Information & Security

G. Sharkov et al.
vol. 53, no. 2 (2022): 287-302
https://doi.org/10.11610/isij.5319

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Towards a Robust and Scalable Cyber Range Federation for Sectoral Cyber/Hybrid Exercising: The Red Ranger and ECHO Collaborative Experience

George Sharkov [1,2] (✉), *Christina Todorova* [1,2], *Georgi Koykov,* [1,2] *and Ivan Nikolov* [1,2]

[1] *European Software Institute – Center Eastern Europe, Sofia, Bulgaria*
https://esicenter.bg/

[2] *Cybersecurity Laboratory at Sofia Tech Park, Bulgaria*
https://sofiatech.bg/

ABSTRACT:

Cyber exercising is essential to crisis management preparation and maintaining a robust cybersecurity posture. To prepare for growing hybrid threats, complex cyber-hybrid scenarios with practical cooperation at the technical, operational, and higher decision-making levels are increasingly being used, leveraging the power of cyber ranges. Alas, owing to a lack of suitable simulation infrastructure and the ability to adapt cyber ranges to varied situations, such complex scenarios often remain inaccessible. The federation of cyber ranges is one potential response to this challenge, providing a solution for the individual cyber range limitations in terms of resources to replicate complex cybersecurity-relevant realities.

The current contribution describes the authors' experience designing the Red Ranger, a Composite Cyber Range. We detail the design and development to facilitate the agility required to support a working multi-faceted federation with the ECHO Cyber Range to allow for an "exercise-as-a-service" model to provide adequate and accessible cyber-hybrid mechanisms for crisis response training and preparation.

ARTICLE INFO:

RECEIVED: 29 JULY 2022
REVISED: 15 Sep 2022
ONLINE: 23 SEP 2022

KEYWORDS:

cyber range, training, federated, exercising, simulation, cybersecurity

✉ Corresponding Author: gesha@esicenter.bg

Introduction

The present cybersecurity landscape favours the advancement of the classic cyber-exercising paradigm and tools. Against the backdrop of the current data-driven economy, recent cybersecurity events show that cyber threats, combined with a profound digitalisation process, are growing more complicated, intertwined, and sophisticated.[1] The challenges related to this massive shift toward the e the "datafication-of-everything" pose an imperative over cybersecurity as a keystone in the foundation of a reliable hyperconnected world.[2]

At an EU level, building the appropriate toolset of knowledge, skills and competences, raising awareness, and cultivating information analysis and triage skills, have been pointed out as crucial for strengthening industry sectors' stability, security and trustworthiness beyond the critical infrastructures and the security sector.

This landscape necessitates providing hands-on, realistic and thus hybrid cybersecurity training. Complex cyber-hybrid scenarios that need practical cooperation at the technical, operational, and higher decision-making levels are increasingly being used to prepare for developing hybrid threats. Such simulations imitate seemingly unrelated occurrences in several places, enterprises, or systems that may swiftly build to a sectoral or national catastrophe. Unfortunately, such diversified scenarios are often unavailable owing to a lack of appropriate simulation infrastructure and knowledge to adapt them to different situations. An opportunity to approach this deficit is through cyber ranges.

Cyber ranges are interactive platforms that comprise simulations, network representations, system tools, and applications that enable the hands-on practice of technical and operational skills, knowledge, and abilities.[3] Regardless of cyber ranges often being used as testbeds for developing cybersecurity solutions or other software, training and exercise are the most typical reasons for their usage.[4]

Hands-on experience with cyber ranges has become one of the most sought-after benefits for cybersecurity experts.[5] Still, its application has spread beyond the cybersecurity professional circle into the general workforce of companies, where cybersecurity skills must be exercised, strengthened, and maintained to ensure a competitive advantage.

Overall, cyber ranges have the potential to assist increase the stability, security, and performance of teams, security infrastructures, and operational procedures by enabling high-fidelity exercising and simulations of functional scenarios in a sandboxed environment.

The limited capabilities and capacity of most cyber ranges now on the market to replicate the complex reality and linkages in inter-sector scenarios provide a significant issue. While sector-specific cyber ranges have existed for a while, developing complex cyber/hybrid scenarios, and demonstrating cascading effects on multiple sectors, remains exceedingly tricky. As a specific cyber range may be prepared entirely in one area but lacking in another, this implies investing significant resources into expanding the existing capabilities of the exercise infrastructure or investing in new ones to generate diverse scenarios for cyber

exercising and capability development. Therefore, it is critical to design the scalability and modality of the infrastructures to allow the interoperability of several cyber ranges of multiple cyber range providers from various sources to construct complex scenarios – a concept known as cyber range federation. *One such cyber range provider is the Red Ranger, collaborating with the ECHO pilot project.*

The *ECHO Federated Cyber Range* aims *to address the problem of fragmented capabilities* by establishing a mechanism by which the independent cyber range capabilities can be interconnected and accessed via a convenient portal for configuration and management to allow for an "exercise-as-a-service" model to provide adequate and accessible cyber-hybrid mechanisms for crisis response training and preparation.

