This paper was presented at the XXXVII ISPIM Innovation Conference, held in Granada, Spain on 07 June to 10 June 2026. ISBN 978-952-65771-2-8.

Cyber Ranges as Catalysts of Cybersecurity Innovation

Reda Bensouda*

Université du Québec en Outaouais, 283 Boul. Alexandre-Taché, Gatineau, QC J8X 3X7, Gatineau, Canada

E-mail: reda.bensouda@uqo.ca

* Corresponding author

Rhizlane Hamouti

Université du Québec en Outaouais, 283 Boul. Alexandre-Taché, Gatineau, QC J8X 3X7, Gatineau, Canada

E-mail: rhizlane.hamouti@uqo.ca

Hajar Moudoud

Université du Québec en Outaouais, 283 Boul. Alexandre-Taché, Gatineau, QC J8X 3X7, Gatineau, Canada

E-mail: hajar.moudoud@uqo.ca

Abstract: As cyber threats grow in scale and complexity, cybersecurity can no longer be reduced to a technical function. This paper argues that cyber ranges, controlled simulation environments traditionally used for training, can be reconceptualized as innovation platforms capable of driving cybersecurity capacity building at the ecosystem level. Drawing on an exploratory qualitative case study embedded in a Canadian university cyber range initiative, the paper extends the operational model by introducing an explicit innovation layer structured around three functions: data and knowledge valorization, experimentation and applied research, and ecosystem orchestration. Three key learning mechanisms and governance dimensions are identified as enablers of cross-organizational coordination and collective intelligence. The findings support a shift from a capability-centric toward a platform-centric view of cybersecurity innovation, where value emerges from dynamic interactions among infrastructures, actors, and governance structures within multi-actor ecosystems.

Keywords: Cyber ranges; Cybersecurity; Capacity building; Innovation Ecosystems; Critical Infrastructures; Collaborative Innovation.

This paper was presented at the XXXVII ISPIM Innovation Conference, held in Granada, Spain on 07 June to 10 June 2026. ISBN 978-952-65771-2-8.

1. Introduction and problem statement

The accelerated digital transformation of organizations, sectors, and territories is accompanied by an intensification of cyber threats and by growing interdependencies among critical socio-technical systems. In this context, cybersecurity can no longer be reduced to a technical function or a compliance requirement. It must instead be understood as a systemic condition for resilience, trust, and innovation within digital ecosystems. From an innovation management perspective, this evolution introduces a structural challenge. Cybersecurity capacity is not determined solely by technological sophistication, but also by the ability of heterogeneous actors (public institutions, firms, and academic organizations) to coordinate, learn collectively, and align investments within fragmented governance environments. These actors operate under divergent incentives, asymmetric maturity levels, and strict constraints regarding data sharing and risk disclosure. The central issue is therefore not only the strengthening of cybersecurity controls, but the absence of mechanisms enabling cross-organizational learning and coordinated experimentation at the ecosystem level. As cyber risks become systemic, the capacity to innovate in cybersecurity increasingly depends on infrastructures that support simulation, collaboration, and shared learning across institutional boundaries. This paper argues that existing approaches to cybersecurity capacity building remain insufficiently integrated with innovation ecosystem perspectives. In particular, the role of experimental infrastructures (such as cyber ranges and security testbeds) remains under-theorized as potential innovation platforms.

2. Literature review and theoretical gap

Cybersecurity Capacity and Maturity Models

As cybersecurity threats grow in both scale and complexity, organizations and nations face mounting pressure to move beyond ad hoc responses toward structured, measurable approaches to capability development. To address this challenge, the literature has proposed numerous cybersecurity capability and capacity maturity models aimed at structuring the assessment and development of cybersecurity capabilities. As highlighted by Miron and Muita (2014), Cybersecurity Capability Maturity Models (CMMs) (e.g., The International Organization for the Standardization (ISO) and the International Electrotechnical Commission ISO/IEC standards, the National Institute of Standards and Technology (NIST) standards, the Cybersecurity Capability Maturity Model (C2M2)), describe progressive levels of maturity in governance, processes and technical controls. However, these models often remain descriptive, sector-specific, and difficult to operate in environments characterized by strong interdependencies among critical infrastructures. Their limited capacity to support cross-organizational coordination and learning underscores the need for more systemic and practice-oriented approaches.

