BULETINUL

UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"

Nr. 2/ 2025

ISSN 1584-1928
eISSN 2065-8281

Publicație fondată în anul 1937

PUBLICAȚIE ȘTIINȚIFICĂ CU PRESTIGIU RECUNOSCUT
DIN DOMENIUL „ȘTIINȚE MILITARE, INFORMAȚII ȘI ORDINE
PUBLICĂ" AL CONSILIULUI NAȚIONAL DE ATESTARE A
TITLURILOR, DIPLOMELOR ȘI CERTIFICATELOR UNIVERSITARE,
INDEXATĂ ÎN BAZELE DE DATE INTERNAȚIONALE CEEOL,
GOOGLE SCHOLAR, INDEX COPERNICUS, CROSSREF

EDITURA UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
BUCUREȘTI, 2025

Referenți

Articolele publicate în Buletinul Universității Naționale de Apărare „Carol I”, ISSN 1584-1928, se regăsesc – titlu, autor, abstract, conținut, bibliografie – și în varianta în limba engleză a revistei, ISSN 2284-936X
L 2284-936X

Cuprins

Nr. 2/2025

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

Stadiul cunoașterii în domeniul logisticii sustenabile: perspective economice și militare

The State of the Art in Sustainable Logistics: Economic and Military Perspectives

Lt.col.Dr. Daniela-Elena HRAB*
*Universitatea Națională de Apărare „Carol I", București, România
e-mail: edaniela.hrab@gmail.com

Abstract

Abordarea sustenabilă a logisticii se conturează ca o necesitate atât în domeniul economic, cât și în cel militar. Prezentul studiu are ca scop explorarea stadiului cunoașterii din domeniul logisticii sustenabile în ambele sfere de activitate, pentru a identifica aspectele care necesită atenția sporită a cercetătorilor. Utilizând metoda analizei documentelor, studiul aduce în prim plan cinci arii tematice abordate până în prezent în domeniul economic, reliefând necesitatea extinderii lor și în domeniul militar. Analiza efectuată arată că digitalizarea logisticii și implementarea tehnologiilor prietenoase cu mediul sunt două condiții esențiale pentru tranziția acesteia către sustenabilitate. Totodată, studiul subliniază importanța unei abordări interdisciplinare și a cercetării impactului social al sustenabilității logistice, inclusiv în contextul acțiunilor umanitare la care participă și forțele militare. Concluzia principală vizează necesitatea definirii clare a conceptului de logistică militară sustenabilă, cu luarea deopotrivă în considerare a evoluției din mediul economic și a cerințelor de ordin operațional.

The sustainable approach to logistics is emerging as a necessity in both the economic and military domains. This study aims to explore the current state of knowledge in the field of sustainable logistics within these spheres of activity, in order to identify gaps that should be addressed by future research. Based on a literature review methodology, the study brings to the forefront five thematic areas that have been addressed so far in the economic field, highlighting the need to extend them into the military domain as well. The analysis shows that the digitisation of logistics and the implementation of environmentally friendly technologies, which also reduce the negative impact on the health of end users, are two essential conditions for the transition toward sustainability. At the same time, the study emphasises the importance of an interdisciplinary approach and of researching the social impact of sustainable logistics, including the dimension related to humanitarian actions involving military forces. The main conclusion points to the need for clearly defining the concept of sustainable military logistics, taking into account developments in the economic environment and operational requirements.

Cuvinte-cheie:
logistică; apărare; sustenabilitate; dezvoltare durabilă; soluții alternative; tehnologii.

Keywords:
logistics; defence; sustainability; sustainable development; alternative solutions; technologies.

