Cyber Trainer & Ranges:
A Dual Use Success Story

Defense and Dual-Use Technologies 2018

Sevilla, Spain , 3 - 4 October 2018

Fabio Cocurullo, Head of Engineering and CTO

Leonardo, CyberSecurity and ICT Line of Business

LEONARDO
SECURITY & INFORMATION SYSTEMS

1948 • 2018

What is a Cyber Trainer / Range?

"Interactive, simulated representations of a system, tools, and applications that are connected to a simulated Network level environment and support the execution of cyber attack ("red" team) and defence operations ("blue" team)

"Systems can be composed of a combination of Information and Communication Technologies, SCADA – Operational Technologies, Internet of Things Devices, Embedded systems, even if most present instances are limited to ICT

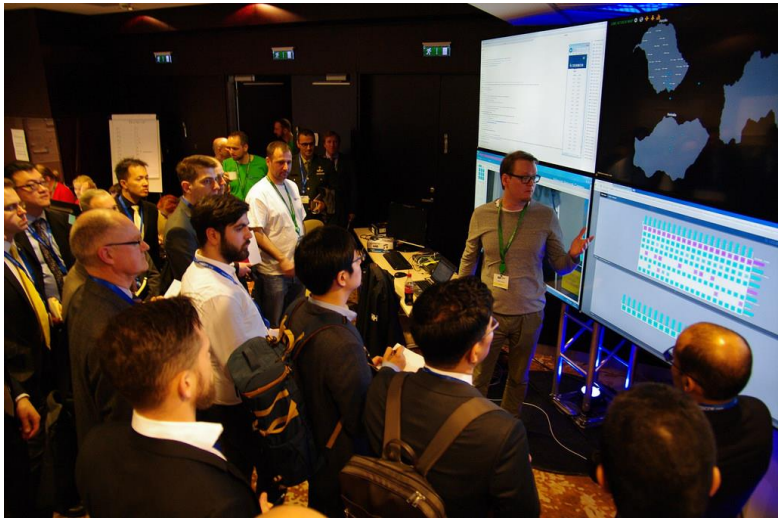


Photo: NATO Cooperative Cyber Defence Centre of Excellence

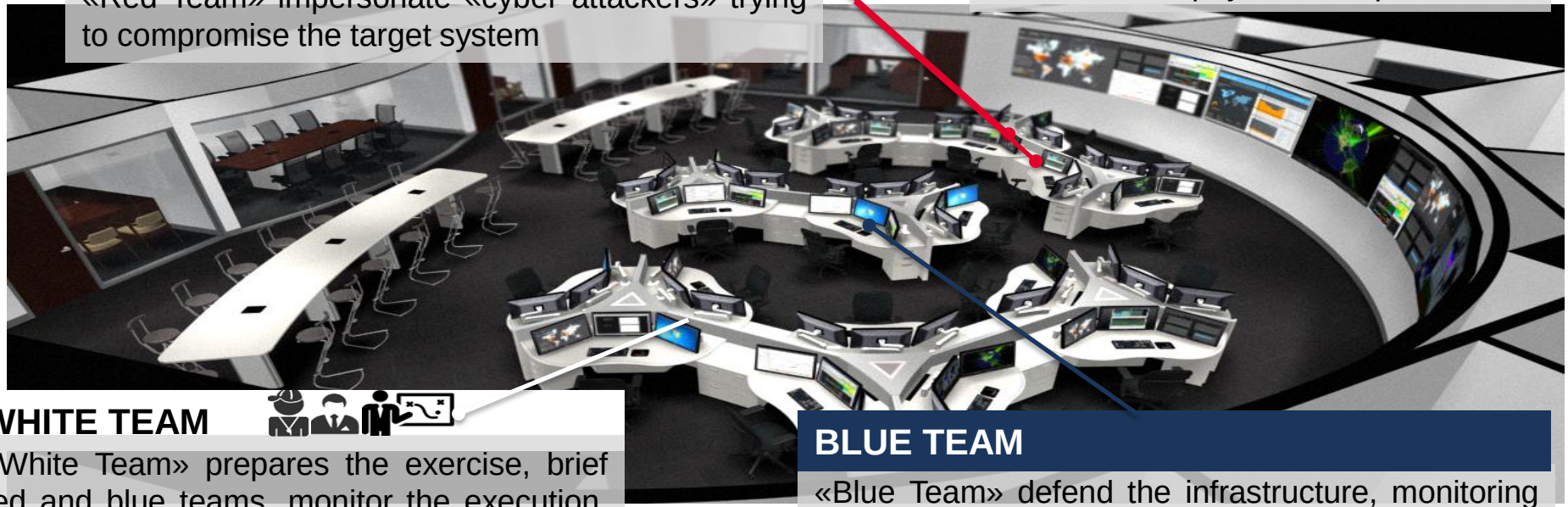
Full trace of the sessions is kept and can be subsequently replayed and analysed by "white team"

A Functional View

RED TEAM

«Red Team» impersonate «cyber attackers» trying to compromise the target system

Target Infrastructure: Virtualized with simulated and physical components



WHITE TEAM

«White Team» prepares the exercise, brief red and blue teams, monitor the execution, score performance, define methodologies and discipline

BLUE TEAM

«Blue Team» defend the infrastructure, monitoring it, detecting attacks and managing response

Cyber Range: A Safe, Legal Environment to Conduct Activities

Performance-based learning and assessment
prepare for cyber credentialing examinations
Classroom education, competition.

