Hybrid Exercising for Cyber-Resilient Healthcare and Cross-Sector Crisis Response Operability

George Sharkov[1, 2][0000-0001-5086-311X], Christina Todorova[1,2][0000-0002-8061-2941],
Georgi Koykov[1], Georgi Zahariev[1,2]

[1] European Software Institute – Center Eastern Europe, Sofia, Bulgaria
[2] Cybersecurity Laboratory at Sofia Tech Park, Sofia, Bulgaria

Abstract. Achieving a rigorous and resilient cybersecurity posture at a national level nowadays translates to ensuring not only the robustness of critical infrastructures but also that of supporting businesses, academic, and government structures, and their cooperation and readiness to provide a network of support in times of crisis. Approaching resilience maturity is quite the compound subject matter in itself; however, one of the main components on the roadmap to ensuring operational and technical resilience is exercising.

Hybrid type of exercises are the intersection between the technical and the managerial-tabletop exercising and are used as a mechanism to maintain a common baseline of readiness for cyber incidents, to increase cross-sector cooperation, and to target specific issues and weaknesses, identified otherwise or from previous exercises.

In this paper, we present our approach for the creation of a complex generic cyber range containing a variety of exercise polygons simulating and propagating vertical escalations related to the healthcare sector, its logistics, and supply chains within the context of COVID-19. We further share organizational aspects for the creation of a complex intersection of technical, tabletop, communications, and operational exercise environment and experience. The application of AI/ML methods and tools for exercise facilitation is overviewed. Lessons learned from three types of pilot exercises in critical infrastructures are discussed.

Keywords: Cybersecurity, Resilience, Cyber Range, Cyber Polygons, Hybrid Exercise, Crisis Response, Standard Operating Procedures, AI/Machine Learning, Telemedicine.

1 Background

The ever-increasing sophistication of the cybersecurity landscape at a global level, combined with the steadily expanding cybersecurity attack surface, implies **a need for targeted efforts for establishing a collaborative network of support across businesses, industries, countries, regions, and beyond**. Thus, maintaining and improving the collaboration and trust between representatives from interdependent sectors, business, and academia, as well as between government structures is therefore essential for safeguarding fundamental rights, ensuring security and safety both at the physical and in cyberspace.

The highlighted importance of cybersecurity in the light of the global efforts to limit the spread of the coronavirus and the shift to increasingly remote work settings within the past year has resulted in an unprecedented growth in investments in cybersecurity and refocusing on IT risk and resilience [1]. It has been revealed, however, that not the innovation in the field is what is the most needed. It is the maintenance of sustainable cooperation and readiness to provide a network of support in times of crisis, along with cyber awareness and hygiene, as well as continuous education, that underpin the digital transformation of society and that lead the way to secure information space, including in sectors, such as healthcare, and especially in the context of the imposed by pandemic "work from home" [2].

A 2020 INTERPOL assessment of the impact of COVID-19 on cybercrime [3] has shown a significant target shift from individuals and small businesses to major corporations, governments, and critical infrastructure. Examples of common attacks aiming to disrupt the operation of various organizations and critical services, according to the same report, include ransomware or DDoS attacks. With **cybercriminals increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit, the healthcare sector, among other sectors of critical importance has become a target for exploitation in 2020, revealing blind spots and an overall failure in cybersecurity baseline maintenance failure**.

Sectors of critical importance, such as healthcare and education, have been among the most attacked in the recent year, nevertheless, they continue to maintain a basic cybersecurity baseline, which is not up to par with the increasing numbers of attack against them, not with the sophistication of attacks and the expansion of the attack surface [4]. In addition, in healthcare, in particular, cybersecurity-related vulnerabilities could jeopardize the safety of the patients, not only in terms of their data and privacy, but also to their lives. With the COVID-19 pandemic putting healthcare in center-stage, chronic cybersecurity vulnerabilities in the sector, such as ill-maintained networks, systems, and software, have become apparent, and combined with the smart devices and medical equipment used in modern healthcare, with its cybersecurity weaknesses, the lack of holistic approach to cyber-resilience has become apparent [1].

Against this backdrop, the development of cybersecurity solutions and innovation in cybersecurity is often not applicable to sectors of critical importance, such as healthcare. A vast majority of both the scientific and the commercial advances in cybersecurity are focused on developing complex solutions for either large enterprises or specific infrastructures, which makes them inaccessible for organizations with small IT and cybersecurity teams and capacities to be able to afford, administrate, manage or even maintain.

Hospitals and schools, especially in the Bulgarian context, often only maintain a small team of IT professionals, who are responsible for the maintenance of networks, websites, web platforms, and existing infrastructures of their organization, and who have little to no time or capacity for the implementation of new security solutions. Likewise, state-run hospitals likely have a limited budget for IT and cybersecurity, which further needs to be prioritized for the maintenance of existing equipment [5].

By the same token, the IT staff in healthcare is not necessarily familiar with information security as a discipline, which often results in the ill-maintenance of software and networks in hospitals. Finally yet importantly, due to time constraints, resulting from the limited number of IT professionals in such organizations, combined with the multitude of tasks they need to perform as part of their daily jobs, the cybersecurity posture of this sector of critical importance has been suffering from chronic cybersecurity neglect, which has only recently become apparent.

