UTILIZAREA POLIGOANELOR CIBERNETICE PENTRU INSTRUIREA ÎN DOMENIUL SECURITĂȚII CIBERNETICE CA PLAN DE ACȚIUNE ÎN FAȚA AMENINȚĂRILOR HIBRIDE

General-maior Stayko PROKOPIEV

Comandant al Colegiului Național de Apărare „G.S. Rakovski”, Sofia, Bulgaria

Conf. univ. dr. Veselina ALEKSANDROVA

Colegiul Național de Apărare „G.S. Rakovski”, Sofia, Bulgaria

Dr. Elitsa PAVLOVA

Universitatea de Economie Națională și Mondială, Sofia, Bulgaria

Dr. Violeta VASILEVA

Future Innovation Labs, Sofia, Bulgaria

DOI: 10.55535/GMR.2025.3.19

Cyber ranges are a key tool for developing effective strategies and tactics to protect against hybrid threats, which combine traditional military methods with cyberattacks. In this scientific paper, the authors examine the significance of using cyber ranges in cybersecurity training, analysing their architecture, main principles of design and implementation, and their lifecycle. The question of how these platforms can be used to enhance strategic resilience and national defence through simulating various scenarios and vulnerabilities is explored. Specific recommendations for integrating cyber ranges into action plans against hybrid threats are also provided. The employment of cyber ranges for the preparation of personnel, organizations, and consequently states can increase their readiness and capability to respond to complex and multifaceted hybrid threats, ensuring better protection of their critical infrastructures and information systems. This approach not only supports strategic resilience and strengthens national defence but also creates a foundation for international cooperation and knowledge exchange in the field of cybersecurity.

Keywords: hybrid threats; cyber range; cybersecurity; strategic resilience; cyberattacs;

Traducere și adaptare: **Diana-Cristiana LUPU**.

INTRODUCERE

În ultimii ani, suntem martorii unei dezvoltări rapide a tehnologiilor informaționale și a spațiului cibernetic, un fenomen global care a schimbat caracteristicile comportamentului societăților și, în special, al indivizilor. Internetul, ca rețea globală care afectează toate sferele vieții publice, reprezintă nu numai spațiul care acumulează cele mai multe informații, ci și locul unde se concentrează un potențial semnificativ de infrastructură și servicii critice la nivel statal și corporatist. Rețeaua globală devine un factor din ce în ce mai important pentru securitatea și apărarea națională. Toate acestea duc la noi provocări și amenințări hibride în spațiul cibernetic, caracterizate de o mare dinamică, imprevizibilitate și complexitate. Dezvoltarea capabilităților ofensive pentru desfășurarea de operații cibernetice extinse, de către organizații teroriste și extremiste, precum și de către entități statale individuale, ca instrument pentru atingerea obiectivelor distructive și inumane împotriva societății și a cetățenilor, reprezintă unul dintre principalele motive pentru regândirea rolului spațiului cibernetic ca element al amenințărilor hibride și ca al cincilea domeniu de conflicte și interacțiune.

Riscurile și amenințările sporite, în mediul geopolitic și strategic de securitate, precum și în spațiul cibernetic, creează condiții pentru amplificarea vulnerabilităților în sistemele informaționale de comunicații militare pentru comandă și control. Este nevoie de implementarea eficientă și la timp a măsurilor de protecție pentru sistemele proprii, precum și de dezvoltarea unor capabilități de apărare cibernetică compatibile cu cele ale statelor membre ale NATO. Securitatea cibernetică necesită resurse, precum cele materiale, umane, financiare și tehnologice.

La summitul NATO de la Varșovia din 2016, spațiul cibernetic a fost recunoscut ca domeniu operațional. De asemenea, au fost identificate domenii prioritare, cum ar fi consolidarea capabilităților colective ale Alianței, incluzând apărarea cibernetică în procesul de planificare, precum și creșterea investițiilor statelor membre în acest domeniu, având în vedere că, timp de mulți ani, lupta armată și războiul au fost purtate în patru domenii fizice, care există în mod obiectiv – pe uscat, în aer, în spațiul maritim și în spațiul cosmic. După reuniunea de la Varșovia, este definit al cincilea domeniu – spațiul cibernetic (Grigorov, 2016).