Info articol
Primit: 12 aprilie 2025; Evaluat: 5 mai 2025; Acceptat: 16 mai 2025; Disponibil online: 27 iunie 2025
Citare: Hrab, D.E. 2025. „Stadiul cunoașterii în domeniul logisticii sustenabile: perspective economice și militare."
Buletinul Universității Naționale de Apărare „Carol I", 14(2): 7-20. https://doi.org/10.53477/2065-8281-25-08

Sustenabilitatea este un concept comun domeniilor economic și militar. Din perspectivă economică, aceasta reprezintă scopul final al procesului de dezvoltare durabilă (Blewitt 2018, 4-74), o formă superioară a dezvoltării economice (Pezzey 1992, 10), caracterizată prin decuplarea de la unicul țel care viza obținerea beneficiilor economice și manifestarea unei griji sporite față de mediu și oameni, pentru asigurarea disponibilității pe termen îndelungat a resurselor naturale (United Nations 1987, 16). La nivel militar, sustenabilitatea reprezintă capacitatea de a susține o operație cu o putere de luptă adecvată, prin asigurarea resurselor umane și materiale necesare pe întreaga durată a acesteia (NATO Standardization Office 2022, 399), un rol important revenind logisticii militare.

Astfel, în cele două domenii, conceptul de sustenabilitate are legătură cu disponibilitatea neîntreruptă a resurselor necesare, diferența constând în faptul că, în domeniul militar, sustenabilitatea vizează buna desfășurare a operațiilor militare, perspectiva protejării mediului și cea a grijii sporite față de comunități fiind mai puțin vizibile. Cu toate acestea, ținând cont de faptul că unul dintre cele 17 obiective ale dezvoltării durabile (ODD), anume ODD nr. 16, se referă la asigurarea climatului de pace și a unor instituții eficiente (United Nations 2015, 25-26), se poate deduce că organizația militară poate contribui la facilitarea condițiilor de pace și, pe această cale, a celor necesare dezvoltării durabile. Însă posibilitatea unei contribuții mai ample a organizației militare la îndeplinirea altor ODD nu trebuie subestimată.

La nivelul anului 2017, problematica ce ține de managementul logistic și de lanțurile de aprovizionare-livrare se afla în topul primelor zece arii tematice, în legătură cu care cercetătorii manifestau interes pentru îmbogățirea cunoașterii din domeniul dezvoltării durabile (Wichaisri și Sopadang 2017, 4). Din perspectiva abordării integratoare a celor trei piloni ai dezvoltării durabile (economic, social, mediu) (United Nations 2015, 1), entitățile economice au ajuns la concluzia că abordarea sustenabilă a managementului logistic poate genera beneficii atât prin sporirea avantajului competitiv, cât și prin reducerea impactului asupra mediului (Wichaisri și Sopadang 2017, 4-12) și funcționarea eficientizată a lanțurilor de aprovizionare-livrare (Stroufe 2018, 326-329).

La nivel militar, modul în care este asigurat sprijinul logistic poate avea o contribuție însemnată la retenția resursei umane în această organizație (Vie, Trivette și Lathrop 2021, 28), aducând astfel beneficii și din perspectiva sustenabilității resursei umane. Mai mult decât atât, alternativa unor soluții logistice sustenabile este menționată ca deziderat în documente de nivel strategic. Spre exemplu, NATO are în vedere dezvoltarea de sisteme prietenoase cu mediul, bazate pe tehnologii cu emisii scăzute de carbon (NATO 2021), utilizarea unor combustibili alternativi (NATO 2020, 39-42), precum și participarea la sporirea rezilienței surselor de apă și hrană (NATO 2016). Viziunea NATO este împărtășită și la nivelul UE, fiind adusă în prim plan perspectiva dotării cu echipamente prietenoase cu mediul, dar și cerința elaborării unor strategii ale forțelor armate din statele membre, pentru combaterea schimbărilor climatice (Uniunea Europeană 2022, 5). Mai mult decât atât, necesitatea

unei abordări sustenabile la nivelul UE este menționată expres în Carta albă, emisă recent, din care răzbat idealuri specifice dezvoltării durabile, respectiv sporirea calității vieții cetățenilor europeni și a climatului de securitate (Comisia Europeană 2025, 1).

