BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

https://buletinul.unap.ro/index.php/en/

Theoretical Concepts used in building Cyber Resilience

Capt. cdr. Claudiu-Cosmin RADU*

*Command and Staff Faculty, "Carol I" National Defence University
PhD student in Intelligence and National Security
e-mail: radu.claudiu@unap.ro

Abstract

In the context of intensifying cyber threats, cyberspace resilience has become a strategic priority for organizations, governments, and international alliances. Cyber scenarios, in their various forms, provide a controlled environment in which response capabilities to cybersecurity incidents can be tested, trained, and validated. The aim of this paper is to analyze how these scenarios contribute to the development of an organizational culture of resilience, allowing the identification of vulnerabilities, strengthening decision-making under pressure, and proactively adapting to new types of threats. The study explores current practices adopted at the European and international level, revealing how scenario-based exercises support strategic planning, training of technical and operational teams, and interinstitutional cooperation. Moreover, the direct benefits to organizational flexibility and post-incident recovery capacity are also analyzed. Finally, the article formulates a series of recommendations for integrating scenarios into the cyber risk management cycle, highlighting their value not only as training tools but also as fundamental elements in the security architecture of a modern organization.

Keywords:

cyber resilience; cyber scenarios; cyber exercises; wargaming; civil-military collaboration; planning; TTX exercises.

Article info
Received: 14 May 2025; Revised: 6 June 2025; Accepted: 11 June 2025; Available online: 27 June 2025

Citation: Radu, C.C. 2025. "Theoretical Concepts used in building Cyber Resilience". *Bulletin of "Carol I" National Defence University*, 14(2): 267-284. https://doi.org/10.53477/2284-9378-25-29

In a profoundly digitalized society, organizations face an increasingly diverse spectrum of cyber threats that target sensitive data and can severely disrupt the functioning of essential IT systems To deal with these challenges, it is imperative to adopt innovative resilience-building methods that ensure not only resilience to attacks but also rapid and efficient recovery. An accessible and effective solution in this regard is the use of cyber scenarios. These provide organizations with the opportunity to anticipate emerging threats and to build responses tailored to the specific nature of those threats. As the complexity and sophistication of cyberattacks intensify, traditional defence mechanisms become increasingly inadequate. At the same time, the growing number of interconnected devices expands the potential attack surface, exposing critical institutional networks to vulnerabilities that are progressively harder to control. In such circumstances, scenarios become essential tools for testing response capabilities, validating business continuity plans, and optimizing security architecture.

Amidst the profound transformations driven by accelerated digitalization, cyberspace has become a strategic domain, essential for the functioning of critical infrastructures, government services, economic activity, and social communication. The more societies have come to rely on information technologies, the more deeply vulnerable digital systems have become in the face of increasingly complex and hard-to-predict risks. From geopolitically motivated cyberattacks to ransomware campaigns that paralyze hospitals, public administrations, or civilian companies, cyber threats have diversified significantly and evolved into increasingly sophisticated and operationally coordinated forms. These attacks are often orchestrated by specialized groups, whether motivated by economic gain or strategic agendas, and benefit from advanced technical resources, hierarchical structures, and coordinated action methods at the transnational level. Against this backdrop, cyberspace has become a constant source of instability, vulnerability, and systemic risk, affecting critical infrastructures, supply chains, and essential systems of digital governance.

The concept of cyber resilience has gained significant importance in both national and international security strategies. Resilience is no longer seen merely as the capacity to recover from an incident, but rather as a proactive set of measures, competencies, and mechanisms that allow for the anticipation, absorption, adaptation, and systemic improvement of functions affected by disruptive events. According to the European Union Agency for Cybersecurity (ENISA), resilience can be associated with the capacity of cyber systems to withstand, respond to, and recover from an attack or malfunction, while ensuring the continuity of essential services.

One of the most effective methods for testing and improving resilience is the use of cyber scenarios. Based on these scenarios, complex, structured exercises are developed, grounded in either hypothetical situations or real-world case studies, simulating attacks, security breaches, or crisis situations. Through these scenarios, organizations can assess not only the response of technical teams but also managerial capacity, internal and external communication, as well as decision-making processes under stress and informational uncertainty.

Cyber scenarios can take various forms. Some of the most widely used are Tabletop Exercises (TTX), which involve strategic discussions based on hypothetical scenarios and simulated situations. Others include Live-Fire Exercises (LFX), which simulate real attacks in a controlled environment. Cyber Wargaming tests tactical and operational capabilities in a competitive framework. In addition, Capture-the-Flag (CTF) competitions focus on identifying and exploiting vulnerabilities within a simulated environment. All of these formats contribute, in varying degrees depending on the purpose and structure of the exercise, to the development of an organizational culture oriented toward prevention, preparedness, and adaptability.

The importance of scenarios is highlighted by numerous international initiatives, such as the *Locked Shields* exercises organized by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) or the *European Cybersecurity Challenge* coordinated by ENISA, which emphasize interinstitutional cooperation, real-time response evaluation, and collective learning. Essentially, cyber scenarios enable a systemic approach to risk management by contributing to the identification of vulnerabilities, the testing of continuity plans, and the enhancement of resilience, not only technical but also organizational. Thus, they become not merely didactic or technical tools, but true laboratories of cybersecurity. Basically, the future is explored through the lens of cyber scenarios.

