Information & Security

Published since 1998

G. Sharkov et al.
vol. 50, no. 2 (2021): 129-148
https://doi.org/10.11610/isij.5029

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

Research Article

A System-of-Systems Approach for the Creation of a Composite Cyber Range for Cyber/Hybrid Exercising

George Sharkov [1,2] **(✉), *Christina Todorova*** [1,2]**, *Georgi Koykov,*** [1,2] ***Georgi Zahariev*** [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:

The current cybersecurity landscape is conducive to the enhancement of the traditional cyber-exercising paradigm and instruments. Considering the complex nature of cyberattacks and their cascading impact, moving away from purely technical or entirely decision-making exercises is becoming paramount for realistic exercising of emergency response. Complex cyber-hybrid scenarios, exercising effective collaboration at the technical, operational, and higher decision-making levels, are increasingly employed to prepare for the emerging hybrid threats. Such scenarios simulate seemingly independent incidents in different locations, businesses, or systems that may quickly escalate to a sectoral or a national crisis. Unfortunately, such diverse scenarios often remain inaccessible due to the lack of proper simulation infrastructure and expertise to adapt them to various contexts. The current contribution presents the authors' experience in designing a Composite Cyber Range, following a Systems-of-Systems approach for the dynamic activation or incorporation of playgrounds and on-the-run integration of custom-made emulation and overlay ranges to support an "exercise-as-a-service" model for the provision of adequate and accessible cyber-hybrid mechanisms for crisis response training and preparation.

Article Info:

Received: 01 Sep 2021
Revised: 14 Sep 2021
Online: 20 Sep 2021

Keywords:

Cybersecurity, Resilience, Cyber Range, Hybrid Security, Crisis Response, Standard Operating Procedures

✉ Corresponding Author: E-mail: gesha@esicenter.bg

Context

We live in a world of complex systems-of-systems interacting in a supply chain with other complex systems-of-systems. In today's interconnected world, critical infrastructures have strong dependencies within their industry and with industries and academia beyond their operational environment. This ever-increasing complexity and interdependency also increase the risk within the supply chain. A systems-of-systems approach, as a holistic intervention in the cybersecurity operational realm, is consequently needed to enhance the competitiveness at a regional level, strengthen the cybersecurity capabilities of individual organizations and entire sectors, and generate creative space for the development of new security solutions that increase collaboration between actors.

Cyber exercising is a necessary prerequisite for cyber-resilience. Exercises are an integral part of the emergency planning process, and the training of the staff involved in emergency planning and response is fundamental to an organization's ability to handle any type of emergency.[1] Similarly, organizations must exercise their continuity plans regular and sufficient basis to ensure they remain viable,[2] which makes exercising a vital part of organizational resilience and flexibility.

Choosing the right type of exercise is paramount for achieving the desired outcomes of the exercise in itself.[3] There are, however, several types of cybersecurity exercises, according to the mechanics of the gameplay and the exercised capabilities. Three main *types of cybersecurity-related exercises* are often distinguished, namely technical, tabletop and hybrid.

Tabletop exercises. A tabletop exercise is commonly described as a facilitated discussion of a scripted scenario,[4] where key personnel is assigned emergency management roles. Tabletop exercises provide a way to exercise and test existing crisis response plans and procedures in a safe environment and are a milestone in the process of strategy improvement and the identification of weaknesses in procedures.

Technical exercises. Technical exercises, on the other hand, serve as a mechanism to test, improve and exercise the technical rigor, resilience, and capabilities of cybersecurity and IT specialists. In this category of exercises fall the CTF (Capture-the-Flag) exercises, where teams of players use offensive techniques to solve security challenges.[5] Technical exercises are a well-proven way to exercise and teach new concepts in an academic as well as in a corporate setting.

Hybrid exercises. Hybrid exercises are at the intersection between tabletop and technical exercises. Most often, hybrid exercises would involve both management and technical personnel in a common scenario with technical and operational challenges, where cooperation and dialogue between these two groups are required.

The audience of an exercise is traditionally dependent on the type of exercise and the choice of cyber range.

Cyber ranges are interactive platforms containing simulations, representations of networks system tools, and applications that support the hands-on exercising of technical and operational skills, knowledge, and abilities.[6] Although cyber ranges can be used as testbeds for the development of cybersecurity technologies or other software in general, a common goal for the use of cyber ranges is indeed training and exercise.[7]

Four main *types of cyber ranges* are often distinguished, namely simulation cyber ranges, emulation cyber ranges, overlay cyber ranges and hybrid ranges.[6]

Simulation Cyber Ranges. This type of cyber range is based on the concept of recreating a given environment based on the realistic usage of its components. Being one of the more popular types of cyber ranges, due to simulations running mainly on virtual machines, requiring almost no dedicated hardware, and thus easily replicable and more cost-effective compared to other cyber range types. Often simulations are designed for a particular use case or technology, so the scope and the audience of the simulations could be quite limited to a distinct scenario.

Emulation Cyber Ranges. Emulations cyber ranges running on dedicated infrastructure, providing closed-network experiences with multiple interconnected environments. Emulations include traffic generation that mimics numerous protocols, source patterns, traffic flows, attacks, and underlying internet connectivity.

Overlay Cyber Ranges. As the name suggests, those are cyber ranges running on top of actual physical infrastructure granting high-fidelity over simulation ranges, but also being more expensive and resource-intensive to develop, deploy, and use.

Hybrid Cyber Ranges. Also called Composite Cyber Range, they are a combination of any of the above-mentioned ranges in a single or federated infrastructure. Hybrid exercises are hard and resource-intensive to develop, coordinate and employ, however, are suitable for exercise scenarios, requiring the participation of both technical and operational personnel from several organizations, which is among the core reasons for the authors of this paper to choose the development of a Composite Cyber Range for a hybrid exercise.