Nevoia de logistică militară sustenabilă este cât se poate de reală. Cercetătorii arată că îndeplinirea cu succes a misiunilor este condiționată de adoptarea unor practici logistice sustenabile, precum utilizarea tehnologiilor care reduc nevoia de aprovizionare cu produse petroliere și diminuarea nevoii de dislocare a resurselor materiale (Mosher și alții 2008, 51). În plus, sustenabilitatea este văzută ca o modalitate de evitare a îmbolnăvirii militarilor, ca urmare a deversărilor toxice, a expunerii la insecte care generează și răspândesc boli, la condiții sanitare precare și la efectele managementului defectuos al deșeurilor toxice care ar putea fi utilizate de adversar (Mosher și alții 2008, 5-6). Ca urmare a efectelor negative produse de fenomenele meteorologice extreme, pe care dezvoltarea durabilă își propune să le combată (United Nations 2015, 2-8), procese logistice, precum reaprovizionarea sau mentenanța, pot fi afectate, ca urmare a apariției unor rupturi în lanțurile de aprovizionare-livrare (Best și alții 2023, 22,73).

În baza lecțiilor identificate de armata americană în Afganistan și Irak, orientarea logisticii către soluții sustenabile ar putea contribui la reducerea pierderilor de tehnică și personal, precum și la scăderea consumurilor enorme de combustibili fosili (Harrington 2016). Se impune, astfel, regândirea actualelor modalități de furnizare a sprijinului logistic prin soluții care diminuează amprenta logistică și emisiile de carbon (Belcher și alții 2019, 75-76). Spre exemplu, disponibilitatea unor surse alternative de apă, de energie electrică și combustibil ar putea conferi sprijinului logistic caracter sustenabil sporit (Cooper 2019, 4-7). Drept urmare, importanța prezentului demers științific reiese din necesitatea stabilirii unui punct de plecare pentru punerea în practică a dezideratului logisticii sustenabile, manifestat atât la nivelul societății civile, cât și la nivel militar.

În acest context, prezentul studiu are drept obiectiv explorarea stadiului cunoașterii din domeniul logisticii sustenabile, pentru a canaliza eforturile logisticienilor spre definirea unor probleme de cercetare de interes actual (Kumar 2011, 17-27). În vederea îndeplinirii acestui obiectiv, studiul utilizează metoda revizuirii literaturii relevante, parcurgând două etape principale: 1) explorarea stadiului cunoașterii și a principalelor preocupări științifice din domeniul civil al logisticii sustenabile; 2) analizarea studiilor din domeniul logisticii militare sustenabile.

Astfel, utilizând sintagma ”*sustainable logistics*” drept cheie de căutare în baze de date, precum Google Scholar, ProQuest, Scopus și Web of Science, au fost identificate studii relevante, sub forma unor articole științifice sau a unor capitole de cărți. Selecția a avut la bază efectuarea unor teste scientometrice, fiind luate în calcul aspecte precum: numărul de citări, factorul de impact al jurnalului, raportat la domeniul respectiv, răspândirea geografică și predilecția cercetătorilor din domeniu

pentru unele teme (Grigore 2021, 1-5). Au fost luate în considerare studiile cu un număr de peste opt citări. În secțiunile următoare, corespunzătoare celor două etape menționate anterior, este analizat conținutul acestora, pentru identificarea celor mai semnificative rezultate și stabilirea stadiului cunoașterii în domeniul logisticii sustenabile.

Stadiul cunoașterii în domeniul civil al logisticii sustenabile

Studiile dedicate revizuirii literaturii din domeniul logisticii sustenabile s-au focusat pe cinci linii tematice principale. Primele trei au abordat logistica sustenabilă, în general, cu particularizare pe latura de mediu (Ren și alții 2019, 1-20), respectiv soluțiile alternative pentru micșorarea amprentei de carbon (Awwad, Shekhar și Iyer 2018, 584-591); beneficiile tehnologiilor specifice Industriei 4.0 pentru sporirea sustenabilității logisticii (Sun și alții 2022, 9560-91; Grzybowska, Awasthi și Sawhney 2020, 1-18); sistemele de asistare a deciziei în sprijinul logisticii sustenabile (Qaiser și alții 2017, 1376-1388).

Spre exemplu, primul dintre studiile selectate a analizat articole publicate în perioada 1999 - august 2019, în jurnale cu sistem "*peer-review*", identificate în bazele de date Web of Science și Scopus, utilizând instrumente de analiză bibliometrică, precum VOS (Visualization of Similarities), reliefând creșterea interesului pentru acest domeniu (Ren și alții 2019, 2-4), după cum reiese din Figura 1.