In response to these limitations, the Cybersecurity Capacity Maturity Model for nations (CCM) developed by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford offers a systemic perspective on cybersecurity capacity building at the national level (Müller, 2015; GCSCC, 2017). The CCM structures cybersecurity capacity around five interdependent dimensions: strategy and governance, culture and society, skills and human capital, legal and regulatory frameworks, and technical controls. While conceptually robust and widely applied in national assessments, the CCM

remains largely analytical and provides limited guidance on how its dimensions can be translated into concrete practices, coordinated interventions and innovation processes in complex and multi-actor contexts.

Overview of Cyber Ranges and Testbeds

Cyber ranges have emerged as key infrastructures supporting cybersecurity training, experimentation, and capability development. Initially designed as controlled environments for technical exercises, their role has progressively expanded toward more complex socio-technical systems enabling education, research, and innovation. In parallel, security testbeds have evolved as complementary infrastructures primarily focused on the validation and testing of technological systems. Distinguishing and articulating the complementarity between these two environments is essential for structuring effective cybersecurity capacity-building strategies and advancing experimentation practices.

Recent developments in the Canadian academic ecosystem illustrate this evolution. Several cyber ranges initiatives have been deployed, reflecting growing institutional investment in experiential cybersecurity infrastructures. For instance, the University of Ottawa hosts the uOttawa–IBM Cyber Range, integrated within its Cyber Hub, which provides an immersive environment for cyber incident response involving students, industry, and public actors (uOttawa, 2023). Similarly, the Canadian Institute for Cybersecurity has developed specialized testbeds designed for attack detection and mitigation across heterogeneous industrial protocols (Firouzi, 2025). These initiatives highlight the coexistence of training-oriented and technology-oriented infrastructures within a shared ecosystem.

A systematic literature review by Yamin and al. (2020) contributes to structuring this landscape by proposing a taxonomy of cyber range systems based on core components such as scenarios, monitoring, environments, learning mechanisms, teaming, and management functions. Building on this framework, cyber ranges can be associated with two primary and complementary objectives. The first relates to training and education, where cyber ranges provide structured learning environments combining theoretical knowledge with hands-on exercises. The second objective relates to testing and security assessment; a domain more traditionally associated with security testbeds. Testbeds enable controlled experimentation for evaluating systems, validating robustness, and testing cybersecurity techniques through predefined and reproducible experimental setups.

This differentiation is further reinforced by Chouliaras et al. (2021), who emphasize the pedagogical and training functions of cyber ranges. According to their analysis, cyber ranges enable immersive and experiential learning by placing users in realistic attack-defense situations, often involving team-based exercises and decision-making under pressure. These environments are particularly effective in addressing the cybersecurity skills gap, as they allow participants to develop both technical competencies and cognitive abilities such as situational awareness and coordination. In contrast, testbeds play a more limited pedagogical role, as their primary objective remains the technical evaluation of systems rather than the development of human capabilities.

From a broader technical perspective, Zhang et al. (2020) propose a comprehensive taxonomy of cyber ranges based on architectures, functionalities, and application domains. Their work shows that cyber ranges can be classified into simulation-based, emulation-based, and hybrid environments, offering varying levels of realism and

scalability. Importantly, they demonstrate that cyber ranges are increasingly used beyond training, including for cyber defense strategy evaluation and large-scale experimentation. Complementing this perspective, more recent work by Sánchez et al. (2026) reflects ongoing efforts to formalize and standardize cyber ranges usage, particularly within competency-based frameworks such as the European Cybersecurity Skills Framework (ECSF). This evolution underscores the institutionalization of cyber ranges as core infrastructures supporting structured training, assessment, and certification processes. Conceptually, cyber ranges and testbeds differ. Testbeds are designed to produce controlled, reproducible technical knowledge through structured experimentation, whereas cyber ranges generate situated, experiential knowledge through dynamic, scenario-based, and adversarial interactions. Rather than being strictly separated, these infrastructures can be understood as forming a continuum between technological validation and socio-technical experimentation. Across these contributions, the distinction between cyber ranges and testbeds can be synthesized in Table 1 as follows:

