sciendo

Land Forces Academy Review
Vol. XXX, No. 3(119), 2025

EMERGING TECHNOLOGIES IN CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE-BY-DESIGN: THE CASE OF CYBER RANGES

Adrian-Victor VEVERA
The National Institute for Research and Development in Informatics – ICI Bucharest, Romania
Victor.vevera@ici.ro

Alexandru GEORGESCU
The National Institute for Research and Development in Informatics – ICI Bucharest, Romania
Alexandru.georgescu@ici.ro

Ella Magdalena CIUPERCĂ
The National Institute for Research and Development in Informatics – ICI Bucharest, Romania
Ella.ciuperca@ici.ro

ABSTRACT

Resilience-by-design is emerging as a key practice in developing and enhancing the resilience of critical infrastructure systems. Cybersecurity is a key concern for critical infrastructure operator and therefore an important issue to address in order to enhance resilience. One important tool in this regard is cyber ranges. The present article lays out their use in resilience enhancement, using academic and industry sources, while compiling the emerging technologies and paradigms that are making cyber ranges more effective than before. The research is the result of a practical knowledge transfer project between two countries with the goal of creating a federated energy cyber range.

KEYWORDS: resilience, cyber range, cybersecurity, training, critical infrastructures

1. Introduction

Critical Infrastructure Protection (CIP) has become the standard framework for analyzing, mapping, understanding and protecting the complex systems on which our nations and the European Union's prosperity, efficiency, security and defense rely. The framework provides key concepts, perspectives, tools and modes of operation that enable the development of the multistakeholder strategic-decisional-operational construct that enables CIP in practice (Gheorghe, Vamanu, Katina & Pulfer, 2018). Critical Infrastructures (CI) are socio-technical systems composed of technical assets, facilities, resources and organizations that operate them which generate critical goods and services and whose disruption or destruction would cause significant loss of human life,

DOI: 10.2478/raft-2025-0047
© 2025 Adrian-Victor Vevera et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

economic damage, loss of functionality (Bucoveţchi & Simion, 2015) or, we would add in a hybrid threats context, also the loss of confidence in the state system and institutions on the part of citizens, investors, partners and allies. Resilience is the overarching concept used to express the strength of CI against all hazards, expressing both the capacity to prevent the materialization of a harmful event, as well as, in the case of its materialization, the ability to minimize damages, prevent catastrophic consequences and resume a minimum acceptable level of functioning in as short a time as possible (Bucoveţchi, Georgescu, Gheorghe, & Popescu, 2024). Resilient systems also learn from incidents, extracting lessons and applying the lessons learned to further adapt to the new security environment. In the new European context, with a significant legislative and institutional upgrade of the CI governance apparatus through the CER Directive, the NIS 2 Directive, the Cyber Resilience Act and numerous other general and sectoral initiatives, there is a focus on translating the lessons learned from the previous crises (the global financial crisis, the refugee crisis, the Covid-19 pandemic and attendant disruptions and the second invasion of Ukraine) into a framework that is fit for a more interdependent European Union (Badea, Halmaghi, Ranf & Bucovețchi, 2024).

This is also necessary because of the normalization of hybrid threats against civilian critical infrastructures using measures short of war and means with attribution issues offering plausible deniability to systemic rivals and adversaries, especially but not exclusively cyber and electronic attacks (Badea, Constantinescu, Ranf & Bucoveţchi, 2022). Since the threshold for attacks is quite low in terms of know-how and resources (though increased quantities of each also increase the probability of success), there is also a profusion of actors who can engage in such attacks with or without state support outside of actual state agents, such as organized crime groups, terrorist and ideological groups, lone wolves, enemies within and more (Vevera, Cîrnu & Rădulescu, 2022).

The article starts from the importance of critical infrastructure protection and the threat posed by cyber-attacks to analyze the importance of cyber ranges in the CIP and resilience-by-design and to trace key paradigms and technologies which enhance the value of cyber ranges for system design, training, scenario formulation, exercises, as well as proactive and reactive CI security amelioration. Following an analysis of cyber range state-of-the-art resulting from the analysis of academic, industry and regulator output, we combine academic and industry sources to investigate the leading emerging technologies and paradigms that are reshaping cyber range capabilities and use. The results of the research behind this article and of future research will inform practical applications to assist a non-European partner, as part of a NATO Science for Peace and Security project, to create a federated energy cyber range to enhance national and by, extension, European resilience to hybrid threats.

2. Cyber Range Functionalities

The National Institute for Standards and Technology of the US defines cyber ranges as "*interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates*

network services such as webpages, browsers, and email as needed by the customer" (National Institute for Standards and Technology, 2018, p. 1). Cyber ranges are both a platform and a simulation environment which, ideally, provide sufficient capability to adequately model a cyber or cyber-physical system to the point where interactions with it can be used to generate various benefits such as: security testing, security research, competence building, security education, the development of cyber capabilities, competence assessments, recruitment, digital dexterity "*the ability and desire to exploit existing and emerging technologies for business outcomes*" (European Cyber Security Organization, 2020) and, overall, to improve cyber resilience through all of the above. Cyber ranges create the safe space necessary for a wide variety of cyber resilience enhancing activities, both directly and indirectly, for a wide variety of actors from private sector, government, military, academia, law enforcement and more (Alexandru, Vevera, & Ciupercă, 2019).

