LOCKED SHIELDS

2024

FÖRSVARSMAKTEN


WELCOME!
LOCKED
SHIELDS
2022
FÖRSVARSMAKTEN

SWEDISH CYBER DEFENCE

FÖRSVARSMAKTEN

SWEDISH CYBER- DEFENCE SYSTEM

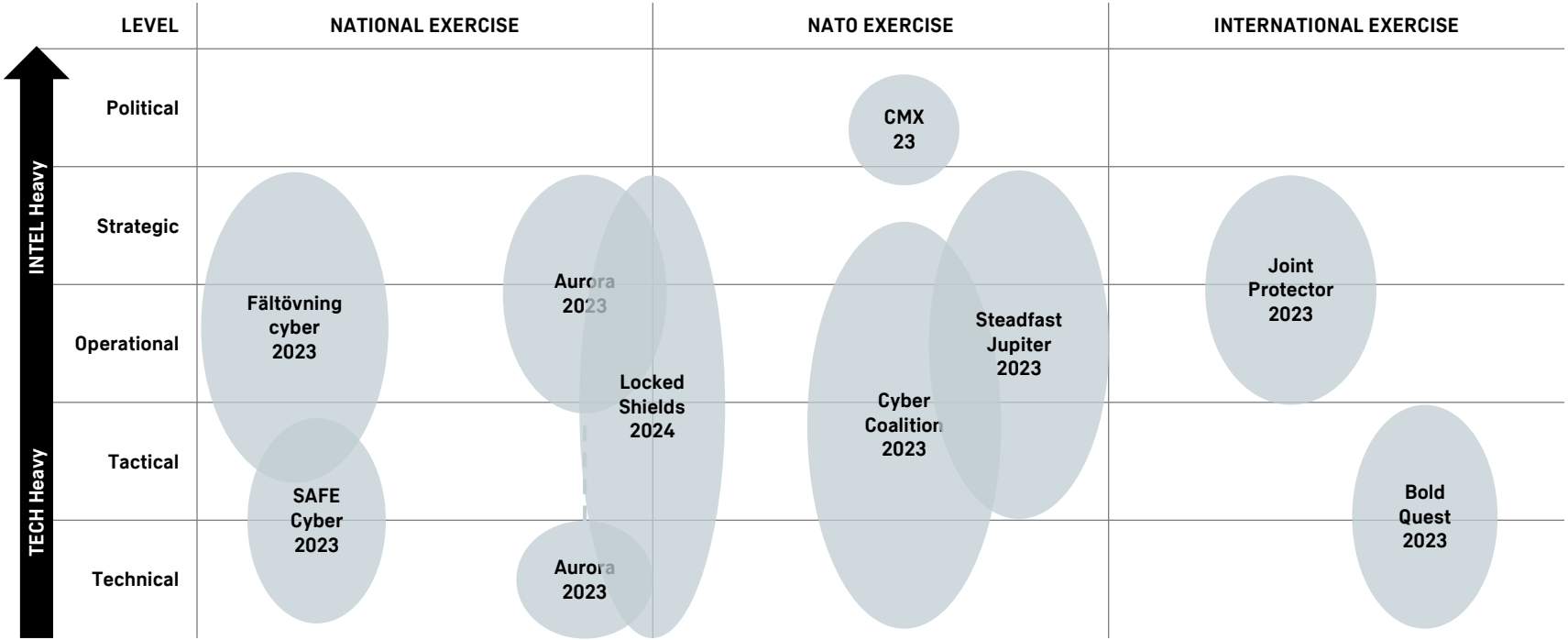
”The cyber defence relies on efficient collaboration between military strategic, operational and tactical command and control, service branches, combat forces and joint defence forces. This is achieved by a coherent cyber- defence system, led and developed on the military strategic level”.

