Report

Cybersecurity Competence Pilot Projects

Addressing the Central Objectives

June 2019

Disclaimer

The work described in this document
conducted within the project cyberwa
project has received funding from the
Union's Horizon 2020 (H2020) resea
innovation programme under the Gra
no. 740129. This document does not
opinion of the European Union, and t
Union is not responsible for any use
made of its content.

Table of Contents

TABLE OF TABLES

1 Preparing the European Cybersecurity Competence Network

Earlier this year four pilot projects were launched in order to operate a pilot for a European Cybersecurity Competence Network and to develop a common European Cybersecurity Research & Innovation Roadmap. This shall contribute to strengthening the EU's cybersecurity capacity and tackling future cybersecurity challenges.

In addition to already participating at cyberwatching webinar in April[1], CONCORDIA[2], CyberSec4Europe[3], ECHO[4] and SPARTA[5] all participated at the Concertation meeting addressing how each project will address four topics which are central to the objectives of each project:

- Cyber ranges
- Threat intelligence
- Certification and standards
- Skills and capacity building

A key objective for the European Commission is that the projects collaborate and agree on shared definitions of these topics. Already with a joint website published, the Concertation meeting and previous webinar are important platforms for the projects to indeed align activities.

Presentations were provided by each project:

- Gabi Dreo, CODE & coordinator, CONCORDIA[6]
- Géraud Canet, CEA & SPARTA[7]
- Wim Mees, Royal Military Academy & coordinator, ECHO[8]
- David Goodman, Trust in Digital Life & CyberSec4Europe[9]

1.1 Cyber ranges

Cybersecurity exercise is a powerful tool for enhancing an organization's readiness and resilience against modern cyber threats. The complexity of the enterprise's IT environment has created the need to conduct larger scale cybersecurity exercises to train personnel and develop business and IT processes to handle different cyber incidents. Cybersecurity exercises provide opportunities for organisations to demonstrate critical capabilities and exercises reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets

A cyber range as a multipurpose virtualization environment supporting three "security-by-design" needs knowledge and hands-on skills development; improved system assurance in development; and improved system assurance through security test and certification evaluation. Cyber ranges facilitate high-fidelity simulations, improving stability, security and

[1] https://www.cyberwatching.eu/pilots-european-cybersecurity-competence-networks
[2] https://www.cyberwatching.eu/projects/1138/concordia
[3] https://www.cyberwatching.eu/projects/962/cybersec4europe
[4] https://www.cyberwatching.eu/projects/1043/echo
[5] https://www.cyberwatching.eu/projects/1136/sparta
[6] https://www.cyberwatching.eu/sites/default/files/CONCORDIA.pdf
[7] https://www.cyberwatching.eu/sites/default/files/SPARTA.pdf
[8] https://www.cyberwatching.eu/sites/default/files/ECHO.pdf
[9] https://www.cyberwatching.eu/sites/default/files/CyberSec4Europe.pdf

performance of cyberinfrastructures and information technology (IT), operations technology (OT), and industrial control systems (ICS). They are a vital part of the cybersecurity ecsosysem, enhancing training capabilities for professionals, strengthening the Cybersecurity Ecosystem, and representing real-world Cyber threat scenarios in a virtual environment.

There are two main definitions of cyber ranges:

NIST[10] defines cyber ranges as interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing

EDA [11] defines cyber range as: a multipurpose environment in support of three primary processes: knowledge development, assurance and dissemination. It consists of three complementary functionality packages[12],: Cyber Research Range (CRR) Cyber Simulation & Test Range (CSTR), Cyber Training & Exercise Range (CTER).

What are the exisiting cyber ranges?

