



CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence
Tallinn, Estonia



NATO Cooperative Cyber Defence Centre of Excellence



Lieutenant Colonel Martin Gürtler
Chief of Staff / Deputy Director

27 June 2012



CYBER DEFENCE EXERCISE LOCKED SHIELDS 2012

Disclaimer:

This briefing is a product of the CCD COE. It does not represent the opinions or policies of NATO and is designed to provide an independent position.



Concept

- Technical Blue-Red Team Cyber Defence Exercise (CDX)
- Game-based approach
- Competition between the Blue Teams
- Related to Multinational Experiment 7 (MNE7)
- Organizers:
 - Swiss Armed Forces Command Support Organization,
 - Finnish Defence Forces,
 - Estonian Cyber Defence League
 - NATO CCD COE

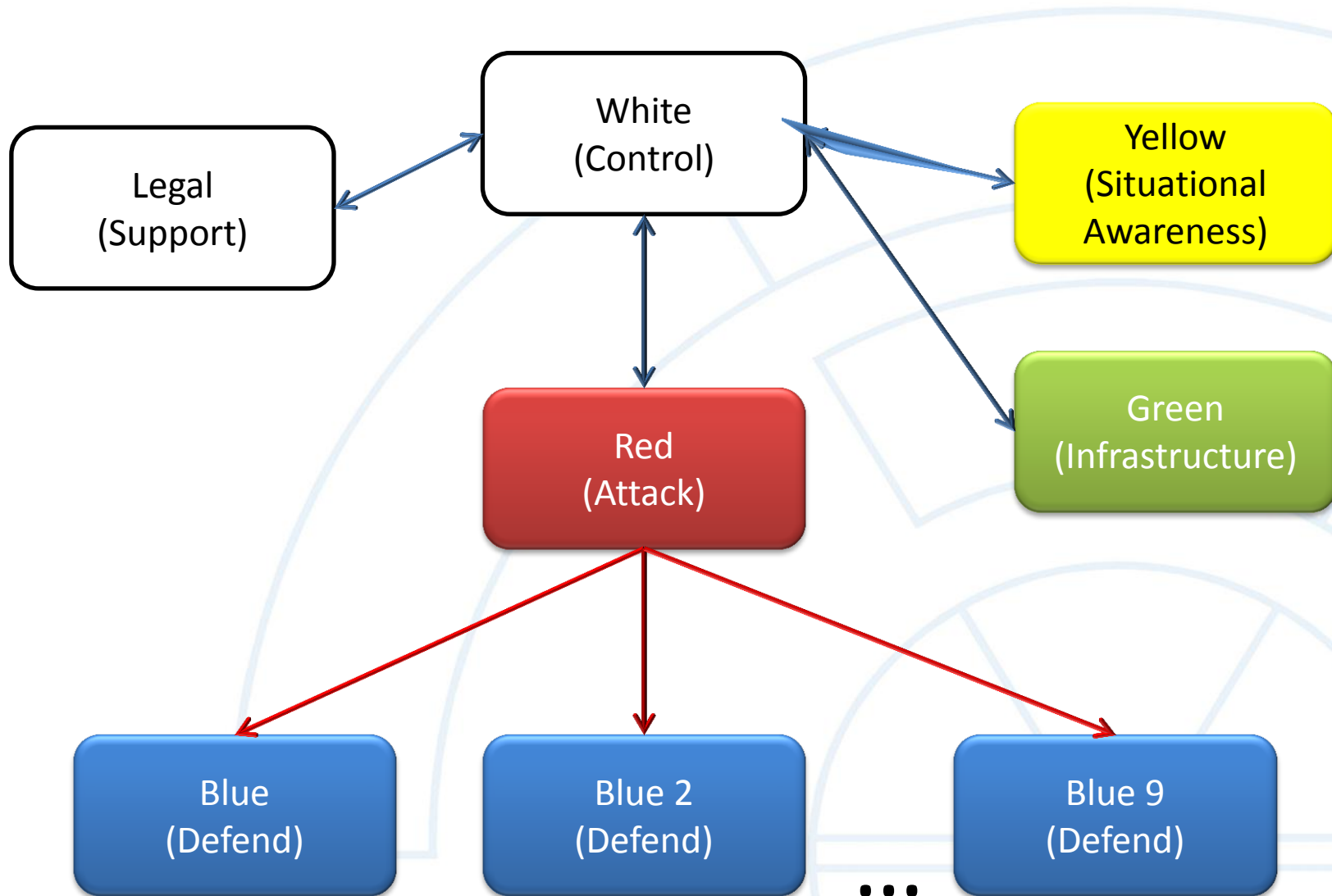
Objectives

- Train teams of IT specialists to detect and mitigate large-scale cyber attacks
- Train legal experts
- Improve international cooperation of CD practitioners
- Exchange information and experiences to strengthen the international community
- Learn from the activities of Blue and Red teams
- Create the technical infrastructure to be reusable
- Improve the capability to conduct technical CDEXs

Scenario

- Blue:
 - Small telecommunication companies. Primary IT team not available, backup team in charge of securing the systems and networks.
- Red:
 - Cyber crime group called Radical BattalioN whose activities had been lately hampered by law enforcement cooperating with ISPs (Blue Team...)
 - Hacktivists (The Janitors) who were disappointed of ISPs using spyware to monitor the customers

Teams



Locations

- Blue: at their home locations
- Red: Tallinn
- White: Tallinn
- Yellow: Helsinki, Bern
- Green: Bern, Tallinn
- Legal: Helsinki

Timeline

- May 2011: First Planning Conference