Table 1: Comparative Analysis of Cyber Ranges and Security Testbeds.

Dimension	Security Testbed	Cyber Range
Primary Purpose	Testing, validation, system evaluation	Training, simulation, capability development
Core Logic	Experiment-driven, controlled	Scenario-driven, adversarial
Focus	Technological, system-level	Human, organizational, operational
Dynamics	Static or predefined experiments	Real-time, interactive, evolving
Users	Engineers, researchers	Professionals, students, decision-makers
Functions	Performance testing, interoperability validation	Training, exercises, simulation, skill assessment
Pedagogical Role	Limited	Central (experiential learning)
Research Applications	System validation, architecture testing	Strategy testing, human factors, coordination
Multi-actor Interaction	Limited	High
Outputs	Technical performance data	Skills, readiness, coordination insights

Beyond this differentiation, recent literature suggests an increasing convergence between cyber ranges and testbeds. Emerging hybrid platforms combine the technical realism and validation capabilities of testbeds with the scenario-based and adversarial features of cyber ranges. These integrated environments enable the simultaneous evaluation of technologies, organizational processes, and human responses, particularly in the context of complex and interconnected critical infrastructures. In parallel, the concept of Federated Cyber Ranges has gained traction, particularly in Europe. Initiatives such as the Cyber Ranges Federations aim to interconnect distributed cyber ranges infrastructures across countries, enabling shared scenarios, resource pooling, and cross-border collaboration. This federated approach enhances scalability, interoperability, and collective learning, while supporting coordinated cybersecurity capacity-building at the regional level. It also reflects a shift toward more integrated and networked experimentation environments, aligned with the needs of complex and interconnected critical infrastructures. Despite these advances, the literature remains fragmented. Most studies focus on technical, functional, or pedagogical aspects, with limited attention to the role of these infrastructures in enabling multi-actor coordination, collective learning, and innovation processes. Their integration within broader innovation ecosystems, linking academia, industry, and public institutions, remains underexplored. This gap calls for a reconceptualization of cyber ranges and testbeds not as isolated technical infrastructures, but as interdependent components of broader innovation platforms that enable testing, experimentation, coordination, and the co-evolution of technologies, practices, and institutions.

Cybersecurity and Innovation

The cybersecurity and privacy (PACS) market has expanded rapidly in recent years, fueled by the multiplication of attack vectors, the diffusion of emerging technologies such as IoT, cloud, and mobile systems, and the tightening of regulatory requirements (Dooly, 2014). This evolution is reshaping the conditions under which innovation occurs in the sector. At the same time, significant structural constraints persist, including the inherent complexity of cybersecurity technologies, a highly saturated marketplace, limited differentiation between competing solutions, and persistent challenges in demonstrating value when investments are primarily justified in terms of risk mitigation rather than direct financial returns. Under these conditions, the capacity to test, validate, and deploy solutions in realistic environments becomes a critical success factor, highlighting the role of collaborative innovation ecosystems that bring together technical expertise, access to complex operational contexts, and mechanisms that facilitate the transition from development to market adoption.