Excerpt from H22-R

CYBER EXERCISES WITHIN THE SWEDISH ARMED FORCES

FÖRSVARSMAKTEN

EXERCISES AND EXERCISE LEVELS



SWEDEN AND NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

- → Sweden has been a contributing part since 2017 and is represented in the steering committee
- → There is a seconded researcher from the Swedish Armed Forces at the CCD COE Strategy Branch and Sweden are active in all functions:
  - → Research
  - → Exercises
  - → Training
- → Sweden has several participants in courses held by CCD COE

INTRODUCTION LOCKED SHIELDS

- → Locked Shields are arranged by the (NATO) Cooperative Cyber Defence Centre of Excellence (CCD COE)
- → Locked Shields are the worlds largest Cyber Security Exercise
- → Locked Shields is executed annually.

 Strategical

 Operative

 Tactical

 Technical

THE RESPONSIBILITY OF THE SWEDISH ARMED FORCES IN LOCKED SHIELDS

The Swedish Armed Forces are, through the membership in CCD COE, responsible to plan, organize and analyze the Swedish participation in Locked Shields, this includes:

- → Decision and focus of national exercise aim and objectives
- → Decision of invited participants, organizations and partner nation(s)
- → Decision of exercise facility and prerequisites

SWEDISH OBJECTIVES WITH LOCKED SHIELDS 2024

The overall Swedish aim with participating in Locked Shields 2024 are:

- → Establish and maintain international and NATO cooperation and contacts
- → Establish and maintain civilian and military collaboration and strengthen Swedish total defence
- → Enhance the individual competence and broaden the personal network

SWEDISH PARTICIPATION IN LOCKED SHIELDS PREVIOUSLY YEARS

2022

Primary exercise objective

Exercise the participants in technical cyber defence, command and control and coordination.

Training audience

1. The energy sector
2. The electronic communication sector

2023

Primary exercise objective

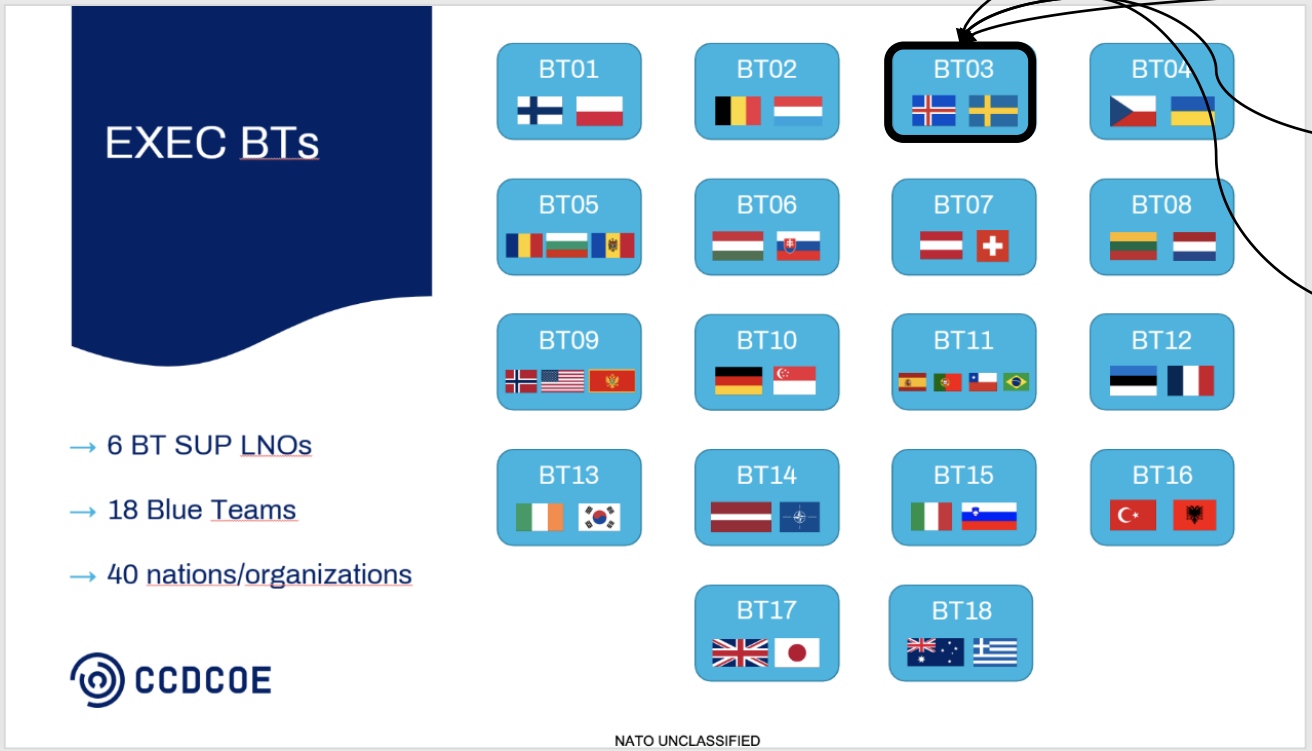
Exercise the participants insight within cyber security and enhance the participants cyber security ability