To contribute to the improvement of the Bulgarian cybersecurity system and for the creation of a common capacity between state, business, and academia for the handling of large-scale cybersecurity crises with a possible hybrid impact on society and the economy, ESI CEE and the British Embassy in Sofia, in strategic partnership with the Ministry of Defense, Security Council and other Bulgarian government structures set out to create the GB-BG Cyber Shockwave Exercise series.

A unique feature of the GB-BG Cyber Shockwave Exercise series is that it aims to bring together representatives from different government structures, industries, and academia to establish trust, cross-sector collaboration, and a common crisis response baseline.

To achieve that, the implementation team aimed at simulating a crisis to engage participants in a realistic response. Thus, the team began its development of a Composite Cyber Range, including multiple sub-ranges, with additional infrastructures, tools, and machines, to provide an immersive and stimulating environment for the cooperation between technical and non-technical personnel from government, industry, and academia.

Methodology

Many approaches towards incident analysis and cybersecurity preparedness exist throughout the literature. One such model is the Chain of Events model where an undesired outcome is most often considered as a series of contributing factors.[8] Conversely, another common approach to the top-down deductive failure analysis is the Fault Tree Analysis, where cause-elimination is used to reduce risk in systems reliability research.[9]

Such management methodologies, however, have their limitations, especially within the context of cybersecurity and cyber-defence training and simulation.[10] With the increasing reliance on complex and interconnected systems, as well as considering the diversity of the contemporary cyber attacks and their cascading hybrid impact, a more holistic approach for the development and execution of realistic cybersecurity simulations was needed. Thus, the implementation team chose to abide by a Systems-of-Systems (SoS) approach for the scenario, the challenge, and the range development and continuous improvement.

The System-of-Systems approach is rooted in the Systems Theory - a multidisciplinary theory,[11] which is concerned with the interrelationship and interdependence of objects and their attributes (i. e. "systems"), and the holistic study of those systems and their complex dynamics.[12]

According to Skyttner, several core principles comprise the fundamentals of the SoS approach, which are further underlying the creation of the Red Ranger cyber range. These principles are illustrated in Figure 1 below.

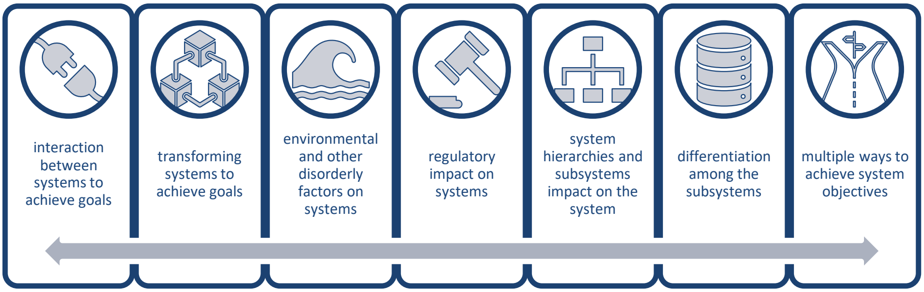
interaction between systems to achieve goals
transforming systems to achieve goals
environmental and other disorderly factors on systems
regulatory impact on systems
system hierarchies and subsystems impact on the system
differentiation among the subsystems
multiple ways to achieve system objectives

Figure 1: Fundamental Principles of the SoS Approach.(adapted from Skyttner, 2005) .

Following those principles, and to better address those principles within the context of the complex SoSs that we work with, we designed a highly modular system of interconnected cyber ranges to ensure the flexibility and adaptability of the infrastructure to a variety of contexts, systems, and subsystems.

The modularity of the system ensures differentiation among the subsystems, as well as the ability to transform different components, edit them out or repurpose them without harming the overall system and its functionality.

The interactions between systems are a given principle of the designed system, which heavily relies on the interdependencies within its components. As shown in Figure 4 further in the chapters below, a standard Composite Cyber Range would follow four-faceted modularity, enabled through VPN tunneling with a dedicated VPN server added to each range to ensure interoperability.

To be able to better address the vulnerabilities and attack-vector landscape of the systems we design exercises for, a generic model referring to tactics and techniques described in the ATT&CK Framework by MITRE [13] was introduced as a foundation for the development of specific threat models and impact scores and rankings behind the Cyber Picture Component of the cyber range. The Cyber Picture is a dashboard providing visualization of information for various types of incidents, including cyber incidents, but also kinetic and hybrid incidents on sectoral, organizational, and national levels. Each sector or critical infrastructure included in the dashboard has an impact score attached to it. A global score from 1 to 100 indicates the current risk impact on this sector, where the score changes based on participant actions and exercise events. More information about the Cyber Picture Module and its function is available further below.

Technical Implementation

To achieve any given contextual use case, an appropriate exercise scenario is designed, developed, and implemented as a simulated cyber/hybrid crisis through a dedicated technical orchestration platform, designed by the authors of this paper, called *The Red Ranger*.

The *Red Ranger* provides servers with different types of software, simulations of "official" and "attacked" or compromised web platforms, and a communication environment. Within the *Red Ranger* infrastructure, those servers are called "playgrounds."

In a baseline configuration, the *Red Ranger* includes the following playgrounds:

- *Playground 1*: Servers with different types of software, simulations of official and "attacked" web platforms, and a communication environment.
- *Playground 2*: SOC (Security Operations Center) – a simulation of security operations and monitoring center.
- *Playground 3*: Cyber Picture – dashboard providing visualization of information for various types of incidents, including cyber incidents, but also kinetic and hybrid incidents on sectoral, organizational, and national levels.
- *Playground 4*: Cyber Map – a visualization of the public internet infrastructure (Bulgarian servers and online services per location, divided into economic sectors and other indicators). The servers and services simulated in the training ground have been added to the Cyber Map.
- *Playground 5*: *MonSys* – a service availability monitoring web-based platform, limited to the systems, simulated within the environment, complemented by an additional platform for visualization (Grafana).