Research methodology

The primary aim of this research is to analyze the roles of cyber scenarios and exercises in strengthening and maintaining organizational resilience within cyberspace. The study is conducted within a qualitative, exploratory-analytical framework, specific to the field of cybersecurity, with a focus on documentary and contextual analysis.

The methodology is based on the study of specialized literature, the NATO and EU doctrinal framework, as well as relevant documents in the field of cybersecurity and cyber defence.

Using this methodological approach, the research has achieved the following primary objectives:

1. Reviewing the specialized literature to clarify the theoretical concept of scenarios and cyber scenarios. This stage provides the epistemological foundation of the paper and is based on academic and technical literature, as well as on validated institutional sources (ENISA, NIST, CCDCOE).

2. The literature review on the functions and applicability of cyber scenarios aims to demonstrate that they are not just didactic or operational tools, but essential mechanisms that can be integrated into the contemporary cybersecurity architecture and in the process of building organizational resilience. In support of this demonstration, the analysis is complemented by benchmarking the most commonly used exercise formats: Tabletop Exercises (TTX), Live-Fire Exercises (LFX), Red/Blue Team Exercises and Capture-the-Flag (CTF), which are analyzed in terms of their role in developing cyber capabilities, theoretical and operational readiness, and developing an organizational culture oriented towards deterrence, adaptation and rapid response.

The research employs secondary qualitative methods to analyze data and information from open sources, studies, and specialized reports. This methodological choice is justified by the multidimensional nature of the subject, as well as by the objective of providing an integrative analytical framework with practical applicability across institutional, military, and civilian environments.

Multiple types of scenarios and exercises applied in national and international contexts were analyzed, with the goal of highlighting their impact on the development of cyber resilience. The analysis was guided by operational criteria, assessing the practical relevance of each exercise format and its alignment with institutional defence and response objectives. The inherent limitations of qualitative research, such as the lack of validation through quantitative empirical data, do not undermine the practical value of the conclusions, as the approach focuses on identifying best practices, lessons learned, and strategic directions for strengthening cybersecurity architecture through structured scenarios and exercises. Moreover, the adopted methodology aims to support the central argument that cyber scenarios and exercises are not merely training tools, but strategic components of cyber resilience that can directly enhance an organization's ability to prevent, respond to, and recover from emerging cyber threats.

1. Literature review on the theoretical concept of scenario

Scenarios should not be confused with forecasts or predictions of the future; they are hypothetical but plausible situations designed to test systems' reactions and to train personnel specialized in cyber defence and security. By their nature, scenarios provide a controlled framework in which crisis events can be simulated, enabling the evaluation of response capabilities, adaptability, and coordination among the actors involved. Furthermore, scenarios may serve as a valuable resource in the planning and decision-making process for military commanders, offering operational and strategic benchmarks based on lessons learned from previous exercises or wargames.

One of the core objectives of using scenarios is to reduce operational uncertainty and, implicitly, the number of unforeseen incidents. This has a direct impact on the level of stress and pressure placed on specialists who, through training, develop operational reflexes that can be triggered automatically in real-life situations. Thus, even if a cyber incident cannot be avoided, the ability to detect and respond to it in minimal time represents a major strategic advantage. In this regard, **the effectiveness of scenarios** is measured not only by the fidelity of the simulation but also by their capacity to generate real changes in organizational behavior: reducing reaction times, increasing team cohesion, refining decision-making processes, and, not least, strengthening trust in one's own defence mechanisms. The more a scenario is adapted to the organization's specific context and rigorously constructed, the higher its formative yield, directly contributing to the enhancement of cyber resilience.

In recent years, an increasing number of studies have focused on exercises and wargames from a military perspective. As outlined in previous sections, the purpose of this article is to analyze the importance of scenarios in improving cybersecurity. This approach may be both military and civilian. Moreover, joint exercises conducted by member states of alliances and international organizations, along with partnerships between civilian and military structures, directly contribute to strengthening cyber resilience. The synergistic effect arises from training specialists in various operational contexts, both simulated and realistic. Although they may seem abstract at first glance, these scenarios significantly reduce uncertainties, providing essential support in the institutional preparedness and response process. In addition, they shorten the response time in the event that hypothetical situations materialize.

The scenario, composed of multiple hypotheses, is based on a presumed attack that tests operational and legal procedures, as well as information exchange protocols with alliance partners. Participants collaborate to identify the threat as quickly as possible and to limit its impact on the national systems of each state involved. It is important to emphasize the synergy of collaboration between military and civilian institutions. Moreover, joint exercises among allied states and cooperation between civil and military institutions are essential for optimizing resilience in the face of cyber threats. Cyberattack scenarios should test not only operational but also legal procedures (Nucă 2024), ensuring that all involved parties can react efficiently and in a coordinated manner. These exercises contribute to specialist training, developing both practical and theoretical skills essential for managing exceptional situations in cyberspace. Furthermore, international collaboration within these exercises helps build trust among states and establish common standards for responding to cyber threats. Additionally, cybersecurity and cyber governance are fundamental elements for ensuring the sustainable functioning and durable development of any organization or society (Popa 2015, 22).