The ECSO (2020) definition describes cyber ranges as "*a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases*".

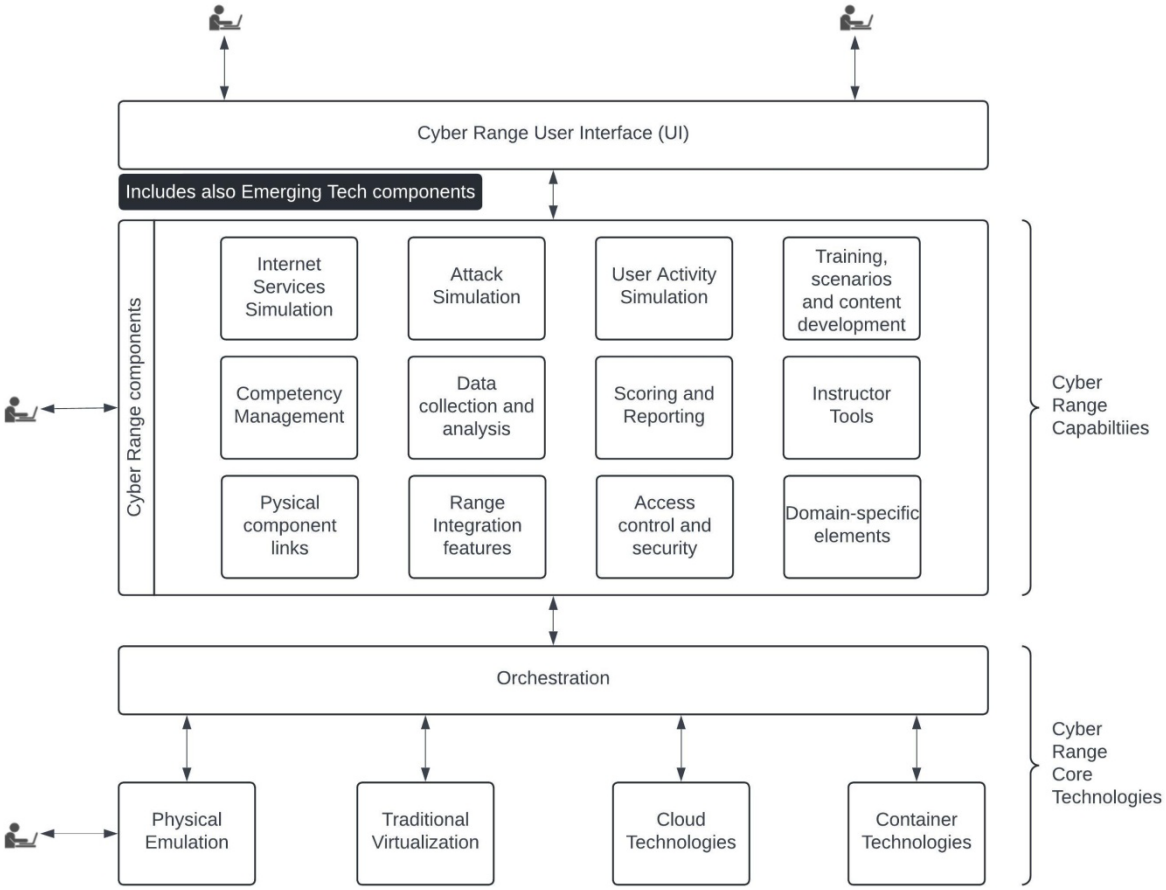


Figure no. 1: *Main elements of cyber range*
(Source: Authors' compilation)

As can be seen in Figure no. 1, cyber ranges consist of a series of key components: a hardware substrate, a virtualization technology that enables the simulation of various system, orchestration systems which is "*the technology responsible for the creation of automation workflows including the mass configuration, creation, modification and deletion of virtual machines, self-provisioning, and automation of tasks between the virtual infrastructure and other cyber range components or other systems interfacing with the cyber range*" (ECSO, 2020, p. 15), systems for the support of cyber range capabilities such as attack simulation and scenario and content development, and a user interface that brings everything together.

There is significant variation in cyber range configuration, with most systems being developed over time, in an accretive manner, with key components outsourced to specialized firms (such as the conventional virtualization software or containerization software). Some cyber ranges can be delivered as fully packaged products (the Airbus CyberRange, for instance). The system need not have a physical presence in the user facility or in the service provider facility, it can be run as Platform-as-a-Service or Software-as-a-Service, and a custom build low budget cyber range could even eschew orchestration (automated configuration) software in favour of fully manual control. The requirement of having certain capabilities is fully dependent on the intended use cases, with some specific applications requiring bespoke software modules and other components, such as a physical component testing bench.

In the context of CIP, a cyber range may be used to assess and remedy the cybersecurity vulnerability of a particular facility, CI network, CI component or underlying technology. Cyber range services can be important assets in cybersecurity audits, in personnel training and in developing the Operator Security Plan and the investment plan for resilience enhancement. CI systems are sufficiently diverse to enable dedicated cyber ranges specialized in specific CI domains or subdomains, such as energy generation, energy transmission, energy balancing or offshore facilities (McFly, Peterson & Reynolds, 2022). The increasingly distributed nature of modern CI, where interconnectivity across extensive CI networks is made possible by digital command, control, communication and data gathering systems, makes cyber ranges a necessity for understanding and preparing for the new cybersecurity environment (McFly et al., 2022).