- Oct 2011: Main Planning Conference, Helsinki
- Jan to Mar 2012: most intensive preparation period
- Feb 2012: Final Planning Conference, Bern
- Feb 2012: Test Run
- 26-28 Mar 2012: Execution
- 29 Mar 2012 : Hot Wash-Up
- Aug 2012: After Action Review

Participants

- More than 250 participants in total
- Approximately 110 as Blue Team members
 - Execution: FIN, CHE, ITA, DEU, DEU-AUT, DNK-NOR-SWE, ESP, SVK, NCIRC
- Approximately 165 participated in other teams
 - 40 Red Team members
 - 15 Green Team members
 - 15 White Team members
 - 15 Legal Team members
 - 30 Yellow Team members
 - 50 MNE7 SA team members

Execution I

- Janitors (hacktivists) conducted more visible attacks
 - Large defacement campaign
 - Stealing customer e-mails and publishing them
 - Stealing documents, for instance a memo's about cartel discussions between ISPs
 - Denial of Service
- Radical BattalionN (cyber criminals) started with more quiet activities and espionage
 - Placing backdoors, conducting phishing campaign to infect workstations in internal networks, stealing customer database, finally taking down the SCADA system

News Feeds

Own3d by the Janitors – Customer Mailboxes Deleted

1

CERT Not Sure About The Janitors

Blue8: This Is Cyber War

Posted on [March 28, 2012](#)



Blue8 sent LS News a surprising e-mail calling yesterday's attack "Cyber war that has been brought upon us by wrath or the Radical Battalion hackers."

"We believe that we may have lost the battle, but the war is not over yet. Our company has suffered multiple

successful attacks and our web, multiple times to prevent further access to two databases, but not both our users and our customers the Blue8.



re is spreading via ISPs? about the new virus. They seem to be in all

Legal Team: This is Not Cyber War

1

Posted on [March 28, 2012](#)