As there is no strict definition of a cyber range, offerings vary globally in terms of scale, complexity and realism varies globally. Existing cyber ranges vary from larger IT vendors (e.g. IBM, Cisco or Palo Alto networks) cyber ranges to national cyber ranges providing commercial training, development, and research services (Finnish JYVSECTEC's RGCE) and other university or state-owned cyber ranges (Czech KYPO or Swedish CRATE)

Typical cyber ranges may be:

- A pre-defined simple and limited environment to provide infrastructure for Capture The Flag (CTF), e.g. a single virtual machine. Network accessible but limited environment to perform CTF exercises.
- Locally accessible infrastructure, participants must utilize their own laptops and actual work emails and systems; no malware can be used.
- Locally accessible complex and large scale infrastructure, where all equipment and devices are provided by the cyber range vendor/operator, which allows real malware running without fear of malware leaking to Internet or exercising parties business network

[10] https://www.nist.gov/sites/default/files/documents/2018/02/13/cyber_ranges.pdf

[11] https://www.eda.europa.eu/docs/default-source/procurement/annex-a---cyber-ranges-cst.pdf

[12] **Cyber Research Range (CRR)** A facility where in close cooperation with research centres, private sector, academic institutions knowledge development (research) takes place. Where newly gained knowledge can be utilised in new products, processes and/or services (development). A facility where e.g. ICT, network information & architecture (NII) in a variety of configurations and circumstances can be analysed. Currently used systems can be analysed as well.

Cyber Simulation & Test Range (CSTR) A facility within the cyber range where the current ICT-reality of a specific network configuration can be simulated, in which possible effects of cyber operations can be tested. The CSTR enables experimental testing of cyber capabilities in a realistic manner, but in a safe, isolated setting.

Cyber Training & Exercise Range (CTER) In order to achieve the necessary growth and sustainability in human capital, a state-of-the-art training & exercise functionality is needed. Modeling & simulation is a valuable asset where knowledge and skills concerning cyber capabilities and cyber operations can be trained and tested. A setting where cyber operators under simulated circ'umstances can be trained for utilizing cyber capabilities.

What technologies do they use?

The cyber range environment is run on a virtualised infrastructure (networks, servers, end user workstations). Depending on the cyber range, the usage of commercial solutions varies, but almost all cyber ranges utilise open source solutions widely to provide training and exercise environments.

- These solutions vary from basic information security controls (IDSs, firewalls, endpoint-protections (AVs) to more advanced machine learning / data analytical solutions.
- In addition, many of the traditional IT infrastructure solutions (Windows domains, proxies, DNS, etc.) are used to create realistic organisational environments for exercises
- For threat actor modelling, many cyber ranges utilise openly available pen-testing tools and red-teaming tools but also different custom-made tools and malware to represent real cyber attacks
- An ideal Cyber Range should also provide means for trainers in order to record the trainings session including screen captures, session events, trainee goals, and trainer comments. Combined with an automated *scoring system* during the training, trainees can automatically be evaluated and graded, making it easy to track performance and achievements for a debriefing after the CyberRange Training.

What open problems do cyber ranges face?

The main challenges that cyber ranges face are outlined below.

Technological	Companies and organizations are increasingly utilising cloud services, and providers are usually focused on global actors such as Amazon, Apple, Microsoft, Facebook, Google, Alibaba. Modelling these vendors' services realistically is non-trivial. Increasingly, security control mechanisms are run on cloud environments for performing the analytics and computing required
Research	For example, data analytics/deep-learning on cybersecurity requires suitable data sets not openly available
Economic	Organisations should increase cyber range usage in their annual business continuity plans to test, develop and verify preparedness against modern threats. Many organizations have not identified the need to exercise, often through lack of understanding of the benefits, usually seen as training for technical personnel, whereas they should be seen as tools to develop the whole organization’s capabilities on handling cyber attacks and preparing personnel against major incidents.

Table 1 Challenges around cyber ranges

The four competence centre pilot projects will address the topic of cyber ranges in different ways as outlined below.