3. Emerging Technologies and Paradigm Shifts for Cyber Ranges

Cyber range technology is continuously evolving to keep up with the threat landscape, with the needs of users and beneficiaries and with the new digital paradigms. This section highlights the principal emerging digital technologies and paradigms that are changing the face of cyber ranges. It is important to remember that cyber ranges are, at most, a platform, not a concrete system emerging in a ready state from a factory or software laboratory. This means that, by their nature, cyber ranges are highly variable, updateable, and upgradeable in keeping with the needs and resources of the operating entity. This state allows also for significant experimentation by operators, which can lead to surprising functionalities and technology integrations.

3.1. Artificial Intelligence

There is a significant current enthusiasm about the potential application for artificial intelligence in a wide range of fields (Kovaci & Iacob, 2024). In the main report of the National Security Commission on AI in the US, Schmidt (2021) described the potential of AI by quoting Thomas

Edison on electricity: "*It is a field of fields… it holds the secrets which will reorganize the life of the world*", and that the existing application count for "*very little in comparison with the possibilities that appear*".

Artificial Intelligence can be, indeed, a game changer in terms of cyber range construction and operation. Table no. 1 summarizes the main contributions that AI can make to cyber ranges, in order to distil the numerous ideas discovered over the course of the research process.

Table no. 1

AI contributions to Cyber Range construction and operation

AI contributions to Cyber Range construction and operation	
AI as systems architect	Artificial Intelligence can automate much of the work of building the virtual networks and systems (tied to whatever physical components have been added by the designers) that will be tested as part of cyber range operation. The landscape of the system that is being studied (such as a power plant or an office building) can be rendered in greater detail and with less human effort through the use of AI working from plans, sensor networks and other information sources.
AI as attacker	AI can play the role of cyber-attacker to simulate various means of attack, degrees of sophistication, vulnerabilities and channels of intrusion used or timing (Dinu, Vasile & Georgescu, 2024). The added diversity costs less in terms of human input, provides a new dimension of simulation (given that AI is actually being used as a cyber-attacker in the real world) and is more adaptable to changing needs. The AI can also be used to shorten the time to implementation for novel ideas of testing a system, whether by simulating a new component or quickly developing malware to test hypotheses regarding vulnerabilities.
AI as game master	Artificial Intelligence can be used to formulate an endless variety of scenarios, cutting down on the reuse of materials and increasing the value of repeat trainings through added diversity (Immersive, 2024).
AI as subject of RLMS	Artificial Intelligence is increasingly being used as a component in industrial control systems and other core functions of networks for Critical Infrastructure operation. This means that AI itself is being targeted by attackers for sabotage (disruption, subversion, damage) (Sambucci & Paraschiv, 2024). Therefore, cyber ranges through their core training, testing and research functions must also accommodate scenarios and systems that integrate AI functioning thereby creating a range learning management system that can accommodate AI dimensions under real-world conditions.
AI as rapporteur	AI capabilities can be used to produce after-action reports, extract important lessons, assign grades to participants, and produce feedback (Rotună, Dumitrache & Sandu, 2022). This is a significant element of the workload of a cyber range during normal use.

(Source: Authors' compilation)

3.2. Blockchain Technology

Blockchain is another basic and emerging digital technology with an incredibly wide range of potential applications, many of them related to critical infrastructure operation. Beyond cryptocurrencies and other highly visible applications of blockchain technology, we find a wide array of applications related to identity management, origin control, e-government, logistical tracking, distributed markets, secure communications, conflict resolution in overlapping systems, distributed system organization and more (Georgescu & Cîrnu, 2019). These applications make use of the core feature of "distributed ledger" technology – the use of a distributed network of nodes to algorithmically validate changes to a ledger without a costly or potentially corruptible intermediary.

Future cyber ranges must be ready to integrate blockchain features in their operation and to simulate the functioning of blockchain networks in order to adequately represent systems that have integrated

blockchain components. Because of the nature of blockchain architecture and its distributed systems, cyber ranges have to develop new functionalities to support blockchain intelligence analysis (Vacusta & Nica, 2023).

Cyber ranges may also integrate blockchain technology as part of their core user features, given the usefulness in controlling identity, controlling access and privileges for various types of users, and ensuring the integrity of communications which can later be audited (including the results of exams, product tests, experimental system validation which might be tampered with) (Dumitrache, Sandu, Rotună & Cohal, 2022).