The *Red Ranger* is a dedicated technical cyber range and orchestration platform designed by the authors of this paper to implement complex cyber/ hybrid exercises.

The current contribution describes the authors' experience designing the Red Ranger, a Composite Cyber Range, to facilitate a working multi-faceted federation with the ECHO Federated Cyber Range.

In this paper, we will provide a very brief overview of the ECHO Federated Cyber Range, which has been the subject of previous scientific contributions, focusing only on the modalities of the federation which allow the Red Ranger integration. Following that, we present a summary of the architecture of the Red Ranger. Within the scope of this description, we will limit ourselves to a practical architectural overview, showing the approach toward building a scalable, agile and easily adaptable cyber range to respond to the challenges the cyber range federation poses. Last but not least, we conclude with a use case scenario implemented through the Red Ranger in federation with the ECHO Federated Cyber Range (E-FCR). Lastly, we offer some concluding words illuminating this technology's ongoing research and prospects.

The ECHO Federated Cyber Range

The ECHO Project, being one of the four pilots launched by the EC to establish and operate a Cybersecurity Competence Network, naturally aims to facilitate sharing capabilities for cybersecurity hardening and defence across Europe. The project's principal purpose is to organise and optimise the EU's existing fragmented cybersecurity efforts, including cyber ranges. The ECHO Federated Cyber Range (E-FCR) ensures the connection between cyber range capabilities.

The E-FCR provides the infrastructure needed to enable security roadmaps research, experimentation, test, and certification of new security technologies, as well as to support advanced cybersecurity training (including distributed computer-assisted exercises with specific scenarios) and preparation of qualified cybersecurity experts. The vision of the ECHO project consortium for the E-FCR is to establish it as a significant marketplace for cyber range services in Europe. As such, the E-FCR has been designed to incorporate factors, including 1) bridging supply and demand, 2) bringing together all necessary talent required

for a scenario, and 3) catalysing innovation by encouraging access to a pool of inventors.

The core principles guiding the ECHO consortium in developing the E-FCR are demonstrated in Figure 1 below.

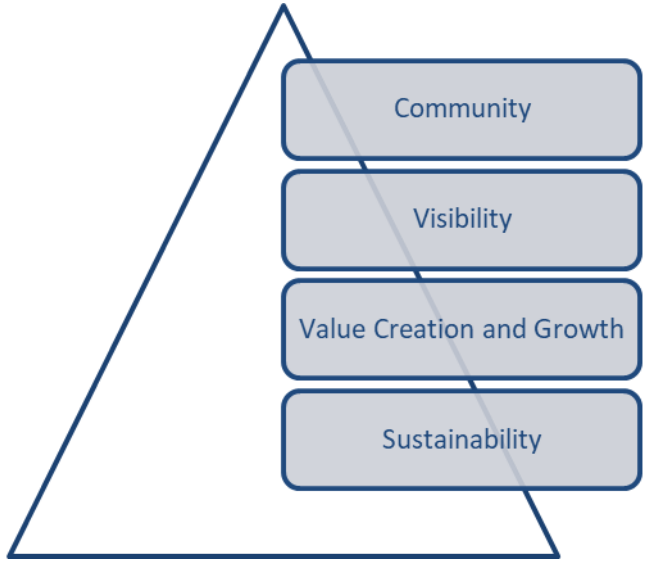

Figure 1: Core Design Principles of the E-FCR.

The crown principle of the E-FCR, as seen in Figure 1, is attracting and growing a vast and vibrant community, with a strong security focus and a particular demand for talent for cyber range orchestration.

The E-FCR is envisioned as an infrastructure capable of integrating many cyber range providers and functioning as a capacity and capability concentrator.

As such, the E-FCR cannot function in itself and requires cyber range providers, which mandates the deployment of *E-FCR Agents* on the federated ranges.

The architecture of the E-FCR is comprised of four main layers, as described by Oikonomou et al. (2021), namely the *Client Tier, Front Tier, Mid Tier*, and *Back Tier*. Each layer offers unique entry points and links to lower tiers while containing multiple key E-FCR components.

Beginning with the *Client Tier*, especially the E-FCR Dashboard, we may characterise it as the container of several sub-components that together make up the actual user interface of the E-FCR platform.