If we strictly refer to the similarity of cyber scenarios with military scenarios, some experts argue that the scenario is closely linked to the concept of a contingency plan, as it involves identifying and establishing a specific course of action applicable under well-defined circumstances (Petrescu 2017, 62). In planning practice, commanders prioritize identifying the most probable threat or the most dangerous course of action by the adversary, as well as formulating an appropriate response to the respective situation. The efficiency of the decision-making process is enhanced by using scenarios within wargames, allowing planning efforts to focus on formulating operational solutions adapted to various hypotheses regarding the evolution of tactical or strategic situations. Thus, the risk of being surprised by the enemy is reduced through a clearer anticipation of maneuver possibilities and alternative courses of action (Joint Chiefs of Staff 2020, III-4).

Currently, the scenario has become an essential tool in the planning process of military actions, offering a coherent and structured methodology for analyzing possible future situations. This approach helps clarify the inherent uncertainties of the operational environment and supports decision-making by outlining plausible perspectives on the evolution of the situation (Schoemaker 1995). A complete scenario should include a description of the initial state, the articulation of a possible or desired end state, and a logical sequence of events leading from the current to the final state, provided that certain determining factors are met (Van der Heijden 2005, 152). In order to be effective, a scenario must be sufficiently coherent, transparent, and logical, so that it can be analyzed and evaluated in relation to the formulated hypotheses (Godet 2006).

It is essential to emphasize that scenarios are not intended to eliminate uncertainty completely, nor to predict future developments with precision. They do not forecast the future, but delineate a reference framework that defines its boundaries, thereby enabling a more nuanced understanding of potential operational developments (Wright and Goodwin 2009). Scenarios have been defined over time in different ways and from different perspectives. However, one of the most well-known scenario theorists, Philip van Notten, defines a scenario as *"a coherent and comprehensive description of an alternative and hypothetical future situation, reflecting different perspectives on the past, present and possible future developments, and serving as a basis for further decisions and actions"* (van Notten 2005, 20). In his paper, van Notten synthesizes several academic and applied perspectives on scenarios, highlighting that the term has at least four major meanings: as a sensitivity analysis tool, a contingency plan, a strategic decision-making instrument, and an exploratory method of learning and anticipation. The latter meaning is central in contemporary research and is supported by an emerging consensus in the specialized literature: scenarios are not predictions but plausible and structured representations of possible alternative futures (van Notten 2005, 18).

The practical relevance of scenarios derives not only from their descriptive value but also from their ability to influence decisions and stimulate strategic thinking. Thus, Postma emphasizes internal logic by stating that *"scenarios are descriptions of coherent pictures of future events and situations"* (Postma and Vijverberg 1995), while Fahey and Randall emphasize probability: *"scenarios are plausible descriptive narratives of alternative projections of a specific part of the future"* (Fahey and Randall 1998). Other authors, such as Van Asselt and Rotmans, propose an integrative view, which includes not only the future, but also reinterpretations of the past and the present: *"scenarios are narrative descriptions of alternative images of the future, constructed based on mental and conceptual models that reflect different perspectives on the past, present and future"* (Rotmans 1998).

Scenarios are analytical constructs designed to outline a variety of future conditions, including opportunities, threats, and potential obstacles that can significantly influence the achievement of desired objectives. They guide the interpretation and approach to uncertain situations while providing a reference framework for decision-making and the selection of courses of action. A defining attribute of scenarios is their conceptual flexibility, which allows for the integration of a wide range of development directions. Each direction is based on a specific set of values associated with determining factors, whose interactions give the scenario operational coherence and relevance. The constituent elements of the scenario are interconnected through logical and functional relationships, built on methods, principles, procedures, and rules that together form an integrated normative system. This system supports a structured deployment of actions and contributes to shaping a strategic response adapted to the complexity of the analyzed environment.

Scenario definitions converge toward a complex and multidimensional vision, in which a scenario is simultaneously: a logical narrative about possibilities, a decision-making and learning tool, a framework for strategy testing, and a conceptual map of future uncertainties and trends. This integrated approach places the scenario at the center of the strategic resilience and anticipatory planning process in the face of systemic uncertainties.

In the context of cybersecurity, regardless of whether scenarios are based on real, fictional, or combined foundations, they must meet a set of essential requirements. First, they must be credible, meaning they should project possible situations in cyberspace, taking into account the complexity of digital infrastructure, informational interdependencies, and potential attack vectors. A realistic scenario enables a realistic assessment of cybersecurity capabilities and response procedures without altering the relevant parameters of the operational environment or the nature of the simulated threats. An essential condition directly linked to realism is the objectivity of the information used in constructing the scenario. It is crucial that the cyber environment, including triggering events, involved actors, exploited vulnerabilities, and institutional responses, be described clearly and precisely. The presentation should be free from ambiguity, redundancy, or excessive detail, as this could have a negative impact on understanding or practical application. However, the cyber scenario must be complete, objective, and well-structured, which means that all defensive and response skills must be integrated into a clear operational framework. This involves modelling both the *technical* aspects (networks, systems, data flows) as well as the *organizational and legal* aspects (decision flows, communication, and interinstitutional collaboration following existing legislation).