În tranziția către capabilități centrate pe rețea, sisteme de înaltă tehnologie pentru comanda și controlul trupelor, informații, țintire și controlul armelor inteligente, dependența sistemelor noastre devine, de fapt, foarte mare. De exemplu, dacă operațiunile cibernetice duc la inoperabilitatea sistemului de poziționare globală (GPS), sistemele de rachete ghidate și controlate de GPS nu vor putea funcționa. Operațiile cibernetice pot duce la consecințe catastrofale dacă, în timpul unei acțiuni militare, forțele armate nu au luat măsuri adecvate pentru a-și proteja propriile sisteme de comandă, control, ghidare și atac. De aceea, NATO a identificat spațiul cibernetic ca fiind al cincilea domeniu, important pentru apărare.

Este necesară elaborarea de politici și documente de orientare pentru apărarea cibernetică a Armatei, în acord cu luarea în considerare a spațiului cibernetic ca al cincilea domeniu. Acestea sunt legate de sustenabilitatea strategică și apărarea națională, precum și de necesitatea de a contracara activ amenințările hibride, atacurile cibernetice și războaiele hibride.

În acest scop, oportunitățile oferite de apartenența noastră la NATO și la UE pot fi utilizate pentru a participa la inițiative comune de constituire a capabilităților comune; pentru a schimba informații privind incidentele cibernetice și a oferi asistență reciprocă pentru instituțiile statului și organizațiile internaționale într-un mod coordonat; pentru a coopera cu mediul de afaceri și cu cel academic; pentru a dobândi capacități de specialitate în domeniul securității cibernetice; pentru a îmbunătăți pregătirea prin instruire periodică și participarea la exerciții cu poligoane cibernetice.

ARHITECTURA POLIGONULUI CIBERNETIC

Arhitectura poligonului cibernetic include o platformă de lucru, o interfață cu utilizatorul, scenarii, proiecte, infrastructură și echipe. Interfața cu utilizatorul formează un spațiu cibernetic realist, alcătuit din dispozitive reale și mașini virtuale. Înregistrarea în platformă acoperă funcțiile elementelor de profil ale instructorului și, respectiv, ale participantului.

Platforma constă dintr-un set de tehnologii utilizate ca fundament pe care pot fi dezvoltate aplicații, procese și servicii. Platforma conține principalele elemente care oferă procese automatizate, cum ar fi crearea de mașini virtuale, simularea traficului de rețea, instalarea de pachete software, crearea în masă a conturilor de utilizatori în rețea, monitorizarea stării spațiului de lucru și vizualizarea informațiilor pentru instructori și participanți. Elementele pot fi dezvoltate sau implementate utilizând, personalizând și configurând soluții din surse deschise. Cu toate acestea,

soluțiile trebuie să respecte standardele pentru a asigura interoperabilitatea și reutilizarea lor.

Principalele elemente ale platformei poligonului cibernetic au legătură cu următoarele aspecte:

1. *Urmărire.* Platforma trebuie să fie capabilă să urmărească starea elementelor spațiului de lucru, extrăgând informații legate de starea serviciilor, proceselor, aplicațiilor și actualizărilor de software; înregistrarea și ștergerea utilizatorilor (inclusiv a drepturilor utilizatorilor și a sesiunilor) și a fișierelor; firewall-uri; sisteme de detectare a intruziunilor; date despre traficul de rețea.
2. *Registru*. Registrul gestionează baza de date a platformei, care menține înregistrările participanților în funcție de datele obținute din urmărire și de cele transmise de *„Instructor”.*
3. *Feedback* și rapoarte. Feedback-ul și rapoartele permit vizualizarea datelor despre evoluția atacurilor cibernetice care au loc într-un anumit exercițiu; modificări ale rezultatelor echipelor care participă la un anumit curs; scorul echipei; elemente ale spațiului de lucru. Vizualizarea datelor de antrenament este esențială pentru îmbunătățirea eficacității exercițiilor.
4. *Automatizare*. Elementul include mecanisme care automatizează funcțiile spațiului de lucru pentru generarea traficului de rețea, conturi de utilizator virtuale care efectuează acțiuni virtuale și atacuri cibernetice automate. Generarea traficului de rețea sporește realismul platformei. Generatoarele de trafic de rețea ar trebui să simuleze traficul diferitelor protocoale (de exemplu, HTTP – Hypertext Transfer Protocol, SMTP – Simple Mail Transfer Protocol, POP – Post Office Protocol, FTP – File Transfer Protocol, ICMP – Internet Control Message Protocol) și să ofere mijloace pentru specificarea sursei, destinației, duratei și cantității de trafic generat.
5. *Interfa*ță utilizator. Spațiul este creat automat pe baza scenariului selectat de instructor și descărcat din repertoriul de scenarii. Elementele spațiului de lucru sunt interconectate cu elementele platformei și includ computere virtuale sau fizice, dispozitive mobile, dispozitive de rețea, servere, servicii, tehnologii integrate, rețele wireless etc.

Interfețe utilizator

Interfețele utilizator pentru instructori și participanți oferă diverse funcționalități, care sunt prezentate în *tabelul 1.*

Tabelul 1: Capabilități de interfață cu utilizatorul (IU) pentru instructorul poligonului cibernetic și participant (concepția autorilor)

Funcționalitate/ Element IU	**Instructori**	**Participanți**
Afișaj/Dashboard	Vizualizare sesiuni, statut participanți, rezultate exerciții	Progres personal, sarcini următoare, nivel actual
Scenarii și misiuni	Creare, configurare și management scenarii	Accesare scenarii, executare misiuni, raportare rezultate
Monitorizare în timp real	Urmărire acțiuni participanți și trafic de rețea în mediul simulat	Vizualizarea acțiunilor personale și a consecințelor acestora asupra sistemului
Analiză și rapoarte	Generarare rapoarte individuale și de grup, evaluare aptitudini	Acces la raportul personal și la recomandările de optimizare
Modul comunicare	Chat intern, posibilitate de a trimite instrucțiuni și feedback	Chat intern pentru întrebări și colaborare în echipă
Gamificare	Stabilire criterii pentru punctaj și realizări	Acumulare puncte, realizări, comparație cu alți participanți
Integrare cu sisteme externe	Adăugare amenințări și atacuri cibernetice reale pentru antrenament	Acumulare puncte, realizări, comparație cu alți participanți
Management roluri și acces	Definire niveluri de acces și roluri	Acces limitat, doar la misiunile de antrenament și rezultatele proprii
Laboratoare interactive	Stabilirea unor medii virtuale pentru diferite scenarii	Exerciții practice într-un mediu de simulare securizat
Feedback și evaluare	Feedback direct, comentarii individuale	Posibilitate de auto-evaluare și primire de recomandări personalizate

Scenarii

Scenariile sunt create prin combinarea sarcinilor, condițiilor, obiectivelor și materialelor de învățare stocate într-un depozit. Elementele scenariului includ: mașini virtuale și dispozitive de rețea utilizate ca șabloane în timpul creării spațiului

de lucru; scripturi pentru crearea și implementarea spațiului de lucru; fișiere de configurare pentru elementele platformei. Un scenariu definește pașii pe care participanții trebuie să îi urmeze pentru a finaliza exercițiul. Fiecare pas include sub-obiective, un set de condiții și elemente de învățare. Sunt stabilite atribute pentru a descrie detaliile scenariului, inclusiv numele, descrierea, nivelul de dificultate și complexitatea.