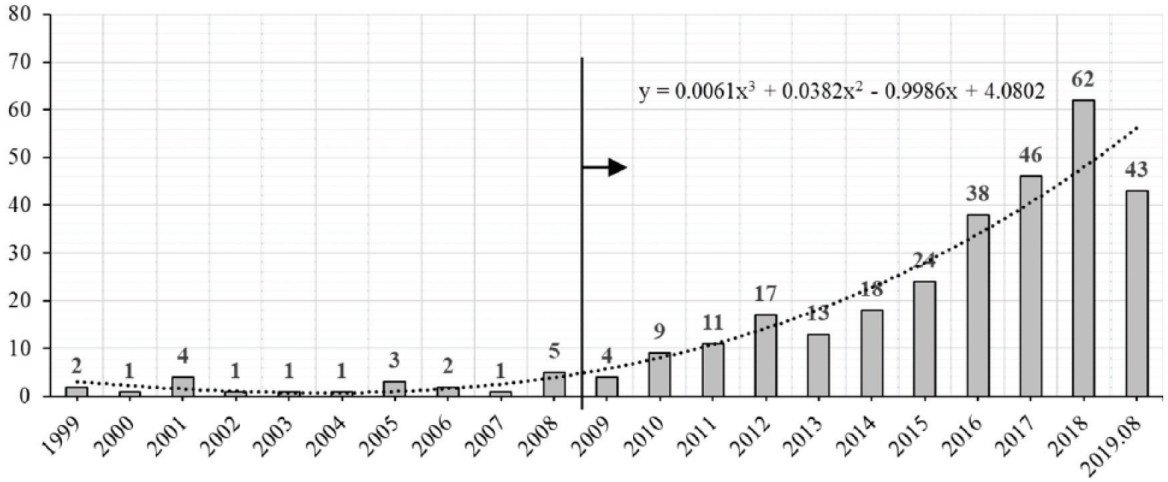

Figura 1 Evoluția publicațiilor din sfera logisticii sustenabile în perioada 1999 - august 2019 (Ren și alții 2019, 5)

Analizând totalitatea studiilor dedicate logisticii sustenabile, rezultă că studiul menționat este deosebit de relevant, acesta stând la baza elaborării unor cercetări ulterioare, după cum arată Figura 2.

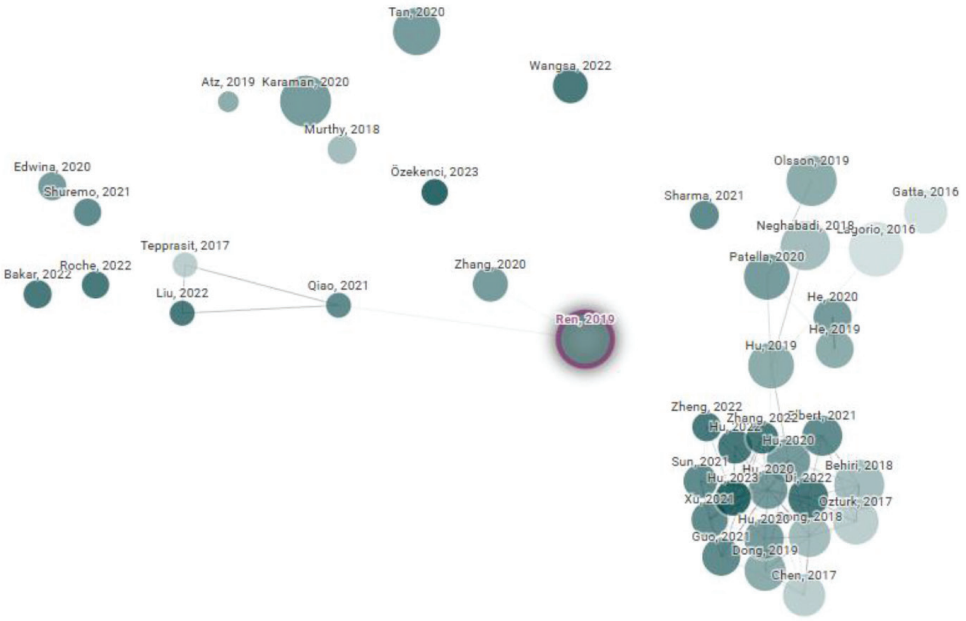

Figura 2 Publicații relevante pe tema logisticii sustenabile (2016-2023)
Sursa: concepția autorului, cu utilizarea https://www.connectedpapers.com/main/f90ddfa099de3c61a5ecb275d4a04e74323b2cd7/A-Systematic-Literature-Review-of-Green-and-Sustainable-Logistics%3A-Bibliometric-Analysis%2C-Research-Trend-and-Knowledge-Taxonomy/graph, accesat la 10.03.2025.