- *Playground 6*: Crisis Communications Dashboard – a dedicated dashboard aimed at facilitating crisis communication management between various players, teams, departments, and countries. Divided into public communications and sensitive communications sections, this dashboard provides the space for integrated interdepartmental information and communications exchange.

Additionally, a series of tools are added to the exercise environment to support the blue teams in the process of tackling the simulated crisis. Some notable tools, developed and implemented so far, are:

- JEMM-platform: a tabletop platform based on Playground 3, with a dedicated environment for the players, including monitoring of reaction groups, center for crisis management, situational center, as well as a complete virtual platform for exercise management (a dedicated private cloud).
- A virtual environment: "internal" internet environment with secure access, simulations of 6 news agencies websites (websites, video, and blog), social network, and a specialized protected file server with materials, documents, and files.
- Status page: an exercise landing page with a two-fold purpose, namely 1) for the participants to verify the status of their connection to the exercise infra-structure and its assets, links to all resources, and 2) to provide a library of all exercise materials, most recent information, updates, and links to the other platforms.

All exercise roles (institutions, teams, or individuals) are provided with an account and an associated official exercise-only email address. Further technical details about the Red Ranger, including its technical realization, are available in the following subchapters. The chapter Technical Realization and Building Process provides information about the process for deploying the generic cyber range architecture. The following chapter, Generic Architecture of the Composite Cyber Range provides a more in-depth overview of the structure of a generic cyber range. Last but not least, the chapter Composite Cyber Range Scope and Elements overviews the different modules or sub-ranges and their main components.

Technical Realization and Building Process

A generic architecture of the Composite Cyber Range will include any given number of the currently existing playgrounds and tools. To initiate a building process, a first step is to define a minimum list of playgrounds and supporting tools to be deployed for a specific context.

This baseline configuration, also called *service description manifest*, includes information about the playgrounds to be deployed, as well as participants lists, used within the configuration of a directory server (in a generic building process, this is most often *FreeIPA*, https://www.freeipa.org/page/Main_Page) to provision and authenticate accounts. The description of each section of the service description manifest is as follows:

- *Cyber Range Providers* – A list of all the cyber range providers involved in this service.
- *Service Overview*
  - *Categories* – A list of service categories (i.e., phishing, exploitation, forensics, cryptography, etc.)
  - *Government Sectors* – All Sectors Involved (i.e., transportation, telecommunications, healthcare, etc.)
  - *Description* – General overview of the service and its main components.
  - *Additional Services* – Additional services used in this exercise (i.e., external monitoring service, such as MonSys (https://monsys.app/), vulnerability scanners, firewalls, etc.)
  - *Session Schedule* – A schedule according to which the session will be executed.
  - *Session Type* – Session information, including whether the session is held entirely online or whether it is hybrid.
- *Scenario Description*
  - *Overview* – Scenario overview in English.
  - *Handbook* – A pdf version of the handbook for the players.
  - *Players/Teams* – A list of all the teams and players involved with their contacts.
  - *Assets* – Additional tools or virtual machines used by the scenario.
  - *Timeline* – A list of events that will happen during the scenario.

The deployment of a standard range follows a three-phase model, as illustrated in Figure 2 below. This deployment model aims to provide a maximum level of automation and flexibility of configuration, making the creation and setup of services needed for a particular exercise scenario easier and quicker for the designers of the respective cyber range instance, or even multiple instances.

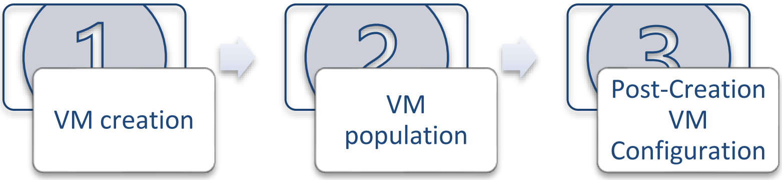

Figure 2: The Three-Phase model of the Exercise Cyber Range.

The first phase is the creation of virtual machines. It is within those virtual machines that the exercise email servers, the media websites, as well as any supporting infrastructure, are hosted.

The second phase requires the population of the virtual machines created in Phase 1 with appliances, for instance, a Zimbra (https://www.zimbra.com/ email server, WordPress (https://wordpress.com/) open-source content management system for the exercise media websites, FreeIPA open source identity management system, and a NodeBB (https://nodebb.org/) forum configuration for the Crisis Communications Dashboard. Internally developed software and its requirements are also deployed in this phase.

The FreeIPA Directory Server holds all participant credentials and DNS records for the exercise and is connected to all exercise services that require log-in to facilitate the authentication process of participants through an LDAP (https://ldap.com/) Protocol. It is managed automatically, meaning that all users and/or DNS records could be altered during the exercise if needed. File sharing servers, such as NextCloud are also deployed during this phase, in case file-sharing or file servers are needed according to the specific scenario of the exercise.

Email and file servers are configured to support *LDAP* integration so that a single log-in functionality is supported. Some exercise scenarios could also recure a Rogue Mail Server, using the same technology as the regular exercise mail server, however, used for attack simulations in certain storylines, such as phishing attach simulations. This mail server is also defined within the service description manifesto, if needed, and deployed automatically during the first two phases of the deployment.

The third phase considers the post-creation configuration, which includes creating users and DNS entries in *FreeIPA*, restoring *WordPress* backups, setting email headers for the *Zimbra* email (an automatic mail header, displaying a banner, used to warn participants that an email is part of the exercise and that sharing is forbidden), and setting the authentication and user provisioning to use the *FreeIPA* directory manager.

