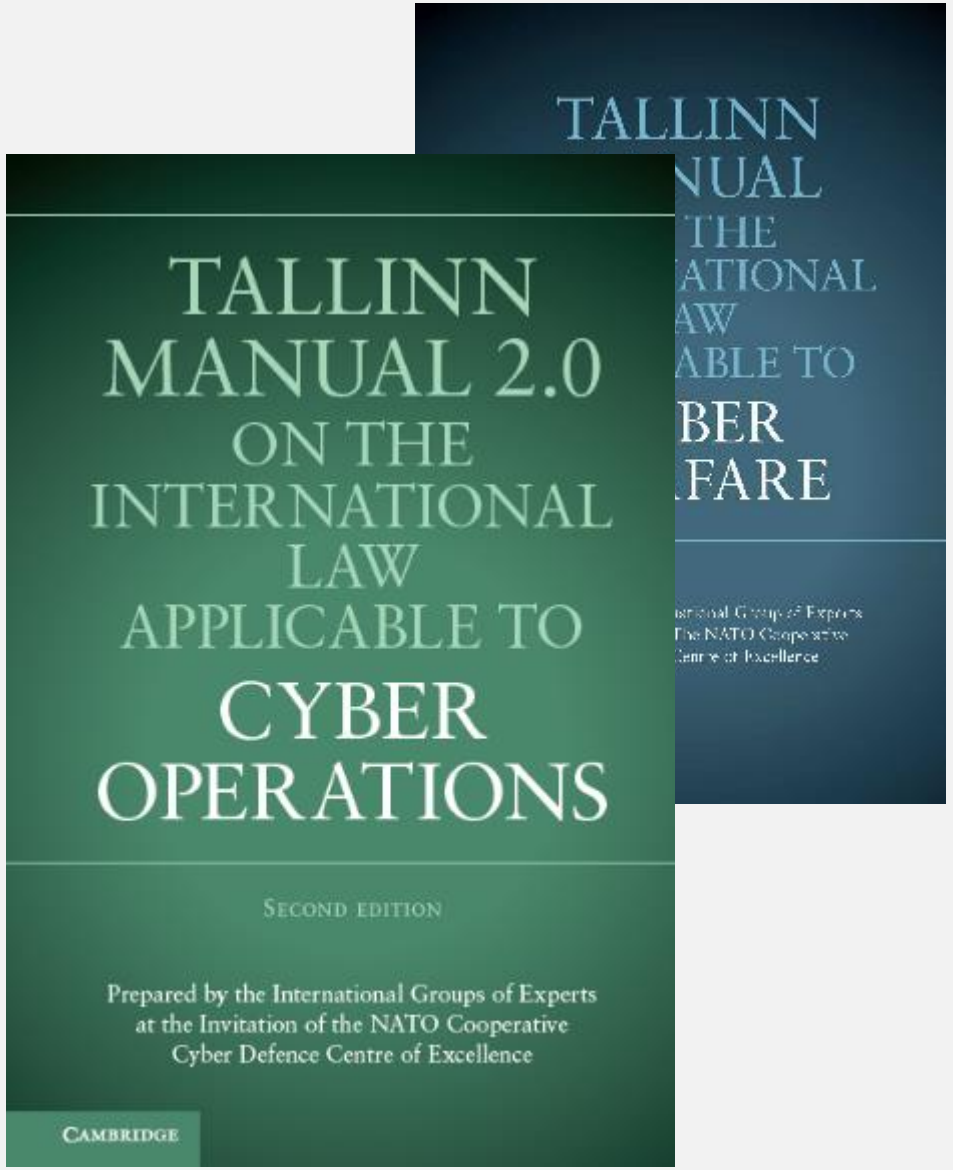
→ Create an in-depth resilience

- Regular strategic decision-making exercises

CCDCOE

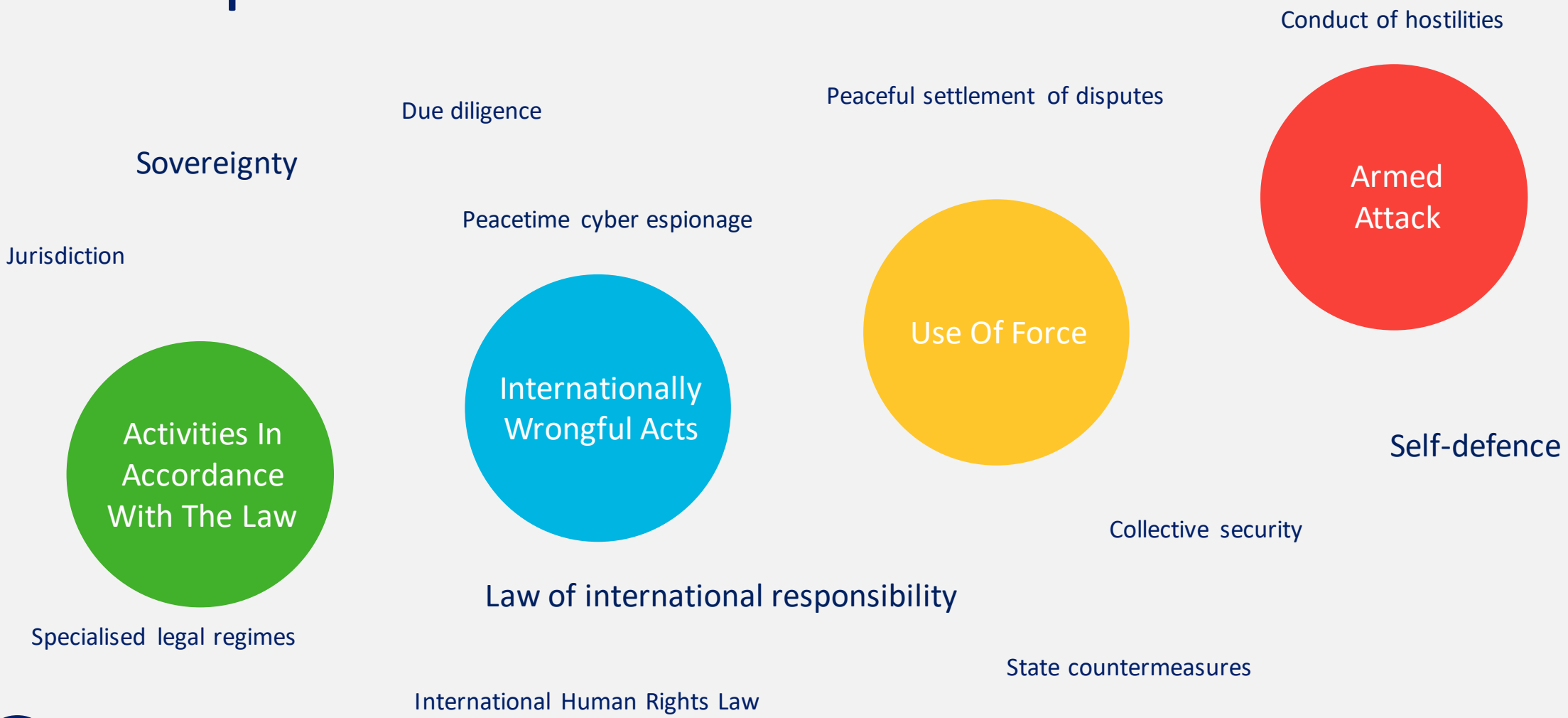
The Tallinn Manual

- Hosted by CCDCOE in 2009-2013; 2013-2017; 2021+
- International Group of Experts of scholars and practitioners from around the globe
- State consultations
- Interpretation of existing international law (*lex lata*) in the cyber context
- Rules and commentary



