BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”
https://buletinul.unap.ro

Concepte teoretice utilizate în consolidarea rezilienței cibernetice

Theoretical concepts used in building cyber resilience

Cpt. cdor instr. avs. drd. Claudiu-Cosmin RADU*
*Facultatea de comandă și stat major, Universitatea Națională de Apărare „Carol I”
e-mail:radu.claudiu@unap.ro

Abstract

În contextul intensificării amenințărilor cibernetice, reziliența în spațiul cibernetic a devenit o prioritate strategică pentru organizații, guverne și alianțe internaționale. Scenariile cibernetice, în diversele lor forme, oferă un cadru controlat în care se pot testa, antrena și valida capacitățile de răspuns în fața unor incidente de securitate cibernetică. Scopul prezentei lucrări este de a analiza modul în care aceste scenarii contribuie la dezvoltarea unei culturi organizaționale a rezilienței, permițând identificarea vulnerabilităților, consolidarea proceselor decizionale sub presiune și adaptarea proactivă la noi tipuri de amenințări. Studiul explorează practicile actuale adoptate la nivel european și internațional, relevând modul în care exercițiile bazate pe scenarii susțin planificarea strategică, antrenarea echipelor tehnice și operaționale și cooperarea interinstituțională. De asemenea, sunt analizate beneficiile directe asupra flexibilității organizaționale și capacității de recuperare postincident. În final, articolul formulează o serie de recomandări privind integrarea scenariilor în ciclul de management al riscurilor cibernetice, subliniind valoarea acestora nu doar ca instrumente de pregătire, ci și ca elemente fundamentale în arhitectura de securitate a unei organizații moderne.

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.

Cuvinte-cheie:
rezilienţă cibernetică; scenarii cibernetice; exerciții cibernetice; wargaming; colaborare civil-militară; planificare; exerciții de tip TTX.

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

Info articol
Primit: 14 mai 2025; Evaluat: 6 iunie 2025; Acceptat: 11 iunie 2025; Disponibil online: ? iunie 2025
Citare: Radu, C.C. 2025. „Concepte teoretice utilizate în consolidarea rezilienței cibernetice”
Buletinul Universității Naționale de Apărare „Carol I”. 14(2): 51-68. https://doi.org/10.53477/2065-8281-25-12

În contextul unei societăți profund digitalizate, organizațiile se confruntă cu un spectru tot mai diversificat de amenințări cibernetice, care vizează date sensibile și care pot perturba grav funcționarea sistemelor informatice esențiale. Pentru a face față acestor provocări, este absolut necesară adoptarea unor metode inovatoare de consolidare a rezilienței, care să asigure atât rezistența în fața atacurilor, cât și o recuperare rapidă și eficientă. O soluție accesibilă și eficientă în acest sens este utilizarea scenariilor cibernetice. Acestea oferă organizațiilor oportunitatea de a anticipa amenințări emergente și de a construi răspunsuri adaptate specificului amenințării. Pe măsură ce complexitatea și sofisticarea atacurilor informatice se intensifică, mecanismele tradiționale de apărare devin ineficiente. În același timp, creșterea numărului de dispozitive interconectate extinde aria potențială de compromitere, expunând rețelele instituționale critice la vulnerabilități din ce în ce mai dificil de controlat. În asemenea circumstanțe, scenariile devin instrumente esențiale pentru testarea capacității de reacție, validarea planurilor de continuitate a activității și optimizarea arhitecturii de securitate.

Pe fondul transformărilor profunde, generate de o digitalizare accelerată, spațiul cibernetic a devenit un domeniu strategic, esențial pentru funcționarea infrastructurilor critice, a serviciilor guvernamentale, a activităților economice și a comunicării sociale. Cu cât s-a accentuat dependența de tehnologiile informaționale, cu atât s-a adâncit și vulnerabilitatea sistemelor digitale în fața unor riscuri tot mai complexe și greu de prevăzut. De la atacuri cibernetice, motivate geopolitic, până la campanii de tip ransomware, care paralizează spitale, administrații publice sau companii civile, amenințările din spațiul cibernetic s-au diversificat considerabil și au evoluat spre forme tot mai sofisticate și coordonate operațional. Acestea sunt adesea orchestrate de grupuri specializate, fie cu motivații economice, fie cu agende strategice, beneficiind de resurse tehnice avansate, de structuri ierarhizate și de metode de acțiune concertată la nivel transnațional. Din perspectiva acestei dinamici, spațiul cibernetic a devenit o sursă constantă de instabilitate, vulnerabilitate și risc sistemic, afectând infrastructuri critice, lanțuri de aprovizionare și sisteme esențiale de guvernanță digitală.

Conceptul de reziliență cibernetică a câștigat o importanță deosebită în strategiile de securitate la nivel național și internațional. Reziliența nu mai este privită doar ca o capacitate de recuperare după un incident, ci ca un ansamblu proactiv de măsuri, competențe și mecanisme care permit anticiparea, absorbția, adaptarea și îmbunătățirea sistemică a funcțiilor afectate de evenimente perturbatoare. Potrivit Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), reziliența poate fi asociată cu capacitatea sistemelor cibernetice de a rezista, de a răspunde și de a se recupera în urma unui atac sau a unei disfuncționalități, asigurând continuitatea serviciilor esențiale.

Una dintre metodele cele mai eficiente pentru testarea și îmbunătățirea rezilienței este utilizarea scenariilor cibernetice. Pe baza acestor scenarii, sunt dezvoltate exerciții complexe, cu structură prestabilită, bazate pe situații ipotetice sau inspirate

din cazuri reale, care simulează atacuri, breșe de securitate sau situații de criză. Prin intermediul scenariilor, organizațiile pot evalua nu doar reacția echipelor tehnice, ci și capacitatea managerială, comunicarea internă și externă, precum și procesele de luare a deciziilor, în condiții de stres decizional și de incertitudine informațională.

Scenariile cibernetice pot lua mai multe forme. Unele dintre cele mai utilizate sunt exercițiile de tip Tabletop (TTX), care implică discuții strategice, pornind de la scenarii ipotetice și situații simulate. Altele includ Live-Fire Exercises (LFX), care simulează atacuri reale într-un mediu controlat. Cyber Wargaming testează capabilitățile tactice și operaționale într-un cadru competitiv. În plus, competițiile Capture-the-Flag (CTF) se concentrează pe identificarea și exploatarea vulnerabilităților într-un context de simulare. Toate aceste formate contribuie, în mod variabil, în funcție de scopul și structura exercițiului, la dezvoltarea unei culturi organizaționale orientate spre prevenție, pregătire și adaptabilitate.