This process is performed automatically through the use of a dedicated builder machine, as shown in Figure 3.

The builder machine uses a combination of *Terraform* (https://www.terraform.io/) and Ansible (https://www.ansible.com/) to deploy the exercise infrastructure.

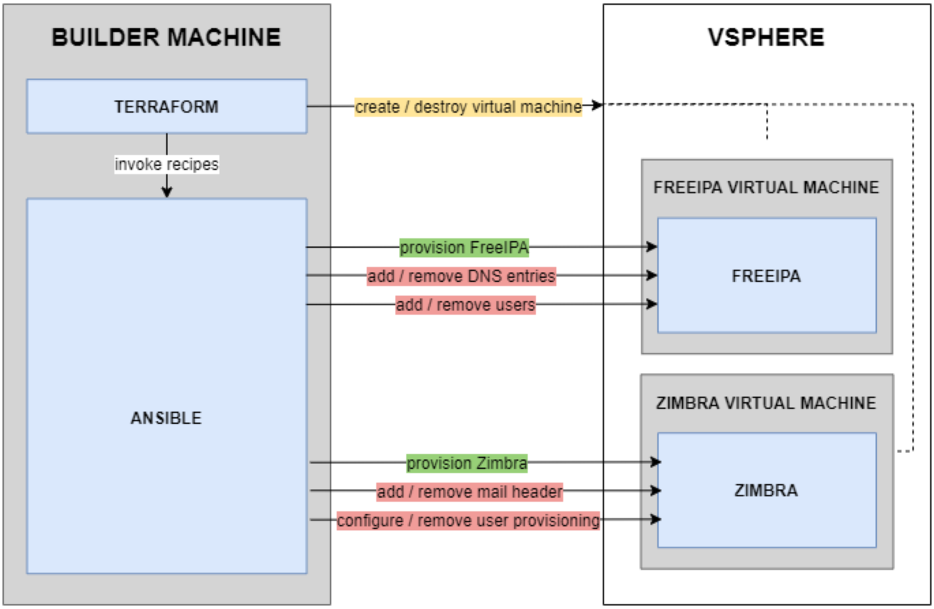

Figure 1: Automatization of the Exercise Environment Deployment.

Terraform is an open-source tool for infrastructure as code, which in the case of the exercise cyber range is used to manage the three environment deployment phases described above. As *Terraform* works with most cloud computing services as well as private cloud solutions, its implementation for on the exercise private *vSphere* (*https://www.vmware.com/products/vsphere.html)* server is rendered easy and seamless.

The cyber range implementation team has developed *Terraform* modules, which are responsible for the creation of those the pieces of infrastructure that make up the range, such as *Zimbra*. Those pieces of infrastructure are in a modular structure with dedicated modules for each service. *Terraform* is used in this process also to invoke various *Ansible* recipes at various stages.

Ansible is yet another open-source provisioning tool used to create a state in SSH-accessible machines. Within the cyber/hybrid exercise context, we are using it to perform the task of provisioning, for which *Terraform* on its own is unsuited. In both Phase 2 and Phase 3 of the exercise deployment process, *Terraform* calls on *Ansible*, following which *Ansible* connects to the virtual machine and provisions a given appliance, and applies the post-installation configuration.

If we adopt only a *FreeIPA* configuration and apply it, the *FreeIPA Terraform* module will first execute Phase 1 and call on *vSphere* to create a virtual machine appropriate for *FreeIPA*. Once a machine is created, *Terraform* will enter Phase

2 and will use *Ansible* to deploy *FreeIPA* on the virtual machine. With this, Phase 2 is concluded, resulting in the deployment of a *FreeIPA* configuration. The execution of Phase 3 heavily depends on the configuration of the module. If no additional configuration is provided, the deployment ends there.

In conclusion, phases one and two are automatically performed when a module is invoked, and the final product is an appliance hosted on a virtual machine. Each specific module defines what configuration will be passed on the *Terraform* module that triggers Phase 3. For *FreeIPA*, this could be the list of exercise participants, *LDAP* service users that other systems will use, and DNS entries. Conversely, for *Zimbra*, the Phase 3 configuration can consist of an email header configuration that will appear in all emails and configuration for a directory server, such as *FreeIPA*, that can be used to provision and authenticate accounts.

If a Phase 3 configuration is present, *Terraform* will invoke the appropriate *Ansible* recipes to create the users, add the DNS entries, and change the configuration. Additionally, the implementation team has established *Ansible* recipes that are responsible for the destruction of those resources, so should a *Terraform* configuration change and is re-applied, users can be removed, DNS entries can be wiped, and email headers can be reset in the future emails.

The result of these three phases is a generic infrastructure for a Composite Cyber Range.

Generic Architecture of the Composite Cyber Range

The Systems-of-Systems approach underlying the cyber range infrastructure development process implied a need for modularity of design to ensure the flexibility and adaptability of the infrastructure to a variety of contexts and systems. This is illustrated in Figure 4.

This modularity infrastructure is ensured by *Terraform* and Conductor (an internally developed exercise event execution manager, described in further detail in the "Scope and Elements of the Composite Cyber Range" chapter further below), which provides the range with the ability to maintain its assets across multiple infrastructures and providers. Thus, the Red Ranger is split into multiple sub-ranges, each with a dedicated contextually driven purpose and specificity, yet consolidated to operate as one.

As shown in Figure 4, a standard Composite Cyber Range would follow four-faceted modularity, enabled through VPN tunneling with a dedicated VPN server added to each range to ensure interoperability. The dedicated exercise OpenVPN (https://openvpn.net/) server allows remote access to the exercise cyber range. Before the exercise execution, each team or individual participants (if needed) receives a dedicated VPN Configuration, separating participants from each other. The VPN Server is further used to connect with other cyber ranges when the exercise is conducted through multiple instances of the cyber range.