Echipe

Munca în echipă ajută la evaluarea scenariilor de atac în condiții reale (Yamin, 2020). Echipele roșie și albastră sunt comune tuturor poligoanelor cibernetice. Echipa roșie efectuează atacul asupra computerelor utilizatorilor folosind viruși, programe malware și multe altele, concepute de echipa albă. Echipa verde este responsabilă de simularea conexiunilor cu fir sau fără fir dintre utilizatori și computerele sau smartphone-urile lor și infrastructura de rețea. Membrii echipei albastre își asumă fie rolul de apărători ai sistemului, protejându-l de atacurile cibernetice, fie rolul de investigatori ai unui atac cibernetic și a consecințelor acestuia. Echipa albă creează scenarii de atac cibernetic pentru a urmări succesul sau eșecul echipei albastre. Echipa galbenă raportează conștientizarea situației prin reproducerea utilizatorilor inocenți care compromit securitatea rețelei. Unele poligoane cibernetice folosesc o echipă gri și una violet. Griul reprezintă traficul normal și solicitările de servicii care trebuie sprijinite, iar violetul reprezintă o colaborare între echipele roșie și albastră, responsabile de tehnicile de protecție.

În timpul exercițiului, instructorul oferă sfaturi legate de conținutul învățării și primește informații de la elementele de urmărire, verifică modul în care cursanții au reușit să efectueze acțiunile corespunzătoare în timpul alocat și îi evaluează.

PRINCIPII DE BAZĂ PENTRU SELECTAREA ȘI IMPLEMENTAREA POLIGONULUI CIBERNETIC

Proiectarea și implementarea poligoanelor cibernetice ar trebui să fie ghidate de câteva principii de bază, pentru ca acestea să asigure o valoare educațională maximă și să reproducă dimensiunile operaționale ale provocărilor legate de securitatea cibernetică. (Hart et al., 2020).

❖ ***Acuratețe și realism***

Mediile de instruire sunt esențiale pentru dezvoltarea unor abilități direct transferabile în contexte operaționale. Zonele de intervenție cibernetică ar trebui să reproducă cu acuratețe topologiile de rețea, configurațiile de sistem, serviciile și aplicațiile, având caracteristici de performanță și constrângeri realiste, activitățile

tipice ale utilizatorilor și procesele de lucru în cadrul cărora să se detecteze evenimente legate de securitate. În mod similar, comportamentul advers ar trebui să reflecte tacticile, tehnicile și procedurile documentate ale actorilor de amenințare reali. Reprezentarea realistă a impactului, atât cu privire la atacurile reușite, cât și la măsurile defensive, îi ajută pe cursanți să înțeleagă evenimentele relevante pentru deciziile lor – impactul asupra activităților, întreruperile serviciilor care pot apărea din cauza incidentelor de securitate sau acțiuni de atenuare. Acuratețea tehnică asigură faptul că abilitățile dobândite în timpul instruirii pot fi aplicate direct în scenarii din lumea reală.

❖ ***Scalabilitate și flexibilitate***

Natura dinamică a securității cibernetice necesită medii de învățare care se pot adapta la o varietate de nevoi. Poligonul cibernetic trebuie să funcționeze cu un număr variabil de participanți, de la instruire individuală la exerciții de echipă extinse, care implică zeci sau sute de participanți. Platformele de învățare trebuie să susțină scenarii de complexitate variabilă, de la exerciții centrate pe dezvoltarea competențelor până la simulări cuprinzătoare de răspuns la incidente. Mediul trebuie să fie configurabil pentru a reprezenta diferite sectoare de afaceri, structuri organizaționale și arhitecturi tehnice.