Studiul a scos în evidență câteva subteme ale cercetării din domeniul logisticii sustenabile, corespunzătoare laturii de mediu a sustenabilității. Cele mai relevante cincisprezece lucrări analizate de autorii acestuia, cu un număr de citări cuprins între 73 și 330, au abordat subiecte precum: logistica verde, luarea deciziilor pentru logistica sustenabilă, logistica inversă și latura de mediu a logisticii sustenabile, cele mai multe preocupări fiind în Europa, cele din China și din America nefiind de neglijat (Ren și alții 2019, 8-11). Grupând tematic studiile analizate, se poate observa, în afară de predilecția pentru latura de mediu a sustenabilității logisticii, și numărul redus al cercetărilor care oferă o perspectivă integratoare asupra acestui domeniu.

Tot din cadrul ariei tematice care vizează protecția mediului, un studiu relevant pentru problematica logisticii sustenabile sugerează utilizarea mecanismelor logisticii verzi pentru reducerea emisiilor de carbon. Autorii acestuia aduc în atenție rolul conceptului de ”*last mile logistics*” (logistica finală), corespunzător ultimului segment din lanțul de aprovizionare-livrare, specific comerțului electronic (între distribuitor și consumatorul final) în emiterea gazelor cu efect de seră, prezentând, totodată, soluții și strategii de reducere a acestora (Awwad, Shekhar şi Iyer 2018, 586).

Referitor la impactul negativ asupra mediului al acestui segment din lanțul de aprovizionare-livrare, autorii dezbat soluții, precum: utilizarea combustibililor alternativi, a vehiculelor electrice, a centrelor de distribuție urbane și a tehnologiei dedicate eficientizării alegerii rutelor de transport (Awwad, Shekhar şi Iyer 2018, 586).

Accentul este pus pe analizarea caracteristicilor vehiculelor destinate transportului și ale rutelor de parcurs, astfel încât să fie aleasă varianta care asigură cel mai scăzut consum de combustibil, deci cea mai redusă amprentă de carbon (Awwad, Shekhar și Iyer 2018, 586). Soluțiile prezentate nu au un caracter general valabil, autorii arătând că, în diferite circumstanțe, pot exista variante mai eficiente (spre exemplu, vehiculele hibrid pot avea o amprentă de carbon mai redusă și nici nu necesită timp îndelungat de încărcare a bateriilor, precum cele electrice) (Awwad, Shekhar și Iyer 2018, 586). Autorii punctează, la finalul studiului, nevoia de identificare a impedimentelor implementării soluțiilor prezentate, precum și ideea utilizării cuprinzătoare a acestora, pentru obținerea unor rezultate concludente.

Trecerea timpului a produs schimbări benefice, fapt ce reiese din existența unui studiu care analizează lucrările publicate pe tema aplicării tehnologiilor specifice Industriei 4.0 pentru sustenabilitatea logisticii, pe baza analizei bibliometrice și a conținutului publicațiilor. Problematica adoptării unor tehnologii care facilitează implementarea sustenabilității s-a conturat, astfel, ca o a doua arie tematică principală. Astfel, potrivit analizei autorilor, 40% din preocupările cercetătorilor au vizat digitalizarea sistemelor logistice; 22,6% – studiile interdisciplinare; 20,9% – transportul sustenabil; 10,4% – obiectivele de producție și achiziții sustenabile, pe cel mai îngust segment al preocupărilor aflându-se depozitarea sustenabilă – 5,2% (Sun și alții 2022, 9560-91).