Importanța scenariilor este subliniată de numeroase inițiative internaționale, precum exercițiile Locked Shields, organizate de Centrul de Excelență NATO pentru Cooperare în Domeniul Apărării Cibernetice (NATO CCDCOE), sau de European Cybersecurity Challenge, coordonat de ENISA, care pun accent pe cooperarea interinstituțională, pe evaluarea răspunsului în timp real și învățarea colectivă. În mod esențial, scenariile cibernetice permit o abordare sistemică a riscurilor, contribuind la identificarea punctelor slabe, la testarea planurilor de continuitate și la consolidarea rezilienței nu doar tehnice, ci și organizaționale. Ele devin, astfel, nu doar instrumente didactice sau tehnice, ci veritabile laboratoare de securitate cibernetică. Practic, se explorează viitorul prin intermediul scenariilor cibernetice.

Metodologia cercetării

Această cercetare are ca scop principal analiza rolurilor scenariilor și exercițiilor cibernetice în consolidarea și menținerea rezilienței organizaționale în spațiul cibernetic. Studiul se desfășoară în cadrul unei abordări calitative de tip exploratoriu-analitic, specifică domeniului securității cibernetice, cu accent pe analiza documentară și contextuală.
Metodologia este fundamentată pe studierea literaturii de specialitate, a cadrului doctrinar NATO și UE, precum și a documentelor relevante din domeniul securității și apărării cibernetice.

Utilizând metodologia amintită, am atins următoarele obiective principale de cercetare:
1. Studiul literaturii de specialitate pentru a clarifica conceptul teoretic de scenariu și scenariu cibernetic. Această etapă asigură fundamentul epistemologic al lucrării, fiind bazată pe literatura academică și tehnică, precum și pe surse instituționale validate (ENISA, NIST, CCDCOE);
2. Analiza literaturii de specialitate privind funcțiile și aplicabilitatea scenariilor cibernetice urmărește să demonstreze că acestea nu sunt doar instrumente didactice

sau operaționale, ci constituie mecanisme esențiale, integrabile în arhitectura contemporană a securității cibernetice și în procesul de consolidare a rezilienței organizaționale. În sprijinul acestei demonstrații, analiza este completată prin evaluarea comparativă a celor mai frecvent utilizate formate de exerciții: Tabletop Exercises (TTX), Live-Fire Exercises (LFX), Red/Blue Team Exercises și Capture-the-Flag (CTF). Acestea sunt analizate din perspectiva rolului lor în dezvoltarea capabilităților cibernetice, a pregătirii teoretice și operaționale și a dezvoltării unei culturi organizaționale orientate spre descurajare, adaptare și reacție rapidă.

Cercetarea valorifică metode calitative de tip secundar, prin care sunt analizate date și informații din surse deschise, studii și rapoarte specializate. Alegerea acestei metodologii este justificată de natura multidimensională a subiectului, precum și de obiectivul de a oferi un cadru integrator de reflecție, cu aplicabilitate practică în mediul instituțional, militar și civil.

Au fost analizate multiple tipuri de scenarii și de exerciții, aplicate în contexte naționale și internaționale, cu scopul de a evidenția impactul lor asupra dezvoltării rezilienței cibernetice. Analiza a fost ghidată de criterii operaționale, urmărind relevanța practică a fiecărui format de exercițiu și corelarea acestuia cu obiectivele de apărare și reacție instituțională. Limitările inerente cercetării calitative, precum absența validării prin date empirice cantitative nu afectează valoarea aplicativă a concluziilor, întrucât demersul s-a axat pe identificarea bunelor practici, a lecțiilor învățate și a direcțiilor de consolidare a arhitecturii de securitate cibernetică prin scenarii și exerciții structurate. De asemenea, metodologia adoptată urmărește să sprijine argumentativ ideea că scenariile și exercițiile cibernetice nu sunt doar instrumente de instruire, ci componente strategice ale rezilienței cibernetice care pot contribui direct la capacitatea organizațională de a preveni, de a răspunde și de a recupera în fața amenințărilor cibernetice emergente.

Studiul literaturii de specialitate privind conceptul teoretic de scenariu

Scenariile nu trebuie confundate cu previziuni sau preziceri ale viitorului, ele reprezintă situații ipotetice, dar plauzibile, construite pentru a testa reacția sistemelor și pentru a antrena personalul specializat în apărare și securitate cibernetică. Prin natura lor, scenariile oferă un cadru controlat, în care pot fi simulate evenimente de criză, permițând evaluarea capacităților de reacție, adaptabilitate și coordonare a actorilor implicați. Mai mult decât atât, scenariile pot constitui o resursă valoroasă în procesul de planificare și luare a deciziilor pentru comandanții militari, oferind repere operaționale și strategice, bazate pe lecțiile învățate în urma exercițiilor anterioare sau a jocurilor de război.

Unul dintre obiectivele centrale ale utilizării scenariilor constă în reducerea incertitudinii operaționale și, implicit, a numărului de incidente neprevăzute.

Acest aspect are un impact direct asupra nivelului de stres și de presiune, exercitat asupra specialiștilor, care, prin antrenament, dezvoltă reflexe operaționale ce pot fi activate automat în situații reale. Astfel, chiar dacă un incident cibernetic nu poate fi evitat, capacitatea de a-l detecta și de a răspunde într-un timp minim reprezintă un avantaj strategic major. În acest sens, **eficiența scenariilor** nu se măsoară doar prin fidelitatea simulării, ci și prin capacitatea acestora de a genera schimbări reale în comportamentul organizațional: reducerea timpilor de reacție, creșterea coeziunii dintre echipe, rafinarea proceselor decizionale și, nu în ultimul rând, întărirea încrederii în propriile mecanisme de apărare. Cu cât un scenariu este mai bine adaptat specificului organizației și mai riguros construit, cu atât randamentul său formativ este mai ridicat, contribuind direct la creșterea rezilienței cibernetice.

În ultimii ani s-au realizat tot mai multe studii despre exerciții și jocuri de război, din perspectivă militară. Așa după cum a fost evidențiat în secțiunile anterioare, scopul acestui articol este acela de a analiza importanța scenariilor în creșterea securității cibernetice. Această abordare poate fi, deopotrivă, atât militară, cât și civilă. De asemenea, exercițiile desfășurate în comun de statele membre ale alianțelor și organizațiilor internaționale, alături de parteneriatele dintre structurile civile și cele militare, contribuie direct la consolidarea rezilienței cibernetice. Efectul sinergic derivă din antrenarea specialiștilor în contexte operaționale diverse atât simulate, cât și realiste. Deși pot părea abstracte la prima vedere, aceste scenarii reduc considerabil incertitudinile, oferind un sprijin esențial în procesul de pregătire și reacție instituțională. În plus, scurtează timpul de răspuns, în cazul în care situațiile ipotetice ajung vreodată să devină reale.