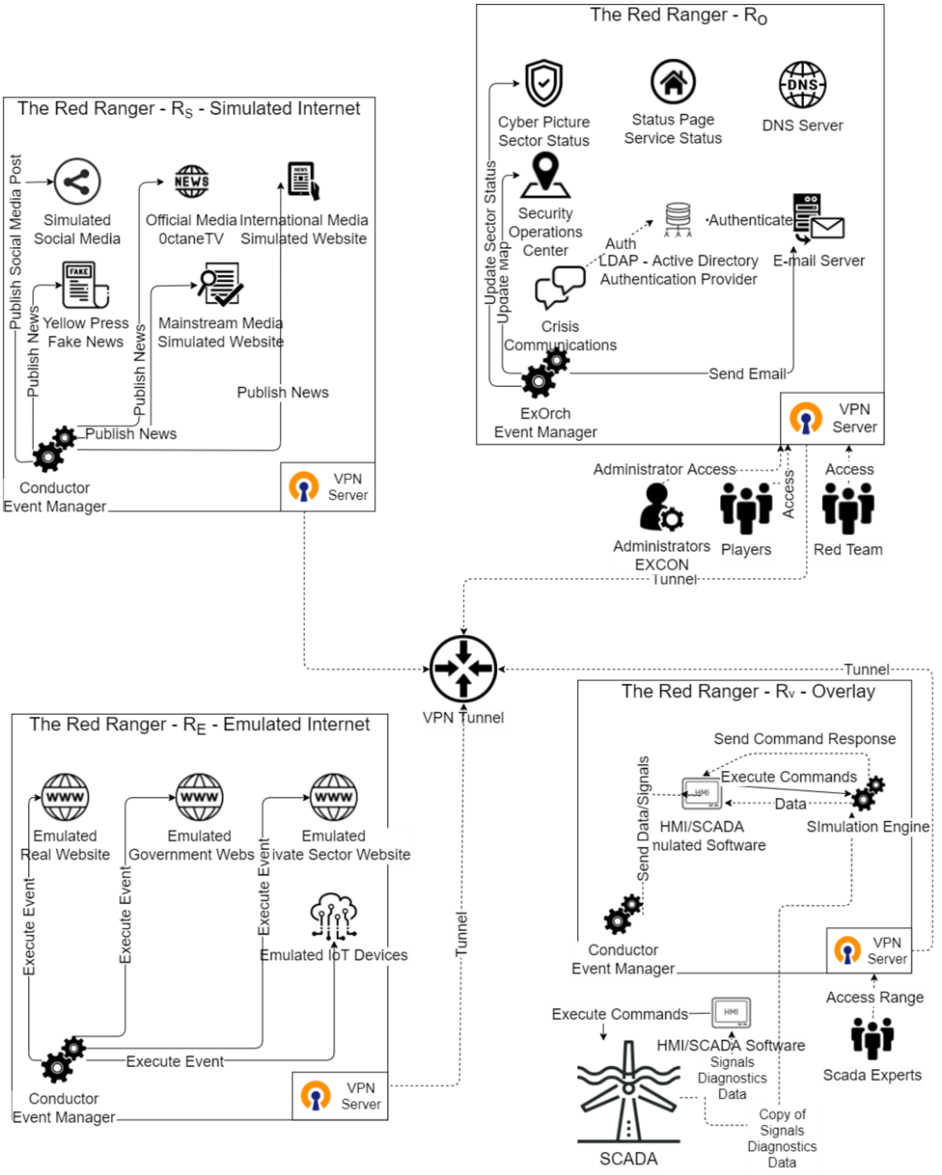

Figure 2: Standard Exercise Cyber Range Configuration.

Scope and Elements of the Composite Cyber Range

A standard orchestration of the Composite Cyber Range follows a granulation into four core sub-ranges. Those four are namely Range Zero (R_0), Emulated Internet Cyber Range (R_E), Simulated Internet Cyber Range (R_S), and Overlay Cyber Range (R_V).

Range Zero (R_0)

Range Zero (R_0) serves as an infrastructural backbone providing the *standard baseline of components described in the service description manifesto*. R_0 includes core situational and organizational components, such as mail server, *LDAP* server, status page, and some multi-purpose dashboards, as shown in Figure 4. Among the core components illustrated in the Figure 4 that have not been discussed in detail so far are:

- *Status Page*. A basic landing page with a two-fold purpose, namely 1) for the participants to verify the status of their connection to the exercise infrastructure and its assets, and 2) to provide a library of all exercise resources and materials, most recent information, updates, and links to the other platforms. The status page displays a brief description of the cyber range, as well as links to the different playgrounds and useful information for the players (i.e., contact book, exercise playbook, presentations, software installation files, etc.). Furthermore, the exercise status page displays the current range infrastructure status in either green (available) or red (not available), allowing participants to detect connectivity and availability issues and report them to technical support. The status page is statically deployed and runs on the client-side only. It is powered by NuxtJS and implements specific checks for the exercise infrastructure, such as DNS, HTTP, HTTPS, etc., to display infrastructure status in real-time.
- *Conductor (Event Manager).* The Conductor is an internally developed software for exercise event orchestration. An internal broker queue is responsible for the timely execution of all events, which could range from sending an email to posting a news article and enabling a technical challenge. The Conductor is written in *Python3* and offers an Excel interface for injects so that organizers can use .xslx files to feed injects into the exercise event manager. It is a fully scalable software product (tested simultaneously with nine machines), which further offers a *MongoDB* database interface for injects. Last but not least, the Conductor offers a REST API interface for communication with other software. It offers a dashboard for displaying exercise events from the Conductor server. The dashboard is also internally developed and serves to display past and incoming events as a timeline. Through the dashboard, the exercise administrators can easily pause, delay or stop an incoming event from execution completely, if necessary. Past events can be executed again manually. The dashboard is also written in *Python3*, using the *Pyramid* framework and also offering REST API access.
- *Crisis Communications Dashboard.* The Crisis Communications Dashboard is a dedicated dashboard aimed at facilitating crisis communication management between various players, teams, departments, and countries. Divided into public communications and sensitive communications sections,

this dashboard provides the space for integrated interdepartmental information and communications exchange.