The Client Layer is directly linked to the Front Tier. The *Front Tier* is essentially an intermediary component, a reverse proxy, in charge of establishing communication between the Client and Mid tiers. Notably, this component serves as a single point of access to the system.

The *Mid Tier* refers to more essential components and a clear separation into two sub-layers.

1. *A Front and Mid-Tier connector*. This is the principal entry point for all requests entering the current tier. The Access Portal component is primarily responsible for routing incoming requests to the proper micro-service, or recipient subcomponent, situated in the Mid Tier while ensuring that only authorised requests can proceed.
2. An essential components sub-layer. This inner layer of the Mid Tier connects components critical to the federation management. Those are described in more detail in Table 1 below.

Table 1. Mid Tier Core Components.

Component	Description
Billing Manager	A component that defines the whole billing process.
Capacity and Capability Map	A structure denoting the available capacities and capabilities.
Cyber Range Gateway	An entry-level communication point.
Quality of Service	A component gathering information on metrics.
Service Catalogue	A structure responsible for storing and making available any service.
Service Request Repository	A component storing and making available all the information regarding service requests.
Service Broker	A structure used to handle the processing of a request and defines its distinct stages.
User Manager	A component managing the user repository of the system and providing user information.

Lastly, there is the *Back Tier* of the E-FCR, essentially the back-end of the system, holding database management systems primarily, which effectively control the outputs of other Tiers' components.

The scenarios and federations are managed on the Client Tier through a dedicated GUI through a dedicated component named the Service Designer. The Service designer employs a Service Description Language, which aims to create human-readable content that could still be machine parsed. The ECHO Service Description Language (ESDL) is used chiefly through a wizard application within the Service Designer and then checked by the same application for semantic accuracy.

The Red Ranger was mainly federated and configured through this level of readiness of the E-FCR. Notwithstanding, many architectural particularities make the Red Ranger effortlessly and readily extendable into another complex

service broker, such as the E-FCR. These architectural perks are discussed in the chapter below.

The Red Ranger

The Red Ranger was developed to link many cyber ranges to analyse the combined effects of numerous hypothetical events played out throughout the course of the same exercise. The connections may be accomplished via a virtual private network (VPN) or Ethernet technology. It is planned to integrate E-FCR federation procedures, which will make it simpler to federate with simulations already available on the E-FCR market.

The capabilities of the E-FCR are ultimately increased by external cyber ranges, such as the Red Ranger, which offers cyber ranges and simulations that apply to any given circumstance but are designed for general use in the long run.

Core Features

The objective of the cyber range federation is to expand its members' capabilities and capacity by combining different cyber ranges that serve the same function into a single configuration. Maintaining and exercising control over the various components of the infrastructure is simplified through the use of a *highly-modular infrastructure*, as will be discussed below and in the next sub-chapter.

The most important aspect of the design is the *automation* of the cyber ranges' deployment process, allowing for increased support for various devices, servers, and activities. An automated environment may bring out the best in a cyber range by enhancing its stability, security, and infrastructure.

Among the core advantages of implementing automation is that it allows scalability while significantly shortening the process of initialising, setting up and breaking down test environments may shorten both these processes significantly.

Scalability is one of the fundamental aspects that helps to enhance the cyber range's performance within the federation and, ultimately, the exercise scenario. This is accomplished by deploying a cyber range numerous times to boost the federation's overall performance and limiting the chance of unavailability of a given component. Given that each deployment represents a marginally unique cyber range, The Red Ranger includes a framework for scenario federation, which implies that several scenarios may be joined together to examine the expected repercussions of numerous crises for various sectors.

Lastly, a core feature to be discussed is *privacy and confidentiality*. Within the cyber range, this is mainly ensured through Virtual Private Networks (VPN), configured to enable remote access and file sharing, eliminating the need for users to participate in the activity directly. As security within the range setting depends marginally on concealing Internet Protocol (IP) addresses, a VPN may be used to get a new IP address. Also, through a VPN, the users gain access to a restricted subset of internal infrastructures available for the exercise.

High-Level Architecture

The Systems-of-Systems methodology underpinning the cyber range infrastructure development process emphasised the requirement for design modularity to assure the infrastructure's flexibility and adaptation to many settings and systems.

Figure 2 shows this example depicting a conventional composite cyber range with four-faceted modularity enabled by VPN tunnelling and a dedicated VPN server added to each range to assure interoperability. We have used dedicated OpenVPN servers for the pilot federations with the E-FCR.