ECHO will create a marketplace of ranges. Many ranges are broad in scope while others are very specific focusing on one field only. This will be promoted to companies and cyber-specialists and a variety of users will be able to submit and run scenarios and rent capacity

- ECHO Federated Cyber Range (FCR)

    - Interconnect existing and new cyber range capabilities through a convenient portal.
    - Ranges differ in scope from very broad to very specific including focus on one field only.
    - The FCR will enable access to emulations of **sector specific and unique technologies**
    - The Portal will operate as a **broker** among cyber ranges. For example, companies running their own training could through ECHO, rent and very specific technologies into a scenario.
- To be used as virtual environment for:
    - Development and demonstration of **technology roadmaps**
    - Delivery of specific instances of the **cyberskills training** curricula

Cybersec4Europe will provide a lightweight cyber range from existing proven building blocks:

- modern virtual engines and containers
- technologies for software provisioning, configuration, application management and deployment,
- interoperability standards including REST APIs,
- available datasets and testing data generators as well as virtual learning environments

Cybersec4Europe maps existing cyber ranges and open tools in cybersecurity, industry requirements and will provide a specification for implementation, including a sample integration/ federation infrastructure for cyber ranges and testing. It will also examine and provide open tools for certification and validation, closely aligned with education and standardization.

The prototype of the common portable virtual lab will facilitate not only the actual deployment of opensource tools, but also will support hands-on learning with gamification features for engaging and efficient learning, sample training materials, as well as guidelines for developers describing how to prepare their tools and other supplementary materials (documentation, user interface, testing data, APIs) will also be provided.

CONCORDIA will provide specific training based on world cyber threat scenarios and develop appropriate tools for their use. In order to achieve this CONCORIDA will:

- develop a common portfolio platform to present a Federation of Cyber Ranges across Europe in order to provide Cyber training facilities to the consortium and to others according to specific needs,
- implement means in order to *share scenarios* and *scoring methods* between different CyberRanges and
- provide best practice guidelines for implementing and hosting CyberRanges.

For the purpose of education and training, these prepared and deployed scenarios are designed to provide realistic experience for the trainees. For defender (blue team) training, scenarios may be built on known attack vectors, exploiting vulnerabilities that were not patched, or zero days that are utilized for the first time. Whereas red team training may contain penetration testing scenarios. In these situations the specialists under training learn e.g. how to discover the indicators of compromise, what are the right questions to ask, and how to act immediately based on a short investigation.

In order to provide these realistic scenarios in a Cyber Range, main building blocks have to be built and constantly evolved within CONCORDIA as the threat landscape is evolving as well:

- *Network architecture simulation*: An essential research activity will be the investigation how to map real-world network environments into the simulated cyber range

environment. This task include to develop automated network discovery/mapping capabilities to simulate topology, components, tools, configurations and services realistically.

- *Real-world traffic composition*: Beyond the network architecture, mimicking a real-world network traffic is crucial to achieve real-world scenarios. This comprises capture of traffic, analysis and processing of traffic as well traffic composition.
- *Automated adversary behavior*: A third research aspect will be the automation of adversary behavior to enable reproducability of training sessions. Especially, the development of an automated attack generator that is able to adapt to a changing network architecture is in scope of this task.
- *Scoring methodology*: Scoring is an integral part of scenario-based training to document the progress of specialists under training. The choice of scoring components is tightly connected to its technical implementation. The weights of scoring components will be developed and continuously improved as the scenario evolves.

CONCORDIA will develop and continuously evolve cyber range training to achieve better automated and custom-tailored training that correspond to the evolving cyber threat landscape.

SPARTA has no cyber range development, but research to provide enablers. SPARTA will create a catalogue of cyber ranges in Europe which is fully labeled with categories:

- handle complexity of cybersecurity threats and deal with early cyber attacks' kill chain phases
- develop methods and solutions for prediction and awareness- and knowledge-based cybersecurity management
- exchange of Threat Intelligence information between sharing partners and the actionability on such data regarding the GDPR

1.2 Threat intelligence

Threat intelligence, or cyber threat intelligence, is information an organization uses to understand the threats that have, will, or are currently targeting the organization. This info is used to prepare, prevent, and identify cyber threats looking to take advantage of valuable resources.