❖ ***Izolare și securitate***

Un nivel adecvat de izolare este esențial, atât din motive de securitate, cât și din motive educaționale. *Separarea completă* a rețelei asigură faptul că activitățile rău intenționate din mediul de învățare nu pot afecta sistemele de producție. *Izolarea datelor* înseamnă că mediile de învățare ar trebui să utilizeze seturi de date sintetice sau sanitizate corespunzător. Mediile de învățare ar trebui să reproducă caracteristicile datelor de producție, fără a expune informații sensibile. Sunt necesare *mecanisme robuste de autentificare și autorizare* pentru a restricționa accesul la scenarii de învățare și componente ale sistemului, pe baza rolurilor și permisiunilor de acces ale cursanților. O altă parte importantă o reprezintă sistemele de înregistrare și monitorizare care urmăresc toate activitățile din mediul de învățare. Mecanismele de prevenire a extragerii neautorizate a instrumentelor, tehnicilor sau scenariilor din mediul de învățare ajută la protejarea proprietății intelectuale și la prevenirea potențialei utilizări necorespunzătoare a materialelor de învățare.

❖ ***Reproductibilitate și standardizare***

Experiențele de învățare consecventă necesită abordări sistematice.

RECOMANDĂRI PENTRU INTEGRAREA POLIGONULUI CIBERNETIC ÎN PLANURILE DE RĂSPUNS LA ATACURILE HIBRIDE

Amenințările hibride prezintă provocări complexe și multiple, care necesită strategii de răspuns coordonate și adaptive. În contextul rezilienței strategice moderne și al apărării naționale, spațiul cibernetic joacă un rol din ce în ce mai important, ca arenă pentru conflicte și atacuri. Una dintre metodele eficiente de pregătire și răspuns la aceste amenințări este utilizarea poligoanelor cibernetice – medii virtuale care simulează condiții și scenarii din lumea reală. Recomandările specifice pentru integrarea poligoanelor cibernetice în planurile de răspuns la amenințările hibride includ următoarele:

Dezvoltarea unor scenarii realiste. Primul pas către integrarea cu succes a poligoanelor cibernetice este dezvoltarea unor scenarii realiste care să reflecte potențialele amenințări hibride. Aceste scenarii ar trebui să includă combinații de atacuri fizice, informaționale și psihologice, precum și interacțiuni între diferiți actori (guvern, sector privat, societatea civilă). Este important ca scenariile să fie actualizate periodic, pentru a reflecta noile tendințe și tactici ale adversarilor.

Instruire și simulări. Poligoanele cibernetice oferă o oportunitate unică de a desfășura instruire și simulări care pregătesc personalul pentru situații din lumea reală. Aceste exerciții pot include instruire pentru detectarea incidentelor și răspuns, gestionarea crizelor și coordonare interinstituțională. Instruirea ar trebui să fie sistematică și periodică, pentru a asigura pregătirea continuă și dezvoltarea abilităților.

Cooperare și coordonare. Măsurile eficiente de contracarare a amenințărilor hibride necesită o cooperare strânsă între diversele părți interesate. Poligoanele cibernetice pot servi drept platforme pentru exerciții comune și schimb de informații între instituții guvernamentale, companii private și parteneri internaționali. Această cooperare nu numai că îmbunătățește interoperabilitatea, dar edifică încrederea și înțelegerea reciprocă între participanți.

Pregătire tehnologică și infrastructură. Integrarea cu succes a poligoanelor cibernetice necesită disponibilitatea unei infrastructuri tehnologice adecvate. Aceasta include sisteme informatice de înaltă performanță, software de simulare și instrumente de analiză a datelor. În plus, trebuie furnizate canale de comunicații fiabile și rețele securizate pentru a asigura securitatea informațiilor și continuitatea operațiilor.

Monitorizare și evaluare. Integrarea domeniilor de instruire cibernetică în planurile de răspuns la amenințările hibride ar trebui să fie supusă unei monitorizări

și evaluări continue. Aceasta include analizarea rezultatelor simulărilor, identificarea punctelor slabe și a lacunelor, precum și implementarea unor măsuri corective. Revizuirea și actualizarea regulată a procedurilor și politicilor asigură eficacitatea și adaptabilitatea acestora la condițiile în schimbare.