Scenariul, format din mai multe ipoteze, se bazează pe un presupus atac care testează procedurile operaționale și legale, precum și cele privind schimbul de informații cu partenerii din alianțe. Participanții vor colabora pentru a identifica amenințarea cât mai repede posibil și pentru a limita impactul acesteia asupra sistemelor naționale ale fiecărui stat, în parte. Este important de subliniat sinergia colaborării dintre instituțiile militare și cele civile. Mai mult, exercițiile comune statelor din alianțe și colaborarea dintre instituțiile civile și cele militare sunt importante pentru optimizarea rezilienței în fața amenințărilor cibernetice. Scenariile unor atacuri cibernetice trebuie să testeze nu doar procedurile operaționale, ci și cele legale (Nucă 2024), asigurându-se că toate părțile implicate pot reacționa eficient și coordonat. Aceste exerciții contribuie la formarea specialiștilor, dezvoltând abilități atât practice, cât și teoretice, esențiale pentru gestionarea situațiilor de excepție în mediul cibernetic. În plus, colaborarea internațională în cadrul acestor exerciții ajută la consolidarea încrederii dintre state și la crearea unor standarde comune de răspuns la amenințările cibernetice. Mai mult decât atât, securitatea și guvernanța spațiului cibernetic reprezintă elemente fundamentale pentru asigurarea funcționării sustenabile și a dezvoltării durabile a oricărei organizații sau societăți (Popa 2015, 22).

Dacă ne referim strict la asemănarea scenariilor cibernetice cu scenariile militare, unii specialiști susțin că scenariul este strâns corelat cu conceptul de plan de

contingență, întrucât presupune identificarea și stabilirea unui mod de acțiune specific, aplicabil în circumstanțe bine determinate (Petrescu 2017, 62). În practica procesului de planificare, comandanții propun cu prioritate identificarea celei mai probabile amenințări sau a celui mai periculos curs de acțiune al adversarului, precum și elaborarea unui răspuns adecvat, în contextul situației respective. Eficiența procesului decizional este amplificată prin utilizarea scenariilor din cadrul jocurilor de război, care permit concentrarea eforturilor de planificare asupra formulării unor soluții operaționale, adaptate diverselor ipoteze privind evoluția situației tactice sau strategice. Astfel, este redus riscul de surprindere din partea inamicului printr-o anticipare mai clară a posibilităților de manevră și a cursurilor alternative de acțiune (Joint Chiefs of Staff 2020, III-4).

În prezent, scenariul s-a impus ca un instrument esențial în cadrul procesului de planificare a acțiunilor militare, oferind o metodologie coerentă și structurată pentru analizarea unor posibile situații în viitor. Această abordare contribuie la clarificarea incertitudinilor inerente mediului operațional și la susținerea procesului decizional prin conturarea unor perspective plauzibile asupra evoluției situației (Schoemaker 1995, 25-40). Un scenariu complet ar trebui să includă descrierea stării inițiale, enunțarea unei stări finale posibile sau dorite și o succesiune logică de evenimente care conduc de la starea actuală la cea finală, cu condiția îndeplinirii anumitor factori determinanți (Van der Heijden 2005, 152). Pentru a fi eficient, un scenariu trebuie să fie suficient de coerent, transparent și logic, astfel încât să poată fi analizat și evaluat, în raport cu ipotezele formulate (Godet 2006).

Este esențial de subliniat că scenariile nu au rolul de a elimina complet incertitudinea și nici de a anticipa cu exactitate viitoarele evoluții. Ele nu prezic viitorul, ci conturează un cadru de referință care stabilește limitele acestuia, facilitând astfel o înțelegere mai nuanțată a posibilelor dezvoltări ale situației operaționale (Wright și Goodwin 2009, 813-825). Există mai multe definiții, date scenariilor de-a lungul timpului, fiind privite din perspective diferite. Însă unul dintre cei mai cunoscuți specialiști în teoria scenariilor, Philip van Notten, definește scenariul ca fiind *„o descriere coerentă și exhaustivă a unei viitoare situații alternative și ipotetice, care reflectă perspective diferite asupra trecutului, prezentului și posibilelor dezvoltări în viitor și care servește drept bază pentru deciziile și acțiunile ulterioare”* (van Notten 2005, 20). În lucrarea sa, van Notten sintetizează mai multe perspective academice și aplicative asupra scenariilor, evidențiind faptul că termenul are cel puțin patru accepțiuni majore: ca instrument de analiză a sensibilității, ca plan de contingență, ca instrument decizional strategic și ca metodă exploratorie de învățare și anticipare. Această din urmă accepțiune este centrală în cercetarea contemporană și este susținută de un consens emergent în literatura de specialitate: scenariile nu sunt previziuni, ci reprezentări plauzibile și structurate ale unor viitoare alternative posibile (van Notten 2005, 18).

Relevanța practică a scenariilor nu derivă doar din valoarea lor descriptivă, ci și din capacitatea lor de a influența deciziile și de a stimula gândirea strategică. Astfel,

Postma accentuează logica internă, afimând că *„scenariile sunt descrieri ale unor imagini coerente ale evenimentelor și situațiilor viitoare"* (Postma și Vijverberg 1995, 15), în timp ce Fahey și Randall insistă asupra probabilității: *„scenariile sunt narațiuni descriptive plauzibile a unor proiecții alternative ale unei părți specifice a viitorului"* (Fahey și Randall 1998, 6). Alți autori, precum Van Asselt și Rotmans, propun o viziune integratoare, care include nu doar viitorul, ci și reinterpretarea trecutului și prezentului*: „scenariile sunt descrieri narative ale unor imagini alternative ale viitorului, construite pe baza unor modele mentale și conceptuale care reflectă perspective diferite asupra trecutului, prezentului și viitorului"* (Rotmans 1998, 158).

Scenariile reprezintă construcții analitice, menite să contureze o varietate de condiții viitoare, incluzând oportunități, amenințări și potențiale obstacole, care pot influența în mod semnificativ capacitatea de atingere a obiectivelor dorite. Acestea ghidează modul de interpretare și abordare a situațiilor incerte, oferind, totodată, un cadru orientativ în luarea deciziilor și alegerea cursurilor de acțiune. Un atribut definitoriu al scenariilor este flexibilitatea lor conceptuală, care permite integrarea unei game largi de direcții de dezvoltare. Fiecare direcție este fundamentată pe un set specific de valori, asociate factorilor determinanți, ale căror interacțiuni conferă scenariului coerență și relevanță operațională. Elementele constitutive ale scenariului sunt interconectate prin relații logice și funcționale, construite pe baza unor metode, principii, proceduri și reguli, care, împreună, formează un sistem normativ integrat. Acest sistem susține o desfășurare articulată a acțiunilor și contribuie la modelarea unui răspuns adaptat complexității mediului analizat.