Therefore, **to ensure that people are safe and secure in the digital world, and to have confidence in the digital transformation, critical infrastructures need to ensure and regularly exercise and improve their cyber-resilience, operational readiness, and crisis response capabilities** to match the unprecedented sophistication of cyber threats and cyber-attacks.

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 [6]. Similarly, organizations must exercise their continuity plans regular and sufficient basis to ensure they remain viable according to the full cycle of protect-sustain-recover resiliency processes, as defined by CERT-RMM [7], which makes exercising a vital part of organizational resilience and flexibility.

From the implementation perspective, we can distinguish three main types of cybersecurity-related exercises, namely technical, tabletop and hybrid. This might be viewed as a technical interpretation of the more general classification, introduced by MITRE in their [8], where three main types of exercises are listed, namely: Tabletop (scripted events, usually performed on paper), Hybrid (scripted injects with real probes/scans) and Full Live (real and scripted events). Another, more detailed view on the types of exercises is given in [9], where the six type of exercises are defined as: Tabletop (*Suitable for cyber incident management, leadership, and reviewing and evaluating processes*); Root cause exercises (*Suitable for anticipating problems and targeting risk management actions*); Functional (*Suitable for exercises focusing on crisis leadership, crisis communications and cooperation*), Technical (*Suitable for improving technical preparedness, famil-*

iarization with systems and recovery tests); the classical CTFs, Capture-the-flag (*Suitable for improving technical skills and familiarizing the participants with systems*), and a combined larger-scale Major joint exercises.

As seen in Figure 1, we define hybrid type of exercises at the intersection between technical and tabletop-managerial exercises. **With hybrid type of exercises, we aim at combining in one experience the "managerial" and "technical" aspects of dealing with cyber-enabled complex hybrid nature of incidents and crises, through realistic practical simulations and scenarios, using specific infrastructure (cyber range)**.

With this paper, we aim to share ESI CEE's experience with organizing hybrid type of exercises to maintain a common baseline of readiness for cyber incidents and increase cross-sector cooperation to target specific issues, weaknesses, and blind spots at a national and regional level. Three different meanings or use of "hybrid" are addressed – the observable growing malicious impact of cyber-enabled hybrid crises (frequently addressed as a "modern hybrid warfare" [10]) which we address commonly as "cyber/hybrid scenario", then the "hybrid type" of exercises as described above. And the third, more design and development aspect – the types of cyber ranges used for such exercises, providing simulation, emulation, overlay or mixed ("hybrid") type of technical setup and infrastructure [11].

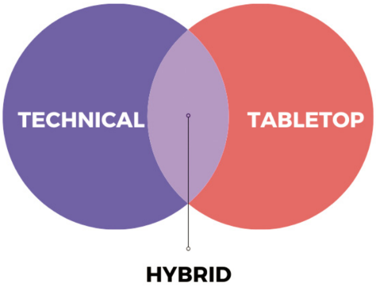

Fig. 1. Hybrid type of exercises: an intersection between technical and tabletop-managerial exercises.

2 GB-BG cyber shockwave series of cyber/hybrid exercises

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 cyber-enabled 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.

This collaboration and the project are a practical step towards the implementation of the Bulgarian cybersecurity strategy "Cyber-Resilient Bulgaria 2020"[1] (adopted in July 2016, updated and extended until 2023 in February 2021). It is implemented within the context of the adopted in 2018 Cybersecurity Act, Strategies Regulations, and Plans for the development of capabilities for the protection of the cyberspace and the digital economy and society in the EU and NATO.

Unlike most common cyber exercises, which cover either the "managerial" or "technical" side, through the GB-BG Cyber Shockwave Exercise series, we aim to:

1. Combine in one exercise the "managerial" and "technical" aspects of dealing with cyber/hybrid nature of incidents and crises, i.e. we aim at combining tabletop exercises with technical-operations exercises through realistic practical simulations, using specific infrastructure (Cyber Range), built with the help of experts from the NCSC (National Cyber Security Center, UK), international consultants and instructors, ESI CEE (European Software Institute – Center Eastern Europe), CySecResLab, the cybersecurity and resilience lab of ESI CEE
2. Base our exercises on realistic tasks and possible threats related to the critical infrastructure and control systems, transport, and logistics, including the impediment to military exercises and, more generally, to collective defense capabilities and operations (NATO). The simulated disruptions would have a hybrid nature and a multifaceted cascading effect both in terms of defense capabilities and on society as a whole, as well as on the national and the collective security (including a regional and cross-border impact).
3. Test the procedures and mechanisms for interaction between the "industry/services" and the state bodies (including joint coordination with member states from the regions, such as Romania, and NATO structures), following and testing the natural and realistic "vertical" of escalation and identifying areas for improvement and creating inputs for further action.

As implicit goals, the GB-BG Cyber Shockwave initiative aims to bring together representatives from different government structures and establish trust, as well as cross-sector collaboration and engagement. To achieve that, the partners aim at engaging the private sector to improve the overall situational awareness and achieve an accurate picture of the current state of affairs on different levels of granulation.

Last but not least, and especially with the latest editions of the GB-BG Cyber Shockwave series of exercises, we aim at testing and identifying areas of im-

[1] https://cyberbg.eu/

provement in the strategic and crisis communications capabilities in government structures.