În ceea ce privește soluțiile de aplicare în practică a tehnologiilor pentru obținerea sustenabilității logisticii, studiul scoate în evidență douăsprezece soluții inovatoare, studiate de cercetători în perioada 2017-2020 (Sun și alții 2022, 9560-91). Se poate remarca astfel orientarea masivă a logisticii din sfera civilă către exploatarea beneficiilor digitalizării și ale integrării progresului tehnologic, în scopul obținerii sustenabilității. În ciuda numeroaselor preocupări existente pe linia importanței implementării tehnologiilor specifice Industriei 4.0 pentru atingerea sustenabilității, studiul semnalează lipsa preocupărilor de identificare a provocărilor generate de această transformare (Sun și alții 2022, 9560-91). Cu alte cuvinte, un efort științific consistent a fost făcut pe linia teoretizării și demonstrării beneficiilor aferente integrării acestor tehnologii, însă nu au fost identificate măsurile necesar a fi luate și consecințele acestora, aspecte care se constituie în importante lacune ale cunoașterii din domeniul logisticii sustenabile.

Drept urmare, autorii propun, ca direcții viitoare de cercetare, următoarele: completarea viziunii tehnologice a Industriei 4.0 cu cea umană, specifică Industriei 5.0, pentru sprijinirea laturii sociale a logisticii sustenabile; implementarea unor algoritmi ce sprijină sistemul decizional, care iau în calcul cele trei dimensiuni ale dezvoltării durabile; nevoia de analizare aprofundată a amprentei de mediu, generată prin utilizarea energiei pentru producerea și reciclarea bunurilor; dezvoltarea unor modele analitice de optimizare a modului în care pot fi implementate tehnologiile specifice Industriei 4.0; utilizarea digitalizării pentru sporirea autonomiei sistemelor logistice; exploatarea avantajelor implementării soluțiilor de transport

semiautonome; acordarea unei atenții sporite modului în care tehnologiile Augmented Reality/AR și Additive Manufacturing/AM pot spori sustenabilitatea logisticii; dezvoltarea laturii sustenabile a logisticii inverse; utilizarea tehnologiilor Industriei 4.0 pentru sporirea rezilienței în condiții speciale, precum pandemiile (Sun și alții 2022, 9560-91). Analizând cele prezentate în acest studiu, se poate remarca potențialul enorm al tehnologiilor inovatoare pentru sporirea sustenabilității logisticii, acest deziderat părând a fi imposibil de îndeplinit, fără luarea măsurilor de digitalizare a logisticii.

În strânsă legătură cu perspectiva oferită de Industria 5.0, un concept apropiat de logistica sustenabilă este Logistica 5.0, canalizată pe identificarea unor soluții de ambalare, de transport și depozitare prietenoase cu mediul și pe sporirea preocupării față de consumatori (Trstenjak și alții 2022, 2). Totuși, componenta referitoare la tehnologii rămâne importantă și în Logistica 5.0, studiile arătând că atât pandemia de COVID-19, cât și războiul ruso-ucrainean au scos în evidență urgența adoptării unor soluții logistice inteligente (Jafari, Azarian și Yu 2022, 1-27). Astfel, logistica de tip sustenabil trebuie să răspundă atât acțiunilor din sfera celor trei piloni ai dezvoltării durabile, cât și celor specifice logisticii inteligente.

O altă lucrare axată pe analiza literaturii dedicate producției și logisticii sustenabile, în contextul creat de cea de-a patra revoluție industrială, întărește rolul proceselor automatizate în aplicarea managementului sustenabil (Grzybowska, Awasthi și Sawhney 2020, 1-18). Tehnicile matematice și statistice folosite de autori au condus și la identificarea evoluției istorice a celor două concepte, producția sustenabilă fiind studiată începând cu anul 1987, iar logistica sustenabilă începând cu anul 2004, fiind un concept asociat cu industria ecologică și economia circulară (Grzybowska, Awasthi și Sawhney 2020, 5). Studiul s-a bazat pe un eșantion, format din 892 de lucrări științifice, produse de cercetători din 91 de țări, cele mai multe fiind publicate în jurnale științifice, pe primele două locuri aflându-se *Journal of Cleaner Production* și *Sustainability*. Autorii au identificat și existența mai multor etape în preocupările cercetătorilor interesați de sustenabilitate (perioada activării: 1980-2006, perioada de creștere: 2007-2015 și perioada de expansiune: 2016-2018), logistica sustenabilă aparținând celei de-a treia perioade, fiind identificat un trend al înlocuirii acestui concept cu cel de sustenabilitate a lanțului de aprovizionare-livrare (Grzybowska, Awasthi și Sawhney 2020, 15).