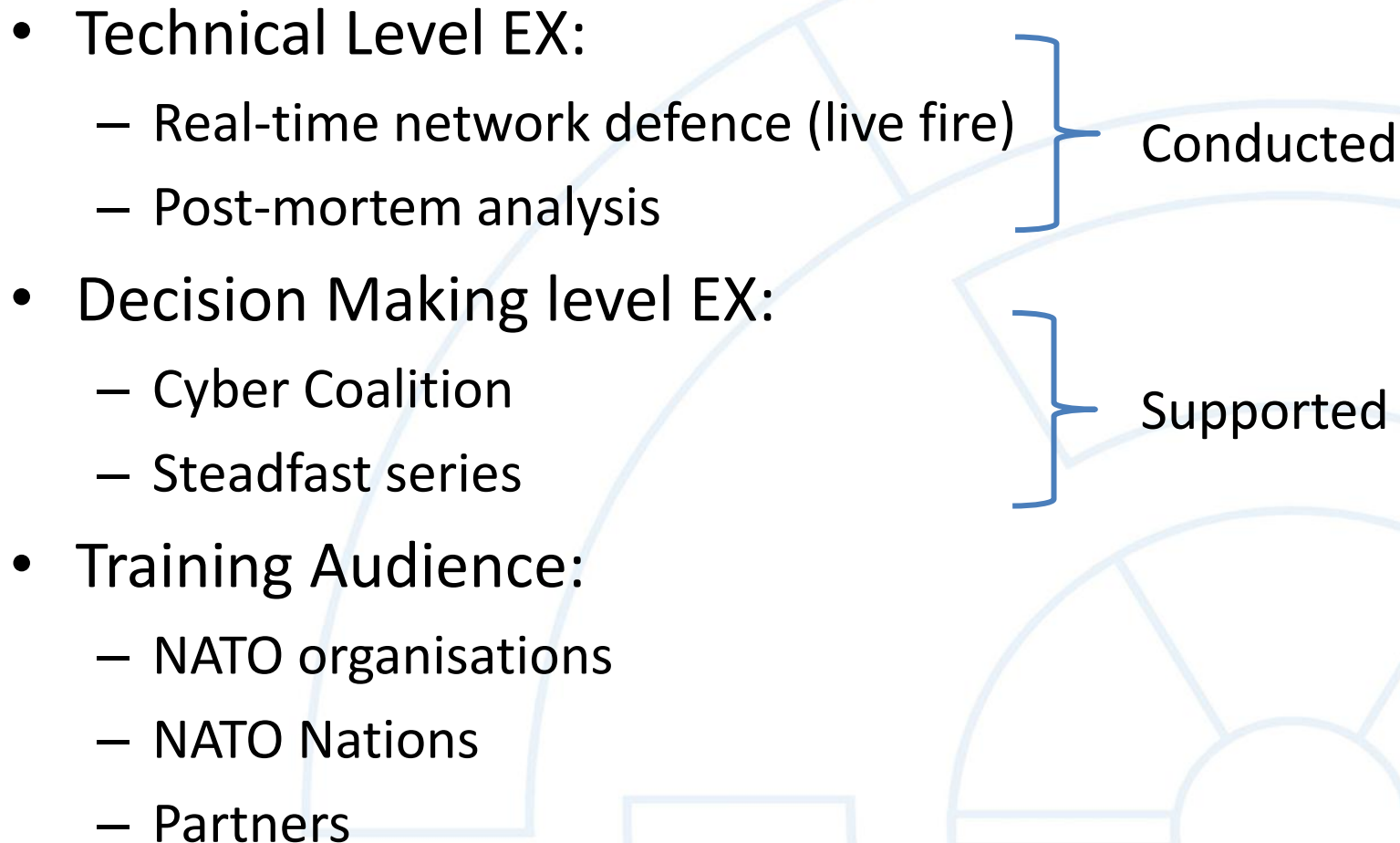
Execution II

- Red Team kept all Blue Teams very busy.
 - Almost all common attack types were used
- White Team put additional pressure with injecting business tasks and playing journalists to ask comments about on-going events
- Many Blue Teams had difficulties with protecting web applications especially those that were custom built
- Challenge for Blue teams to provide adequate comments for the media

Findings

- Very useful CDEX on technical level
- Legal part to be reconsidered
- Challenge to set up EX environment remotely

CDEX Future

- Technical Level EX:
 - Real-time network defence (live fire)
 - Post-mortem analysis
 - Decision Making level EX:
 - Cyber Coalition
 - Steadfast series
 - Training Audience:
 - NATO organisations
 - NATO Nations
 - Partners
- Conducted
- Supported
- 
- A diagram illustrating the structure of CDEX Future. It features a large, light blue circular graphic on the right side, composed of concentric arcs and radial lines, resembling a stylized globe or a complex network. The text and list items are positioned to the left of this graphic. Two blue brackets on the right side of the list items group them into two categories: "Conducted" and "Supported". The "Conducted" category includes the "Technical Level EX" items, and the "Supported" category includes the "Decision Making level EX" items. The "Training Audience" items are not grouped by a bracket.