Cybersec4Europe will provide an elastic intrusion detection system suitable for cloud deployment based on a multi-disciplinary approach that makes use of network traffic analysis, employs online and offline complementary approaches to overcome:

a) online failure diagnosis for arbitrary faults using a white-box approach through the instrumentation of services and the use of domain-knowledge to finger-point the root of the fault, and
b) offline graph-mining for fault-detection by using graph-mining to collect common interaction patterns and then use it to detect faulty patterns through supervisioned learning.

The objective is to define the requirements and mechanisms to share digital evidence between different expert systems, providing solutions to allow interoperability, either through the unification of languages, formats and interfaces, or through trusted intermediate translators systems respecting the privacy, business requirements and the regulations of different countries

The system will enhance the state of the art for reliability, safety and privacy guarantees of security intelligence techniques based on artificial intelligence, machine learning and data

analytics. The investigating mechanisms used will be capable of interacting with Threat Intelligence Information Services to capture evidence of malware activity at an early stage.

Research challenges addressed will include on log and event management, threat detection and security analytics with privacy-respecting big data analytics with the goal of enabling security intelligence in defensive systems, by ensuring the underpinning intelligence systems are fortified.

Based on existing information-sharing tools available on the market today, the **ECHO** Early Warning System will provide a sharing capability allowing information between disparate operational units across organizational boundaries:

- **Security operations support** tool enabling members to **coordinate and share** cyber relevant information in near-real-time
- Secure information sharing **between organizations**; across organizational boundaries and national borders
- Coordination of **incident management workflows**
- Retain **independent management and control of cyber-sensitive** information
- Account for **sector specific needs** and protection of **personal information protection** (GDPR compliant)
- Includes sharing of **reference library** information and **incident management** coordination

CONCORDIA is developing a Threat Intelligence platform for Europe which can be used to share threat information across academic, industrial and other organizations, involving especially the European CERT community. While many initiatives have addressed the needs of cybersecurity data sharing by improving the amount ofactionable information shared, other initiatives focused on new types of actionable information, the qualityof information shared or the preconditions of trusted team-to-team relationships that will lead to share more widely, earlier or even more risky information that might be used against the own organization.
With the development of the CONCORDIA's Threat Intelligence platform these critical issues will be addressed:

- Build a central threat intelligence platform for the exchange of actionable information related to security attacks or incidents to be used within the CONCORDIA consortium supporting the maintenance of trust circles for sharing available information within sub-groups depending on the need of companies and governmental bodies.
- Develop access models for the sharing: (i) open, available to all, (ii) sensitive, available to dedicated organizations, and (iii) restricted, available to selected organizations.
- Based on the CONCORDIA's Threat Intelligence platform, develop applications which support (i) the tagging of likely attributions of attacks, and (ii) the assessment of proactive countermeasures in case of a new emerging attacks, identified vulnerabilities, or campaigns of actors.
- The CONCORDIA's Threat Intelligence platform will support the collection, sharing and discussion of cross-sector threat intelligence by adding specific modules for specific sectors, building on the support of trust circles to ensure the sharing based on sector or governmental sharing policies.
- Develop federated machine learning approaches to share models instead of data.

In addition, CONCORDIA is developing sector-specific threat intelligence platforms for the telco and finance sector.

Next to sharing of threat information, CONCORDIA is planning to host a platform which enables to inform stakeholders about incidents in their constituency. Further researchers are able to provide information such as vulnerabilities in certain networks to the platform and share it with the vetted CSIRTs responsible for the network.

Another aspect, CONCORDIA will work on, is the topic of Course of Actions. Today, within Threat Intelligence mostly the part of sharing and detection is covered but not the part of automated incident response. In CONCORDIA we contribute to the standardization efforts in that area and will develop prototype implementation of such standards.

SPARTA deals with early phases of attacks by predicting where and when an attack may take place. Exchange of information is vital for this.

1.3 Certification and standards

Cybersecurity certification and standards are an essential part of a successful Digital Single Market ensuring trust and security in products and services.