In parallel, the evolution of innovation models provides a useful lens for understanding how such processes can be organized and managed. Earlier linear conceptions (such as technology-push and market-pull) have gradually given way to more interactive and integrated approaches that recognize the importance of feedback loops, cross-functional coordination, and the interplay between technological capabilities and market needs. More recent perspectives further extend this view by emphasizing system-level integration, inter-organizational networks, and the growing importance of external stakeholders, including academic institutions, industry partners, and public actors, as reflected in open innovation approaches. Across these models, innovation is generally conceptualized as a structured but non-linear process, involving successive phases of idea generation, selection, development, and implementation, often supported by iterative methodologies and validation practices. In many cases, this process continues beyond initial deployment to include learning, scaling, and adaptation, underscoring the ongoing

and coordinated nature of innovation activities across strategic, technological, and organizational domains.

Within this context, organizational ambidexterity offers a relevant analytical perspective for cybersecurity innovation. It captures the need for firms to simultaneously ensure robust protection of existing systems (exploitation) while continuously experimenting with emerging technologies and approaches (exploration). As Carayannis et al. (2019) emphasize in their concept of "ambidextrous cybersecurity," this dual capability is central to cyber resilience, where security and innovation must evolve in parallel rather than sequentially. This tension is particularly visible in fast-moving digital environments, where organizations are required to integrate security constraints without slowing down innovation cycles. Empirical studies further show that firms continuously oscillate between these two logics depending on project maturity, technological uncertainty, and risk exposure (Zadeh & Jeyaraj, 2022). At the same time, embedding security early in the innovation process can create structural frictions, as highlighted by Schinagl et al. (2022), who examine paradoxical tensions in digital security governance. In their work, ambidexterity is not framed as a mechanism to resolve these tensions, but rather to manage their persistent coexistence. Three key paradoxes are identified: institutionalization versus professionalization, security versus innovation, and mindfulness versus mindlessness. Together, these dimensions underscore that cybersecurity governance operates through the simultaneous presence of opposing logics, which must be continuously balanced rather than eliminated. In this sense, cybersecurity innovation is not only a matter of technological development, but also of organizational design and dynamic capability management.

3. Research question

This research explores the following question: How can cyber ranges be leveraged as experimental environments to foster innovation in cybersecurity and support cybersecurity capacity building?

4. Research design

This research adopts an exploratory qualitative case study combined with an action research approach. Such a design is particularly appropriate for investigating emerging socio-technical infrastructures while simultaneously contributing to their design and evolution. The research is embedded in the ongoing development of a new cyber range environment within a Canadian university, enabling iterative co-design, experimentation, and feedback loops among stakeholders. In addition, one of the researchers is actively involved in the ecosystem surrounding this cyber range, providing privileged access to processes, interactions, and decision-making dynamics. Data sources include academic literature, institutional documents, and strategic reports related to cyber range development.

5. Findings

While Yamin et al. provide a comprehensive model of cyber range functionalities focused on scenario execution, monitoring, and training outcomes, their framework remains limited in capturing how these outputs are transformed into innovation processes and ecosystem-level value. This paper introduces an additional "innovation layer" that

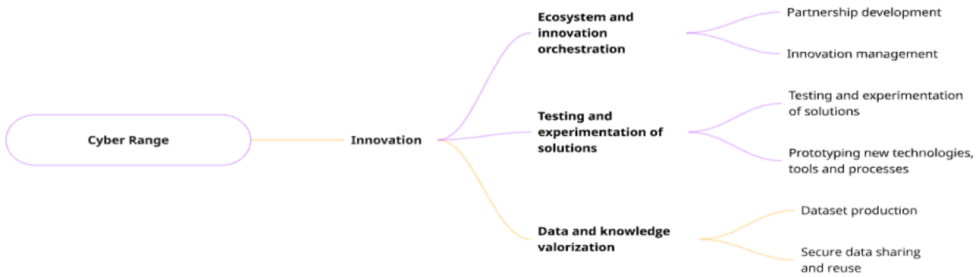
extends the model by integrating mechanisms of data valorization, applied research, and multi-actor innovation orchestration.