3.3. Quantum Computing Technology

New cyber range adaptations also must take into account the potential for quantum computing to upend existing standards on data encryption. The capabilities of quantum computers are advancing by leaps and bounds and will be able to solve problems that are far too complex for classical computers which include solving the algorithms behind encryption keys that protect our data. The IBM 433 qubit Osprey processor was revealed on November 9, 2022, followed in 2023 by the Condor with 1,000 qubits. IBM's roadmap shows a progression toward a 4,000 plus qubit quantum computer, codenamed Kookaburra, due in 2025 (Gambetta, 2022). The apparent imminent arrival of commercial quantum computing has spurred different actors into action: the United States passed the Quantum Computing Cybersecurity Preparedness Act requiring federal agencies to migrate information technology systems to post-quantum cryptography, the EU's Cyber Resilience Act is also concerned with the transition of public authorities and other actors to post-quantum solution. The National Institutes for Standards and Technology in the US released its first four quantum-proof algorithms in July 2022 but, not long after, the NIST's CRYSTALS-Kyber public-key encryption and key encapsulation mechanism had been broken through a combination of AI and side-channel attacks (Ji, Wang, Ngo, Dubrova & Backlund, 2023). The development process has continued, but it is a race between hackers (some of whom are using a "steal now, decrypt later" approach), hardware developers pushing the cutting edge, and post-quantum solution developers (with products such as lattice-based approaches, code-based cryptography, multivariate cryptography and hash-based cryptography) (Abelian, 2024).

Cyber ranges fit into this issue for two reasons. Firstly, they will inevitably integrate quantum computing as part of their toolbox for developing realistic simulations of networks and systems, given the large numbers of quantum computing applications. Secondly, they will employ quantum computing to test the security of new cryptographic standards or of cybersecurity products themselves. Quantum computing itself is an addition to cybersecurity, through its applications in random number generation and in quantum-enhanced machine learning (basically an AI approach). Until true quantum-safe technologies are on the market, critical infrastructure operators will need to do running evaluations and adaptations to the quantum state-of-the-art (Soviany & Gheorghe, 2023) for instance by assessing their quantum security exposure, by training personnel with the necessary skills, and by employing measures such as doubling key sizes for widely utilized symmetric encryption algorithms, by planning larger output sizes for hashing algorithms (Dargan, 2024). Figure no. 2 illustrates the main issues where cyber ranges come into play in the current transition period, including for the development of a quantum transition plan at the level of the affected operators.

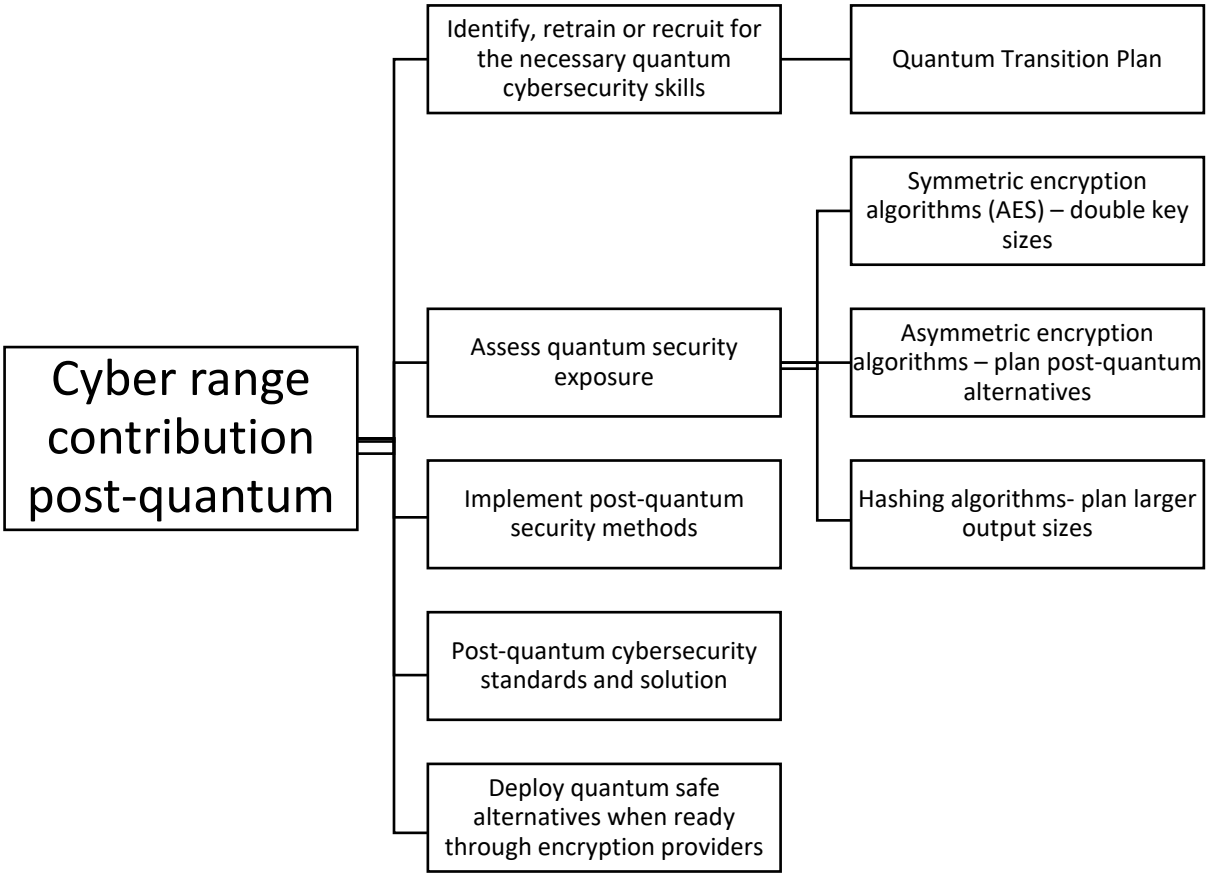


Figure no. 2: *AI contributions to Cyber Range construction and operation*
(Source: Authors' compilation)

Cyber ranges will be needed to assess the results of any implemented changes and desired investment plans. Cyber ranges can also validate non-quantum system transformations, such as the use of private 5G networks, zero-trust architectures, offline data storage (and archiving), one-time pads (Soviany, Gheorghe & Gheorghe-Moisii, 2024), the re-encryption of old data, quantum key distribution and more (CyberArk, 2024; KPMG, 2024).