The Cybersecurity Act, which came into force in June 2019, can be divided into two parts: in the first part, the role and mandate of ENISA are specified, whilst, in the second part, a European system of certification of the cybersecurity of devices connected to the Internet and other digital products and services is introduced. The Competence Centre pilot Projects focus on this field and contribute to the activities of ENISA with the broader aim of effective enforcement of cybersecurity as a result of harmonized standards and a corresponding certification system to ensure compliance.

A key ingredient of a successful standard is contribution from a variety of expert sources. **CONCORDIA** will focus on exploitation and contribution to existing international best Cybersecurity measures, techniques, methods etc. and Cybersecurity skills.

At the end of the applicable process, independent assessments will be carried out against these standards with the aim of providing the appropriate validation (this includes people as well as process assessments)

As an R&I project **SPARTA** will carry out research into providing enablers for certification and standards. Assessment is a key aspect of certification, yet it is not scaling up to handle modern digital systems. Main activities include

- Development of more agile assessment and certification frameworks, similar to agile development
- Automation, supporting developers in writing requirements and executing tests
- Assessing systems of systems, beyond individual components, and modularizing assessment to enable assessment of complex systems and services
- Lifetime dynamicity of environments who may have long lifespans, but where individual components might be replaced or upgraded
- Execution elasticity, particularly for services

ECHO is delivering a cybersecurity certification scheme to support ENISA. The ECHO Cybersecurity Certification Scheme:

- Leverages and builds upon work of **ENISA** (EU Cybersecurity Certification Framework) and **ECSO** (e.g., meta-scheme development)
- Provide **product oriented** cybersecurity certification schemes
  - Support sector specific and inter-sector security requirements
- Support **delivery and acceptance of technologies** resulting from technology roadmaps
  - **Improve security assurance** through use of **certified products**
- Support development of **Digital Single Market**
  - Limit duplication and fragmentation of the cybersecurity market

- **Common** cybersecurity **evaluation methods, acceptance** throughout Europe
- Applicability across **Information Technologies** (IT/ICT) and **Operations Technologies** (OT/SCADA)

CyberSec4Europe defines governance and supporting services for security certification, with research, support, guidance and training for validation and certification of security properties of devices and systems for EU industry.

- Investigating certification for critical infrastructure components
- Aligning efforts with ENISA and ECSO framework policy work
- Cooperating with tools / services, standardization, conformity and validation
- Reducing time to certification of critical sector cyber physical systems by designing a unified certified-by design IoT-enabled CPS framework where overall assurance is guaranteed for the complete system.
- Assessing the Cybersecurity Act, ISO27001 and GDPR following approval of EU Cybersecurity Act.
- Aligning with ECSO, on future certification and harmonisation including governance structures and aspects of the further global penetration of the cybersecurity certification scheme.

CONCORDIA is supporting ENISA in setting up and maintaining the European cybersecurity certification framework by providing the technical background for specific certification schemes. Support the certification authorities with testing and validation capabilities within the European Cybersecurity Certification Frameworks for ICT products and services as proposed by the EC. Certification is known to be an important trust-building measure for services and solutions on the market, but also expensive and often slow task leading to time-to-market delays. By granting access to CONCORDIA's virtual labs to certification authorities and providing them with testing and validation capabilities, solutions and services developed by CONCORDIA members will be better tested, quicker certified, and sooner on the market. Furthermore, CONCORDIA will contribute to the certification process and policies via TUV.

CONCORDIA also focuses especially on IoT software verification to develop new continuous assessment methods to not just certify an IoT device prior to deployment but perform fully automated certification after each update. With for example TUV and RISE CONCORDIA has also approved certification bodies in the consortium.

1.4 Skills and capacity building

As reported in D3.2 and discussed at Concertation meeting in 2018, there will be a global shortfall of 3.5 million cybersecurity experts by 2021 There is therefore, a strong need to create technical capabilities in the area of cybersecurity and to change the societal view. The situation is further compounded by a current lack of trainers who also need to be educated themselves. The Competence Centre Pilot projects each address the issue of improving Europe's capacity building in the field.