Extending the cyber range model with an innovation layer

This paper proposes an extension of the cyber range operational model introduced by Yamin et al. (2020) by integrating an explicit innovation layer that captures how cyber range activities contribute to innovation processes and ecosystem-level value creation. The original model provides a structured representation of the operational core of cyber ranges, organized around six interrelated components: scenario design, environment configuration, monitoring, learning, teaming, and management. These components enable the execution of realistic cyber exercises that combine technical infrastructures with human and organizational dynamics. As a result, cyber ranges generate immediate outputs such as performance assessments, training outcomes, and structured feedback, which are typically mobilized through short-term feedback loops to improve training effectiveness and simulation design.

While this operational perspective is robust, it remains primarily focused on exercise execution and capability development and does not fully account for how the outputs of cyber range activities are transformed into broader innovation processes. This limitation reflects a more general gap in the literature, where cyber ranges are predominantly conceptualized as training or testing infrastructures, with limited integration of innovation management and ecosystem dynamics. To address this limitation, we propose the addition of an innovation layer that extends the model beyond the boundaries of exercise execution. Figure 1 shows that this layer is organized into three complementary, non-overlapping functions that operate on the outputs of the operational core.

Figure. 1. Innovation layer.



The first function, knowledge and data valorization, focuses on transforming simulation outputs into reusable and shareable assets. This includes the production and curation of datasets, the capitalization of exercise traces, and the implementation of secure data-sharing mechanisms. This function enables the conversion of raw operational data into structured knowledge that can inform decision-making, research, and policy development.

The second function, experimentation and applied research, captures the role of cyber ranges as controlled environments for advanced testing and validation. Beyond training, cyber ranges support the prototyping of new technologies, the evaluation of cybersecurity strategies, and the development of proofs of concept. This function positions cyber ranges

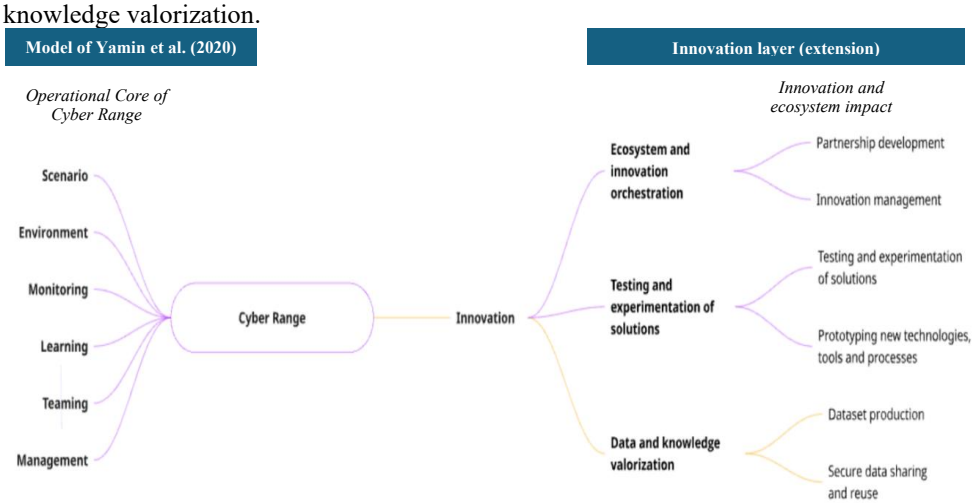
as infrastructures for applied research and innovation, rather than solely as training platforms.

The third function, ecosystem and innovation orchestration, extends the model to a multi-actor context. It encompasses partnership development, co-innovation processes, and innovation management activities such as portfolio prioritization and roadmap development. This function reflects the embedding of cyber ranges within broader innovation ecosystems and highlights their role in coordinating interactions among public authorities, industry, academia, and societal stakeholders.

These three functions collectively enable the transformation of operational outputs into longer-term innovation outcomes, including technological innovations, organizational transformations, governance and policy innovations, and ecosystem-level impacts.