Definițiile scenariului converg spre o viziune complexă și multidimensională, în care acesta este în același timp: o narațiune logică despre posibilități, un instrument de decizie și învățare, un cadru pentru testarea strategiilor și o hartă conceptuală a incertitudinilor și tendințelor viitoare. Această abordare integrată plasează scenariul în centrul procesului de reziliență strategică și de planificare anticipativă în fața incertitudinilor sistemice.

În contextul securității cibernetice, indiferent dacă scenariile sunt concepute pe fundamente reale, fictive sau combinate, ele trebuie să îndeplinească o serie de cerințe esențiale. În primul rând, acestea trebuie să fie verosimile, ceea ce înseamnă că trebuie să proiecteze situații posibile în mediul cibernetic, ținând cont de complexitatea infrastructurii digitale, de interdependențele informaționale și de potențialii vectori de atac. Un scenariu realist va permite o evaluare realistă a capacităților de apărare cibernetică și a procedurilor de răspuns, fără a modifica parametrii relevanți ai mediului operațional sau natura amenințărilor simulate. O condiție esențială, direct legată de realism, este obiectivitatea informațiilor utilizate la construirea scenariului. Este esențial ca mediul cibernetic, inclusiv evenimentele declanșatoare, actorii implicați, vulnerabilitățile exploatate și reacțiile din partea instituțiilor să fie descrise într-un mod clar și precis. Prezentarea ar trebui să fie fără ambiguități, redundanțe sau detalii excesive, deoarece acestea ar putea avea un impact negativ asupra înțelegerii sau aplicării practice. Cu toate acestea, scenariul

cibernetic trebuie să fie complet, obiectiv și bine structurat, ceea ce înseamnă că toate abilitățile defensive și de răspuns trebuie integrate într-un cadru operațional clar. Acest lucru implică modelarea atât a aspectelor *tehnice* (rețele, sisteme, fluxuri de date), cât și a aspectelor *organizaționale și legale* (fluxuri de decizie, comunicare și colaborare interinstituțională, să fie în conformitate cu legislația în vigoare).

O altă cerință esențială este flexibilitatea. Scenariul trebuie să permită testarea reală sau simulată, astfel încât să reflecte fidel dinamica incidentelor cibernetice și să permită ajustarea succesiunii evenimentelor, în funcție de reacțiile analizate. Pentru a determina punctele forte și slăbiciunile sistemului cibernetic în cauză, validarea poate fi realizată prin exerciții practice sau prin modelare digitală.
În cele din urmă, o caracteristică esențială este coerența. Scenariul trebuie să fie construit pe o linie clară și logică, să descrie situația operațională într-un mod fluent și coerent și să permită actorilor implicați în gestionarea crizei și luarea deciziilor să se integreze într-un mod eficient. El trebuie să abordeze descrierea situației într-o manieră fluentă și articulată, cu informații, prezentate în strânsă corelație, care să plaseze eficient structura destinatară în mediul operațional necesar îndeplinirii obiectivelor (Petrescu 2017, 66). O astfel de structură garantează relevanța scenariului pentru creșterea capacității de reacție, adaptabilitate și reziliență în fața amenințărilor cibernetice emergente.

Scenariile reprezintă instrumente metodologice fundamentale, utilizate pentru a explora incertitudinile legate de evoluțiile viitoare. Potrivit definiției oferite de Kosow și Gaßner, un scenariu este *„o descriere plauzibilă a unei situații viitoare, incluzând traseele de dezvoltare care ar putea conduce către această situație"* (Kosow și Gaßner 2008, 49). Scenariile nu trebuie confundate cu predicțiile sau cu prognozele certe. Ele sunt construcții ipotetice destinate să ofere un cadru de reflecție sistematică asupra factorilor determinanți și interdependențelor care modelează posibilele viitoare situații. Potrivit acelorași autori, scenariile au mai multe funcții esențiale:

a) explorarea cunoașterii existente și identificarea lacunelor informaționale;
b) facilitarea comunicării dintre diferiți actori implicați în procesul decizional;
c) formularea obiectivelor strategice în condiții de incertitudine;
d) sprijinirea planificării și luării deciziilor prin anticiparea posibilelor schimbări și provocări (Kosow și Gaßner 2008).

Utilitatea practică a scenariilor cibernetice se manifestă în multiple dimensiuni, dintre care se evidențiază în mod deosebit sprijinul pe care acestea îl oferă în procesul decizional, în instruirea forțelor specializate și în testarea procedurilor de colaborare interinstituțională. Prin simularea unor incidente complexe, scenariile permit factorilor de decizie să anticipeze tipologii de comportament ale adversarului, să identifice punctele critice ale infrastructurii informatice și să adapteze rapid strategiile de răspuns la incidente cibernetice, în funcție de evoluția amenințării.

În planul formării profesionale, scenariile contribuie semnificativ la dezvoltarea abilităților tactice și strategice ale personalului din structurile specializate în

securitate cibernetică. Prin expunerea controlată la situații de criză, specialiștii învață să reacționeze eficient sub presiune, să gestioneze fluxuri informaționale contradictorii și să colaboreze în timp real cu specialiști interni și internaționali. În plus, scenariile favorizează cultivarea gândirii critice, a capacității de analiză anticipativă și a înțelegerii interdependențelor dintre componentele unui ecosistem digital complex.

La nivel instituțional, implementarea scenariilor facilitează armonizarea doctrinelor și a protocoalelor de acțiune dintre structurile militare, civile, publice și private. Exercițiile bazate pe scenarii cibernetice oferă o platformă eficientă pentru testarea interoperabilității, pentru verificarea compatibilității procedurilor legale și pentru identificarea lacunelor în mecanismele de alertare, comunicare și reacție. Astfel, scenariile devin instrumente cheie în procesul de consolidare a rezilienței cibernetice la nivel național și internațional în cadrul unor alianțe.