PRINCIPALELE PROVOCĂRI ÎN PROIECTAREA ȘI IMPLEMENTAREA UNUI POLIGON CIBERNETIC

Principalele provocări în proiectarea și implementarea unui poligon cibernetic sunt legate de costurile ridicate ale pregătirii, cerințele ridicate de testare, dezvoltarea unei strategii de învățare și evaluare. Faza de pregătire necesită multe resurse, personal specializat, precum și o perioadă lungă de timp. Conform unui studiu privind evaluarea exercițiilor de apărare cibernetică utilizând un proces de analiză vizuală, un poligon cibernetic ar trebui să fie un mediu sigur, legal și izolat de rețelele externe și de internet (Ošlejšek, 2018). Acesta este motivul pentru care trebuie acordată o atenție deosebită instalării aplicațiilor și instrumentelor, constituirii serviciilor de rețea, furnizării accesului controlat la internet, precum și implicării personalului specializat pentru testarea și efectuarea optimizărilor și ajustărilor. O altă provocare cu care se confruntă poligoanele cibernetice educaționale este aceea că acestea trebuie să se bazeze pe bune practici de predare, incluzând, printre altele, obiectivele de învățare și caracteristicile participanților. Instruirea în domeniul securității cibernetice necesită formarea unui mediu de învățare interactiv și multistratificat. Scenariile de exerciții trebuie să satisfacă nevoile și nivelul de experiență al cursanților. Integrarea tehnologiilor emergente, cum ar fi inteligența artificială și gemenii digitali, transformă abordările tradiționale, în timp ce eforturile de standardizare continuă să se dezvolte la nivel mondial.

CONCLUZII

În concluzie, se poate rezuma că integrarea poligoanelor cibernetice în planurile de răspuns la amenințările hibride este un element crucial pentru consolidarea securității naționale și internaționale. Prin dezvoltarea de scenarii realiste, desfășurarea de activități de instruire și simulări, promovarea cooperării, asigurarea infrastructurii tehnologice necesare, precum și monitorizarea și evaluarea continuă, capacitatea de a preveni și de a răspunde la amenințări complexe poate fi îmbunătățită semnificativ. Poligoanele cibernetice eficiente necesită arhitecturi modulare, scalabile, având caracteristici de simulare de înaltă calitate și respectând cadrele pedagogice stabilite și mecanismele de evaluare cuprinzătoare.

Poligoanele cibernetice reprezintă un instrument puternic care poate ajuta organizațiile și statele să abordeze provocările generate de amenințările hibride, cu scopul de a dobândi reziliența strategică și a asigura apărarea națională.

PRECIZĂRI

Realizarea prezentului articol a fost finanțată de Ministerul Educației și Științei în cadrul implementării Programului Științific Național – Securitate și Apărare – finanțat de Ministerul Educației și Științei al Republicii Bulgaria în cadrul implementării Strategiei Naționale pentru Dezvoltarea Cercetării Științifice 2017-2030 și adoptat prin Hotărârea Consiliului de Miniștri nr. 731 din 21 octombrie 2021.

BIBLIOGRAFIE:

1. Grigorov, M.I. (2 decembrie 2016). *Petiyat domeyn i zaplahite v kiberprostranstvoto*, https://armymedia.bg/2016/12/02/петият-домейн-и-заплахите-в-киберпрос/, accesat la 10 septembrie 2025.
2. Hart, S., Margheri, A., Paci, F., Sassone, V. (2020). *Riskio: A Serious Game for Cyber Security Awareness and Education.* Computers & Security, 95, 101827. doi:https://doi.org/10.1016/j.cose.2020.
3. Ošlejšek, R.J. (2018). *Evaluation of Cyber Defense Exercises Using Visual Analytics Process.* EEE Frontiers in Education Conference (pp. 1-9), doi:https://doi.org/10.1109/FIE.2018.8659299.
4. Yamin, M.M. (2020). *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*, 101636. Computers & Security (88).