Cyber Ranges for a Resilient Europe

AUGUST 2022

Main Authors

Martin Horak - CONCORDIA
Jakub Čegan - CONCORDIA
Konstantina Papachristopoulou - SPIDER
Damir Haskovic - FORESIGHT

This Policy Brief Compilation booklet has been produced with the support of Trust-IT Services, provider of the Horizon Results Booster, funded by the European Commission. The Policy Briefs have been written by projects and project groups that took part in the Horizon Results Booster.

Disclaimer

The information, views and recommendations set out in this publication are those of the projects that took part in the Horizon Results Booster and cannot be considered to reflect the views of the European Commission. The Horizon Results Booster is funded by the European Commission N° 2019/RTD/J5/OP/PP-07321-2018-CSSDEVRIR-CSSDEVRI01.

Table of contents

Executive Summary

In recent years, cyber-attacks targeting large and small organisations, critical infrastructures and public-sector organisations have evolved faster than ever with cybercriminals developing and boosting their attacks at an alarming pace. This context has been driving a rapidly growing need for well-trained cybersecurity professionals.

The Cyber-range project group is a cluster of 3 EU H2020 research projects (CONCORDIA, SPIDER, FORESIGHT) which are addressing this growing challenge offering innovative forms of training and greater usage of online tools such as cyber ranges. The project group has come together under the umbrella of the Horizon Results Booster programme (HRB) of the European Commission to jointly disseminate results that help tackle key challenges in the cybersecurity training sector.

1. Topic Overview

The cybersecurity market has grown exponentially in recent years driven by a growing number of cyber-crimes targeting large and small organisations, critical infrastructures and public-sector. The impact of cyber-crime has been further fuelled by global events such as the COVID-19 pandemic, increasing digitalization and the adoption of emerging technologies such as Internet of Things (IoT), Artificial Intelligence (AI) and Machine Learning (ML) which can increase vulnerability.

Cyber ranges are recognised as a key resource to educate and train corporate staff (including not only security experts, but also non-experts) using realistic environments as a means to validate organisational capabilities and capacities. Originally used by the military, they are now being deployed by private sector, universities, research institutions and governmental bodies to test infrastructure and improve technical skills. With a dearth of cybersecurity experts in the workforce, improving the expertise and preparedness of existing staff members can be critical in ensuring better cyber resilience.

The drive for an increased use of cyber ranges is also led by EU authorities and initiatives such as the European Union Agency for cybersecurity (ENISA) and the European Cyber Security Organisation (ECSO) which are constantly calling for innovative forms of training and greater usage of online tools such as cyber ranges for upskilling employees.

1.1 Topic

Although the field of cybersecurity has expanded exponentially, the number of skilled and qualified workers is still not enough to meet the worldwide demand. Cyber ranges have been gaining in popularity over the last years allowing users to train in both realistic environments and scenarios and gaining hands-on experience in security aspects of varied complexity, depending on their role and level of expertise. Cyber ranges have now become the perfect playground for a very wide and diverse range of scenarios with increased complexity and involving different actors with respect to traditional training methods, accelerating effective learning of best practices and promoting a deeper understanding of the consequences of any action.

1.2 Main challenges

The development of a number of cyber range technologies, products, national and international initiatives to tackle the evolving cyberthreat landscape has increased in recent years. However, these innovations bring with them major challenges on different levels.

Lack of identification of proper skills and roles for cybersecurity training.

Several approaches exist to address cybersecurity education, awareness and training. However, they focus on compliance, e.g., using blanked approaches in applying data confidentially, integrity and availability risk reducing controls, without tailoring to the actual human factors involved. Human interaction that is central to business, processes, and system operation needs to be better understood if cybersecurity awareness needs are to be effectively addressed.

Lack of models for cybersecurity economics.

While cybersecurity metrics are available for a variety of data types, their economic value is hard to evaluate (e.g., in the case of reputation loss). A lack of common definitions and methodologies can result in big differences when assessing the economic implications of cybersecurity incidents.

Low accessibility and usability of cyber ranges.

Europe has well-established cyber range knowledge and experience, yet the technology is not widespread. This is mainly due to two reasons: from a technology perspective these systems still require a lot of different expertise in order to be properly set up, installed, managed and then to operate. From an accessibility perspective, there are still entry barriers for organisations and academia related merely to solution pricing and costs as well as emulation costs. These could be very expensive depending on the complexity of the infrastructure. Furthermore, the proprietary nature of most solutions restricts collaboration of organisations.

Difficulties in generating evidence-based cybersecurity simulation scenarios.

The development of evidence-based simulation scenarios and guidelines for cybersecurity experts is an important step in redesigning cybersecurity education. Currently, there are no appropriate tools and methods for supporting current and future generated evidence-based simulation scenarios.

Lack of integration of soft skills, technical side and management side.

Cyber ranges are usually looked on as a mostly technical issue. In reality though, they should also be seen as highly relevant to senior management and a key part of an organisation's cyber-strategy in terms of identifying critical assets and which parts of the organisation should be protected. One of the biggest challenges is understanding how to bring together the simulation of the technology with the simulation of controls and cyber-attack simulation into the decision making process. Understanding how to track and monitor this integration is key.

2 Recommendations

2.1 Making cyber ranges more accessible

The European Union should invest in creating strategies to enhance the accessibility of cyber ranges. Europe could **leverage on open source solutions** by establishing an open cyber range to provide a suitable place to train future generations of cybersecurity experts. This would provide transparency, allow auditing, and limit vendor lock-in. The cyber range has to be governed by a foundation composed of EU cyber security agencies ENISA, The European Cybersecurity Competence Network and Centre (ECCC), universities, and partners from the industrial sector. At the same time, Europe should push towards the **development and adoption of preferably open cloud based cyber range environments**, which will allow access to this technology also for smaller organisations without the need of hosting it at the user's physical premises.