The proposed extension also introduces a distinction between short-term and long-term feedback loops. Short-term loops operate within the operational core to continuously improve scenarios, environments, and training processes. In contrast, long-term loops connect innovation outcomes back to the cyber range, informing the design of new scenarios, the evolution of infrastructures, and the development of new capabilities. This dual-loop structure reflects an iterative and cumulative dynamic consistent with living lab approaches, where cycles of co-design, experimentation, and debriefing progressively shape both learning and innovation trajectories. By integrating this innovation layer, the model shifts from a purely operational perspective to a systemic and innovation-oriented framework. It reconceptualizes cyber ranges as platforms that not only support cybersecurity capacity building, but also enable the co-evolution of technologies, organizations, and ecosystems through structured experimentation, data valorization, and multi-actor coordination. Figure 2 provides a global overview of cyber ranges as innovation platforms.

Figure. 2. Conceptual model of cyber ranges as innovation platforms, integrating the operational core defined by Yamin et al. (2020) with an extended innovation layer encompassing ecosystem orchestration, solution experimentation, and data and knowledge valorization.



Learning mechanisms

From an innovation perspective, cyber ranges generate value through structured learning loops that connect simulation outputs with organizational and strategic decision-making. Three main mechanisms can be identified. The first mechanism is experiential learning amplification. By exposing participants to realistic adversarial conditions, cyber ranges enable forms of tacit knowledge acquisition that are difficult to achieve through traditional training or analytical modelling. This includes situational awareness, coordination under uncertainty, and adaptive decision-making. The second mechanism is cross-organizational learning transfer. When multiple institutions participate in shared scenarios, the learning generated transcends individual organizations and contributes to a broader diffusion of practices. This is particularly relevant in critical infrastructure sectors, where no single actor possesses a complete view of systemic risk. Cyber ranges thus act as intermediaries for distributed knowledge integration. The third mechanism is iterative capability refinement. Repeated exposure to evolving scenarios allows organizations to progressively refine their processes, policies, and technical configurations. Over time, this leads to measurable improvements in cybersecurity maturity, not as a static assessment outcome but as an emergent property of continuous experimentation. These mechanisms suggest that cyber ranges should not be understood as episodic training environments, but as continuous learning infrastructures embedded within innovation ecosystems.

Coordination Mechanism of Cyber Ranges

Beyond their technical and pedagogical functions, cyber ranges operate through a set of coordination mechanisms that are critical for ecosystem performance. The empirical observations from the Canadian case suggest that three governance dimensions are particularly influential. First, scenario governance emerges as a foundational mechanism. Scenarios are not neutral technical artefacts but negotiated representations of threats, priorities, and institutional concerns. Their design requires iterative alignment among stakeholders with different risk perceptions and operational constraints. Over time, scenario governance becomes a mechanism for structuring collective attention, ensuring that exercises reflect both technical realism and strategic relevance. Second, data governance plays a central role in enabling or constraining collaboration. Cyber ranges exercises generate sensitive operational data, including vulnerability patterns, response strategies, and organizational behaviours. The ability to share, anonymize, and re-use this data across institutions determines the extent to which learning can be scaled beyond individual exercises. In practice, data governance becomes a balancing act between confidentiality requirements and collective intelligence generation. Third, participation governance influences ecosystem sustainability. Unlike traditional training environments, to operate as innovation platforms, cyber ranges must rely on sustained engagement from heterogeneous actors, including public agencies, private firms, and academic institutions. Participation is not only a matter of access but also of incentive alignment, including recognition mechanisms, shared value creation, and tangible benefits derived from participation in exercises. These three governance layers collectively shape the emergence of what can be described as “structured learning ecosystems,” where repeated interactions generate cumulative capability development rather than isolated training outcomes. In this sense, governance is not an administrative layer but an active enabler of innovation processes.

6. Contribution

Taken together, the empirical observations and theoretical framing suggest that cybersecurity innovation cannot be fully understood through linear maturity models or isolated infrastructure perspectives. Instead, it emerges from dynamic interactions among technological platforms, organizational actors, and governance structures embedded within multi-level ecosystems. This implies a shift from a capability-centric view of cybersecurity toward a platform-centric view of cybersecurity innovation. In this view, value is not located in individual infrastructures, but in the coordination mechanisms that connect them and enable continuous cycles of experimentation, learning, and adaptation.