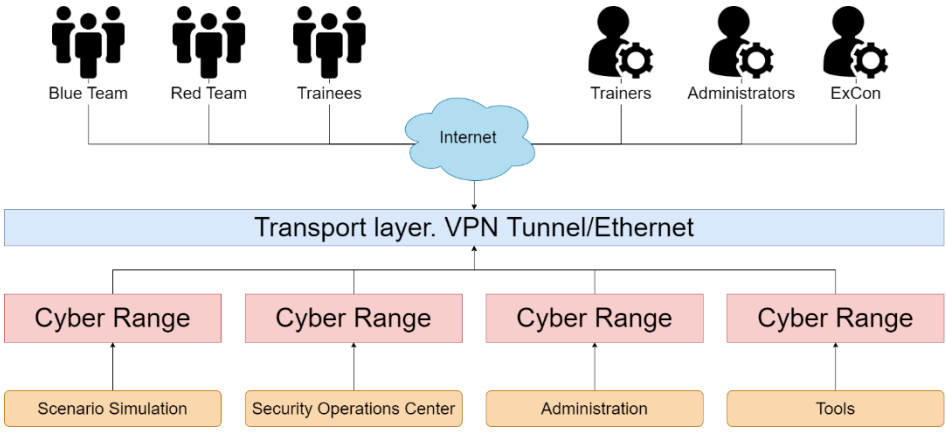

Figure 2: A High-Level Architecture of the Red Ranger.

In Figure 2, we have a simple depiction of the Red Ranger's high-level architecture, which demonstrates how the service is broken into smaller federated cyber ranges, each with a specific role.

This modularity essentially provides insurance that each component of the cyber range may exist on its own, independently of the remainder of the services. Figure 3 below describes the critical components of the cyber range (depicted in Figure 2) in more detail.

We may consider the Administration cyber range the main cyber range since it has all the tools to perform the simulation/exercise. The Administration Cyber Range offers essential infrastructure and backbone services for cyber range and scenario operations. Its main components can be seen in Figure 4 below.

As evident from Figure 4, besides the OpenVPN server, which was discussed above, and the DNS Server, which serves the somewhat apparent purpose of handling the DNS records, we have the following components:

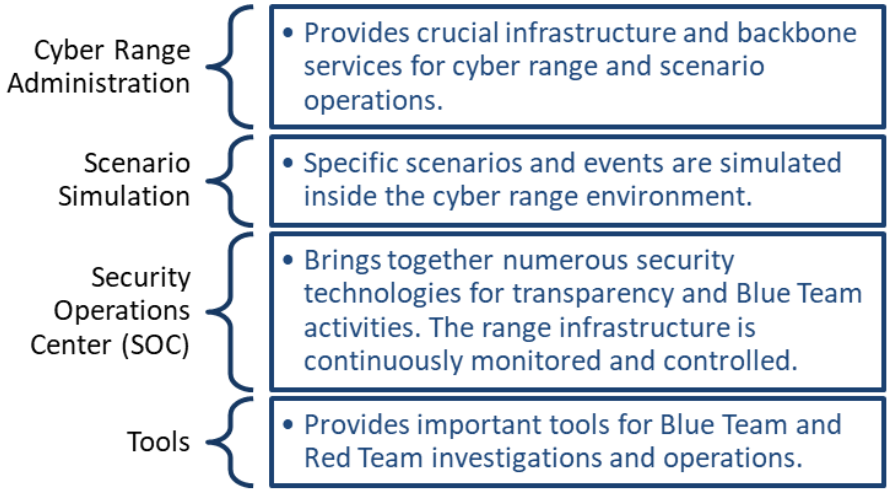

Figure 3: Components of the High-Level Architecture of the Red Ranger. An At-A-Glance Overview.

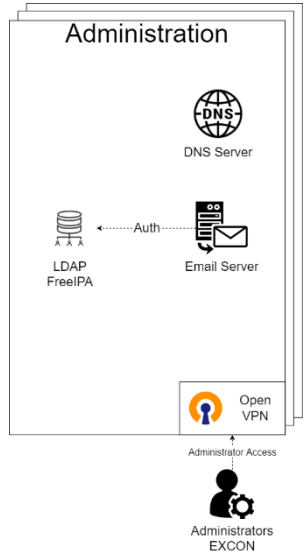

Figure 4: The Administration Cyber Range of the Red Ranger and Its Components.

- FreeIPA.[1] An integrated identity and authentication solution. Manages user access to resources and VMs. DNS Provider. Centralised authentication, authorisation, and account information. Assists in user access to the Cyber Range resources and services.
- Zimbra Mail Server.[2] An open-source mail server. During an investigation, the teams can communicate via email, and critical exercise information can be sent to the players. Email attacks can be simulated, such as phishing emails with malware attachments.

Should we return briefly to Figure 2, we need to describe the purpose of the Security Operations Center (SOC) component of the Red Ranger.