The onset of the GB-BG Cyber Shockwave initiative began in 2019 with the 0ctane exercise, which simulated a cyber/hybrid crisis related to the supply of gas and the national fiscal system with massive effects related to the disruption of the 2019 local elections in Bulgaria. Following the successful completion of this exercise, the initiative was continued in 2020 with the Embarg0 exercise, organized in two phases, where we simulated a hybrid crisis escalation related to disruption of military maritime supply chain and logistics and jeopardizing a simulated military exercise.

The latest edition of the GB-BG Cyber Shockwave series of exercises was carried out in April 2021 with the PANACEA exercise, which became a regional exercise, including players from Romania as well. The main scenario and specific context of the PANACEA exercise were related to potential cybersecurity-related disruptions affecting the supply chain (logistics, transportation) of medical equipment and medication, and the new type of logistics related to the supply of the COVID-19 vaccine and the implementation of the related vaccination plans.

2.1 Exercise scope and audience

The GB-BG Cyber Shockwave exercise series are usually set up in a two-day active play distributed exercise, and a preparation phase, with an approximate duration of four days before the active exercise days. However, the exercise life cycle usually covers between 3-4 months of planning before the active days of play, as well as between 1-2 months for evaluation and follow-up after the end of the active exercise days.

The life cycle of a standard GB-BG Cyber Shockwave exercise is illustrated in Figure 2 below and further elaborated upon below.

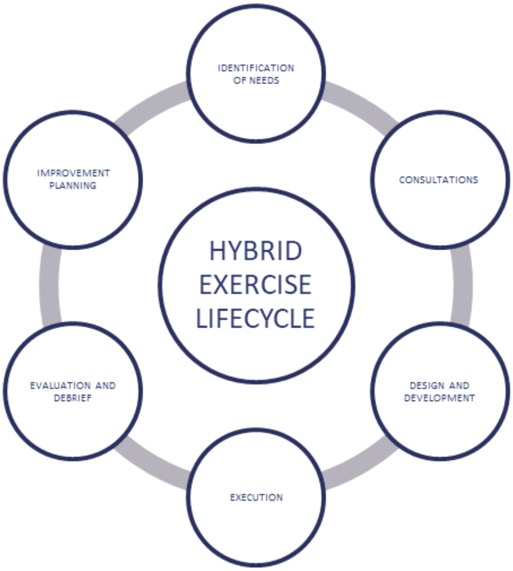

Fig. 2. Standard GB-BG cyber shockwave exercise life cycle.

Although the exercise life cycle follows a mostly process-oriented model, it is in its nature somewhat iterative at the beginning phases, which could also be performed simultaneously in some cases, especially within the context of existing time constraints.

1. **Identification of needs**. The first step of the exercise life cycle. It represents the initial impulse for the exercise implementation, as well as the identification of the target audience, exercise scope and objectives, and main scenario topics. This phase begins with the identification and prioritization of needs and areas to be targeted by the exercise. During this phase, desired exercise outcomes are formulated, as well as a plan on the required human and financial resources for the execution of such an exercise. *Approximate duration: 2-4 weeks.*
2. **Consultations**: Although the onset of this phase is at the formulation of desired exercise outcomes, activities, which logically belong to this phase, could overlap with the design and development phase. Consultations with external stakeholders and potential participants are vital, especially to target challenges and skills specific to a given critical infrastructure, as well as for the formulation of a realistic scenario.
Approximate duration: 2-4 weeks
3. **Design and Development**: This is the longest phase of the exercise life cycle, as it contains high-intensity tasks. Within this phase are the development of the exercise scenario and storylines, the design and devel-

opment of specific exercise ranges and polygons, including the virtual environment and its content, the content design for the other polygons. The phase includes a mix of creative work, software development, scenario and storyline development, material preparation, content development, and much more, depending on the specific exercise context. This phase includes an execution plan, containing not only an exercise plan but also supporting logistics and organization plans (i.e., catering, food, accommodation for participants, transportation to the exercise venue, etc., if applicable)
Approximate duration: 1-3 months

4. **Execution**: Begins with 3-5 days of a preparation phase. The first days of the preparation phase are dedicated to the configuration, and the validation of the connection to the cyber polygons, the configuration of user accounts, etc. Following that, participants start receiving emails with preliminary events, information, and injects. Participants are required to monitor all incoming information about the exercise through their email accounts in the exercise environment. The execution phase culminates with the two active exercise days when participants should be prepared for technical activities remotely (via VPN access) or on-site.
Approximate duration: 1 week
5. **Evaluation and Debrief**: Includes feedback collection from all exercise roles, including the organizers, the players, and the planners, and the creation of an exercise report and after-action reports with lessons learned recommendations, and best practices to distribute to participants. The exercise evaluation is conducted against the desired exercise outcomes, formulated within the identification of needs phase, and deviations are analyzed and consolidated.
Approximate duration: 1-2 months
6. **Improvement Planning**: Includes inputs generated for future exercises, and policymaking, as well as bug reports, exercise environment improvements, software maintenance, back-ups, etc.
Approximate duration: 2-4 weeks

The GB-BG Cyber Shockwave exercise series envisages the participation of both remote and in-place physical participation, facilitated by dedicated VPN connections for each team, individual, or participant. The players who play remote, usually are expected to gather with their teams at their normal place of employment or in incident cells or facilitate a hotline connection between themselves.