The Crisis Communications Dashboard is implemented via an instance of *NodeBB* forum software running as a *Docker* container with *LDAP* Integration for single sign-on. It supports a *MongoDB* database and is powered with several backup mechanisms to ensure that no information reported by the participants is lost and that it can be restored at any given time.

- *Cyber Picture.* The Cyber Picture is another internally developed dashboard for the simulated critical infrastructures status monitoring. Through the Cyber Picture, participants can monitor the current global situation, which is changing during the exercise as a result of their action or inaction, allowing them to address the current situation accordingly. It is an internally developed software, written in *Python* 3, leveraging the *Pyramid* framework and further providing an interface for REST API access. All critical infrastructures are presented in a graph structure with rules between the nodes to simulate and reflecting inter-sector dependencies. Each critical infrastructure has an impact score.
- *SOC (Security Operations Center)*. This is yet another internally developed dedicated dashboard for participants for exercise situational awareness monitoring. It is a simulation of security operations and a monitoring center, where simulated events and developments are displayed on a world map with appropriate icons and descriptions. The maps are updated in real-time to give accurate information to the players.

  The Security Operations Center is written in *Python 3,* leveraging the *Pyramid* framework and further providing an interface for REST API access. This dashboard also offers *OpenStreetMap* (https://www.openstreetmap.org/) integration.

As evident, R_0 contains some of the core exercise playgrounds and instruments. However, in case those are not needed for specific purposes, they are simply not specified in the service description manifesto and are thus not deployed. If needed, however, additional machines and instruments could be deployed. For instance, if there is a need for investigation machines to assist the forensics teams in the investigations, a set of dedicated *Kali Linux* virtual machines could be deployed for every team. Those investigation machines would be configured to support an *LDAP* integration so that participants can use their credentials to log in and use the services on the machines. Furthermore, the R_0 can also include storyline-specific virtual machines that contain technical challenges. A challenge is developed and bundled into an image. The virtual machines are mostly *CentOS*; however, depending on the challenge another *Linux* distribution or a *Windows* operating system could be used. Every challenge is configured with the ability to restore it to its original state, ensuring resilience in case a team manages to damage it.

Emulated Internet Cyber Range (R_E)

The *Emulated Internet Cyber Range (R_E)* is the range with all emulated websites, e-services, or emulated IoT devices.

The emulated websites are a realistic mimicry of real-life websites or web-based services, simulated for the exercise. Those could vary from government websites to privately owned websites or services of importance for the exercise scenario development. Such websites can be a variety of government or private sector websites.

Simulated Internet Cyber Range (R_S)

The *Simulated Internet Cyber Range (Rs)* represents the exercise internet, with its simulated services that do not reflect real-life services. This could include simulated online media websites. Within the exercise mechanics, the simulated internet plays a colossal role in scenario development and immersion. The media websites, for instance, would often reflect on events of consequence to the players' actions or inactivity, thus chronicling the course of the crisis management process.

As visible within Figure 4, an instance of the Conductor is also present in R_S. This is due to one of the main purposes of the Conductor, namely to publish events as news articles during the scenario development. The virtual environment also contains several simulated media websites powered by *WordPress* CMS Software and upgraded with customized backup and restore capabilities. The simulated Internet Cyber Range also provides secure access to simulated social networks, protected file servers, and more.

Overlay Cyber Range (R_V)

The purpose of the *Overlay Cyber Range (R_v)* is to be deployed and integrated on-site with actual SCADA appliances. A simulation engine has to be developed for every specific SCADA system to operate with the signals and data sent by the SCADA system. The data flow from the system is copied on a network level and sent to the Simulation Engine to simulate a variety of scenarios to prevent any damage to the actual SCADA system.

To ensure the proper functioning of the Overlay Cyber Range, we deploy an emulated HID system, which connects to the Simulation Engine data flow, thus serving as an interface for the players to execute commands and perform monitoring and control. Commands executed by the players are sent to the Simulation engine instead of the actual SCADA, and a proper response is crafted based on a machine learning algorithm trained on crisis data. A scaled instance of the Conductor, operating between all cyber ranges within the consolidation, is needed to ensure stable interoperability during the exercise. Sharing events and data between Conductor instances in multiple cyber ranges ensures that if a connectivity problem accrues in Range A (Ra) the event manager will continue to operate in the remaining cyber ranges.

Furthermore, different exercise-specific cyber ranges can be developed, consolidated, and combined for different exercises. The PANACEA exercise, discussed within the “Key Findings and Use Cases” chapter, can be represented with the following consolidation of cyber ranges $PANACEA = R_0 + R_S + R_E + R_X$”, where Rx is the exercise-specific cyber range containing all the virtual and real machines required by the exercise, as well as IoT devices used in the exercise, such as virtual presence robots and thermometers.

This particular use case is described in more detail in the following chapter.

Key Findings from a Recent Use Case

The current SoS approach to creating a Composite Cyber Range and orchestrating a hybrid cybersecurity exercise was validated through the course of the GB-BG Cyber Shockwave Exercise Series, ongoing since 2019. To outline some of the key findings and applications of the methodology, however, we will provide details about the latest exercise from the series, namely the PANACEA Exercise.

