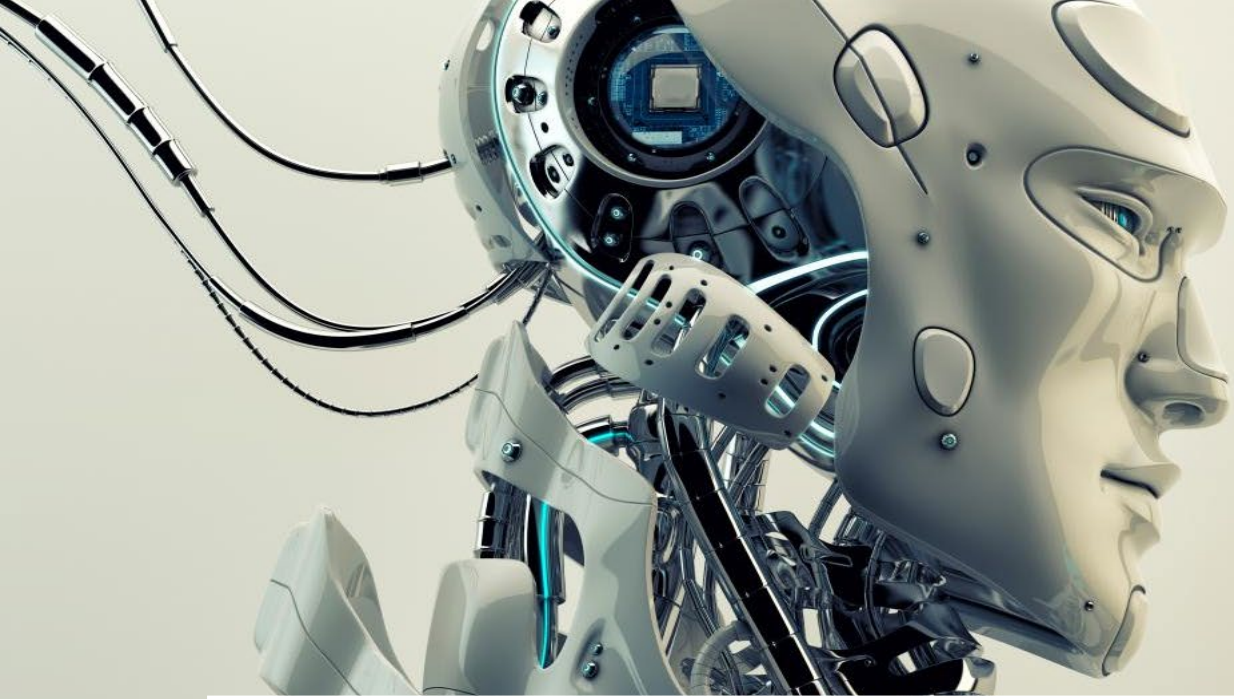


LEARNING FROM CYBERSECURITY EXERCISES — THE CASE OF LOCKED SHIELDS

Rain Ottis, PhD
Professor of Cyber Operations
Tallinn University of Technology

20.11.2024

INTRODUCTION ROUND

- Professor of Cyber Operations at Tallinn University of Technology
  - Head of research group
- ~20 years of experience with cyber security exercises
- Locked Shields White Team throughout the exercise series

EXERCISE TYPES

- Cyber security exercises can come in many forms
  - Seminar
  - Workshop
  - Tabletop exercise
  - Game

  Discussion-based exercises
  - Drill
  - Functional exercise
  - Full-scale exercise

  Operations-based exercises

- See Homeland Security Exercise and Evaluation Program (HSEEP) for details

FULL-SCALE EXERCISE

- An operations-based exercise that is typically the most complex and resource-intensive of the exercise types and often involves multiple agencies, jurisdictions/organizations, and real-time movement of resources.
- The most complicated form of exercises.