The geographic scope of the GB-BG Cyber Shockwave exercise series has evolved to include participants and an audience at a regional level for an operations-based exercise involving larger numbers of organizations and individuals. Choosing the participants follows the decision about the specific context of the exercise, as well as the capabilities which are aimed to be tested and exercised.

There are different roles that people and organizations may play in an exercise. The lifecycle of a hybrid exercise envisages various roles, whilst in many cases in practice, an organization or individual holds multiple roles. Following ENISA's Good Practice Guide on National Exercises [12], among the major roles adopted in the GB-BG Cyber Shockwave series of exercises are:

1. **Exercise organizers.** Those include the organization(s) that drives the process of exercise organization.
2. **Exercise planners.** Those include the organization(s) or individual(s) that participate in the planning of the exercise.
3. **Participant.** An organization or individual that will play during the execution of the exercise.
4. **EXCON (Exercise Control).** The team that directs the exercise.
5. **Facilitator**. A person or organization, whose role is to observe and record the actions and decisions of the participants during the exercise, checking performance of the tested measures, noting effectiveness and weaknesses, communicating with the moderator, and providing much of the material that will be required for evaluating the exercise.
6. **Observer.** Individuals or organizations that are invited to observe the exercise, without participating nor monitoring performance. They may include stakeholders who are not otherwise participating, such as additional organizations outside the scope of the exercise.
7. **Evaluator.** Individuals involved in the process of evaluating the exercise and coming up with follow-up actions and lessons learned.

The exercise planners are the ones, responsible for the exercise scenario.

The exercise scenario is first outlined at a very high level during the identification of needs phase and the consultations phase; however, it is detailed within the design and development phase of the exercise life cycle.

The first considerations of the scenario at a high level are made when the specific needs and scope of the exercise are elaborated and prioritized, with its main goal to test the specific capabilities identified, through realistic simulations. A realistic scenario is critical to the success of the exercise [12].

A scenario includes several storylines, based on which the main events and exercise inject will follow the exact storylines within the same scenario. Depending on the specific context of the scenario, as well as the teams participating and their profile, one team of participants can either work on single or multiple storylines.

2.2 Exercise instrumentation

To achieve the exercise goals, the exercise planners implement the exercise scenario as a simulated cyber/hybrid crisis through a dedicated technical orchestration platform and simulation polygons (Cyber Range). The Cyber Range provides servers with different types of software, simulations of "official" and "attacked" or compromised web platforms, and a communication environment, specifically developed tools and instruments to help the blue teams, JEMM platform, and many more (including red team live interventions), which are deployed according to the scenario. The polygons include simulated security operations and monitoring centers, dashboards for visualization of various types of incidents.

For the GB-BG Cyber Shockwave Exercises, a dedicated Cyber Range and supporting infrastructure are developed by ESI CEE and CySecResLab and include the following polygons:

- **Polygon 1:** Servers with different types of software, simulations of official and "attacked" web platforms, and a communication environment.
- **Polygon 2:** SOC (Security Operations Center) – a simulation of security operations and monitoring center.
- **Polygon 3**: Cyber Picture – dashboard providing visualization of information for various types of incidents, including cyber incidents, but also kinetic and hybrid incidents on a sectoral, organizational, and national levels.
- **Polygon 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.
- **Polygon 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).
- **Polygon 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.

The exercise cyber range also includes:

- **JEMM-platform**: a tabletop platform based on Polygon 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 infrastructure 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 exercise cyber range are available below.

2.3 Technical realization of the exercise environment

The deployment of ESI CEE’s cyber range follows a three-phase model, as illustrated in Fig. 3 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.

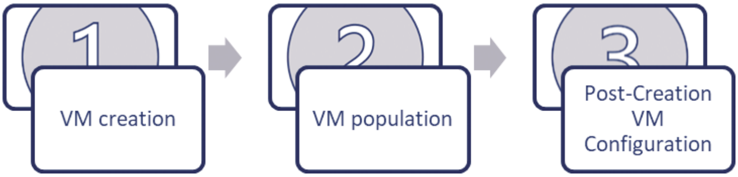

Fig. 3. The Three-Phase model of the exercise cyber range.

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 example, Zimbra[2] email server, WordPress[3] open-source content management system for the exercise media websites, FreeIPA[4] open-source identity management system, and NodeBB[5] forum software for the Crisis Communications Dashboard.

[2] https://www.zimbra.com/

[3] https://wordpress.com/

[4] https://www.freeipa.org/page/Main_Page

[5] https://nodebb.org/

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, and setting the authentication and user provisioning to use the FreeIPA directory manager.

This process is performed automatically, with a dedicated builder machine as shown in Fig. 3 below.

The builder machine uses a combination of Terraform and Ansible to deploy the exercise infrastructure.

Terraform[6] 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[7] 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.