Importanța utilizării scenariilor devine evidentă, mai ales în domeniile caracterizate de incertitudine ridicată, unde schimbările rapide sau neprevăzute pot avea impact major asupra securității, economiei sau mediului social (Kosow și Gaßner 2008). În plus, într-un mediu strategic marcat de incertitudini și amenințări asimetrice și hibride, capacitatea unei organizații de a integra în mod eficient lecțiile învățate din scenarii este esențială pentru îmbunătățirea continuă a arhitecturii sale de securitate. De aceea scenariile nu trebuie integrate doar în exerciții izolate, ci ca elemente ale unui ciclu complex de planificare, învățare, ajustare și perfecționare a apărării cibernetice.

Scenariile cibernetice – elemente fundamentale în exercițiile cibernetice

Un scenariu cibernetic poate fi interesant, unic și special conceput pentru a acoperi zonele vulnerabile sau de ambiguitate din *planul de răspuns la incidente cibernetice*. În plus, un astfel de scenariu poate reprezenta o testare intenționată a limitelor unor sisteme considerate critice sau care asigură securitatea cibernetică a unor instituții sau chiar de securitate națională. Scopul nu este doar verificarea funcționalității în condiții normale, ci și evaluarea modului în care sistemul reacționează atunci când este împins intenționat până la atingerea limitelor sale operaționale. Doar în acest mod se pot identifica punctele slabe și pot fi consolidate înainte să poată fi exploatate de un atac real. În acest proces, libertatea de a analiza chiar și cele mai improbabile scenarii reprezintă cheia unui proces de anticipare eficient și adaptativ. Ce se întâmplă dacă un atacator descoperă o vulnerabilitate tehnică și o combină cu o eroare umană? Sau dacă o breșă, aparent minoră, deschide ușa către o serie de incidente? Cazurile semnificative din trecut au relevat că evenimente extreme, considerate *pur ghinion* sau *teoretic imposibile*, se materializează adesea în lumea cibernetică. Prin exerciții simulate, organizațiile nu doar anticipează eșecurile, ci și exersează răspunsul. Fiecare scenariu este o lecție care transformă vulnerabilitățile de azi în reziliența de mâine.

Identificarea acestor lacune este esențială pentru a avansa în înțelegerea modului în care planificarea scenariilor poate fi integrată în mod eficient în strategiile de reziliență în domeniul securității cibernetice, conducând, în cele din urmă, la o apărare mai solidă împotriva amenințărilor în continuă evoluție. Remedierea acestor lacune nu doar că va îmbunătăți cadrele teoretice, ci va oferi și perspective aplicabile organizațiilor care doresc să integreze eficient planificarea scenariilor în practicile lor de securitate cibernetică.

Scenariile cibernetice reprezintă instrumente esențiale în anticiparea, modelarea și analiza riscurilor asociate spațiului digital. Ele nu doar sprijină procesul de înțelegere a vulnerabilităților, ci constituie și fundamentul metodologic pentru dezvoltarea exercițiilor de pregătire strategică și operațională. Pe măsură ce complexitatea amenințărilor cibernetice a crescut, a devenit necesară standardizarea diverselor forme de antrenament și de testare. Astfel, în prezent sunt recunoscute mai multe tipuri de exerciții cibernetice, adaptate diversității riscurilor și nevoilor de pregătire: Cyber Wargaming, Tabletop Exercises (TTX), Live-Fire Exercises (LFX), Red Team/ Blue Team Exercises, Cyber Range Exercises, Capture the Flag (CTF) Exercises etc.

Cyber Wargaming este un exercițiu analitic, de tip simulare operațională, sau exercițiu de tip *tabletop*, conceput pentru a reproduce în mod controlat dinamica unui conflict cibernetic. Conceptul de cyber wargaming își are rădăcinile în tradiția militară a jocurilor de război, unde simulările erau folosite pentru antrenarea comandanților și testarea strategiilor de luptă. Pe măsură ce amenințările din spațiul cibernetic au devenit mai sofisticate, metodologia militară a fost adaptată pentru mediul digital, permițând evaluarea posturii de securitate, a procesului decizional și a strategiilor de apărare împotriva atacurilor cibernetice. Această continuitate între wargaming militar și cyber wargaming subliniază importanța unei abordări structurate și riguroase a securității cibernetice moderne. Prin desfășurarea acestor exerciții, organizațiile pot anticipa potențiale surprize, pot identifica vulnerabilități ascunse și își pot consolida procedurile de răspuns la incidente. Totodată, utilizând abordarea sa multidimensională – tehnologică, procedurală și umană – Cyber Wargaming oferă un cadru integrat pentru testarea și optimizarea mecanismelor de securitate în condiții simulate de criză. Această abordare permite nu doar detectarea vulnerabilităților tehnice sau organizaționale, ci și formarea decidenților și a personalului operațional pentru a răspunde eficient sub presiune, în contexte tensionate sau de atacuri sofisticate.

Scopul esențial al jocului de război cibernetic constă în evaluarea pregătirii organizaționale pentru incidente cibernetice majore, în testarea capabilităților de răspuns, în îmbunătățirea procesului decizional și în întărirea rezilienței generale față de amenințările cibernetice emergente. Prin simularea conflictelor într-un mediu sigur, Cyber Wargaming contribuie la dezvoltarea unor politici de securitate mai eficiente, la reducerea timpului de reacție, în caz de criză și la întărirea cooperării interdepartamentale în interiorul organizațiilor.

Astfel, această metodologie devine un instrument indispensabil pentru orice organizație care dorește să-și îmbunătățească în mod sustenabil postura de securitate cibernetică și să-și consolideze capacitatea de a gestiona atacurile într-un mediu digital dinamic și advers. Folosirea jocurilor de război în mediul cibernetic necesită consolidare pentru a atinge potențialul maxim. În timp ce forțele armate din numeroase țări recunosc implicațiile amenințărilor cibernetice asupra securității naționale și planifică frecvent jocurile de război cibernetice la nivel național sau împreună cu aliații, sectorul privat și civil se află încă într-un stadiu incipient în adoptarea acestor practici. Jocurile de război cibernetice se diferențiază de măsurile tradiționale de securitate cibernetică precum evaluările tehnice ale sistemelor, testele de penetrare sau scanările pentru vulnerabilități, deși se pot integra atunci când este necesar. În plus față de aceste metode, jocurile de război cibernetic oferă o evaluare comprehensivă a strategiei de securitate cibernetică a unei organizații prin simularea realistă a unui conflict în mediul cibernetic. Aceste exerciții pregătesc companiile și organizațiile civile sau militare pentru luarea rapidă a deciziilor în situații neprevăzute, precum necesitatea închiderii unor părți ale rețelei, cu scopul de a limita extinderea pagubelor. Jocurile de război cibernetice contribuie astfel nu doar la identificarea vulnerabilităților tehnice, ci și la evaluarea generală a strategiilor de apărare, a mecanismelor de răspuns, a competențelor profesionale și a capacității de reziliență provocate de un atac cibernetic. Proiectarea și desfășurarea unui război cibernetic controlat constituie un proces complex care necesită implicarea profesioniștilor experimentați și utilizarea tehnologiilor de ultimă generație. Deoarece scopul unui cyber wargame este de a oferi participanților o experiență aproape în timp real, planificatorii scenariilor trebuie să fie familiarizați atât cu tehnicile recente de atac, cât și cu metodele actualizate de apărare.