Essentially, the Security Operations Center (SOC) is the Blue Team cyber range. It comprises tools and monitoring solutions that aid Blue Teams in investigating and monitoring the situation during the exercise or simulation. Its components are shown in Figure 5 below:

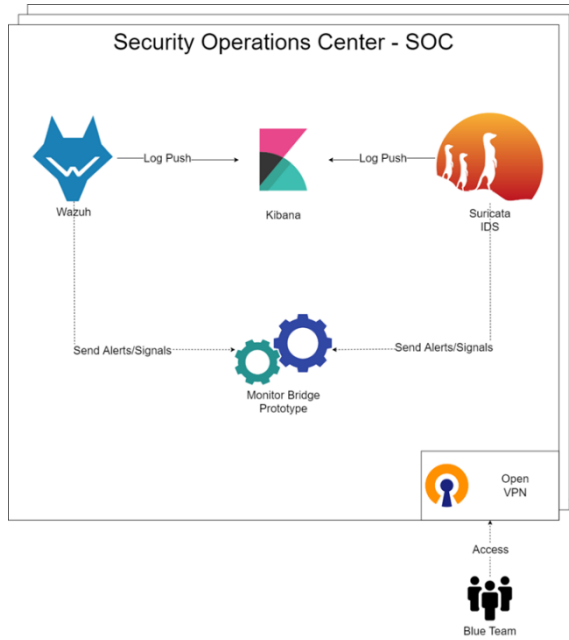

Figure 5: The Security Operations Center Cyber Range of the Red Ranger and Its Components.

[1] https://www.freeipa.org/ - Open Source identity management system.

[2] https://www.zimbra.com/ - Secure Private Business Email & Collaboration | Open Source

During the exercise, an information security team, effectively the Blue Team, monitors and analyses the security posture. The components demonstrated in Figure 5 reflect the purpose of this range itself.

- Wazuh.[3] A threat monitoring system combining tools for threat identification, integrity monitoring, and incident response. This software monitors all cyber range assets for security breaches or attacks, assisting blue teams in properly coordinating a reaction to attacks that occur throughout the scenario.
- Suricata.[4] A network intrusion detection system monitors the network and detects unexpected traffic. Suricata may be used by participants to produce network traffic captures for analysis. Malware detection, MITM attack detection and mitigation, data exfiltration, and more services are available.
- Kibana Elastic Search.[5] Free Open Source software visualising Elasticsearch data and navigating the elastic stack. All the security events and logs are sent to the elastic search for better search and visualisation capabilities over the data received.

Certain participants (SOC Operators) are granted access to these services to monitor and identify security breaches and assaults.

During the simulations, the ECHO Monitor Bridge Prototype – a dedicated service for bridging external monitoring solutions to the ECHO Early Warning System, is deployed. The ECHO Monitor Bridge transforms any alerts or incidents into tickets in the ECHO Early Warning System.

The remainder of the ranges and a more detailed architectural overview of the Red Ranger could be found in Sharkov et al. (2021),[6] where the purposes of each range, in terms of the exercise dynamics, are elaborated in meticulous detail.

Joint Scenario and Deployment for Sectoral Cyber/Hybrid Exercising

A joint scenario and a use case for the Red Ranger's federation with the ECHO Federated Cyber Range have been designed and implemented following a scenario leveraged under the 2022 HYDRA GB-BG Cyber Shockwave in April 2022. The GB-BG series of hybrid exercises is organised jointly with the British Embassy, Sofia. Their goal is to improve the Bulgarian cybersecurity system and create a common capacity between state, business, and academia to handle large-scale cybersecurity crises with a possible hybrid impact on society and the economy.

To organise the scenario for this exercise, the authors leveraged a simulated cyber/hybrid crisis with a cascading effect on the economy and industry. The authors simulated critical disruptions with a cascading impact on other industry

[3] https://wazuh.com/ - The Open Source Security Platform

[4] https://suricata.io/ - Open source threat detection engine

[5] https://www.elastic.co/kibana/ - Kibana: Explore, Visualize, Discover Data

sectors, critical infrastructures, or the general stability of the country. More specifically, HYDRA 2022 was to exercise the "vertical" escalation and crisis handling, engage private and public authorities, and identify real issues in the drinking water supply chain and related industry sectors. *As part of the 2022 HYDRA exercise, the authors implemented the so-called "sensor monitoring scenario", which was then replicated and significantly extended by the same team, leveraging the capabilities of the ECHO Federated Cyber Range in collaboration with the Red Ranger.* The shared resources allowed for the complex implementation described below.

The Sensor Monitoring Scenario comprises a data server for collecting water samples data, a monitor application for detecting abnormalities, and a publicly available information map. In this scenario, an Advanced Persistent Threat is determined to disrupt the water quality evaluation process to create havoc among citizens.