Another essential requirement is flexibility. The scenario must allow for real or simulated testing, so as to faithfully reflect the dynamics of cyber incidents and permit the adjustment of the event sequence based on observed reactions. To determine the strengths and weaknesses of the given cyber system, validation can be carried out through practical exercises or digital modeling.

Finally, an essential characteristic is coherence. The scenario must be built on a clear and logical line, describing the operational situation fluently and coherently, and enabling the actors involved in crisis management and decision-making to integrate effectively. It should address the description of the situation in a structured and articulate manner, with information presented in close correlation, efficiently placing the target structure within the operational environment necessary for achieving objectives (Petrescu 2017, 66). Such a structure ensures the scenario's relevance for enhancing responsiveness, adaptability, and resilience to emerging cyber threats.

Scenarios are fundamental methodological tools used to explore uncertainties about future developments. As defined by Kosow and Gaßner, a scenario is *"a plausible description of a future situation, including development paths that could lead to that situation"* (Kosow and Gaßner 2008). Scenarios should not be confused with predictions or forecasts. They are hypothetical constructs intended to provide a framework for systematic reflection on the determinants and interdependencies that shape possible futures.

According to the same authors, scenarios serve several essential functions (Kosow and Gaßner 2008).

a) Exploring existing knowledge and identifying information gaps;
b) Facilitating communication between different actors involved in the decision-making process;
c) Formulating strategic objectives under uncertainty;
d) Support planning and decision-making by anticipating possible changes and challenges.

The practical utility of cyber scenarios manifests across multiple dimensions, most notably in the support they offer for decision-making, the training of specialized forces, and the testing of interinstitutional collaboration procedures. By simulating complex incidents, scenarios enable decision-makers to anticipate adversarial behavior patterns, identify critical points in IT infrastructure, and rapidly adjust cyber incident response strategies based on threat evolution.

In terms of professional training, scenarios significantly contribute to the development of tactical and strategic skills among personnel in cybersecurity structures. Through controlled exposure to crisis situations, specialists learn to react effectively under pressure, manage contradictory information flows, and collaborate in real-time with internal and international experts. Additionally, scenarios foster critical thinking, anticipatory analysis skills, and an understanding of the interdependencies between components of a complex digital ecosystem.

At the institutional level, the implementation of scenarios facilitates the harmonization of doctrines and action protocols between military, civilian, public, and private structures. Cyber scenario-based exercises provide an effective platform for testing interoperability, verifying the compatibility of legal procedures, and identifying gaps in alerting, communication, and response mechanisms. Thus, scenarios become key tools in strengthening cyber resilience at both national and international levels within alliances.

The importance of using scenarios becomes especially evident in domains characterized by high uncertainty, where rapid or unforeseen changes can have major impacts on security, the economy, or the social environment (Kosow and Gaßner 2008). Furthermore, in a strategic environment marked by uncertainties and asymmetric and hybrid threats, an organization's ability to effectively integrate lessons learned from scenarios is essential for the continuous improvement of its security architecture. Therefore, scenarios should not be limited to isolated exercises but should be integrated as elements of a complex cycle of planning, learning, adjustment, and refinement of cyber defence.

2. Cyber scenarios - fundamental elements in cyber exercises

A cyber scenario can be interesting, unique, and specifically designed to address weaknesses or ambiguities in a *cyber incident response plan*. Moreover, such a scenario may constitute an intentional stress test for systems considered critical or those ensuring institutions' cybersecurity or even national security. The goal is to verify functionality under normal conditions and evaluate how the system reacts when deliberately pushed to its operational limits. Only in this way can vulnerabilities be identified and strengthened before being exploited in a real attack. In this process, the freedom to analyze even the most unlikely scenarios is key to an efficient and adaptive anticipation process. What happens if an attacker discovers a technical vulnerability and combines it with human error? Or if a seemingly minor breach opens the door to a series of incidents? Significant past cases have shown that extreme events, considered *pure bad luck* or *theoretically impossible*, often materialize in the cyber world. Through simulated exercises, organizations not only anticipate failures but also rehearse their responses. Each scenario is a lesson that transforms today's vulnerabilities into tomorrow's resilience.

Identifying these gaps is critical for enhancing our understanding of how scenario planning can be effectively incorporated into cyber resilience strategies. This integration ultimately leads to a stronger defence against evolving threats. Addressing these gaps will not only enhance theoretical frameworks but also offer practical insights for organizations looking to efficiently implement scenario planning in their cybersecurity practices.

Cybersecurity scenarios are essential tools for anticipating, modeling, and analyzing risks associated with the digital environment. They aid in understanding vulnerabilities and provide a methodological foundation for developing strategic and operational training exercises. As cyber threats have become more complex, the need to standardize various forms of training and testing has become increasingly apparent. Today, several types of cyber exercises are recognized, each adapted to different risks and training needs. These include Cyber Wargaming, Tabletop Exercises (TTX), Live-Fire Exercises (LFX), Red Team/Blue Team Exercises, Cyber Range Exercises, and Capture the Flag (CTF) Exercises, among others.