Orice organizație, companie sau instituție poate desfășura jocuri de război independente, dacă dispune de infrastructura tehnică adecvată și de personal calificat. În absența acestor resurse, este recomandată externalizarea către personal specializat. Primul pas în planificarea și organizarea unui joc de război cibernetic constă în clarificarea domeniului de aplicare și a obiectivelor. Domeniul de aplicare poate varia de la testarea unor tactici izolate, până la evaluarea operațională sau strategică a sistemului de securitate cibernetică a organizației. Durata exercițiului, nivelul participanților și gradul de complexitate sunt stabilite în funcție de obiectivele și de așteptările definite inițial. Exercitarea în medii reale presupune riscuri suplimentare, motiv pentru care este recomandată desfășurarea jocului de război într-un cadru sigur, utilizând o platformă de tip Cyber Range. Această soluție permite simularea realistă a mediilor digitale organizaționale, reducând riscul de interferență cu sistemele operaționale reale și asigurând o experiență de învățare, în condiții apropiate de cele reale (Abbas 2024, 3-8).

Prin simularea aproape reală a incidentelor cibernetice, Cyber Wargaming permite organizațiilor să detecteze punctele slabe, să valideze eficiența politicilor de securitate, să actualizeze procedurile operaționale și să pregătească răspunsul coordonat în

situații critice. De asemenea, sprijină construirea unei strategii cibernetice integrate, combinând elementele tehnice, procedurale și umane, pentru a preveni surprizele costisitoare și a gestiona mai eficient amenințările emergente.

Un alt tip de exercițiu care utilizează scenarii cibernetice personalizate pentru antrenament este Cyber Table Top Exercise (TTX). Acesta constă într-o simulare interactivă, bazată pe joc de rol, în cadrul căreia participanții răspund la situații ipotetice, elaborate și prezentate de unul sau mai mulți responsabili de scenariu. De regulă, aceștia își asumă propriile funcții reale din cadrul, însă, în funcție de necesitățile exercițiului, pot interpreta și alte roluri pentru a acoperi funcții critice inexistente. Facilitatorii sau responsabilii de scenariu au rolul de a introduce treptat elemente narative, care, deși, inițial, pot părea banale, ascund adesea probleme semnificative sau indicii ale unor disfuncționalități sistemice. În mod deliberat, pot fi inserate informații contradictorii, menite să testeze capacitatea echipei de a analiza critic, de a prioritiza riscurile și de a menține coerența decizională în situații de incertitudine. Acest tip de exercițiu este conceput pentru a sprijini organizațiile în analiza scenariilor de risc și în pregătirea pentru eventuale amenințări cibernetice. Fiind relativ ușor de implementat, aceste exerciții oferă un instrument eficient și flexibil pentru evaluarea securității cibernetice (Center for Internet Security 2025). Spre deosebire de exercițiile operaționale, un TTX nu are ca obiectiv obținerea unei performanțe individuale, ci urmărește exersarea cooperării, identificarea vulnerabilităților procesuale, precum și consolidarea capacității colective de reacție, în condiții de normalitate, atunci când există timp pentru corectarea deficiențelor. Într-un incident real, acest timp nu mai este disponibil, ceea ce face ca astfel de exerciții să devină esențiale pentru pregătirea eficientă a echipei într-un cadru controlat, dar realist și provocator. Pe lângă valoarea sa formativă, acest tip de exercițiu reprezintă un instrument eficient și convenabil pentru testarea rapidă a capacității organizației de a răspunde la incidente de securitate cibernetică, în conformitate cu propriile planuri și proceduri de reacție. Întrucât în contextul unui incident real nu mai există timp pentru corectarea deficiențelor interne, aceste exerciții devin esențiale pentru pregătirea echipei într-un mediu controlat, dar plin de provocări. De asemenea, coordonarea echipei nu mai poate fi optimizată, motiv pentru care asemenea exerciții sunt esențiale pe timp de pace (Cybersecurity and Infrastructure Security Agency 2025).

Live Fire Exercise (LFX) reprezintă o formă avansată de instruire în domeniul securității cibernetice, în cadrul căreia participanții reacționează în timp real la atacuri simulate, desfășurate într-un mediu tehnic controlat, cu un nivel ridicat de realism. Cea mai amplă și sofisticată demonstrație a acestui tip de exercițiu este *Locked Shields*, organizat anual de Centrul de Excelență NATO pentru Cooperare în Domeniul Apărării Cibernetice, care reunește sute de experți din state membre și partenere. Scopul exercițiului este de a testa într-un cadru simulat, în mod real și operațional, capacitatea de securitate și apărare a infrastructurilor IT și a infrastructurile critice în fața unor atacuri cibernetice cu grad ridicat de complexitate. De asemenea, prin acest exercițiu se urmărește consolidarea pregătirii practice a profesioniștilor din

domeniul securității cibernetice prin implicarea acestora în activități desfășurate în timp real, în cadrul unor echipe extinse, interinstituționale și multidisciplinare. Scenariul este unul complex, fiind conceput astfel încât participanții să se antreneze pentru a proteja rețele informatice guvernamentale, militare și infrastructuri critice naționale împotriva unor atacuri cibernetice multiple. Printre aceste infrastructuri simulate, se regăsesc sistemele bancare, rețelele de distribuție a apei, energiei electrice și gazelor naturale, sistemele de comunicații prin satelit, precum și rețelele de comunicații 5G (Ministerul Apărării Naționale 2023).

Exercițiul este structurat după modelul *Red Team vs. Blue Team*, în care echipele de reacție rapidă din statele membre ale NATO și din țările partenere au sarcina de a apăra, în timp real, o țară fictivă, supusă unui atac cibernetic la scară largă. Pe lângă componentele pur tehnice și operaționale, exercițiul include și aspecte esențiale de luare a deciziilor strategice, elemente juridice, de comunicare publică și coordonare interinstituțională. Astfel, Locked Shields joacă un rol esențial atât în perfecționarea competențelor operaționale, cât și în consolidarea mecanismelor de cooperare internațională în domeniul cibernetic (The NATO Cooperative Cyber Defence Centre of Excellence 2022). În mod complementar, acesta creează un cadru optim pentru testarea și rafinarea procedurilor de răspuns la incidente cibernetice, în condiții de criză intens simulată, asigurând un cadru de evaluare comparativă a performanței echipelor participante. Scenariul exercițiului reflectă astfel, într-o manieră realistă și aplicată, complexitatea apărării cibernetice moderne și nevoia unei reacții coordonate, integrate și bine organizate la nivel aliat.