Cea de-a treia temă importantă din sfera sustenabilității logisticii, abordată în studiile bazate pe analiza literaturii de specialitate, este reprezentată de sistemele de asistare a deciziei. Din această perspectivă, la nivelul anului 2017, cercetătorii au concluzionat că beneficiile utilizării acestor sisteme pentru implementarea logisticii sustenabile sunt reale, având în vedere dificultatea procesului decizional de la nivel strategic, operativ și tactic, în contextul dezideratului dezvoltării durabile (Qaiser și alții 2017, 1). De asemenea, este adusă în discuție necesitatea utilizării unui model sustenabil de alegere între furnizorii locali și cei externi, care permite includerea celor trei dimensiuni ale sustenabilității în analizarea unor criterii, precum costurile

și emisiile de carbon, generate din perspectiva mai multor moduri de transport și a altor operațiuni logistice (Katiraee și alții 2024, 13).
Predilecția pentru identificarea unor instrumente care să asiste factorii decizionali în demersul de eficientizare a costurilor și impactului logisticii asupra mediului, precum și insuficienta atenție acordată laturii sociale a sustenabilității a fost, de asemenea, semnalată (Qaiser și alții 2017, 6). Astfel, se impune exploatarea holistică a fezabilității utilizării instrumentelor decizionale pentru obținerea logisticii sustenabile (Qaiser și alții 2017, 7). Este așadar vorba despre păstrarea tuturor liniilor directoare ale dezvoltării durabile, abordarea axată doar pe o dimensiune a acesteia fiind insuficientă.

Din perspectiva nevoii de întărire a dimensiunii sociale a logisticii sustenabile, studiile mai recente abordează o a patra arie tematică, aratând că personalul care lucrează în acest domeniu trebuie să beneficieze de condiții decente de lucru, reglementate corespunzător, fiind implicat într-o multitudine de operațiuni, precum: gestionarea depozitării, stabilirea rutelor de transport, planificarea și programarea producției, managementul forței de muncă, dimensionarea loturilor (Prunet și alții 2024, 18-19).

Exceptând studiile prezentate, au existat și alte preocupări pe linia logisticii sustenabile, printre problematicile abordate aflându-se logistica umanitară, în strânsă legătură cu latura socială a logisticii sustenabile, reprezentând astfel cea de-a cincea temă principală în problematica logisticii sustenabile. Autorul investighează posibilitatea considerării logisticii umanitare sustenabile ca pe un domeniu distinct de cercetare, axându-se pe principiile de respectat și pe modalitățile concrete de punere în practică. Astfel, abordarea sistemică este evidențiată ca factor favorabil implementării sustenabilității în logistica umanitară, pentru luarea în considerare a pilonilor dezvoltării durabile (Remida 2015, 11-29).
De asemenea, autorul evidențiază trei niveluri de obiective care pot fi vizate, respectiv: la nivel strategic, abordarea integratoare a pilonilor dezvoltării durabile; la nivel tactic, cel mai aproape de logistica umanitară și de beneficiarii acesteia, acțiunile umanitare; iar la nivel „operațional", logistica abordată sistemic, activitățile de planificare, de aprovizionare și cele care țin de alte subsisteme ale logisticii (Remida 2015, 21).

În plus, studiul aduce în atenție și câteva caracteristici ale logisticii umanitare sustenabile, aceasta având potențialul de a lărgi orizontul spațio-temporal, și cerința de a lua în considerare toți actorii implicați. Pentru sustenabilitatea logisticii umanitare, autorul semnalează importanța aplicării unor principii, precum: transdisciplinaritatea, viziunea dual (reacția imediată și efectul de durată, efortul privat și public), fructificarea analogiei cu alte sisteme logistice din alte domenii, precum sistemul militar. Deși studiul reliefează necesitatea obținerii unor efecte de durată prin efectuarea de exerciții în comun cu forțele militare și prin posibilitatea utilizării infrastructurii militare existente, acesta nu investighează modalitatea preluării unor modele de logistică sustenabilă din domeniul militar și nici nu

detaliază sustenabilitatea logisticii militare ca un posibil exemplu pentru cea umanitară (Remida 2015, 26-27).