This paper contributes to the cybersecurity and innovation literature by proposing an integrated platform-based framework that bridges three previously fragmented strands of research: cybersecurity maturity models, cyber ranges, and innovation ecosystems. First, it extends cybersecurity capacity literature by moving beyond descriptive and assessment-oriented maturity models toward an experimentation-based operationalization logic, where maturity is not only measured but actively developed through iterative simulation and co-learning processes. Second, it advances the cyber ranges literature by reframing these infrastructures not merely as training or simulation environments, but as socio-technical innovation platforms that enable coordination, knowledge production, and institutional alignment across heterogeneous actors. This shifts the analytical focus from technical functionalities to ecosystem-level effects. The paper proposes a conceptual shift: from isolated cybersecurity infrastructures toward a cybersecurity innovation platform architecture, where learning, experimentation, and coordination are structurally embedded rather than externally coordinated.

7. Practical implications

This research offers several actionable implications for policymakers, infrastructure developers, academic institutions, and industry stakeholders involved in cybersecurity capacity building. First, it suggests that cybersecurity investment strategies should move away from fragmented funding of isolated infrastructures (test beds, training platforms, SOC simulators) toward the development of integrated cybersecurity innovation platforms. Such platforms explicitly combine experimentation (test beds), simulation (cyber ranges), and coordination (innovation networks) within a coherent governance structure. Second, for public authorities and policymakers, the framework provides a foundation for designing national or regional cybersecurity capacity-building strategies that are infrastructure-driven rather than program-driven. Instead of treating cyber ranges as educational tools only, they can be positioned as strategic policy instruments for resilience building, cross-sector coordination, and innovation stimulation. Third, for universities and applied research centers, the model highlights the importance of positioning cyber ranges and test beds as shared experimentation infrastructures embedded within innovation ecosystems. This enables research activities to move beyond simulation exercises toward real-world co-design with industry and government partners, strengthening both relevance and impact. Fourth, for industry stakeholders, the framework creates opportunities to engage in pre-competitive experimentation environments, where emerging technologies (e.g., critical infrastructure security solutions, AI-based detection systems, resilience tools) can be tested collaboratively before deployment. This reduces innovation risk while accelerating technology validation cycles. Finally, at the ecosystem level, the integration of cyber ranges within innovation

networks enables the emergence of collective intelligence mechanisms, where simulation outputs, incident scenarios, and learning outcomes are systematically reused across organizations. This creates feedback loops that strengthen both organizational preparedness and system-wide resilience.

This paper set out to examine how cyber ranges can be leveraged beyond their traditional role as training and simulation environments to support cybersecurity innovation and capacity building. By bridging the literature on cybersecurity maturity models, cyber ranges, and innovation ecosystems, the study highlights the limitations of existing approaches that remain largely fragmented and insufficiently oriented toward experimentation and multi-actor coordination.

The main contribution of this research lies in the conceptual extension of the cyber range model proposed by Yamin et al. (2020). By introducing an explicit innovation layer, the paper demonstrates how the outputs of cyber range activities, such as simulation data, performance feedback, and experiential learning, can be transformed into broader innovation processes. This layer, structured around data and knowledge valorization, experimentation and applied research, and ecosystem orchestration, reframes cyber ranges as socio-technical platforms that enable continuous cycles of learning, coordination, and value creation. More broadly, the findings support a shift from a capability-centric view of cybersecurity toward a platform-centric perspective. In this view, cybersecurity capacity is not only a function of technological maturity but emerges from dynamic interactions between infrastructures, actors, and governance mechanisms within innovation ecosystems. Cyber ranges, when embedded in such ecosystems, act as catalysts for collective learning, cross-organizational coordination, and the co-evolution of technologies and practices. From a practical standpoint, this perspective invites policymakers and practitioners to rethink cybersecurity investments by prioritizing integrated innovation platforms rather than isolated infrastructures. It also highlights the strategic role of cyber ranges as policy instruments for fostering resilience, supporting collaborative experimentation, and accelerating the validation and adoption of new cybersecurity solutions. This research nevertheless presents several limitations. The study is based on an exploratory qualitative approach and is grounded in a single case context within the Canadian academic ecosystem, which may limit the generalizability of the findings. In addition, the proposed model remains conceptual and would benefit from further empirical validation across different institutional and geographical contexts. Future research could extend this work by conducting comparative case studies of cyber range ecosystems, developing quantitative indicators to assess innovation outcomes, and exploring the governance and economic models that sustain these platforms over time. Further investigation into federated cyber range architectures and their role in enabling cross-border collaboration also represents a promising avenue for advancing both research and practice.