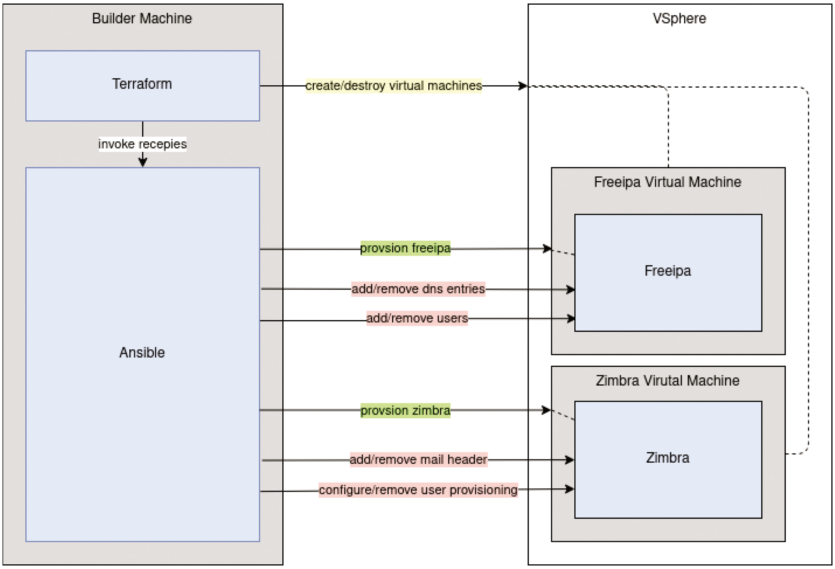

Fig. 4. Automatization of the exercise environment deployment.

[6] https://www.terraform.io/

[7] https://www.vmware.com/products/vsphere.html

Ansible[8] 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.

In conclusion, phase one and phase two are automatically performed when a module is invoked and the final product is an appliance hosted on a virtual machine. What configuration is passed on the Terraform module that can trigger Phase 3 depends on the specific module. For FreeIPA, this could be the list of exercise participants, LDAP[9] 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 future emails

3.4 Architecture of the exercise environment

As mentioned above, to deploy the exercise infrastructure, we need to identify what elements of the cyber range we wish to deploy for the specific context. A minimum configuration must include information about the polygons that we will deploy, as well as a participants list, used within the configuration of a directory server, such as FreeIPA, to provision and authenticate accounts.

A brief architecture of a standard exercise cyber range is shown below in Figure 5, and a short technical overview of the different polygons follows below.

Status Page. To begin with, we have a standard exercise Status page, which is a basic 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. The status page contains a brief description of the cyber range, as well as links to the different polygons, and useful information for the players, such as a contact book, containing in-exercise contact details for other teams, information about the exercise, the

[8] https://www.ansible.com/

[9] https://ldap.com/

scenario, and the main storylines, useful resources, such as exercise playbook, presentations, technical and installation guides, and links to virtual exercise conference rooms. It is powered by NuxtJS[10] and implements specific checks for the exercise infrastructure, such as DNS, HTTP, HTTPS, etc., to display infrastructure status.

ExOrch (Exercise Orchestrator). ExOrch is an internally developed software for executing events that take place during the exercise. The internal broker queue is responsible that all the events are executed at the right time. An event could be – "send an email", "post a news article", "enable a technical challenge", "update exercise status" and more. ExOrch is written in Python3 and offers an Excel interface for injects so that organizers can use excel files to feed automatically deployed injects. It is a fully scalable software product (tested simultaneously with 9 machines), which further offers a MongoDB[11] database interface for injects. Through the ExOrch dashboard, the exercise administrators could easily pause, delay or stop completely an incoming event from executing if necessary. The dashboard is also written in Python3, using the Pyramid[12] framework and 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 through an instance of NodeBB[13] forum software running as a Docker [14]container with LDAP Integration for single sign-on.

Cyber Picture. The Cyber Picture is another internally developed dashboard for the status display of the government sector. Through the Cyber Picture, participants can monitor the current global situation, which is changing during the exercise because 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.

SOC (Security Operations Center) / Exercise Situation Dashboard. This is also internally developed simulation of a security operations and a monitoring center, where simulated events and developments are displayed on a world map

[10] https://nuxtjs.org/

[11] https://www.mongodb.com/

[12] https://trypyramid.com/

[13] https://nodebb.org/

[14] https://www.docker.com/

with appropriate icons and descriptions. It is written in Python 3 leveraging the Pyramid framework and further providing an interface for REST API access, integrated with OpenStreet Map.

VPN Server. A dedicated exercise OpenVPN [15] server, allowing remote access to the exercise cyber range. Before the exercise execution phase displayed in Figure 2 above, each team or individual participants (if needed) receives a dedicated VPN Configuration, separating participants from each other.

A virtual environment. An "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.

It also provides some "emulated" real-life websites by "cloning" those static HTML pages to support the realistic organizations emulation and the scenario development.

The virtual environment also contains several simulated standard types of **media websites** powered by WordPress content management software and improved with customized backups and restore capabilities.