The **CONCORDIA Cybersecurity Ecosystem** will provide virtual labs, services and training activities. CONCORIDA is also building a sustainable CONCORDIA European Education Ecosystem for Cybersecurity including:

- Open source threat intelligence platform – open source
- Pilot DDoS Clearing house
- Mechanisms for community building, support & incentive models

CONCORDIA will also provide services to promote capacity building in Europe:

- Virtual labs

  - Lab infrastructure to support the development of solutions
  - Hosting infrastructure & personnel for the European Threat Intelligence platform
  - Testing and validation capabilities in support of certification
- Services
  - Portfolio of tools (public and proprietary) & best practices for design, analysis and testing of Cybersecurity systems
- Training for professionals
  - Capture-the-Flag, Red-Blue-teaming events (plan/execute/review)
  - Cyber range training – develop realistic scenarios to address the evolving cyber threat landscape

In view of establishing an European Education Ecosystem for Cybersecurity, the following activities are foreseen:

- Pool, assess and disseminate existing courses for professionals organized by the consortium partners
- Develop a methodology for creation of new courses and/or teaching materials
- Develop new courses for mid-level managers and executives
- Develop a framework for CONCORDIA certificate for courses
- Teach-the Teachers – courses and guidelines
- Networking activities

A key part of this is the newly launched the EU cybersecurity training ***map***. The map includes information on cybersecurity courses from industry and academia within the consortium. To date more than 4,000 cybersecurity professionals were trained via the 20+ courses organized by different Concordia partners. Some of the courses are well established on the market, others are brand new, as to respond to the latest challenges of the Cybersecurity sector.

The map targets mainly IT technical team members and experts, middle managers leading IT or non-IT technical departments, executives, who can all find a course that suits their needs for reskilling, upskilling or simply learn about this challenging domain.

Various filters help match specific need for skills development with the offer. You can choose to sort the courses based on the cybersecurity level addressed (Device-, Network-, Software/System-, Data/Application-, User-Centric), or on the industry sector (e.g. Telecom, Finance, Transport/e-Mobility, e-Health or Defence), but also on the format (face-to-face, online, blended) or the language taught.

Over the course of the CONCORDIA project, the map will be continuously updated with the new courses/trainings developed by the project different university and industry partners. Besides, in our effort for establishing a European Education Ecosystem for Cybersecurity, we opened the map for submission of courses/trainings targeting cybersecurity professionals and organized by other European organizations. The map will thus have the potential to become a marketplace for cybersecurity skills for professionals.

The **ECHO** Cyberskills framework will address the needs and skills gap of cybersecurity professionals based on a mapping of the cybersecurity multi-sector assessment framework. The E-CSF will be made up of learning outcomes, competence model and generic curriculum in order to establish a mechanism to improve the **human capacity** of cybersecurity across Europe

- Leverage a **common cyberskills reference**:
  - Derived and refined from ongoing and related work (e.g, ECSO, e-Competence Framework, European Qualification Framework)
- Design modular **learning-outcome based curricula**

- **Hands-on skills development** opportunities through realistic simulation (ECHO Federated Cyber Range)
- Lessons learned feed **knowledge sharing** (ECHO Early Warning System)

Cybersec4Europe will run its platforms as a capability building instrument open to external sources and third-party material outside the consortium (subject to guidelines and quality standards).

By establishing an education and training framework and related instruments to support continuing education and lifelong learning in cybersecurity, organized to demonstrate the effectiveness of governance models and full transfer of pilot results to the future Centre's operations.

- Learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles.
- Knowledge units and curricula, training and awareness to achieve such objectives and competences, setting activities to apply and test such competencies.
- Implementing the CyberSec4Europe education strategy for citizens, students, and professionals through creating and promoting the project brand and the guidelines / procedures to produce and consume content from platforms developed.