EXERCISE GOALS

- Provide training
- Raise awareness
- Improve collaboration
- Test procedures, training, technologies, etc.
- Experiment with new procedures, technologies, etc.
- Measure unit readiness, effectiveness, etc.
- ..

LOCKED SHIELDS

- Organized annually by NATO Cooperative Cyber Defence Centre of Excellence
  - First bilateral exercise in 2008 (Estonia and Sweden)
  - Baltic Cyber Shield in 2010
  - Locked Shields brand since 2012
- Full-scale, live-fire, Red-vs-Blue exercise
- Focus on training Blue Teams (defensive) and improving international collaboration

LOCKED SHIELDS 2024

- ~4000+ people from 40 countries
- ~5000 virtual and physical devices
- ~8000 cyber attacks by the Red Team
- 18 multinational Blue Teams

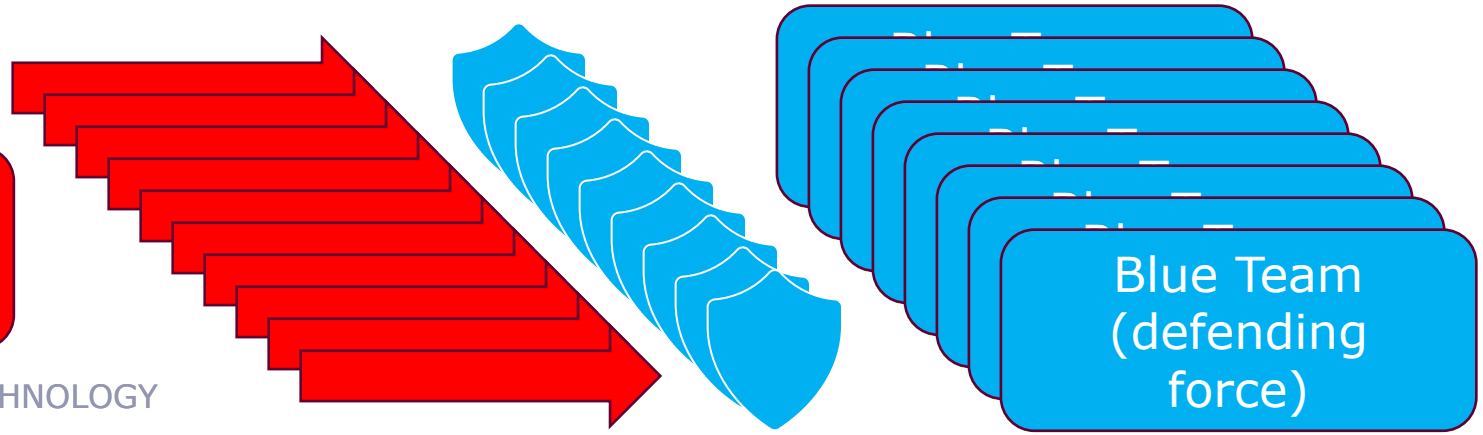
LOCKED SHIELDS ROLES

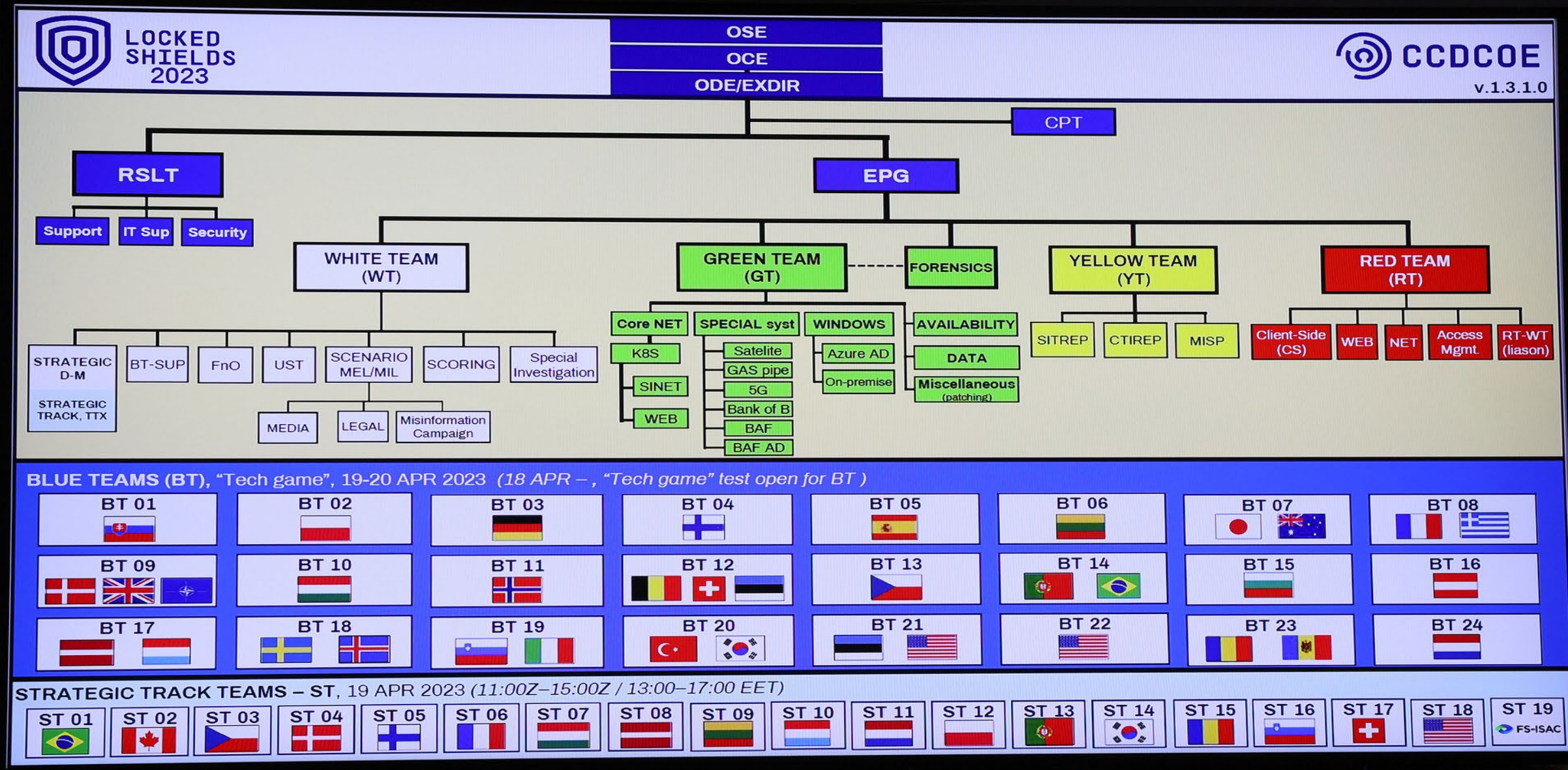
Green Team
(infrastructure)

White Team
(Exercise Control, scenario, information environment, injects, media, legal, scoring, investigations, ..)

Yellow Team
(situational awareness)

Red Team
(attacking force)