[15] https://openvpn.net/

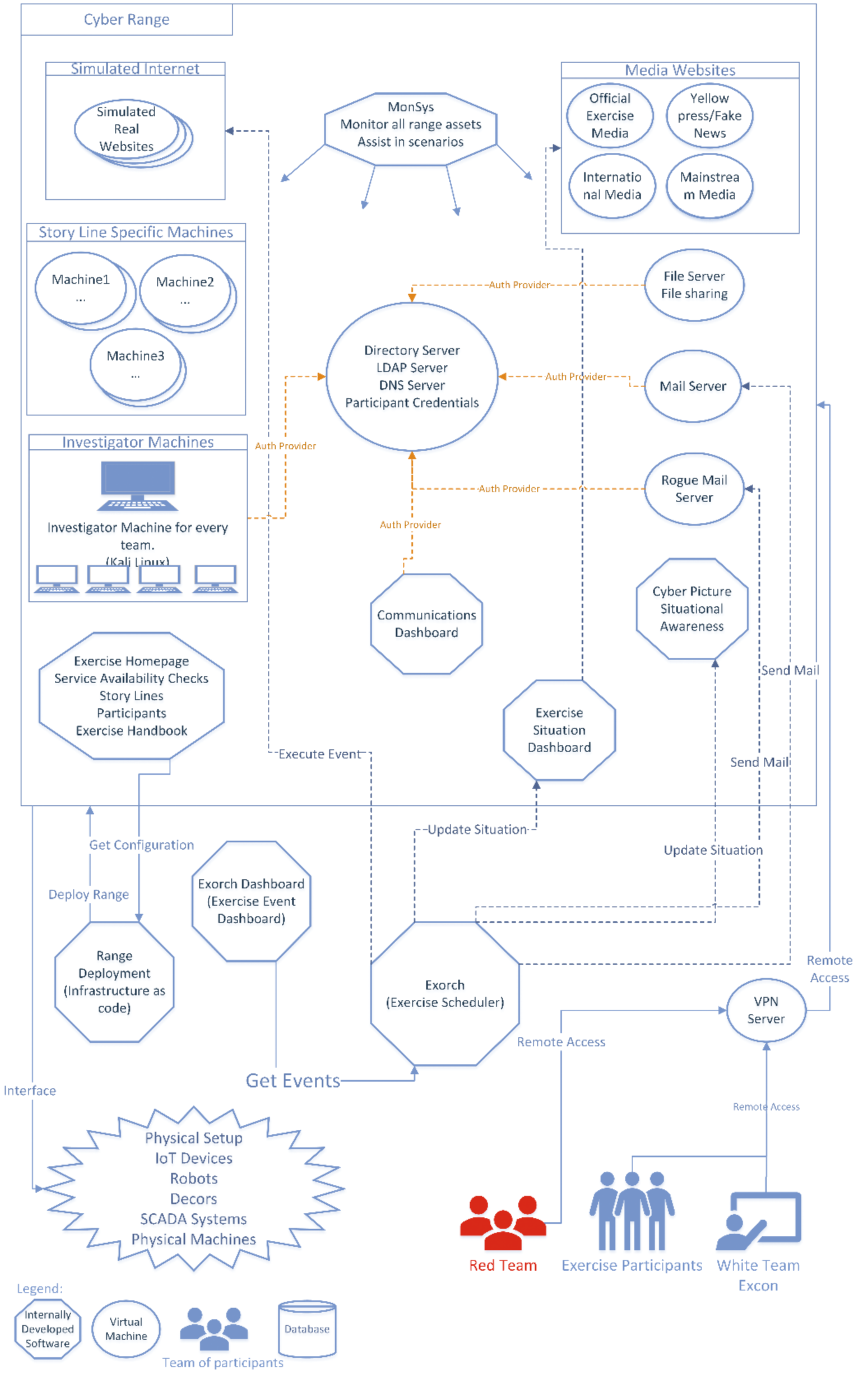

Fig. 5. Standard exercise cyber range configuration.

Investigation Machines. A set of dedicated Kali Linux virtual machines for every team to assist the forensics teams in the investigations. The virtual machines are distributed among players with pre-installed tools, to limit the network traffic during the exercise.

The Investigation machines support an LDAP integration so that participants can use their credentials to log in and use the services on the machines.

The cyber range also includes several **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 can be restored to its original state, to ensure that if a team manages to destroy the challenge itself, there is a restoring mechanism ready to be implemented.

FreeIPA Directory Server. For every cyber range, we implement a directory server that is responsible for the DNS queries and user directories.

File Sharing Server. A simple NextCloud file server to assists in file-sharing during the exercise. Large files such as images, virtual machines, videos, and others are uploaded there. The NextCloud file server also offers LDAP Integration.

Mail Server. A Zimbra Mail Server and WebMail to facilitate official communication between participants. Every participant has a mailbox that they use to communicate with other participants or EXCON. Also powered with LDAP integration to facilitate access.

The exercise cyber range also includes a Rogue Mail Server, using the same technology as the regular exercise mail server, but used for phishing attack simulations in certain exercises.

3 Main outcomes and lessons learned

For outlining the main outcomes related to the application of the current exercise methodology for improving the cyber-resilience in the healthcare sector, further details will be provided about the scenario storylines and the specific findings and outcomes from the 2021 GB-BG Cyber Shockwave Exercise PANACEA.

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 strong hybrid impact. Furthermore, we aimed at testing the standard operating procedures, the collaboration between hospitals and business, government, security institutions, and industry-specific actors.

The scenario was 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. To address the vulnerabilities and attack-vectors landscape, a generic model referring to tactics and techniques described in the ATT&CK framework by MITRE was followed [13].

The exercise scenario developed interactively and dynamically, based on the decisions and actions of the participants – both technical and organizational, as well as their ability to cooperate and collaborate. To achieve the gamification and stimulate the interactivity, an AI/ML engine is deployed for the semi-automatic red-teaming injects, based on the players (and the "blue-team") activities and the success in resolving the challenges. A "success-rate" and "difficulty/severity-level" parameters are monitored and dynamically generate with the orchestrator ExOrch the technical and simulated challenges.