Cyber Wargaming is an analytical exercise akin to operational simulations or *tabletop* exercises, designed to replicate the dynamics of cyber conflicts in a controlled environment. The concept has its roots in military tradition, where wargames were used to train commanders and test battle strategies. As cyber threats have evolved and become more sophisticated, military methodologies have been adapted to the digital landscape. This adaptation allows for the assessment of an organization's security posture, decision-making processes, and defence strategies against cyberattacks. The connection between military wargaming and cyber wargaming highlights the importance of a structured and rigorous approach to modern cybersecurity. By conducting these exercises, organizations can anticipate potential surprises, identify hidden vulnerabilities, and strengthen their incident response procedures. At the same time, using its multidimensional approach - technological, procedural, and human - Cyber Wargaming provides an integrated framework for testing and optimizing security mechanisms under simulated crisis conditions. This approach allows not only the detection of technical or organizational weaknesses, but also the training of decision-makers and operational staff to respond effectively under pressure, in tense contexts or sophisticated attacks.

The essential purpose of cyber wargaming is to evaluate an organization's preparedness for major cyber incidents, test response capabilities, improve decision-making processes, and strengthen overall resilience to emerging cyber threats. By simulating conflicts in a safe environment, cyber wargaming contributes to developing more effective security policies, reducing reaction times during crises, and reinforcing interdepartmental cooperation within organizations.

This methodology is an essential tool for any organization looking to sustainably enhance its cybersecurity posture and improve its ability to manage attacks in a dynamic and adversarial digital environment. The use of wargames in the cyber domain still requires further development to realize its full potential. While many countries' armed forces recognize the implications of cyber threats for national security and regularly conduct cyber wargames at the national level or in collaboration with allies, the private and civilian sectors are still in the early stages of adopting these practices. Cyber wargames differ from traditional cybersecurity measures such as technical assessments, penetration tests, or vulnerability scans, although they can be integrated when necessary. Beyond these conventional methods, cyber wargames offer a comprehensive evaluation of an organization's cybersecurity strategy by realistically simulating a cyber conflict. These exercises prepare both civilian and military organizations to make rapid decisions in unforeseen situations, such as shutting down parts of a network to contain damage. Cyber wargames thus contribute not only to the identification of technical vulnerabilities but also to the overall assessment of defence strategies, response mechanisms, professional skills, and resilience to a cyberattack. Designing and conducting controlled cyber warfare is a complex process that requires the involvement of experienced professionals and the use of state-of-the-art technologies. Since the goal of a cyber wargame is to provide participants with a near-real-time experience, scenario planners need to be familiar with both recent attack techniques and up-to-date defence methods.

Any organization, company, or institution can conduct independent wargames if it has the necessary technical infrastructure and qualified personnel. If these resources are lacking, it is advisable to outsource to specialized experts. The first step in planning and organizing a cyber war game is to clarify the scope and objectives. The scope can range from testing isolated tactics to operational or strategic assessment of the organization's cybersecurity system. The duration of the exercise, the level of participants, and the degree of complexity are determined according to the objectives and expectations initially defined. Conducting exercises in real environments carries additional risks, which is why it is recommended to use a Cyber Range platform. This solution allows for a realistic simulation of the organization's digital environments while minimizing the risk of interfering with actual operations systems and providing a learning experience under conditions close to reality (Abbas 2024).

By simulating near-realistic cyber incidents, Cyber Wargaming enables organizations to detect weaknesses, validate the effectiveness of security policies, update operational procedures, and prepare a coordinated response in critical situations. It also supports the development of an integrated cyber strategy by combining technical, procedural, and human elements to prevent costly surprises and manage emerging threats more effectively.

Another type of exercise using customized cyber scenarios for training is the Cyber Tabletop Exercise (TTX). This involves an interactive role-play simulation in which participants respond to hypothetical situations developed and presented by one or more scenario facilitators. Typically, they assume their actual roles within the organization, but depending on the exercise's needs, they may also play other roles to cover critical missing functions. Facilitators or scenario coordinators gradually introduce narrative elements that, although seemingly trivial at first, often conceal significant issues or systemic dysfunction indicators. Intentionally, contradictory information may be inserted to test the team's ability to critically analyze, prioritize risks, and maintain decision-making coherence in uncertain situations. This type of exercise is designed to support organizations in analyzing risk scenarios and preparing for potential cyber threats. Being relatively easy to implement, these exercises provide an efficient and flexible tool for evaluating cybersecurity (Center for Internet Security 2025). Unlike operational exercises, a TTX does not aim to achieve perfect individual performance but focuses on practicing cooperation, identifying procedural vulnerabilities, and strengthening collective response capacity under normal conditions, when there is time to correct deficiencies. In a real incident, this time is no longer available, making such exercises essential for effective team preparation in a controlled yet realistic and challenging environment. Besides its formative value, this type of exercise is an effective and convenient tool for rapidly testing an organization's capacity to respond to cybersecurity incidents according to its own plans and procedures. Since there is no time to correct internal deficiencies during a real incident, such exercises become essential for team preparedness in a controlled but demanding environment. Furthermore, team coordination can no longer be optimized, which is why these exercises are essential in peacetime (Cybersecurity and Infrastructure Security Agency 2025).