3.4. Digital Twin Technology

A digital twin represents a high-fidelity simulation of an existing network or even physical or cyber-physical system. The final level of detail depends on the resources being allocated, but, at their greatest extent, digital twins deliver a complete reproduction of all aspects of a facility, or system, sometimes incorporating even environmental issues (McKinsey, 2024), with little of the abstraction that current cyber ranges require to keep modelling work manageable. Digital twins can maintain a significant level of fidelity by incorporating data in real time from sensor networks – with the development of the Internet-of-Things paradigm, the actual number of sensors can number trillions, linked together via wireless communications and encompassing all manner of systems and even people. The application of digital twin technology to cyber ranges is obvious – the digital twin can serve as the simulation space for the

cyber range to function for a particular facility, thereby obviating the need to develop a high-fidelity model internally (CybExer, 2023). The space can be segmented according to need and can be kept up-to-date for reasons other than the cyber range functionality. For instance, cyber ranges can import the models developed with Building Information Modelling by architects and engineers planning a facility (which may actually become a critical infrastructure).

By working directly from the plan and with unprecedented scope, cyber ranges can truly become contributors to resilience-by-design. This is especially important when dealing with cyber-physical systems (such as the ones underlying a power plant) where a cyber-attack against an industrial control system or a supervisory control and data acquisition system can lead to dramatic changes in the physical operation of machinery with a digital component – readouts can be faked allowing machinery to exceed tolerances, catastrophic degradation can be set up with little forewarning and the output of key facilities can be degraded in key ways, according to the interests of the attackers. The spread and attendant diminution in price for digital twin technology enhances the capabilities of cyber ranges, though there will still be value in abstracted and less detailed models (CybExer, 2024). Exercise, training and testing can become much more realistic and can incorporate many more variables than in a classically produced simulation space, allowing also for emergent system behaviours that had not been anticipated by the designers.

Of course, using digital twins is not mandatory. It is possible for the simulation of twenty sample workstations in a network to be enough to account for the behaviours of a hundred thousand workstations. It is important that the advanced applications that would benefit from a full digital twin, from a particular system like a satellite to an entire smart city network and even the precise simulation of a facility in all of its aspects, can be covered by a cyber range.

3.5. Architectures Shifts

The architecture of cyber ranges is shifting with the implementation of new technologies and new modes of functioning related also to the underlying business models of cyber range operators. The main factor in the architecture shift deals with the model of virtualization, which is the feature that accounts for most of the activity of a cyber range, even though some applications indeed require the presence of physical components (such as, potentially, the testing of a device or cyber-physical system). Most cyber ranges use conventional virtualization, running either traditional virtualization or with container technology. In traditional virtualization, the virtual machines running on the hardware are coordinated by a hypervisor that apportions hardware resources which can be running directly on the hardware or as an application within the operating system (enabling the use of multiple operating systems). Containerized technologies (mostly Docker) have seen significant development and adoption in recent years because of their adaptability and portability. While virtual machines run on individual operating systems, containers share a machine's operating system kernel. Different computing environments can be used to run the same applications as the latter's can be bundled with libraries, configuration files and other elements

required to run. Multiple containers can run on the same virtual machines. By 2022, 75% of cyber ranges were estimated to have container capabilities, because of their orchestration capabilities for complex networks and their cost effectiveness. They do have limitations in the complexity of the system they can represent and the potential security issues if they are misconfigured, but patching is quite easy and only other containers on the same virtual machine can be compromised. In contrast, misconfiguration incidents are lower probability in a traditional virtualization scenario, but any security issues stemming from real vulnerabilities in the hardware may compromise the entire system.

However, the real ongoing shift in cyber range architecture is due to the use of cloud technology as a way to optimize the use of resources by pairing it with demand given the inherent flexibility of cloud-based approaches. Physical resources (ram, disk space, network etc.) become abstracted and are transparently made available to the hypervisor. Depending on the cloud technology used, both modes of conventional virtualization can also be accommodated, but with the added flexibility, workflow management and scalability offered by cloud integration. Private clouds are more costly to set up but enable complete control over data flows. The operator is also usually better supported by the cloud technology vendor. These clouds are equivalent in capability to the traditional virtualization architectures. Public clouds run by third party providers such as Microsoft Azure or Amazon Web Services cost less to set up and are better able to manage costs, while leaving the logistics of hardware to the cloud providers, but they have lower flexibility and higher concerns regarding the security of data flows, especially in the case of cloud misconfiguration, which is a significant vulnerability for all cloud users regardless of vendor diligence (Petcu, Candet, Ştefănescu, Gruia & Craioveanu, 2021). Lastly, there are hybrid cloud virtualization systems which combine the best of both worlds by linking the private cloud infrastructure to the public one in order to achieve resource scalability while maintaining control over data. This can be a great advantage to organizations that prefer a closed data environment like the military or law enforcement and would otherwise continue using private cloud systems.