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 new type of 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[16] was incorporated in the scenario.

Based on all the above, six main storylines have been developed:

SL100: Supply Chain, Medicine and Medical Equipment Distribution Disruptions

Delay, obstruction, confusion of deliveries through simulated technical attacks and attacks against specific systems.

- SL110 – Vaccines' handling conditions corruption. Suspected manipulation of temperature registrations, such as data loggers, thermometers, and/or sensors for refrigerators, containing vaccines, and/or transportation conditions.
- SL120 – Disruption of distribution and transportation plans. Manipulation and attacks against systems, causing vaccine shipping, dispatch, and storage disorganization.

[16] http://www.vgocom.com/

SL200: Critical Healthcare Services Disruption

Hybrid Impact Healthcare Services and Systems.

- SL210 – Leaked patients' data. Ransomware and related investigations.
- SL220 – Leaked credentials for access to medical facilitation systems.
- SL230 – Telepresence robot (VGo) in a medical facility is hacked and remote control by adversaries was obtained.

SL300: Data and National Statistics Manipulations

- A series of attacks against core information channels.
- SL310 – Manipulated data and information channels investigation.
- SL320 – Crisis communication and response to misinformation.

SL400: Escalations in the Context of the Upcoming Parliamentary Elections

- SL410 – Escalation to a national crisis (in the context of pre-election days)

SL500: Strategic Communications

Simulation of events depending on the proper identification and handling of internal and external communication processes.

- SL510 – Simulated news about events
- SL520 – Simulated fake news
- SL530 – Misinformation and disinformation identification and response
- SL540 – Social media monitoring
- SL550 – Crisis communications and response

SL600: Cybersecurity-Specific

Technical instruments and injections related to the hybrid scenario.

- SL610 – compromised, exploited, defaced, and manipulated websites
- SL620 – ransomware/cryptolocker
- SL630 – phishing

Among the most important action items in the creation of the healthcare-specific storylines were the study, research, and expert consultations. Especially regarding the logistic details, related to the supply of the coronavirus vaccines, there are many unknown to the public details. An in-depth analysis of the entire supply chain process, including many consultations with experts from state and private organizations, was needed to customize the scenario as much as possible and make it realistic for the participating organizations.

Among the other aspects, what was most appreciated by healthcare professionals participating in the exercise was the ability to reflect as much as possible the latest trends, events, and incidents. Such was the introduction of a telepresence robot as part of the exercise challenges, which is a technology that finds vast application since the onset of the coronavirus pandemic, as it allows physical contact-free visitations in COVID-19 facilities.

Another realistic aspect, appreciated by medical professionals, was the inclusion of the actual thermo-registrars, used for the logistics of the coronavirus vaccines.

By the same token, something implied with the use of various storylines, is the modularity of the exercise. Creating a modular experience allows hospital IT staff to find a place in the investigation of the challenges, where they find most useful. A downside to this approach is that this somewhat discourages teams to work on challenges, involving aspects, that they are previously unfamiliar with. However, on the flip side, it encourages teams to seek cross-sector collaboration and support, to solve or even report on the challenges.

On the topic of challenge reporting, a lesson learned from this exercise is to invite more communication teams, including the medical teams. A few action items that could be used to encourage communication teams to participate more actively are:

- Emphasize the consequences of participant actions, and especially of the communications team's actions for the development of the crisis.
- Provide opportunities prior to the exercise, for the exercise teams and participants to meet each other and exchange information about their core capacities. This proved to be especially important for teams from organizations, that would be expected to communicate in real life, should a crisis occur. A chronic vulnerability in this regard is that technical teams from hospitals do not seem to have generally contacts with technical teams from other organizations that could be able to help and support them during a crisis in real life.
- Support the communication teams with sample pieces of public communications items. As part of the exercise orientation session or as part of the resources distributed among partners, sample press releases, holding lines, or social media status updates should be provided.
- Provide a separate workshop for communication teams, to make sure they can access and use the communications dashboards and tools.
- Provide additional resources, such as stakeholder impact assessment matrix, risk assessment matrix, vulnerability reports, etc., that communication teams can keep using in their daily practice, to improve the usefulness of the exercise for the participants.

Another important lesson from the exercise implementation is to use technical artifacts as part of the challenges for strategic and communication teams, to ensure collaboration between technical and non-technical teams and empower cross-sectoral information exchange.

A core positive outcome from this exercise is the finding that this was the first hybrid exercise that our healthcare representatives participated in, and additionally, obtaining their commitment and readiness to participate in further editions of the exercise.

This exercise was not without its specific challenges. Among them, the core was:

- Unwillingness or inability of healthcare organizations to participate. As this exercise was organized in times of an actual crisis, the resources that healthcare organizations could dedicate to participate in the exercise were very limited.
- Inviting only technical teams from hospitals, without discussing with management of organizations the importance of inviting people, responsible for public and crisis communications.
- Communication channels are discussed but not used.
- Earlier identification and invitation of exercise participants. product.
- Ensure media coverage – emphasize the exercise and its training.