The goal of the PANACEA Exercise scenario was to test and simulate the technical and organizational means and methods for handling an escalating cybersecurity crisis with a hybrid impact. Moreover, testing the standard operating procedures and the collaboration capabilities of hospitals and businesses, government, security institutions, and industry-specific actors has become paramount, especially against the backdrop of the COVID-19 pandemic. The PANACEA exercise scenario was elaborated with the help of experts in the supply chain of vaccines against COVID-19 and tailored to fit the Bulgarian context. The scenario was, however, further expanded to scale at a regional level due to an opportunity to include regional participants from Romania. The main scenario storylines were based on currently known weaknesses and vulnerabilities of a technical and organizational nature, combined with unexpected vectors of hybrid nature to illustrate the possible cascade effect with cyber-physical manifestation and an overall kinetic effect.

The main scenario and specific context were related to potential cybersecurity-related disruptions affecting the supply chain (logistics, transportation) of medical equipment and medication and the logistics related to the supply of the COVID-19 vaccine and the implementation of the related vaccination plans. The purpose was to exercise the “vertical” escalation and crisis handling process, engaging private and public authorities, starting with identified realistic supply chain and logistics issues. The main targets will be in the area of dedicated transportation, storage companies, and services involved, shipping, and relevant logistics. Attacks and malicious activities may apply to different chains, services, or equipment in a seemingly unrelated manner, however leading to a complex impact and equipment or systems failures, compromising the vaccine storage, distribution, and vaccination plans. Other possible areas that were indirectly affected are the customs and border control services, communications, and energy supply.

To address the pandemic-related boom in telemedicine and IoT usage for remote healthcare and patients monitoring and associated cybersecurity risks and new possible attack vectors, a telepresence robot VGo was also incorporated at a later point in the scenario.

The PANACEA exercise followed a semi-generic consolidation of four ranges was deployed, namely Range Zero (R_0), Emulated Internet Cyber Range (R_E), Simulated Internet Cyber Range (R_S), and Specific Cyber Range Infrastructure. The exercise-specific cyber range contained all the virtual and real machines required by the exercise as well as IoT devices used in the exercise, such as virtual presence robots and thermometers.

Based on all the above, six main storylines have been developed, which for the sake of brevity, could be summarized as follows:

1) *Supply Chain, Medicine, and Medical Equipment Distribution Disruptions.* This storyline was deployed in the Specific Cyber Range. Some notable events included vaccines' handling conditions corruption simulation, based on manipulation of several physical devices. Those devices were temperature registrators, including data loggers, thermometers, and sensors for refrigerators, containing vaccines, which are widely used in the supply chain for vaccines distribution. Disruption of distribution and transportation plans were also simulated as part of $R_{X,}$ where dedicated machines were used to emulate attacks against systems, causing vaccine shipping, dispatch, and storage disorganization.

2) *Critical Healthcare Services Disruption.* The storyline was developed under the combination of R_S + R_E + $R_{X,}$ where R_S was used to simulate exercise media websites, R_E was used to emulate public data portals, and R_X was used for executing a ransomware attack to be investigated by the participants. This storyline reloved around the leakage of patients' data due to ransomware, which also leaked access information to medical facilitation systems. This storyline further included challenges executed on an actual VGo robot, also part of R_X.

3) *Data and National Statistics Manipulations.* This storyline relied mostly on the R_S + R_E + R_0 combination of ranges to simulate a series of attacks against core information channels. R_S was used to simulate exercise media websites, R_E was used to emulate public data portals, and R_0 was used to provide the Crisis Communications Dashboard for the response and press releases, as well as for secure information exchange between technical teams from different organizations, and public relations teams from core government agencies and hospitals.

4) *Escalations in the Context of Simulated Upcoming Parliamentary Elections.* Leveraged through R_S, this storyline was mostly immersive, aiming to provide additional context for the escalation of events to the level of a national crisis, simulating political confrontations, protests of citizens, road blockades, and unforeseen climate conditions.

5) *Strategic Communications*. Leveraged mostly through a combination of R_S + R_E + R_0, this storyline included simulations of news and "yellow" articles regarding ongoing events, misinformation and disinformation identifica-

tion and response, social media simulation, monitoring, and response, as well as crisis communications and response.

6) *Cybersecurity challenges, related to the hybrid scenario*. Leveraged through $R_0 + R_E$ to simulate compromised, exploited, defaced, and manipulated websites and web servers, ransomware, and phishing attacks and to facilitate the forensics actions and investigations.

It is noteworthy to mention that R_0 was used as a backbone to provide the necessary infrastructure for all storylines, however specific challenges heavily relied upon some of R_0 assets, such as the Crisis Communications Dashboard and Cyber Picture. Based on this configuration, several advantages and disadvantages to this approach for the development and implementation of a hybrid exercise could be taken out.

Among the most notable advantages were:

- Ability to reflect latest trends, events, and incidents happening in real life;
- Emulation of network and internet resources creates very realistic testing grounds with very realistic traffic generation;
- Provide an environment where existing strategies, along with new ideas, can be tested;
- The ability to provide a simulated environment where technical and operational teams from very diverse organizations can work together to improve their joint and individual cybersecurity capabilities and teamwork;
- The composite configuration provided a high fidelity and realistic scenario that was appreciated by the participants;
- The customizability of the cyber range provided opportunities to dynamically upgrade scenarios and add new elements and tools on the go;
- The Red Ranger Composite Cyber Range is flexible and adaptable enough to be able to easily add and synchronize new virtual components;
- Unprecedented opportunity to simulate on-the-job crisis response activities in a safe environment, where participants and their management could receive and observe real-time feedback.