3.6. Collaborative Approaches

Cyber range use is undergoing transformation not just in relation to the underlying technological tools, but also in the manner in which it is being used, through collaborative approaches that are meant to enhance the overall security impact of the use of a cyber range on the resilience of a critical infrastructure. This resilience is expressed in terms of a preparedness of the system itself, the level of training of its users and the eventual security outcomes of testing and exercises which take place on the cyber range. These collaborative approaches are also made possible by the use of new technologies such as cloud virtualization, or blockchain for secure communication.

3.6.1. Federated Cyber Ranges

The word federation is used more widely in the ICT domain to express a group of computers or network providers agreeing to work according to specific operating standards held in common. In the case of cyber ranges, these standards will

include elements such as how the scenarios are defined and described, how capabilities are advertised, and how federation participants interact with each other including requesting support or services (ECSO). A federation enables multiple cyber ranges to specialize on different areas while maintaining interoperability to hopefully provide the end beneficiary with all of the capabilities he requires without forcing cyber ranges to provision internally for a wide array of capabilities and requirements. Federation is the lighter option in terms of coordinated development and does not necessarily require cyber ranges to interact directly with each other or to communicate; actual integration levels may be low. Federations of cyber ranges in the EU have been the object of several projects in recent years, from one coordinated by the European Defence Agency to the ECHO and CyberSec4Europe projects. One non-cyber range example of a federated functioning is ERNCIP – the European Reference Network for Critical Infrastructure Protection, which is a network of laboratories in Europe providing standardized services across a breadth of specialized fields to CI operators and defenders and where the coordinating role for the federation was provided by the European Commission under the European Programme for Critical Infrastructure Protection.

3.6.2. Integrated Cyber Ranges

Integration is a step up from federation and requires active communication between cyber ranges, including for the purpose of setting up a shared simulation environment. This is harder to set up in a secure way over public infrastructure, including the use of VPN tunnelling. There is also the possibility that cyber ranges sharing the same virtualization platform, such as one of the big cloud services providers, could more easily link up for integration. Either way, it requires the careful setup and discipline for the technical network environment, in addition to the other issues that may appear when it comes to orchestration between cyber ranges potentially using different technologies and with challenges related to IP addressing or bandwidth.

3.6.3. Gamification

Gamification is a philosophy and practice of promoting interaction with a service and the pursuit of certain results or of excellence through the application of ideas derived from video gaming, such as reward systems, point scoring, achievement tracking and more (Vasuthanasub, Bucovețchi, Stanciu & Badea, 2019). These systems are proven to work, despite criticism of cases of unethical implementation (Gheorghe & Polinpapilinho, 2023). Cyber ranges can utilize gamification to promote serious engagement with more complex exercises over longer periods, to incentivize more effort on the part of scenario creators, to motivate attackers or defenders participating in an exercise or testing operation, and to generally obtain better results from human interaction with or through the cyber range (Kianpour, Kowalski, Zoto, Frantz & Øverby, 2019). European projects such as CYRESRANGE are exploring gamification not just as an enhancer of user interaction with the cyber range environment, but also to stimulate the development of a common crowdsourced repository of scenarios, structured trainings,

and certifications schemes to be used by all the participating cyber ranges (Dinu & Cîrnu, 2024).

4. Conclusions

The current security environment is characterized by the normalization and ubiquity of cyber-attacks against critical infrastructures even in situations of undeclared conflict. The disruption of CI functioning can lead, both by definition and by the thresholds currently in use to designate CIs, to significant loss of human life, economic damages, functionality loss and confidence crises. The interdependence between CIs across multiple dimensions (geographic, physical, cybernetic and informational) can lead to cascading and escalating disruptions through the alignment of key breakages in the system-of-system configuration, which can extend crises and augment their damage in unpredictable ways both for attackers and operators/defenders (Pescaroli & Alexander, 2016). Cybersecurity threats are emerging as a preferred means of attack against critical infrastructures, because of the ubiquity and comprehensive nature of digitalization in recent years, because of the low threshold for initiating attack, because of the high cost to benefit ratios and because of issues with attribution and subsequent prosecution, sanction, and retaliation (Cîrnu, Rotună, Vevera & Boncea, 2018). Fostering resilience in such an environment is key because the attackers have the initiative in deciding when, where, in what configuration of hybrid means, for how long and with what purpose they want to strike. In the absence of initiative and given resource constraints, the most effective way to counter such threats is to enhance resilience.

The present paper traced the contribution that cyber ranges can make to resilience enhancement. While the definition of a cyber range is certainly expansive, at the highest level they are sophisticated simulators of existing and potential systems that provide users with a high degree of fidelity for the testing of an infrastructure or of a product, for scenario formulation, for exercises, training, and education, but also for research into the operation of cyber weapons in a safe environment (including to reverse engineer captured tools from malignant actors). Together, these functions support virtuous loops for the enhancement of critical infrastructure resilience, contributing also to the supporting industries and functions that provide valuable tools for operators, investigators, and defenders. Moreover, we presented the main roles that emerging digital technologies and business paradigms can play in enhancing the capabilities of the cyber ranges themselves. This provides the basis for future research as well as planning an upgrade path in the practical implementation of a future federated energy cyber range. These findings not only support resilience-by-design in future infrastructure systems, but can also support the work of the project described in the acknowledgement by ensuring that the resulting federated energy cyber range is configured to receive upgrades in the future that will enable it to remain at the cutting edge of the industry and of the threat actors. As the project implementation continues, we will be able to test specific hypotheses in technology integration within a functional system meant for everyday use.