4 Ongoing research and conclusions

Hybrid type of cybersecurity exercises allow an effective simulation of large-scale cyber incidents and crises with potential huge impacts on the economy and society. They provide a realistic play for hybrid nature scenarios and the imposed need for cross-sector collaboration, as well as coordination between technical, managerial, and strategic teams. This coordination allows for the opportunity to analyze chronic vulnerabilities and blind spots in the collaborative cyber defense at a national and regional level and to prepare for the "hybrid warfare" [14].

The application of this exercise model was examined in this paper, through the lens of the healthcare sector and its need for cyber resilience and cross-sector support in the face of a crisis. Among the main benefits identified was the opportunity of hospital IT teams, which are not directly specialized in cybersecurity and defense, to engage in a dialogue with a supportive cross-sector network of trust and exercise a desired collaboration. This establishment of collaboration habits with competent national authorities, as well as stakeholders from the academia and the private sectors, has been identified to positively influence the chances for rapid reaction response to cyber/hybrid crisis.

Furthermore, hybrid exercises provide hospital IT teams with hands-on experience in dealing with realistic cybersecurity-specific challenges, thus exercising the preparedness and capabilities of the teams to deal with such events, as well as exposing areas for improvement and development of capacity.

This paper also provided an outline of this innovative for Bulgaria approach and overviewed the cyber range used for the exercise, its components, and the methodological approach for the implementation and organization of such exercises, which combines good practices from the UK and the US alike.

The ongoing research of the implementation team focuses on the exploration of AI/ML methods for the creation of a dynamic scenario, which branches automatically based on participants' decisions. This research direction has been motivated by the need to reduce the number of human resources for the scenario branching, during the actual exercise, and leave room for better evaluation of the participants' experience.

We hope that with this research, we can motivate more organizations from the public and private sectors to seek opportunities for integration of 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.

5 Acknowledgements

The three editions of the GB-BG Cyber Shockwave exercises and the implementation of the Cyber Range pilot have been supported by a longer-term project with the UK Embassy in Sofia. The pilot version of the MonSys incorporated in the Cyber Range is a result of a project, financed under agreement № D-094 / 27.09.2019 by the Research and Development and Innovation Consortium (Sofia Tech Park JSC) and Nemetschek Bulgaria. The technical base and maintenance of the Cyber Range and technical polygons are provided by the Cybersecurity Lab under an annual grant by the "Bulgaria National Roadmap for Research Infrastructure 2017-2023".

References

1. Weil T. and Murugesan S. (2020). "IT Risk and Resilience—Cybersecurity Response to COVID-19," in *IT Professional*, vol. 22, no. 3, pp. 4-10, 1 May-June 2020, doi: 10.1109/MITP.2020.2988330.
2. Georgiadou A., Mouzakitis S. & Askounis D. (2021).Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Secur J* (2021). https://doi.org/10.1057/s41284-021-00286-2.
3. INTERPOL, Cybercrime: COVID-19 Impact Report (2020), INTERPOL General Secretariat, available at: https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf.
4. Ahsan Pritom M. M., K. M. Schweitzer, R. M. Bateman, M. Xu and S. Xu (2020). "Characterizing the Landscape of COVID-19 Themed Cyberattacks and Defenses," *2020 IEEE International Conference on Intelligence and Security Informatics (ISI)*, 2020, pp. 1-6, doi: 10.1109/ISI49825.2020.9280539.
5. As Hospitals Cope With COVID-19 Surge, Cyber Threats Loom, Associated Press & CISA, (2020). Available at: https://www.voanews.com/covid-19-pandemic/hospitals-cope-covid-19-surge-cyber-threats-loom, accessed on May 6, 2021.
6. UK Cabinet Office, Exercise Planners Guide (2006). Home Office Publication, available at: https://www.gov.uk/government/publications/the-exercise-planners-guide, accessed on January 10, 2021.

7. Caralli R., Allen J. and White D. (2011). CERT Resilience Management Model (CERT-RMM). SEI Series in Software Engineering, Addison-Wesley Professional.
8. MITRE Cyber Exercise Playbook (2014). Available at: https://www.mitre.org/publications/technical-papers/cyber-exercise-playbook, accessed on May 5, 2021.
9. TRAFICOM: Instructions for organising cyber exercises – A manual for cyber exercise organisers (2020). Available at: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions%20for%20organising%20cyber%20exercises.pdf, accessed on May 15. 2021.
10. Tagarev T. (2018). "Hybrid Warfare: Emerging Research Topics," Information & Security: An International Journal 39, no. 3 (2018): 289-300, https://doi.org/10.11610/isij.3924
11. NIST: The Cyber Range: A Guide. [ebook] NIST (2020). Available at: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf, accessed on May 15, 2021.
12. ENISA, Good Practice Guide on National Exercises. Enhancing the Resilience of Public Communications Networks (2009). Resilient e-Communications Networks. Available at: https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide, accessed on May 15, 2021.
13. MITRE ATT&CK version 9 (2021). Available at https://attack.mitre.org, accessed on May 21, 2021.
14. Tagarev T. (2021). "Understanding Hybrid Influence: Emerging Analysis Frameworks". In *Digital Transformation, Cyber Security and Resilience of Modern Societies*, (edts.) Tagarev, T., Atanassov, K., Kharchenko, V. and Kasprzyk, J., Studies in Big Data, vol. 84 (Cham: Springer, 2021), 449-463, https://doi.org/10.1007/978-3-030-65722-2_29.