The scenario is intended to simulate an essential component of critical infrastructure: automatic sensor data monitoring. The scenario mimics water supply and water quality monitoring for drinkable and raw (untreated) water. However, the configuration of the joint implementation with the ECHO Federated Cyber Range allows the exercise organisers to select what infrastructure the scenario would cover and what would be monitored. This means that the scenario and supporting systems can easily be replicated for other critical infrastructures and create an exercise tailored to fit other specific requirements.

As illustrated in Figure 6 below, the scenario is bundled in a single cyber range.

There are three primary components for the simulation:

- The Raw Data Server. A server which produces simulated sensor readings.

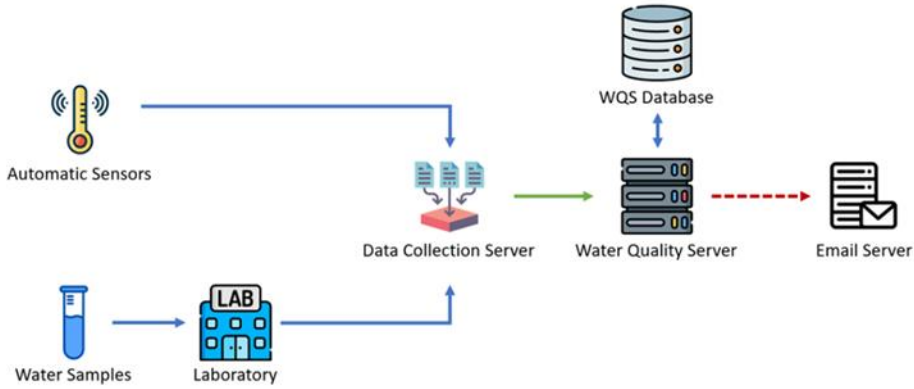

Figure 6: A Federated Water Quality Simulation Cyber Range Implemented Through the Joint Capabilities of the Red Ranger and the E-FCR.

- Sensor Monitor Application. An application for gathering data, producing reports, and, if necessary, raising alerts.
- Information Map. A map that visualises warnings and control points measurements.

It is impractical to employ actual sensors with accurate data for exercise purposes, which is why a Raw Data Server (RDS) was created to imitate data collecting. Even though the server does not collect actual data, data is generated and presented as though it came from multiple control points. Prior to the initialisation of the scenario, the setup specifies all control points and sensor kinds.

The Sensor Monitor Application (SMA) is the scenario's focal point. The principal tasks of this server are to gather sensor data and convert it into human-readable reports, as well as to produce alerts when sensor readings vary from safe bounds. At regular intervals, the data is synchronised from the Raw Data Server. Instead of the whole reading range, just the lowest, maximum, and average data for each sensor are recorded. The server then tests each of these minimums and maximums to check whether they fall within safe limits; if not, an alert is created and transmitted by email, the ECHO Early Warning System, or any other platform that supports push notifications.

The information map is designed to be public and to show the sensors that are being monitored in the scenario. Each control point from the setup is displayed on the map by a colour-coded symbol based on the traffic light protocol, as noticeable in Figure 7 below.

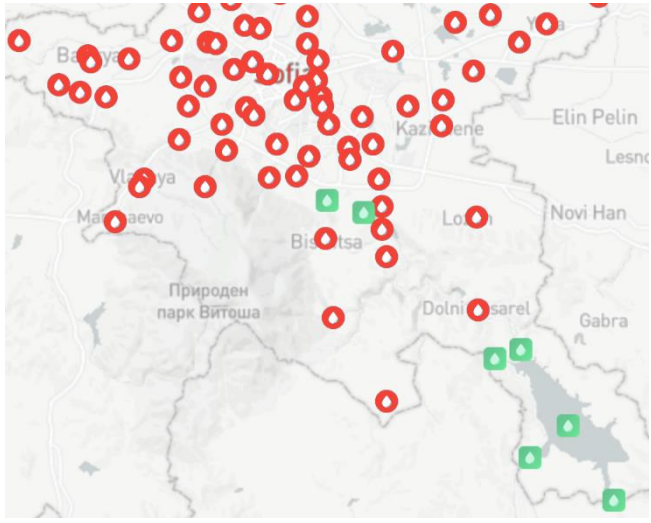

Figure 7: Joint Scenario Information Map Implemented Through the Joint Capabilities of the Red Ranger and the E-FCR.

When more than one sensor reading is outside of safe limits, red is used; when just one sensor reading is outside of normal limits, yellow is used. The control point's name and description are shown when the icon is clicked. The terms of the sensors for which warnings have been established are also shown if the symbol is coloured yellow or red.