LOCKED SHIELDS 2023
OSE
OCE
ODE/EXDIR
CCDCOE
v.1.3.1.0
CPT
RSLT
EPG
Support
IT Sup
Security
WHITE TEAM (WT)
GREEN TEAM (GT)
FORENSICS
YELLOW TEAM (YT)
RED TEAM (RT)
STRATEGIC D-M
STRATEGIC TRACK, TTX
BT-SUP
FnO
UST
SCENARIO MEL/MIL
SCORING
Special Investigation
MEDIA
LEGAL
Misinformation Campaign
Core NET
K8S
SINET
WEB
SPECIAL syst
Satelite
GAS pipe
5G
Bank of B
BAF
BAF AD
WINDOWS
Azure AD
On-premise
AVAILABILITY
DATA
Miscellaneous (patching)
SITREP
CTIREP
MISP
Client-Side (CS)
WEB
NET
Access Mgmt.
RT-WT (liason)
BLUE TEAMS (BT), "Tech game", 19-20 APR 2023 (18 APR – , "Tech game" test open for BT)
BT 01
BT 02
BT 03
BT 04
BT 05
BT 06
BT 07
BT 08
BT 09
BT 10
BT 11
BT 12
BT 13
BT 14
BT 15
BT 16
BT 17
BT 18
BT 19
BT 20
BT 21
BT 22
BT 23
BT 24
STRATEGIC TRACK TEAMS – ST, 19 APR 2023 (11:00Z–15:00Z / 13:00–17:00 EET)
ST 01
ST 02
ST 03
ST 04
ST 05
ST 06
ST 07
ST 08
ST 09
ST 10
ST 11
ST 12
ST 13
ST 14
ST 15
ST 16
ST 17
ST 18
ST 19
FS-ISAC

LOCKED SHIELDS SCORES

- Most aspects of the exercise are scored to provide feedback to the teams
- Scoring agents/bots check for availability
- Red team scores for loss of confidentiality (flags) or integrity (for example, defacement)
- User Simulation Team checks for service functionality
- Separate scores for reporting, media interaction, responses to legal injects, solving forensics tasks, etc.
- Manual scores come with explanation, so the team can learn and improve during the exercise

LOCKED SHIELDS SETUP

- Organizers (including Red Team) gather in Tallinn, Estonia
- Training audience (Blue Teams) typically remain in their country, although some have also deployed to other countries
- Some teams are based on two or more countries
- The exercise world is hosted in a cyber range
  - Mostly virtual machines
  - Some physical network infrastructure
  - Some special systems (power, water, air defence, 5G, satelliite comms, etc.) components are also physical devices
  - All participants access the cyber range over VPN
- All teams have identical starting conditions

LOCKED SHIELDS SETUP

- Blue Teams are not allowed to disconnect their systems from the network – they must defend while providing services
- Red Team follows a pre-determined campaign plan, which is based on timed objectives.
- Red Team is not limited with attack types
- Blue Teams are not allowed to attack
- More focus on information environment

RESEARCH CONSIDERATIONS

- LS keeps pushing the boundaries
- Complexity and size generates interesting problems
- Unclassified
- Academic access – limited, but possible

TECHNICAL RESEARCH

- Federation and use of cyber ranges
- Exercise automation
- Situational awareness (monitoring, analysis, visualisation)
- AI/ML in cybersecurity exercises
- ..
- Examples:
  - Kaur Kullman (2023) "Interactive Stereoscopically Perceivable Multidimensional Data Visualizations for Cybersecurity"
  - Mauno Pihelgas (2021) "Automating Defences against Cyber Operations in Computer Networks”

HUMAN ASPECTS RESEARCH

- Measuring the learning effectiveness of exercises
- Leadership and decision making under pressure
- ..
- Examples:
  - Kaie Maennel (2021) "Advancing Cybersecurity Education through Learning Analytics"
  - Sten Mäses (2020) "Evaluating Cybersecurity-Related Competences through Simulation Exercises"

ORGANISATIONAL/OPERATIONS RESEARCH

- How to plan and execute cybersecurity exercises?
- How do exercises differ from real operations?
- ..
- Examples:
  - Bernhards Blumbergs (2019) "Specialized Cyber Red Team Responsive Computer Network Operations“
  - Marko Arik (expected 2025) "The Planning, Development and Execution of Cyber Operations in the Information Environment"

DEFENDED PHD THESES

- TalTech’s Centre for Digital Forensics and Cyber Security

https://taltech.ee/en/centre-for-digital-forensics-cyber-security/phd-theses

TALLINN UNIVERSITY OF TECHNOLOGY

rain.ottis@taltech.ee