2.2 Cybersecurity training is not just an IT issue

While the cybersecurity skills gap continues to widen, cybersecurity is still mostly seen as an ICT challenge, rather than a business risk. There's a growing need for high level **training for cybersecurity awareness, targeting not only expert professionals but also non-expert users**. A proper mix of security testing, security training, and cybersecurity investment decision support, can improve organisations' security, resilience and sustainability by ensuring that (i) the services, systems, policies and technologies they use are well-tested and complying to their needs, (ii) their staff (experts and non-experts) are effectively trained, and (iii) security investments are cost-effective and appropriate for the particular organisations.

2.3 Open cybersecurity training and exercises

The European Union should support an open format of cybersecurity training and exercises. Human and machine-readable open format based on widely used technologies, provides a **de facto standard for cooperation between organisations** running instances of cyber ranges by greatly supporting the development of new training and exercises. The open format should also **provide interoperability between already operational cyber ranges** by conversion into the native format of the platform.

2.4 European cybersecurity training and exercises community

The European Union should support institutions to create more cybersecurity training and exercises by stimulating community growth. As development requires a specific set of skills, **collaboration seems to be the only option to ensure the proper amount and quality of the content**. It can be facilitated by sharing best practices, organising workshops, and preparing project calls specialised in training and exercise development desirably in correlation with skill frameworks.

Project Group

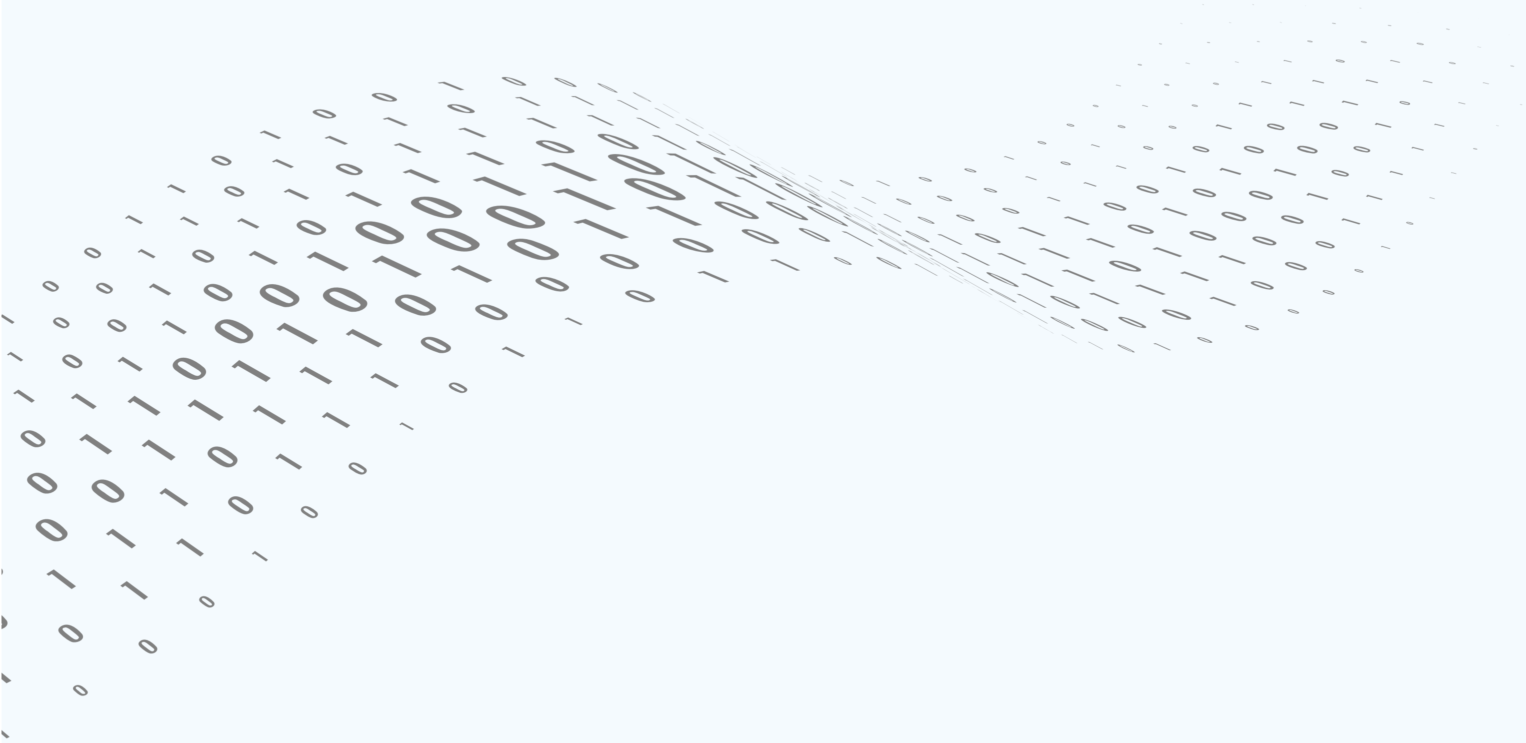
Project Group Leader: Martin Horak, CONCORDIA

Contact: horak@ics.muni.cz

www.concordia-h2020.eu

www.spider-h2020.eu

www.foresight-h2020.eu



The HRB - Horizon Results Booster is an initiative funded by the European Commission, Directorate General for Research and Innovation, Unit J5, Common Service for Horizon 2020 Information and Data.