Locked Shields

> Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world

This annual exercise, organised by CCDCOE since 2010, enables cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies and simulating the entire complexity of a massive cyber incident, including strategic decision-making, legal and communication aspects.

It is a Red team vs. Blue Team exercise, where the latter are formed by member nations of CCDCOE. The participating Blue Teams play the role of national rapid reaction teams that are deployed to assist a fictional country in handling a large-scale cyber incidents and all their multiple implications. In addition to maintaining around 4000 virtualised systems while experiencing more than 2500 attacks, 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 on realistic scenarios and cutting-edge technologies, relevant networks and attack methods.

New Challenges in 2019

This year, Locked Shields introduced new challenges, technologies and specialised systems. In 2019 the exercise was highlighting the need for improved dialogue between experts and decision-makers. For that purpose, the CCDCOE integrated the technical and strategic game, enabling participating nations to practise the entire chain of command in the event of a severe cyber incident, from strategic to operational level and involving both civilian and military capabilities. Reflecting real world cyber threats, the exercise addressed the protection of vital services and critical infrastructure. Many of the business IT-systems and military relevant systems used in the exercise were taken to a new level of complexity as compared to last year, for example the power distribution system had this year also power generation component.

According to the scenario, a fictional country, Berylia, was experiencing a deteriorating security situation, where a number of hostile events coincide with coordinated cyber attacks against a major civilian internet service provider and maritime surveillance system. The attacks caused severe disruptions in the power generation and distribution, 4G communication systems, maritime surveillance, water purification plant and other critical infrastructure components. While the aim of the tech game was to maintain the operation of various systems under intense pressure, the strategic part addresses the capability to understand the impact of decisions made at the strategic and policy level.

More than 1200 experts from nearly 30 nations took part in Locked Shields 2019. While the organisers of the exercise gathered in Tallinn, Estonia, the participating Blue

Teams set up secure online access from their nations. The French team emerged as the winner of Locked Shields 2019.

Essential Takeaways

Locked Shields is a unique opportunity to encourage experimentation, training and cooperation between members of the CCDCOE, NATO and partner nations. It offers an unprecedented opportunity for nations to challenge themselves in an authentic but safe training environment while being aggressively challenged by highly skilled adversaries. The network which the Blue Teams must defend consists of more than 150 virtual hosts per team. The virtualized Blue Team networks are custom-built and include a variety of services and platforms, both civilian and military.

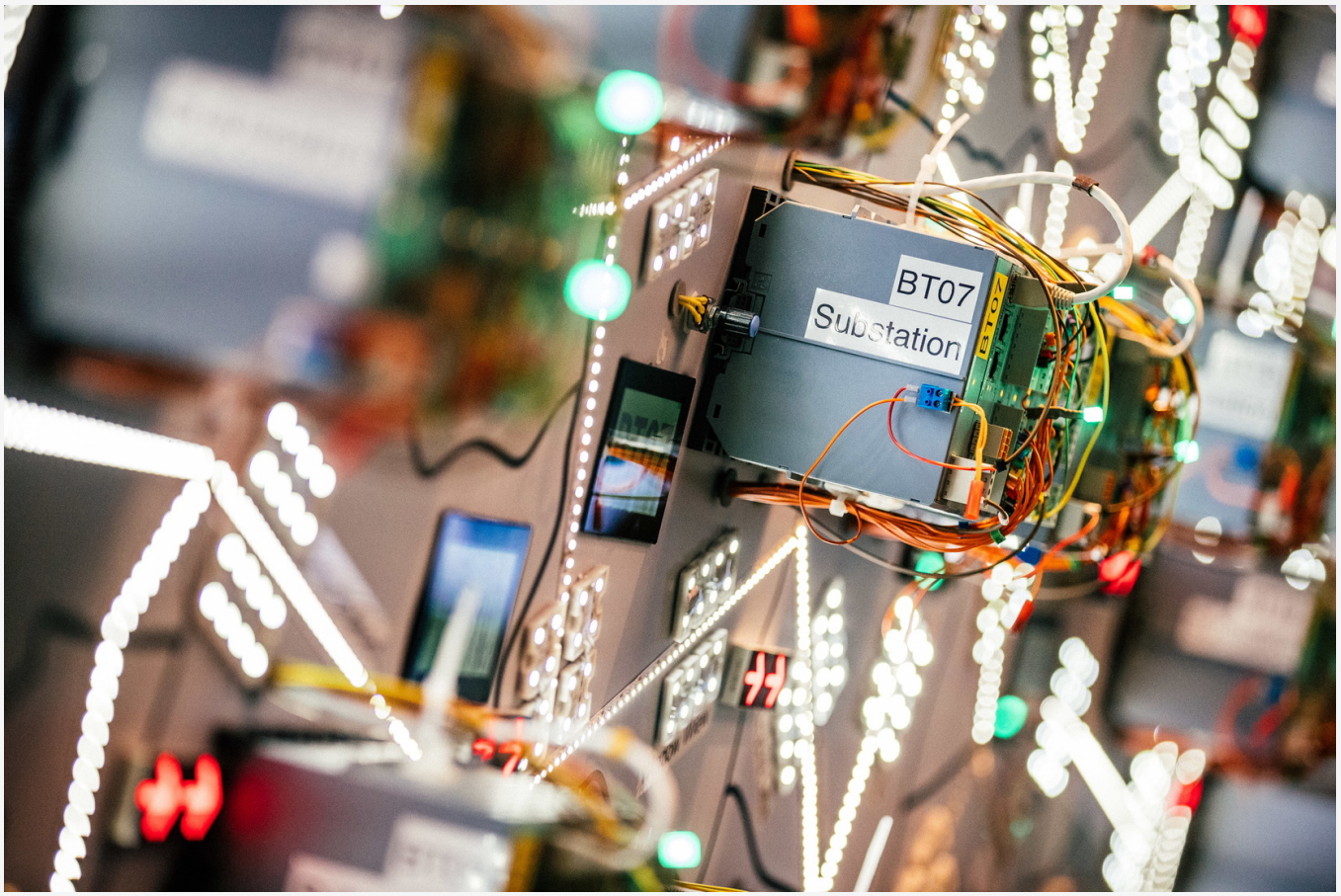
The exercise addresses areas which have proved to be most challenging for Blue Teams in recent years:

- Protecting unfamiliar specialised systems;
- Writing good situation reports under serious time pressure;
- Detecting and mitigating attacks in large and complex IT environments;
- Well-coordinated teamwork.

Locked Shields 2019 is organised by CCDCOE in cooperation with the Estonian Defence Forces, the Finnish Defence Forces, the United States European Command, National Security Research Institute of the Republic of Korea and TalTech. Industry partners in the exercise include Siemens AG, Elisa, Cybernetica, Cisco, Threod Systems, VTT Technical Research Centre of Finland Ltd, Arctic Security, Clarified Security, Iptron, Bittium, STM, Bytelife, BHC Laboratory, and many others.

Locked Shields 2019 Key Facts:

- Live-fire = real-time Red Team vs. Blue Team exercise
- Involves regular business IT, critical infrastructure and military systems
- Integrates technical and strategic decision-making exercise
- More than 1200 cyber defence experts from nearly 30 nations
- Runs on Cyber Range, an innovative platform managed by the Estonian Defence Forces


BT07
Substation
BT07

The NATO Cooperative Cyber Defence Centre of Excellence

ccdcoe-at-ccdcoe.org
+372 7176 800
Address: Filtri tee 12, Tallinn 10132, Estonia