Photo: CyberChallenge IT (CINI)

Analyse and solve complex cyber problems
Develop and test cyber tools and doctrine to use them

Cybersecurity Testing During the Whole Lifecycle
organizational technical environments trial before deployment

Current Status – A quintessential Dual Use Technology

As implied in the name,, ranges were born in the military world

Photo: NATO Cooperative Cyber Defence Centre of Excellence

But testing for safety or performance is nothing new in engineering as Crash Test Facilities, Wind Tunnels and material climatic Testing

Current state of affairs: Cyber Range used by US DoD, NATO; Nations are building national Cyber Range, Commercial solutions covering part of the functional perimeter are being Built; EDA and other organizations are carrying on projects to Federate Ranges
Large companies and industry association are experimenting Cyber Ranges

Cyber Range: Trends

Cyber Range Exhibit a significant “network effect” and are effective when the platform is complete, with a community of experts with significant knowledge, size and real world experience to keep the simulated environment up to date

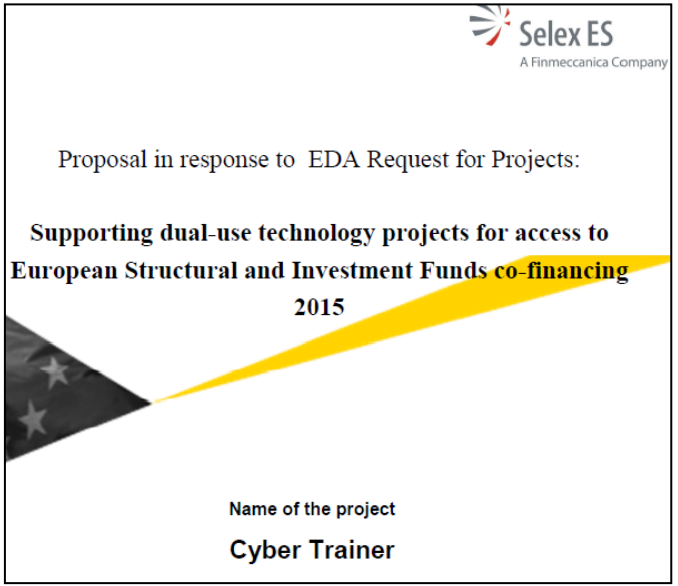
Growing importance of vertical Knowledge and sector-specific Cyber Ranges because at the very end, we are all interested in evaluating not the effect on the infrastructure but the effect on the supported application or on the mission capabilities. This may be achieved by federation (of vertical knowledge)

As with other testing and experimentation facility there is a general understanding that complex facilities tend to be shared.

- The recently proposed regulation of the European Union about the network of competence centres in Europe state this network may host testing facilities.
- EDA is carrying out a federation initiatives between different EU CR

Synergies between funding – 1

- Leonardo is building and improving modules of a its Cyber Range Solution combining
  - Self Investment
  - Natonal Defence Research programs within a consortium, led by Leonardo
  - FESR Project, Funded by Abruzzo (italian Region) 2014-2020, 1.1.1 e 1.1.4 action lines
- Leonardo proposed a Project Outline to an «ESIF Request for Projects» Call by the European Defence Agency (EDA) in 2015.
  - the project proposal included an endorsement letter by Abruzzio Region
- EDA selected the project in Sept. 2015 as strategic and provided free technical assistar for submission to the competent ESIF Man. Authority



The European Defence Agency (EDA) is pleased to inform that your project *CYBER TRAINER*, submitted in response to the «ESIF Request for Projects» (RfP) launched by EDA on 10 February 2015 [Communication N° EDA201502037], was selected to benefit from free technical assistance. As mentioned in the Rules for applicants of the RfP, this support is aimed at developing the complete document portfolio required for the project submission to the competent ESIF Managing Authority (MA).

Synergies between funding – 2

- Abruzzo Region published a competitive call for proposal including the area of cyber trainer in 4Q16
  - The call included terms and conditions an technical score according to the region smart specialization strategy (presence in the region, investment, participation in other regional initiatives)
  - Leonardo submitted a proposal leading a consortium of local companies in early 2017
  - The proposal was selected for funding in late 2017
  - Project started in 1H2018

REGIONE ABRUZZO

Dipartimento Sviluppo Economico, Politiche del Lavoro,

Istruzione, Ricerca e Università

Servizio Ricerca e Innovazione Industriale

POR FESR Abruzzo 2014-2020

Azione **1.1.1:** *"Sostegno a progetti di ricerca delle imprese che prevedano l'impiego di ricercatori presso le imprese stesse".*

Azione **1.1.4:** *"Sostegno alle attività collaborative di R&S per lo sviluppo di nuove tecnologie sostenibili, di nuovi prodotti e servizi".*

- Lesson Learned and possible areas for improvement
  - We did it!
  - Time frame too long considering cybersecurity evolution
  - Double submission (statistically half the probability to win), with the FESR call having to reconcile requisites from different areas
  - Technical Assistance is useful to help companies that do not have a practice in submitting funded proposals