Live Fire Exercise (LFX) is an advanced form of cybersecurity training in which participants react in real time to simulated attacks, conducted in a highly realistic, controlled technical environment. The largest and most sophisticated demonstration of this type of exercise is *Locked Shields*, organized annually by the NATO Centre of Excellence for Cyber Defence Cooperation, which brings together hundreds of experts from member and partner states. The purpose of this exercise is to test, in a simulated but operationally realistic environment, the security and defence capabilities of IT infrastructures and critical systems against highly complex cyberattacks. It also aims to strengthen the practical training of cybersecurity professionals by involving them in real-time activities within broad, interinstitutional, and multidisciplinary teams. The scenario is complex, designed to train participants in protecting governmental, military, and national critical infrastructures from multiple cyberattacks. Among the simulated infrastructures are banking systems, water, electricity, and natural gas distribution networks, satellite communication systems, and 5G networks (Ministry of National Defense 2023).

The exercise is structured on the Red Team vs. Blue Team model, where rapid reaction teams from NATO member states and partner countries are tasked with defending, in real-time, a fictional country subjected to a large-scale cyberattack. In addition to the purely technical and operational components, the exercise includes essential aspects of strategic decision-making, legal elements, public communication, and interinstitutional coordination. Thus, Locked Shields plays a vital role in refining operational competencies and strengthening international cooperation mechanisms in the cyber domain (The NATO Cooperative Cyber Defence Centre of Excellence 2022). It also provides an optimal framework for testing and refining response procedures to cyber incidents under intensely simulated crisis conditions, allowing for comparative performance evaluations of participating teams. The scenario

realistically and pragmatically reflects the complexity of modern cyber defence and the need for coordinated, integrated, and well-organized allied responses.
A distinctive element of the Locked Shields exercise is its holistic nature and performance-oriented approach. Furthermore, it provides a platform for testing defence procedures, interinstitutional collaboration, and developing innovative solutions for military, civilian, and academic environments. Participating teams were challenged to operate outside their professional comfort zones through surprise technical scenarios. In addition to strengthening their own capabilities, participants directly contribute to enhancing the content of the Locked Shields exercise through applied feedback on legal, strategic communication, and operational components.

The significance of this annual exercise lies not only in its technical complexity but also in the emphasis placed on transnational and multidisciplinary collaboration, the simultaneous training of experts from sectors such as defence, industry, and academia, and continuous adaptation to emerging technological challenges. Locked Shields demonstrates that effective preparation for cyber warfare requires a realistic, integrative, and anticipatory approach in which complex scenarios, interoperability, and strategic analysis are as crucial as protecting digital infrastructure itself (The NATO Cooperative Cyber Defence Centre of Excellence 2025). Moreover, multinational cyber exercises hold a central place in the strategic architecture for enhancing allied cooperation and promoting the exchange of best practices in cybersecurity. They provide a valuable operational framework in which allies can test, in a simulated but realistic environment, the interoperability and effectiveness of shared procedures, thereby increasing collective response capacity to real incidents. Additionally, by integrating civilian entities such as universities, research institutes, and private sector companies, these exercises help expand cyber defence capabilities beyond the strictly military domain. This civil-military cooperation enhances adaptability to emerging technological challenges and fosters a comprehensive approach to cyber risks based on complementary resources and competencies. In a global environment characterized by technological interdependencies and increasing digital vulnerabilities, such initiatives are indispensable for maintaining strategic superiority in cyberspace. They not only strengthen the national capacities of each member state but also lay the foundation for a coherent, agile, and effective collective defence. Furthermore, through their anticipatory and deterrent nature, these exercises contribute to reinforcing NATO's defensive posture, enabling coordinated responses to emerging threats and robust protection of critical infrastructures across the Euro-Atlantic area.

According to the definition provided by the National Institute of Standards and Technology (NIST) and cited by several experts, a *Cyber Range* can be *"an interactive, simulated representation of an organization's networks, systems, applications, and tools connected to an environment that simulates the real internet. They provide a safe and legal space for acquiring practical cyber skills, developing IT products, and testing* *security posture*" (Chouliaras, Kittes, et al. 2021). The scenario is identified as one of the central pillars of a modern cyber range exercise. It plays a crucial role in shaping the exercises and generating relevant situations. Scenarios enable the introduction of realistic events with varying network typologies, automated user behaviors, and simulated attacks, contributing to the realism and complexity of the exercise. The purpose may vary, with the main objectives being (Chouliaras, Kittes, et al. 2021):

- *Research* - testing tools, methods, and components.
- *Education and training* - developing practical skills in cybersecurity.
- *Exercises and competitions* - running simulations, *Capture the Flag*, *Red vs. Blue Team,* or *Crisis Management Exercises*.