Un element distinctiv al exercițiului Locked Shields este caracterul său holistic și orientarea spre performanță. În plus, acesta oferă un cadru pentru testarea procedurilor de apărare, pentru colaborarea interinstituțională și dezvoltarea de soluții inovatoare în mediul militar, civil și academic. Echipele participante au fost provocate să interacționeze în afara zonelor lor de confort profesional, prin scenarii tehnice surpriză. Totodată, față de consolidarea propriilor capabilități, participanții contribuie direct la perfecționarea conținutului exercițiului Locked Shields prin feedback aplicat în ceea ce privește componentele juridice, de comunicare strategică și operaționale.

Importanța acestui exercițiu anual constă nu doar în caracterul său tehnic, ci mai ales în accentul pus pe colaborare transnațională și multidisciplinară, pe antrenarea simultană a experților din diverse sectoare, precum apărare, industrie și mediul universitar, precum și pe adaptarea continuă la noile provocări tehnologice. Locked Shields demonstrează că pregătirea eficientă pentru războiul cibernetic necesită o abordare realistă, integratoare și anticipativă, în care scenariile complexe, interoperabilitatea și analiza strategică joacă un rol la fel de important precum protejarea infrastructurii digitale propriu-zise (The NATO Cooperative Cyber Defence Centre of Excellence 2025). Mai mult decât atât, exercițiile cibernetice multinaționale ocupă un loc central în arhitectura strategică pentru întărirea cooperării dintre statele aliate și pentru promovarea schimbului de bune practici

în materie de securitate cibernetică. Acestea oferă un cadru operațional valoros, în care aliații pot testa, într-un mediu simulat, dar realist, interoperabilitatea și eficiența procedurilor comune, sporind astfel capacitatea de reacție colectivă în fața incidentelor reale. Totodată, prin integrarea entităților civile, precum universități, institute de cercetare și companii din sectorul privat, aceste exerciții contribuie la extinderea capabilităților de apărare cibernetică dincolo de sfera strict militară. Această cooperare civil-militară sporește adaptabilitatea în fața noilor provocări tehnologice și favorizează o abordare cuprinzătoare a riscurilor cibernetice, bazată pe resurse și competențe complementare. Într-un mediu global, caracterizat de interdependențe tehnologice și vulnerabilități digitale în creștere, asemenea inițiative sunt indispensabile pentru menținerea superiorității strategice în spațiul cibernetic. Nu doar că întăresc capacitățile naționale ale fiecărui stat membru, dar oferă și baza unei apărări colective coerente, agile și eficace. În plus, prin caracterul lor anticipativ și de descurajare, exercițiile contribuie la consolidarea posturii defensive a NATO, permițând o reacție coordonată la amenințările emergente și o protecție puternică a infrastructurilor critice din spațiul euroatlantic.

Conform definiției formulate de National Institute of Standards and Technology (NIST) și preluate de unii specialiști, un *Cyber Range* poate fi *„o reprezentare interactivă, simulată, a rețelelor, sistemelor, aplicațiilor și uneltelor unei organizații, conectate la un mediu ce simulează internetul real. Acesta oferă un spațiu sigur și legal pentru dobândirea de competențe cibernetice practice, dezvoltarea de produse informatice și testarea posturii de securitate*" (Chouliaras și alții 2021, 1809). Scenariul este identificat ca fiind unul dintre pilonii centrali ai unui exercițiu *Cyber Range* modern. El are un rol esențial în modelarea exercițiilor și în generarea de situații relevante. Scenariile permit introducerea de situații reale, cu tipologii de rețea variabile, cu comportamente automatizate ale utilizatorilor și cu atacuri simulate, ceea ce contribuie la realismul și complexitatea exercițiului. Scopul acestuia poate varia, având drept obiective principale:

- *cercetarea* – testarea de instrumente, metode și componente;
- *educația și formarea* – dezvoltarea competențelor practice în securitate cibernetică;
- *exercițiile și competițiile* – desfășurarea de simulări, exerciții de tip *Capture the Flag*, *Red vs. Blue Team* sau *Crisis Management Exercises* (Chouliaras și alții 2021).

Spre deosebire de celelalte tipuri de exerciții, *Capture the Flag (CTF)* este un exercițiu de securitate cibernetică, desfășurat sub formă de competiție, în care participanții trebuie să identifice și să exploateze vulnerabilități informatice pentru a localiza și a extrage un obiectiv specific, denumit *flag*, reprezentat, de obicei, printr-un fragment de date ascuns. Aceste exerciții simulează condiții reale de atac și apărare, implicând activități precum analiza rețelei, inginerie inversă, criptografie sau forensics digital (Rochford 2024). Scopurile principale ale acestor exerciții sunt următoarele: pe de o parte, ele contribuie semnificativ la dezvoltarea abilităților tehnice și strategice ale participanților, în special în rândul tinerilor talentați sau al echipelor profesioniste;

pe de altă parte, promovează educația în domeniul securității cibernetice și facilitează formarea de rețele de colaborare între organizații, instituții și experți din diverse domenii. În mod particular, formatul ”Attack-Defence” este valoros pentru pregătirea profesională, întrucât simulează condiții reale, în care echipele trebuie simultan să-și apere sistemele și să atace infrastructura adversarului (European Union Agency for Cybersecurity 2021). Prin natura lui competitivă, acest tip de exercițiu oferă un cadru dinamic de antrenament pentru:

a) modelarea amenințărilor cibernetice;
b) căutarea amenințărilor;
c) analiza riscurilor;
d) răspuns la incident;
e) culegerea datelor;
f) eficacitatea detecției;
g) colectarea probelor criminalistice;
h) protecția infrastructurilor critice (Rochford 2024).

În ceea ce privește rolul scenariului într-un exercițiu CTF, acesta este esențial pentru crearea unui cadru realist și coerent în care participanții își pot testa cunoștințele și reacțiile la incidente cibernetice. Scenariile pot fi inspirate din atacuri reale sau pot fi concepute artificial, dar trebuie să fie relevante, stimulative și adaptate nivelului participanților. Scenariul determină natura provocărilor, obiectivele tactice, tehnologiile utilizate și complexitatea exercițiului. Astfel, scenariul funcționează ca element central al exercițiului, oferind coerență în instruire în context operațional. CTF-urile sunt considerate instrumente eficiente atât în antrenamente individuale, cât și în pregătirea operațională a echipelor responsabile de securitatea cibernetică, în funcție de formatul ales.