Future research areas should include practical assessments of the integration of specific technologies into cyber ranges,

such as AI, and whether the additional features provide value to users without compromising system security and other features. Efforts should also be dedicated to raising awareness of the benefits of using cyber ranges for CI operators and the means to increase access to cyber range services for a wider variety of users under different terms of use (including subsidized access). Lastly, there is an additional area of research regarding the control over the proliferation of key advanced cyber range capabilities, which may be misused by different categories of actors or used unethically by legitimate actors, including as part of cyber authoritarianism. These technologies include commercial cyber intrusion capabilities.

Acknowledgements

This article is supported by The NATO Science for Peace and Security Programme, under SPS G6313 – "Cyber Polygon: A Cyber Range Platform Specialized on Energy Sector with Automatic Generation of Virtual Scenarios" project.

REFERENCES

Abelian. (2024). *Comprehensive Guide to Post-Quantum Cryptography: Types and Applications*. Medium. Available at: https://pqabelian.medium.com/comprehensive-guide-to-post-quantum-cryptography-types-and-applications-32dabd971c84.

Alexandru, A., Vevera, V., & Ciupercă, E.M. (2019). National security and critical infrastructure protection. *International Conference Knowledge-Based Organization, Vol. 25, No. 1*, 8-13. DOI:10.2478/kbo-2019-0001.

Badea, D., Constantinescu, M., Ranf, D.E., & Bucoveţchi, O. (2022). Resilience of critical cultural urban infrastructures (CCUI) in the framework of digital transformations. Some managerial markers. *Journal of Defense Resources Management, 13(2)*, 77-88.

Badea, D., Halmaghi, E.E., Ranf, D.E., & Bucoveţchi, O. (2023). Transforming Urban Resilience. *FAIMA Business & Management Journal, 11(3)*, 30-40.

Bucoveţchi, O., Georgescu, A., Gheorghe, A.V., & Popescu, G. (2024). Understanding Resilience – a Conceptual Framework. *Proceedings of the International Conference on Business Excellence, Vol. 18, No. 1*, 2377-2385. Sciendo.

Bucoveţchi, O., & Simion, P.C. (2015). Importance of Interdependencies in Critical Infrastructures' protection. *UPB Sci. Bull., Ser. C, 77(1),* 301-309.

Cîrnu, C.E., Rotună, C.I., Vevera, A.V., & Boncea, R. (2018). Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture. *Studies in Informatics and Control,* ISSN 1220-1766, *Vol. 27(3)*, 359-368. Available at: https://doi.org/10.24846/v27i3y201811.

CyberArk (2024). *Infosec's Guide to Post-Quantum Readiness*. Available at: https://www.cyberark.com/resources/ebooks/infosecs-guide-to-post-quantum-readiness.

CybExer (2023). *Cyber ranges and Digital Twins*. CybExer. Available at: https://cybexer.com/blog/cyber-ranges-and-digital-twins.

CyberSec4Europe Project. (n.d.). Available at: https://cybersec4europe.eu/.

CYRESRANGE Project. (n.d.). Available at: https://cyresrange.net/.

Dargan. (2024). *Quantum Cybersecurity Explained: Comprehensive Guide*. The Quantum Insider. Available at: https://thequantuminsider.com/2024/03/13/quantum-cybersecurity-explained-comprehensive-guide/.

Dinu, A., & Cîrnu, C.E. (2024). Empowering National Cybersecurity: The CYRESRANGE Project. *Romanian Cyber Security Journal, ISSN 2668-6430, Vol. 6(1)*, 75-83. Available at: https://doi.org/10.54851/v6i1y202408.

Dinu, A., Vasile, P.C., & Georgescu, A. (2024). AI-driven solutions for cybersecurity: comparative analysis and ethical aspects. *Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, Vol. 34(3)*, 35-48. Available: https://doi.org/10.33436/v34i3y202403.

Dumitrache, M., Sandu, I.E., Rotună, C-I, & Cohal, A. (2022). Blockchain-era eGovernment services. *Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, Vol. 32(1)*, 7-18. Available at: https://doi.org/10.33436/v32i1y202201.

European Cyber Security Organization – ECSO. (2020). *WG5 PAPER Understanding Cyber Ranges: From Hype to Reality*. SWG 5.1 Cyber Range Environments and Technical Exercises. Available at: https://ecs-org.eu/ecso-uploads/2023/05/2020_SWG-5.1_paper_UnderstandingCyberRanges_final_v1.0-update.pdf.

ECHO Project. (n.d.). Available at: https://www.echonetwork.eu/.

Gambetta, J. (2022). *Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing*. IBM website. Available at: https://www.ibm.com/quantum/blog/ibm-quantum-roadmap-2025.

Georgescu, A., & Cîrnu, C.E. (2019). Blockchain and Critical Infrastructures - Challenges and Opportunities. *Romanian Cyber Security Journal, ISSN 2668-6430, Vol. 1(1)*, 93-100.