The infrastructure for this exercise using the joint capabilities of the E-FCR and The Red Ranger through cyber range federation is illustrated in Figure 8 below.

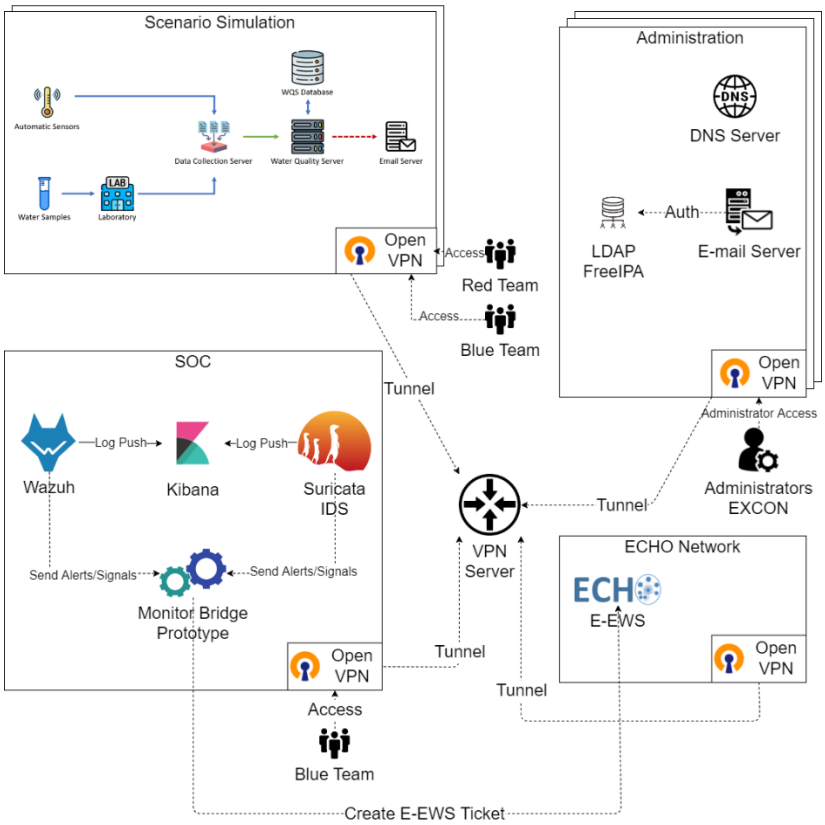

Figure 8: Joint Exercise Infrastructure Implemented Through Federation of the Red Ranger with the E-FCR.

As seen in Figure 8, the Information Map is hosted on a publicly accessible server that sends requests to the Sensor Monitor Application. The attack scenario implies that an attacker has found a vulnerability in SMA and has subsequently exploited it, gaining administrative rights over it.

From there, the database credentials are discovered, and the database is compromised to store values higher than those originally entered. As a result,

SMA starts delivering alerts that the sensor data is abnormal, and the control points on the information map turn red.

SMA is vulnerable to the Log4Shell weakness, which grants remote code execution (RCE) and allows an adversary party to execute malicious code on the server remotely. From this point on, the attacker can create a reverse shell using the same user that operates the server. Trojan malware is installed that connects to the database hourly and inserts a trigger that increases every new value before inserting it into the sensor readings table. After an hour, the trojan will install a new trigger if the database trigger is deleted, making it a persistent threat.

- To replicate and exercise for a realistic scenario, a forensics team must present all of the following to declare the exercise successful:
- Present evidence that the server has been infiltrated;
- Describe the attack scenario and attack vector; explain the attackers' actions;
- Locate and eliminate the trojan malware;
- Locate and remove the database trigger; propose mediation for the vulnerability;
- Suggest a solution for the corrupted data.

This implementation uses the capabilities of the ECHO Network's Early Warning System to extend the capabilities of the Red Ranger's Security Operation Centre and provide Blue Teams with extended forensics, alerting and messaging capabilities beyond the original capacity of the Red Ranger.

Conclusions

The EU will expand its funding for research and innovation over the next decade.[7] Among the central points will be the digital transformation of the economy and society, which will benefit people by promoting the European way of life, supporting democracy and values, and ensuring strategic autonomy. In this setting, the research community's effort is critical in establishing a society of trust and reliability.

Our firm belief is that by conducting research in cybersecurity exercises and cyber range development, we will be able to motivate organisations from the public and private sectors to seek opportunities and support the adoption of regular hybrid exercising as part of their organisational resilience processes.