Training audience

1. The finance sector
2. The electronic communication sector

Icelandic and Swedish team!

LOCKED SHIELDS 2024



Iceland

Swedish Armed Forces

Civilian organizations, selected by Swedish National Cyber Security Center

Specific selected individuals

FÖRSVARSMAKTEN

LOCKED SHIELDS OVERALL

It is a Red team vs. Blue Team exercise, there the latter are formed by member nations of CCD COE.

The Teams take on the role of national cyber Rapid Reaction Teams that are deployed to assist a fictional country in handling a large-scale cyber incident with all its implications.

The teams must be effective in reporting incidents, executing strategic decisions and solving forensic, legal and media challenges. To keep up with technology developments, Locked Shields focuses in realistic scenarios and cutting-edge technologies, relevant networks and attack methods.

The exercise in 2023 involved about 5000 virtualized systems that were subject to more than 4000 targeted attacks on each team.

SCENARIO

Who are we?

We are the CSIRT tasked with supporting Berylia, a:

- → Fictional island country located in the northern Atlantic Ocean
- → Not a NATO member
- → Currently in an armed conflict with Crimsonia

Berylia is suffering multiple coordinated cyber attacks. This has caused severe disruptions to the operation of government and military networks, satellite communications, radar systems, water purification systems and the electric power grid.

This has also eventually lead to public unrest and protests (hacktivism).