Gheorghe, A.V., & Polinpapilinho F.K. (2023). *Gamification for Resilience: Resilient Informed Decision Making*. John Wiley & Sons, 2023.

Gheorghe, A., Vamanu, D.V., Katina, P., & Pulfer, R. (2018). *Critical Infrastructures, Key Resources, Key Assets: Risk, Vulnerability, Resilience, Fragility, and Perception Governance, Topics in Safety, Risk, Reliability and Quality*. Springer International Publishing. Available at: https://doi.org/10.1007/978-3-319-69224-1.

Immersive (2024). *Immersive Labs Unveils GenAI-Powered Cyber Exercise Creator to Rapidly Prepare Workforces for Threats*. Immersive. Available at: https://www.immersivelabs.com/resources/press/ai-scenario-generator.

Ji, Y., Wang, R., Ngo, K., Dubrova, E., & Backlund, L. (2023). A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber. *2023 IEEE European Test Symposium (ETS), Venice, Italy*, 1-5. DOI: 10.1109/ETS56758.2023.10174000.

Kianpour, M., Kowalski, S., Zoto, E., Frantz, C., & Øverby, H. (2019). Designing Serious Games for Cyber Ranges: A Socio-technical Approach. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Stockholm, Sweden, 85-93. DOI: 10.1109/EuroSPW.2019.00016.

Kovaci, P-D, & Iacob, N.M. (2024). Artificial Intelligence and OSINT. Considerations and Challenges. *Romanian Cyber Security Journal, ISSN 2668-6430, Vol. 6(2)*, 45-51. Available at: https://doi.org/10.54851/v6i2y202404.

KPMG (2024). *Quantum is coming — and bringing new cybersecurity threats with it*. Available at: https://kpmg.com/xx/en/our-insights/ai-and-technology/quantum-and-cybersecurity.html.

McFly, S., Peterson, J., & Reynolds, T. (2022). *Distributed Energy Resource Cybersecurity Framework and Cyber Range Integration. National Renewable Energy Laboratory*, NREL/TP-5R00-82545, Golden, Colorado, USA. Available at: https://www.nrel.gov/docs/fy22osti/82545.pdf.

McKinsey (2024). *What is digital-twin technology?*. McKinsey & Co. Available at: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-digital-twin-technology.

National Institute for Standards and Technology. (2018). *Cyber Ranges*. Available at: https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf.

Pescaroli, G., & Alexander, D. (2016). Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Nat Hazards 82*, 175-192. Available at: https://doi.org/10.1007/s11069-016-2186-3.

Petcu, I., Candet, I.B., Ştefănescu, C., Gruia, C.I., & Craioveanu, V. (2021). Security Risks of Cloud Computing Services from the New Cybernetics' Threats Perspective. *Romanian Cyber Security Journal, ISSN 2668-6430, Vol. 3(1)*, 89-97.

Rotună, C.I., Dumitrache, M., & Sandu, I.E. (2022). Assessment of Machine Learning algorithms for automated monitoring. *Romanian Journal of Information Technology and Automatic Control,* ISSN 1220-1758, *Vol. 32(3)*, 73-84. Available at: https://doi.org/10.33436/v32i3y202206.

Sambucci, L., & Paraschiv, E-A. (2024). The accelerated integration of artificial intelligence systems and its potential to expand the vulnerability of the critical infrastructure. *Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, Vol. 34(3)*, 131-148. Available at: https://doi.org/10.33436/v34i3y202410.

Schmidt, E. (coord.) (2021). *Final Report - National Security Commission on Artificial Intelligence.* NSCAI. Washington DC, US. Available at: https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Soviany, S., & Gheorghe, C.G. (2023). The QKD (Quantum Key Distribution) Application in Cyber Security. *Romanian Cyber Security Journal,* ISSN 2668-6430, *Vol. 5(2)*, 87-101. Available at: https://doi.org/10.54851/v5i2y202309.

Soviany, S., Gheorghe, C.G., & Gheorghe-Moisii, M. (2024). Quantum Networks and Cyber Security. A Simulation Case Study for Point-to-Point QKD Links. *Romanian Cyber Security Journal,* ISSN 2668-6430, *Vol. 6(2)*, 27-43. Available at: https://doi.org/10.54851/v6i2y202403.

Vacusta, B., & Nica, C. (2023) Blockchain and Cyber-Security: the Opportunity to Develop a National Data Analysis Platform to Ensure National Security and Financial Stability. *Romanian Cyber Security Journal, Vol. 5(2)*, 65-74. Available at: https://rocys.ici.ro/documents/109/Art._7_ROCYS_2_2023.pdf.

Vasuthanasub, J., Bucoveţchi, O., Stanciu, R.D., & Badea, D. (2019). Serious gaming towards learning of future city management. *Romanian Journal of Information Technology and Automatic Control,* ISSN 1220-1758, *Vol. 29(3)*, 41-50. Available at: https://doi.org/10.33436/v29i3y201904.

Vevera, A.V., Cîrnu, C.E., & Rădulescu, C.Z. (2022). A multi-criteria approach for the calculation of a complex indicator of Cyber Security and Digital Development. *Romanian Journal of Information Technology and Automatic Control,* ISSN 1220-1758, *Vol. 32(4),* 19-32. Available at: https://doi.org/10.33436/v32i4y202202.