In light of this, and motivated by the growing importance of cyber ranges for a variety of purposes, as well as the need for the federation of individual cyber ranges, this work presented the ECHO - Federated Cyber Range, which aims to interconnect existing cyber range capabilities via a convenient portal that acts as a "broker" between user requirements and a pool of available cyber range capabilities. We highlighted the significant characteristics of the E-FCR, the Red Ranger, and an in-depth perspective of the latter's architecture. Ultimately, we provided an example of a scenario federated through the E-FCR, showcasing the

validity of the solution and the potential for inter-sector collaboration opened by the federation.

Through the Red Ranger were able to comprehend better, model, and explain to participants the diversity of casual elements that led to a cybersecurity event with a cascade influence on complex infrastructures and their sub-infrastructure using the Systems-of-Systems Approach. Piloting the E-FCR as a broker for the Red Ranger, we saw further opportunities for bottom-up assessment of existing security controls, policies, and standard operating procedures, requiring collaboration between technical and administrative employees from various agencies.

With the outreach of the ECHO project, the agility of the Red Ranger, and the research interest in complex, cross-sectoral hybrid scenarios, we hope that through this cooperation, we lay the groundwork for the ability to examine chronic vulnerabilities and blind spots in collaborative cyber defence in Europe.

Acknowledgements

The ECHO Project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement №830943. The described scenario leveraged through the Red Ranger was piloted under the GB-BG Cyber Shockwave initiative, supported by the British Embassy – Sofia, Bulgaria.

References

[1] Gema Bello-Orgaz, Jason J. Jung, and David Camacho, "Social Big Data: Recent Achievements and New Challenges," *Information Fusion* 28 (2016): 45–59, https://doi.org/10.1016/j.inffus.2015.08.005.

[2] European Union Agency for Cybersecurity (ENISA), "Research and Innovation Brief. Annual Report on Cybersecurity Research and Innovation Needs and Priorities," Public Report, 2022, https://www.enisa.europa.eu/publications/research-and-innovation-brief.

[3] National Initiative for Cybersecurity Education (NICE), "The Cyber Range: A Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification and Training," Online guide, 2020, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.

[4] Michal Turčaník, "A Cyber Range for Armed Forces Education," *Information & Security: An International Journal* 46 (2020): 304-310, https://doi.org/10.11610/isij.4622.

[5] Nikos Oikonomou et al., "ECHO Federated Cyber Range: Towards Next-Generation Scalable Cyber Ranges," *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, 2021, pp. 403-408, https://doi.org/10.1109/CSR51186.2021.9527985.

[6] George Sharkov, Christina Todorova, Georgi Koykov, and Georgi Zahariev, "A System-of-Systems Approach for the Creation of a Composite Cyber Range for Cyber/Hybrid Exercising," *Information & Security: An International Journal* 50, no. 2 (2021): 129-148, https://doi.org/10.11610/isij.5029.

[7] European Commission, "Priorities and Actions. Leading Innovation Through EU Research," European Comission Website Statement, 2022, https://european-union.europa.eu/priorities-and-actions/actions-topic/research-and-innovation_en.

About the Authors

George Sharkov is a former Cybersecurity Adviser to the Minister of Defense and served as a National Cybersecurity Coordinator for the Bulgarian Government within the period 2014-2017. He was leading the development of the 2016 National Cybersecurity Strategy of Bulgaria. He holds a PhD in Artificial Intelligence, specialising in applied informatics, thermography, genetics, and intelligent systems. Since 2003 he has been the Director of the European Software Institute – Center Eastern Europe. He leads the Cyber Resilience Lab (CyResLab) of ESI-CEE in partnership with CERT-SEI, Carnegie Mellon University. Since 2016, he is also Head of the Cybersecurity Lab at Sofia Tech Park. He is a trainer and an appraiser in software engineering quality management, cybersecurity, and resilience (SEI/CERT RMM), lecturing in software quality, cybersecurity, and business resilience in leading Bulgarian universities.

Christina Todorova is a researcher at the European Software Institute – Center Eastern Europe and an expert at the Research and Development and Innovation Consortium at Sofia Tech Park, with expertise in the design of digitally enhanced learning experiences and curricula, primarily through educational robotics, mobile applications, and virtual learning environments.

Georgi Koykov is a software and DevOps security specialist at the CyResLab (Cyber Resilience Lab) – the cybersecurity division of the European Software Institute – Center Eastern Europe. With extensive practical experience in web development, Georgi is not only at the core of most development projects of the CyResLab, which require a user interface, but he is also among the core experts in the team concerning web security and vulnerability analysis.

Ivan Nikolov is a cybersecurity specialist at the CyResLab (Cyber Resilience Lab) – the cybersecurity division of the European Software Institute – Center Eastern Europe, and an expert at the Research and Development and Innovation Consortium (Sofia Tech Park JSC).