This approach had many more upsides, as it was highly customized to the participants' needs and the recent events in the country and the region. However, there were also notable *drawbacks that need to be underlined*:

- Creating and managing a composite cyber ran Composite Cyber Range for a hybrid exercise is extremely resource-intensive;
- Each deployment of the composite range is unique for each exercise, meaning that although the initial effort is decreased significantly, the customization and preparation for exercise-specific scenarios, events and infrastructures requires research, resources, consultations, development capacity, and time;

- Maintaining a highly customized cyber range is extremely challenging, requiring a team of diverse talent and a lot of time;
- Real-time exercises with Composite Cyber Range and large teams from different organizations can be quite unpredictable and might require additional technical support than originally envisaged, compared to working with simulation or emulation ranges only;
- Requires a substantial planning period and many iterations;
- Specialized devices and equipment are necessary for the creation of a realistic exercise; however, their configuration into the exercise scenario requires a lot of research, creativity, money, and development capacity;
- The cost of such exercise is prohibitive for smaller organizations, who might wish to run such exercise internally and regularly.

Automation on some of the processes is a future direction for development for the Red Ranger and future exercises carried out by the implementation team. Especially within the context of the growing need for exercising the cybersecurity capabilities of organizations in the cyber-physical production systems and supply chains (CPPS), the increasing need for the flexibility and adaptability of the teams and the growing need to research specific industrial production systems, automating as many of the content generation tasks and scenario developments and branching, is a subject of ongoing research for the implementation team.

Conclusions and Ongoing Research

Hybrid cybersecurity exercises carried out through composite ranges, provide an opportunity for high-fidelity simulations of large-scale cyber incidents with potential hybrid impacts on the economy and society simulation. The realistic aspect of hybrid scenarios stems out also from the imposed need for cross-sector collaboration, as well as coordination between technical and strategic teams. This coordination, on the other hand, lays the foundation of the capabilities to analyze chronic vulnerabilities and blind spots in collaborative cyber defense at a national and regional level.

The Systems-of-Systems Approach allowed us to better understand, simulate and relate to participants the variety of casual factors, leading to a cybersecurity incident with a cascading impact on relevant complex infrastructures and their sub-infrastructure. Furthermore, it provided an opportunity for testing the existing security controls, strategies, and standard operating procedures in a bottom-up manner, forcing cooperation between technical and managerial staff from different agencies.

As part of the ongoing research into the improvement of the exercise and cyber range mechanics, the implementation team is currently developing a machine learning component for the Conductor to support the exercise organizers in the generation of news and social media posts, based on players activity and events rollout, with specific parameters, such as topics, and keywords. Similar research in this direction is focused on the exploration of machine learning methods for the dynamic scenario modification based on participants' actions.

This general research direction into the field of artificial intelligence and machine learning has been dictated by one of the main disadvantages of the Composite Cyber Range approach for hybrid exercising – namely, the resource-intensive process around the exercise orchestration. Applying artificial intelligence mechanisms in the process of scenario definition and content generation could help substantially reduce the number of human resources and time needed for scenario branching during the exercise and allow for better technical support and activity evaluation.

We believe that through our research in the field of cybersecurity exercising and cyber range development, we can motivate organizations from the public and private sectors to seek opportunities for the adoption of regular cyber/hybrid exercises as part of their organizational resilience processes and encourage cross-sector cooperation between organizations from critical infrastructures, government entities, academia, and industry.

Acknowledgements

The authors would like to express their sincere gratitude to the British Embassy in Sofia and the Sofia Tech Park for their continuous support and trust for the GB-BG Cyber Shockwave series of exercises.

References

[1] UK Cabinet Office, "Exercise Planners Guide," Home Office Publication, 1998, https://www.gov.uk/government/publications/the-exercise-planners-guide

[2] Software Engineering Institute (SEI), "CERT Resilience Management Model (CERT-RMM) Version 1.2," CERT Program, 2016, https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084.

[3] ENISA, "Good Practice Guide on National Exercises. Enhancing the Resilience of Public Communications Networks," Resilient e-Communications Networks, 2009, https://www.enisa.europa.eu/activities/res-old/policies/good-practices-1/exercises/exercises-on-resilience

[4] Department of Homeland Security, CISA, CISA Tabletop Exercise Package: Exercise Planner Handbook (2020), 5-6, https://www.cisa.gov/.

[5] Tanner Burns, Samuel Rios, Thomas Jordan, Qijun Gu, and Trevor Underwood, "Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education," *Proceedings of The 2017 USENIX Advances in Security Education Workshop*, Vancouver, BC, 2017.

[6] 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.

[7] 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.

[8] ABS Consulting, Principles of Risk-Based Decision Making (Government Institutes, 2002), 16-17.

[9] Enno Ruijters and Mariëlle Stoelinga, "Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools," *Computer Science Review* 15–16 (2015): 29-62, https://doi.org/10.1016/j.cosrev.2015.03.001.

[10] Hamid Salim and Stuart Madnick, "Cyber Safety: A Systems Theory Approach to Managing CyberSecurity Risks – Applied to TJX Cyber Attack," Working Paper CISL# 2016-09, 2016, http://web.mit.edu/smadnick/www/wp/2016-09.pdf.

[11] Ludwig von Bertalanffy, *General System Theory: Foundations, Development, Applications* (New York: George Braziller, 1976).

[12] Lars Skyttner, *General Systems Theory: Problems, Perspectives, Practice* (Hackensack, NJ: World Scientific, 2005).

[13] MITRE ATT&CK®, 2021, https://attack.mitre.org.

About the Authors

George Sharkov – see the CV on p. 22 in this volume, https://doi.org/10.11610/isij.5030.

Christina Todorova – see the CV on p. 22 in this volume, https://doi.org/10.11610/isij.5030.

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 with relation to web security and vulnerability analysis.

Georgi Zahariev 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). Georgi is a content creator and lecturer for cybersecurity trainings at CyResLab and is among the core experts in the team with relation to web security and vulnerability analysis.