References

Carayannis, E. G., Grigoroudis, E., Rehman, S. S., & Samarakoon, N. (2019). Ambidextrous cybersecurity: The seven pillars (7Ps) of cyber resilience. IEEE Transactions on Engineering Management, 68(1), 223–234.

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber ranges and testbeds for education, training and research. Applied Sciences, 11(4), 1809.

Davis, J., & Magrath, S. (2013). A survey of cyber ranges and testbeds.

Dhamak, P., Kumar, A., Daftardar, A., & Rane, S. (2025). Development of an innovation ecosystem framework for construction 4.0: A quadruple helix approach. Asian Education and Development Studies, 1–27.

Dooly, Z., Galvin, S., Power, J., Renard, B., & Seldeslachts, U. (2014). IPACSO: Towards developing an innovation framework for ICT innovators in the privacy and cybersecurity markets. In Communications in Computer and Information Science (Vol. 470, pp. 148–158). https://doi.org/10.1007/978-3-319-12574-9_13

Firouzi, A., Dadkhah, S., Maret, S. A., & Ghorbani, A. A. (2025). CIC IIoT Dataset 2025 – DataSense real-time sensor benchmark. Canadian Institute for Cybersecurity, University of New Brunswick. https://www.unb.ca/cic/datasets/iiot-dataset-2025.html

Global Cyber Security Capacity Centre (GCSCC). (2017). Cybersecurity capacity maturity model (CCMM) framework. University of Oxford.

Heierhoff, S., & Reher, A. (2022). Balancing digital innovation and cybersecurity capabilities through organizational ambidexterity: An investigation in the automotive industry.

Li, W., Biennier, F., & Badr, Y. (2012). Digital ecosystems: Challenges and prospects. In Proceedings of the International Conference on Management of Emergent Digital EcoSystems (MEDES 2012) (pp. 117–122). Association for Computing Machinery. https://doi.org/10.1145/2457276.2457297

Miron, W., & Muita, K. (2014). Cybersecurity capability maturity models for providers of critical infrastructure. Technology Innovation Management Review, 4(10), 33–39. https://doi.org/10.22215/timreview/837

Müller, M. (2015). Cybersecurity capacity maturity model (CCMM): National-level assessment framework. University of Oxford, Global Cyber Security Capacity Centre.

Reischl, A., Weber, S., Fischer, S., & Lang-Koetz, C. (2022). Contextual ambidexterity: Tackling the exploitation and exploration dilemma of innovation management in SMEs. International Journal of Innovation and Technology Management, 19(02), 2250006.

Schinagl, S., Shahim, A., & Khapova, S. (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. Computers & Security, 122, 102903.

University of Ottawa, Faculty of Engineering. (2023). Cyber range. https://www.uottawa.ca/faculty-engineering/spaces/cyber-range

Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636.

Zadeh, A., & Jeyaraj, A. (2022). A multistate modeling approach for organizational cybersecurity exploration and exploitation. Decision Support Systems, 162, 113849.

Zhang, Y., et al. (2020). A survey and taxonomy of cyber ranges: Architectures, functionalities, and applications. Computers & Security, 92, 101713.