CCDCOE

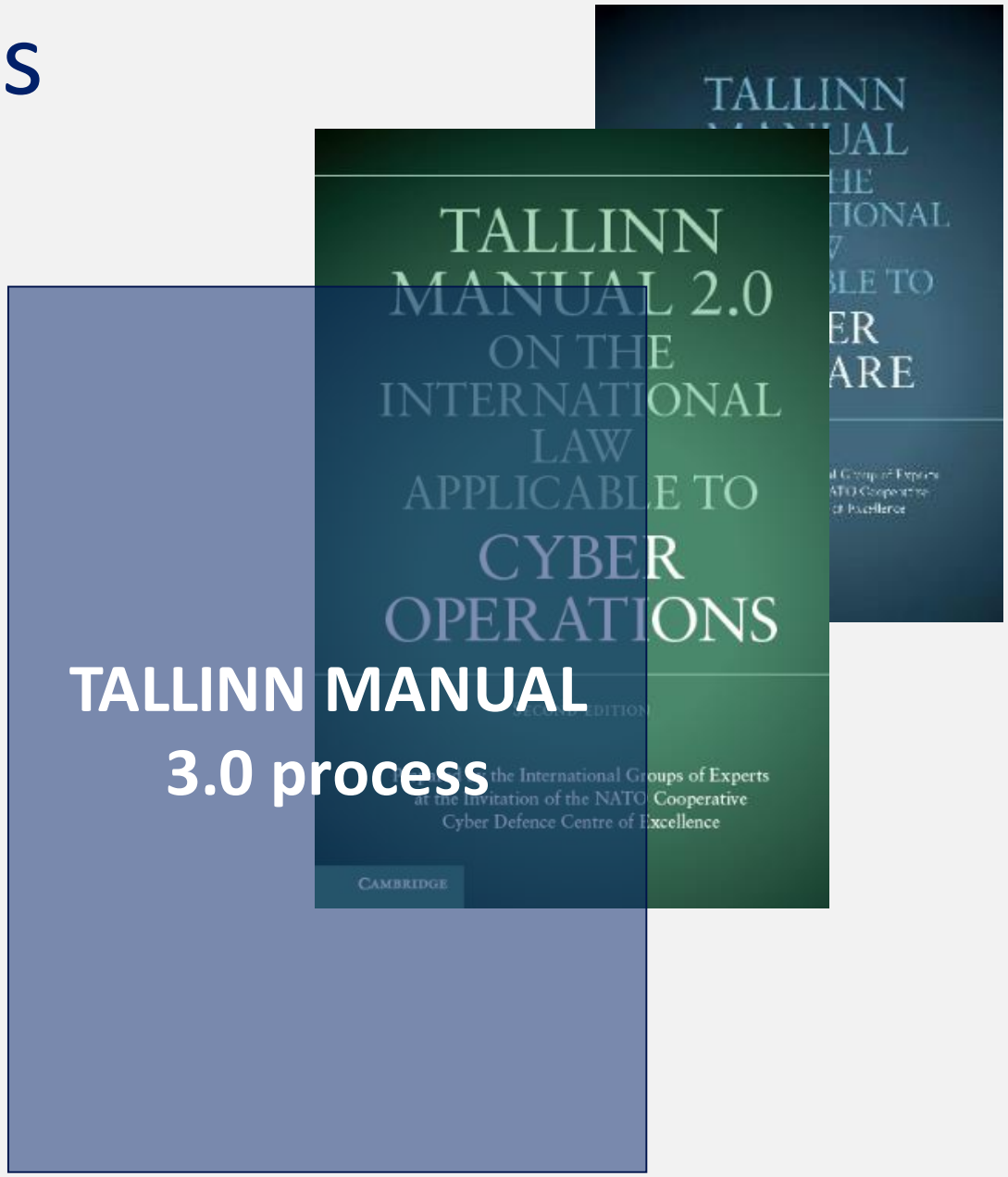
TM scope & areas of law



CCDCOE

Tallinn Manual 3.0 process

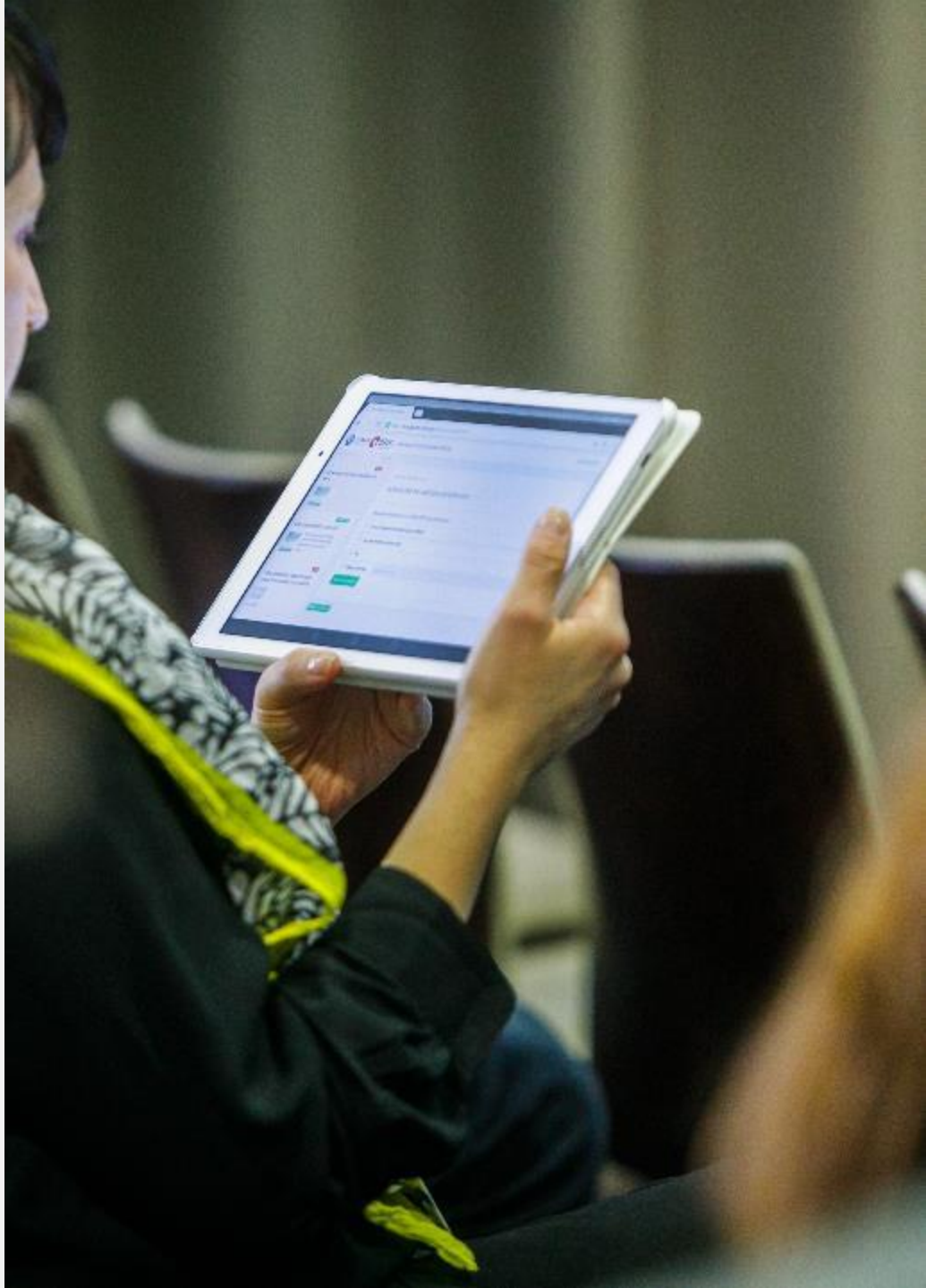
- Launched in 2021
- Revise TM 2.0 in light of the evolving State practice
- Consider new areas of law
- Approach consistent with TM 2.0
- Process and roles: editors, IGE, State consultations
- Publication by 2027



CCDCOE

Strategic Cyber Exercises

- focus on issues such as
  - policy,
  - regulation,
  - rules of engagement and
  - strategic communications



CCDCOE

Crossed Swords

- Developed and conducted since 2014
- Technical exercise: introduce innovative technologies
- Tactics, techniques and procedures
- Encompassing aspects of full-scale operations
- Simulate cyber-kinetic operation
- Integration of offensive cyber with special operations in a realistic environment
- Cooperation between technical teams and Special Operations Forces (SOF)
- Includes Command & Control (C2) and intelligence

CCDCOE

Training audience and objectives

- → Establish situational awareness
- → Perform technical attribution
- → Infiltrate adversary computer networks
- → Collect attribution information
- → Identify source of attack
- → Stop incoming cyber and kinetic threats

CYCON

INTERNATIONAL
CONFERENCE ON
CYBER CONFLICT

CYCON

CyCon 2022: Keep moving!

May 31 – June 3, 2022

Partners

ACADEMIA






NATIONAL


INDUSTRY




INTERNATIONAL





CCDCOE

15th International Conference on Cyber Conflict: Meeting Reality!

30 May – 2 June, 2023 Tallinn, Estonia

Thank you!

CCDCOE

ccdcoe.org
@ccdcoe