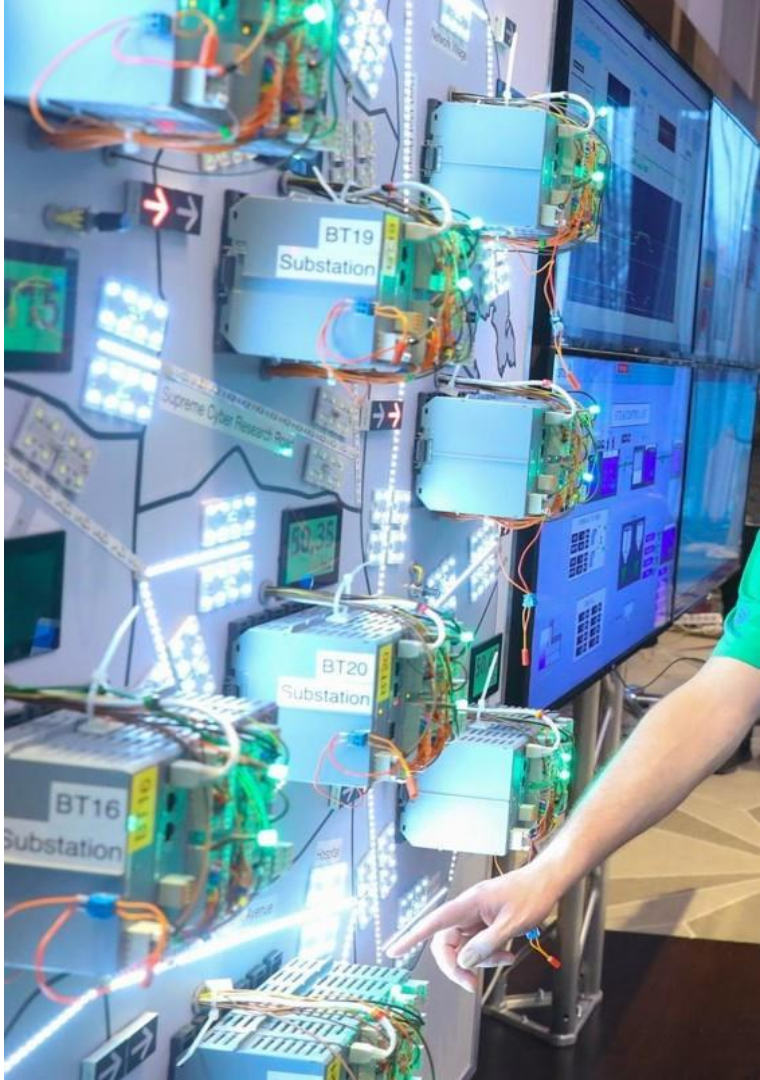
STRATEGY

First 30 minutes (no red team scoring)

1. Lock down services, accounts and permissions
2. Fix misconfigurations
3. Remove known backdoors and vulnerabilities
4. Establish network and endpoint detection response capabilities

During game

1. Keep systems operational and available
2. Provide usability for the user simulation team
3. Report incidents and provide SITREPS to higher command



SCORING PRINCIPLES

Every team starts with 10’000 points

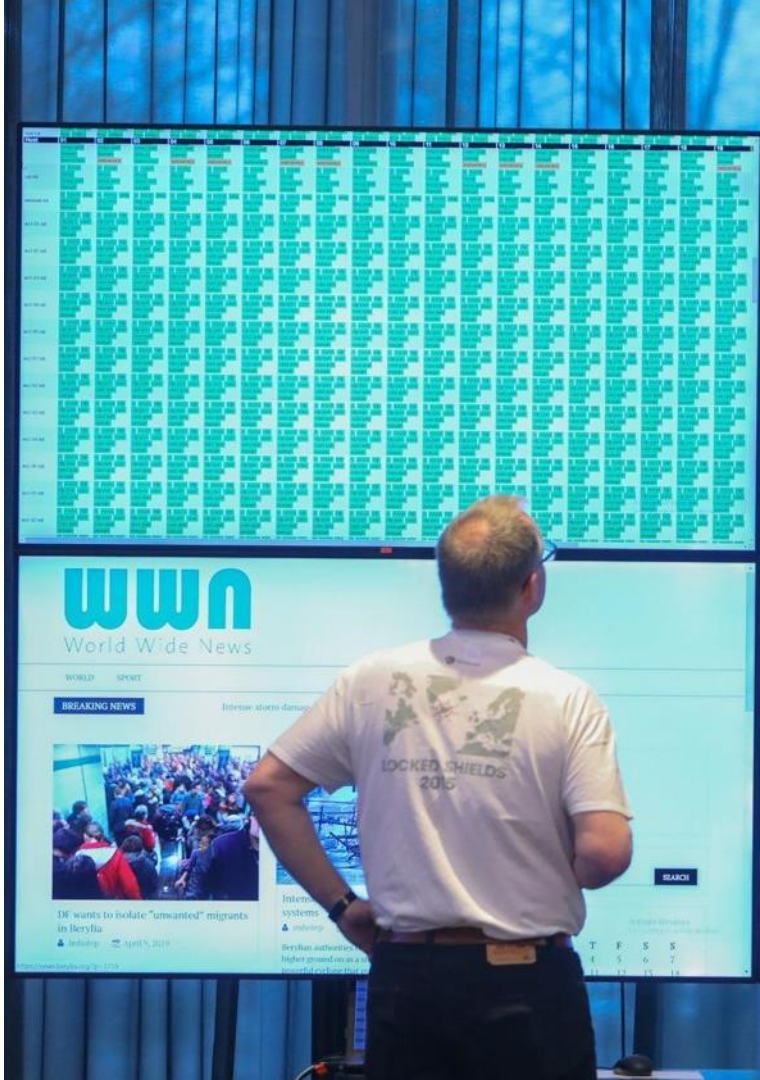
→ Points are withdrawn for capabilities downtime, successful red team attacks and downtime of simulated user systems.