Unlike the other types of exercises, *Capture-the-Flag (CTF)* is a competitive cybersecurity exercise in which participants must identify and exploit cyber vulnerabilities to locate and extract a specific target, called a *flag*, usually represented by a hidden data fragment. These exercises simulate realistic attack and defence conditions, involving activities such as network analysis, reverse engineering, cryptography, or digital forensics (Rochford 2024). The main goals of these exercises are the following: on the one hand, they contribute significantly to the development of the technical and strategic skills of the participants, especially among talented young people or professional teams; on the other hand, they promote cybersecurity education and facilitate the formation of collaborative networks between organizations, institutions and experts from different fields. In particular, the "Attack-Defence" format is valuable for professional training, as it simulates real-life conditions in which teams must simultaneously defend their systems and attack the adversary's infrastructure (European Union Agency for Cybersecurity 2021). By their competitive nature, this type of exercise provides a dynamic training framework (Rochford 2024) for:

a) Modeling cyber threats;
b) Threat hunting;
c) Risk analysis;
d) Incident response;
e) Data collection;
f) Detection effectiveness;
g) Forensic evidence collection;
h) Critical Infrastructure Protection.

Regarding the role of the scenario in a CTF exercise, we could say it is essential for creating a realistic and coherent framework in which participants can test their knowledge and responses to cyber incidents. Scenarios may be inspired by real attacks or artificially constructed, but must be relevant, stimulating, and tailored to the participants' level. The scenario determines the nature of the challenges, tactical objectives, technologies used, and the complexity of the exercise. Thus, the scenario functions as the central element of the exercise, providing coherence in training within an operational context. CTFs are considered effective tools both for individual training and for operational preparation of teams responsible for cybersecurity, depending on the chosen format.

The types of exercises presented above demonstrate how the practice of cyber wargaming is used in various contexts and sectors, both military and civilian, to improve defence capabilities, raise awareness, and build resilience against increasingly sophisticated and persistent cyber threats. Moreover, they can serve as essential tools for preparing and testing defence capabilities against cyberattacks. These exercises simulate realistic attack scenarios, allowing participants to develop practical skills, enhance incident response strategies, and strengthen organizational resilience to cyberattacks.

Conclusions

Cyber resilience can no longer be conceived outside of dynamic and proactive preparedness mechanisms, where cyber scenarios play a fundamental role. In a digital landscape characterized by uncertainty, persistent aggression, and technological complexity, an organization's ability to respond effectively to incidents depends on the maturity with which it periodically tests and validates its own defence capabilities. Cyber scenarios have proven to be among the most effective tools for achieving this objective.

Scenarios, due to their simulated nature, allow for the replication of real or hypothetical contexts that are customized to fit the specific needs of an organization, the types of infrastructures it manages, and the expected level of threats. The scenarios created during cyber exercises - whether they are tabletop exercises (TTXs) focused on strategic decision-making or live-fire exercises (LFXs) that mimic real-time attacks - foster an accelerated learning environment. This enables teams to gain a better understanding of the strengths and weaknesses of their systems. Additionally, scenarios promote integrated learning, both technical and organizational, by bringing together IT experts, decision-makers, legal specialists, and security system managers in a collaborative setting. Another major advantage is the scenarios' capacity to support a collaborative approach to resilience. International exercises, such as Locked Shields or the International Cybersecurity Challenge, emphasize cross-border cooperation and the testing of interoperability mechanisms among agencies, states, and organizations. This collaborative character generates essential synergies for rapid and coordinated responses in the event of large-scale cyberattacks. At the same time, scenarios contribute to the standardization of best practices and the strengthening of the regulatory framework in the field of cybersecurity. In terms of educational dimension, CTFs and applied exercises conducted on cyber ranges are essential tools for training the new generation of experts. They allow not only the testing of technical knowledge but also the development of transversal competencies such as critical thinking, adaptability, and crisis management skills during critical moments. The integration of these formats into national training programs and European initiatives like the Digital Skills Agenda (Misheva 2021) is a necessary step in strengthening the collective defence capability.

However, the practice of devising scenarios does have its limits. In the absence of a well-defined methodological framework, they can become formal, repetitive activities with little impact on learning processes. Additionally, scenarios not adapted to organizational specifics risk generating false results or creating a false sense of security. Therefore, the design and evaluation of exercises must be conducted by professionals using tested methodologies, such as those proposed by ENISA, NIST, or CCDCOE.

Another important aspect is the integration of scenario results into security policies and strategies. Lessons learned must be documented, analyzed, and transformed into concrete measures to strengthen the defence posture. This integration requires a formalized feedback process and an organizational culture open to continuous learning. Only in this way do scenarios become true governance tools in cybersecurity.

Cyber scenarios are more than simple simulation exercises; they constitute a complex framework for training, evaluation, collaboration, and transformation. When implemented strategically, with rigor and vision, they can become the backbone of resilience-building efforts in the digital domain. In a world where cyberattacks are no longer a possibility but a statistical certainty, investing in such tools is not a luxury but an imperative necessity for digital survival and informational sovereignty.