Aceste tipuri de exerciții, prezentate mai sus, demonstrează modul în care practica wargamingului cibernetic este utilizată într-o varietate de contexte și sectoare atât militare, cât și civile, pentru a îmbunătăți capacitățile de apărare, pentru a spori conștientizarea și a dezvolta reziliența față de amenințări cibernetice din ce în ce mai sofisticate și persistente. Mai mult, acestea pot reprezenta instrumente esențiale pentru pregătirea și testarea capacităților de apărare împotriva atacurilor cibernetice. Aceste exerciții simulează scenarii realiste de atac, permițând participanților să-și dezvolte abilitățile practice, să-și îmbunătățească strategiile de răspuns la incidente și să consolideze reziliența organizațiilor în fața atacurilor cibernetice.

Concluzii

Reziliența cibernetică nu mai poate fi concepută în afara unor mecanisme dinamice și proactive de pregătire, în care scenariile cibernetice joacă un rol fundamental. Într-un peisaj digital caracterizat de incertitudine, agresiune persistentă și complexitate tehnologică, capacitatea unei organizații de a răspunde eficient la incidente depinde de maturitatea cu care își testează și își validează periodic propriile capacități

de apărare. Scenariile cibernetice se dovedesc a fi unul dintre cele mai eficiente instrumente pentru atingerea acestui obiectiv.
Prin natura lor simulatoare, scenariile permit replicarea unor contexte reale sau ipotetice, adaptate specificului organizațional, tipurilor de infrastructuri gestionate și nivelului de amenințare anticipat. Scenariile realizate în cadrul exercițiilor cibernetice, indiferent că sunt TTX-uri axate pe decizie strategică sau LFX-uri care simulează atacuri în timp real, creează un mediu de învățare accelerată, în care echipele pot înțelege mai bine punctele forte și lacunele sistemelor. În plus, scenariile facilitează o învățare integrată atât tehnică, cât și organizațională, aducând, în același spațiu de acțiune, experți IT, lideri decizionali, specialiști juridici și responsabili ai sistemelor de securitate.

Un alt avantaj major este capacitatea scenariilor de a susține o abordare colaborativă a rezilienței. Exercițiile internaționale, precum Locked Shields sau International Cybersecurity Challenge, pun accent pe cooperarea transfrontalieră și pe testarea mecanismelor de interoperabilitate între agenții, state și organizații. Acest caracter colaborativ generează sinergii esențiale pentru răspunsuri rapide și coordonate, în caz de atacuri cibernetice la scară largă. În același timp, scenariile contribuie la standardizarea bunelor practici și la consolidarea cadrului normativ în domeniul securității cibernetice.

În ceea ce privește dimensiunea educațională, CTF-urile și exercițiile aplicate, desfășurate pe cyber ranges, sunt instrumente esențiale pentru formarea noii generații de experți. Ele permit nu doar testarea cunoștințelor tehnice, ci și dezvoltarea unor competențe transversale, precum gândirea critică, adaptabilitatea și gestionarea situațiilor deosebite în momente critice. Integrarea acestor formate în programele naționale de formare și în inițiativele europene, de tipul Digital Skills Agenda (Misheva 2021), este un pas necesar pentru întărirea capacității colective de apărare.

Totuși, scenariile nu sunt lipsite de limite. În absența unui cadru metodologic bine definit, acestea pot deveni activități formale, repetitive, lipsite de impact asupra proceselor de învățare. De asemenea, scenariile care nu sunt adaptate specificului organizațional riscă să genereze rezultate false sau să creeze o falsă senzație de siguranță. Din acest motiv, este esențial ca proiectarea și evaluarea exercițiilor să fie realizate de profesioniști, folosind metodologii testate, cum ar fi cele propuse de ENISA, NIST sau CCDCOE.

Un alt aspect important îl reprezintă integrarea rezultatelor acestor scenarii în politicile și strategiile de securitate. Lecțiile învățate trebuie documentate, analizate și transformate în măsuri concrete de întărire a posturii de apărare. Această integrare presupune existența unui proces de feedback formalizat și a unei culturi organizaționale deschise învățării continue. Doar în acest mod scenariile devin veritabile instrumente de guvernanță în materie de securitate cibernetică.

Scenariile cibernetice sunt mai mult decât simple exerciții de simulare, ele constituie un cadru complex de antrenare, evaluare, colaborare și transformare. Implementate strategic, cu rigurozitate și viziune, ele pot deveni coloana vertebrală a eforturilor de consolidare a rezilienței în spațiul digital. Într-o lume în care atacurile cibernetice nu mai sunt o probabilitate, ci o certitudine statistică, investiția în astfel de instrumente nu este un lux, ci o necesitate imperativă pentru supraviețuire digitală și suveranitate informațională.

Toate aceste tipuri de exerciții sau simulări cibernetice pe care le-am amintit în lucrare constituie metode esențiale de antrenament operațional, contribuind la dezvoltarea capacității de reacție în fața unui atac cibernetic real. Totodată, ele oferă un cadru controlat pentru testarea tacticilor ofensive, în scopul evaluării capacității defensive și a gradului de pregătire specifică. Cu o frecvență anuală sau chiar multianuală, aceste exerciții reunesc state membre și partenere în scenarii comune, devenind nu doar un mijloc de consolidare a interoperabilității, ci și o formă modernă de descurajare activă, într-un climat marcat de amenințări cibernetice persistente și asimetrice.

Referințe

Abbas, Nasim. 2024. ”Cyber Wargames and Cyber Security.” *Privia Security,* 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 și 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 și Robert M. Randall. 1998. „What is Scenario Learning?” *Learning from the Future – Competitive foresight scenarios,* 3–21. New York: John Wiley & Sons.

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 și Robert Gaßner. 2008. *Methoden der Zukunfts – und Szenarioanalyse: Überblick, Bewertung und Auswahlkriterien.* Berlin: Institut für Zukunftsstudien und Technologiebewertung.

Ministerul Apărării Naționale. 2023. „Specialiști din MApN, la exercițiul de apărare cibernetică Locked Shields 2023.” https://www.mapn.ro/cpresa/17900_Specialiști-din-MApN,-la-exercițiul-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 legislative 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 Națională de Apărare „Carol I” .

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

Postma, Theodorus J.B.M. și 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 și 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.