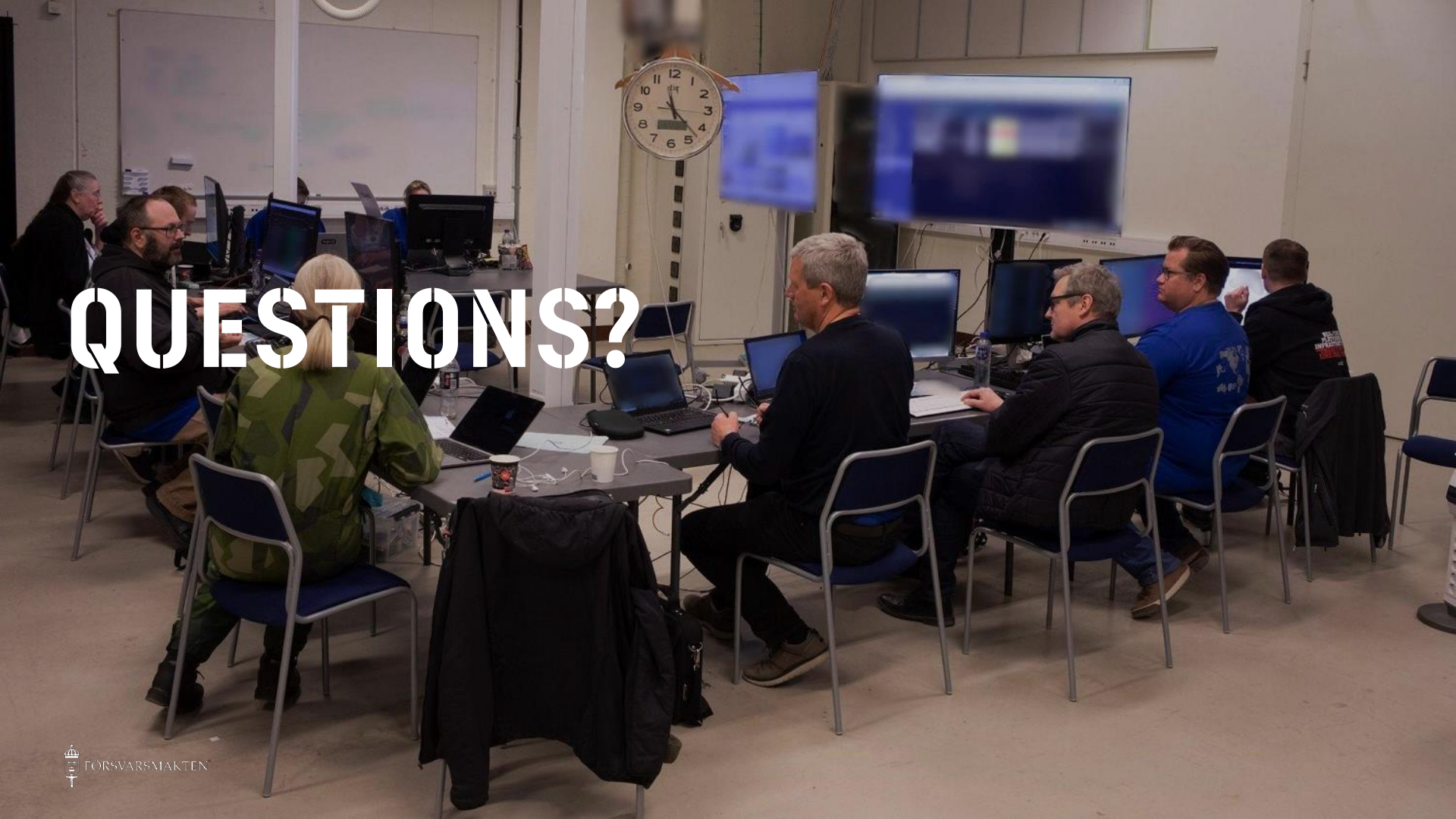
→ Points are added for reports, media responses, legal injection responses and forensics findings.

→ Points can also be added for helping out other teams, i.e. supplying another team with electricity while they fix theirs.

→ Reverting a machine or breaking the rules costs the team points.

→ The team with the most points at ENDEX wins





FÖRSVARSMAKTEN