All these types of cyber exercises or simulations mentioned in this study are essential methods of operational training, contributing to the development of the response capacity to real cyberattacks. At the same time, they offer a controlled framework for testing offensive tactics to evaluate defensive capability and specific preparedness. Held annually or even multi-annually, these exercises bring together member and partner states in joint scenarios, becoming not only a means of enhancing interoperability but also a modern form of active deterrence in a climate marked by persistent and asymmetric cyber threats.

References

Abbas, Nasim. 2024. „Cyber Wargames and Cyber Security." *Privia Security* pp. 3–8.

Center for Internet Security. 2025. *Tabletop Exercises (TTX).* https://www.cisecurity.org/ms-isac/tabletop-exercises-ttx.

Chouliaras, Nestoras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. 2021. "Cyber Ranges and TestBeds for Education, Training, and Research." *Applied Sciences* 11 (4): 1809. https://doi.org/10.3390/app11041809.

Chouliaras, Nestoras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. 2021. "Cyber Ranges and TestBeds for Education, Training, and Research." *Applied Sciences* 11 (4): 1809. https://doi.org/10.3390/app11041809.

Cybersecurity and Infrastructure Security Agency. 2025. *CISA Tabletop Exercise Packages.* https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.

___. 2025. „Cybersecurity Tabletop Exercise Tips ." https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf.

European Union Agency for Cybersecurity. 2021. *ENISA Threat Landscape 2021.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

Fahey, Liam, and Robert M. Randall. 1998. "What is Scenario Learning?" *Learning from the Future* pp. 3–21.

Godet, Michel. 2006. „Creating Futures: Scenario Planning as a Strategic Management Tool." *Economica* 39–45.

Joint Chiefs of Staff. 2020. *JP 5-0, Joint Planning.* https://irp.fas.org/doddir/dod/jp5_0.pdf.

Kosow, Hannah, and Robert Gaßner. 2008. *Methoden der Zukunfts- und Szenarioanalyse: Überblick, Bewertung und Auswahlkriterien.* research report, Bonn: Deutsches Institut für Entwicklungspolitik gGmbH.

Ministry of National Defense. 2023. *Specialiști din MApN, la exercițiul de apărare cibernetică Locked Shields 2023.* https://www.mapn.ro/cpresa/17900_Specialişti-din-MApN,-la-exerciţiul-de-aparare-cibernetica-Locked-Shields-2023.

Misheva, Galina. 2021. *European Skills Agenda.* https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/european-skills-agenda.

Nucă, Nicoleta. 2024. *Aspecte ligislative privind războiul cibernetic sau cyberwarfare. Efectele și răspunderea penală.* https://www.juridice.ro/733058/aspecte-legislative-privind-razboiul-cibernetic-sau-cyberwarfare-efectele-si-raspunderea-penala.html.

Petrescu, Dan Lucian. 2017. *Modele conceptuale avansate pentru proiectarea și realizarea scenariilor militare în contextul mediului operațional de tip hibrid.* București: Universitatea Naţională De Apărare „Carol I" .

Popa, Iulian Florentin. 2015. *Securitatea și guvernanța spațiului cibernetic contemporan.* Cluj-Napoca: Universitatea Babeş-Bolyai .

Postma, Theodorus J.B.M., and A. M.M. Vijverberg. 1995. "Toekomstverkenning met scenario's. Een hulpmiddel bij de bepaling van de strategische koers van een organisatie." *Bedrijfskunde: Tijdschrift voor Modern Management* 67 (2): 13-20.

Rochford, Oliver. 2024. *What is Capture the Flag in Cybersecurity? + Effective Exercises.* https://www.securonix.com/blog/capture-the-flag-in-cybersecurity/.

Rotmans, Jan. 1998. "Methods for IA: The Challenges and Opportunities Ahead." *Environmental Modelling and Assessment* 3 (3): 155–179.

Schoemaker, Paul J.H. 1995. „Scenario Planning: A Tool for Strategic Thinking." *MIT Sloan Management Review* 36 (2): 25–40.

The NATO Cooperative Cyber Defence Centre of Excellence. 2022. *Locked Shields.* https://ccdcoe.org/locked-shields/.

___. 2025. *NATO CCDCOE expands cyber defence cooperation ahead of the worlds largest live-fire exercise.* https://www.ccdcoe.org/news/2025/nato-ccdcoe-expands-cyber-defence-cooperation-ahead-of-the-worlds-largest-live-fire-exercise/.

Van der Heijden, Kees. 2005. *Scenarios: The Art of Strategic Conversation.* 2nd ed. New York: John Wiley & Sons.

van Notten, Philip W. F. 2005. „Writing on the wall : scenario development in times of discontinuity." Amsterdam: Thela Thesis & Dissertation. van Notten, P. W. F., Writing on the wall: scenario development in times of discontinuity. [Doctoral Thesis, Maastricht University], Thela Thesis & Dissertation.com, Amsterdam, 2005, pag. 20. https://doi.org/10.26481/dis.20050408pn.

Wright, George , and Paul Goodwin. 2009. "Decision Making and Planning Under Low Levels of Predictability: Enhancing the Scenario Method." *International Journal of Forecasting* 25 (4): 813–825. doi:10.1016/j.ijforecast.2009.05.019.