Rămânând în sfera logisticii umanitare, un studiu mai recent, bazat pe modelare și pe chestionar sociologic, pledează pentru studierea logisticii aplicabile în cazul dezastrelor naturale sau umane în cadrul programelor universitare, pentru atingerea sustenabilității, pe fondul lipsei logisticienilor și al utilizării masive a voluntarilor fără pregătire de specialitate. Autorul concluzionează, la un moment dat, că folosirea logisticienilor pregătiți poate aduce sustenabilitatea oricărei organizații, aspect ce reliefează rolul însemnat al logisticii pe linia dezvoltării durabile. Una dintre limitele studiului este că acesta a fost realizat prin respondenți din mediul academic, fără a se lua în considerare și alți actori, precum cei din organizația militară, adesea implicată în eliminarea consecințelor dezastrelor și în ajutorarea populației afectate (Khan și alții 2020, 1-30). Astfel, considerăm că activitățile umanitare din sfera logisticii militare ar putea fi încadrate în latura socială a logisticii militare sustenabile, pentru completarea cadrului acestui nou concept.

Stadiul cunoașterii în domeniul logisticii militare sustenabile

În cea de-a doua etapă, în scopul identificării stadiului cunoașterii în domeniul logisticii militare sustenabile, am efectuat căutări în baze de date, precum: Google Scholar și ProQuest. Studiile identificate au fost, de asemenea, ierarhizate, în funcție de contribuția la îmbogățirea stadiului cunoașterii, fiind luate în calcul criterii, precum: numărul de citări, anul apariției, impactul jurnalelor în care au apărut. Întrucât, din perspectivă militară, rezultatele căutărilor nu au fost la fel de numeroase ca cele din sfera logisticii sustenabile economice, nu au putut fi identificate publicații care au analizat deja literatura de specialitate în domeniu. În continuare, sunt prezentate principalele aspecte reieșite din analiza lucrărilor relevante, care au abordat problematica sustenabilității la nivelul logisticii militare.

Un studiu util pentru logisticienii militari care urmăresc eficientizarea și sustenabilitatea acestui domeniu exemplifică importanța analizei multicriteriale în luarea deciziei referitoare la alegerea furnizorilor și axelor de aprovizionare a forțelor militare din teatrul de operații Irak. Autorii furnizează o definiție a sustenabilității axelor de aprovizionare, care presupune folosirea rațională a resurselor, bazată pe dezvoltarea tehnologică, pe adaptarea instituțională și pe investiții (Alazzawi și Żak 2020, 578). Deși definiția are un caracter general, referirea la resurse, la tehnologie, la instituții și investiții o poate încadra parțial în contextul dezvoltării durabile.

Acest aspect reiese și din analiza criteriilor avute în vedere în procesul decizional, formulate expres pe ideea de eficiență economică și de protecție a mediului (Alazzawi și Żak 2020, 579). Lipsește totuși raportarea la dimensiunea socială a dezvoltării durabile, nefiind luate în considerare aspecte referitoare la resursa umană implicată

în realizarea coridoarelor de sprijin logistic și în alegerea furnizorilor, precum și la impactul acestor alegeri asupra beneficiarilor finali.

Un alt studiu abordează detaliat una dintre soluțiile tehnologice inovatoare care generează sustenabilitatea logisticii, respectiv utilizarea imprimantelor 3D pentru fabricarea pieselor de schimb necesare în misiunile forțelor militare și în aprovizionarea sustenabilă cu astfel de bunuri. Studiul este important prin prisma faptului că realizează o analiză a literaturii dedicate acestei problematici, studiază cazul particular al lanțului de aprovizionare-livrare cu piese de schimb din armata olandeză, asigurând accesul celor interesați la opiniile experților, exprimate în urma efectuării unor interviuri structurate. Acestea s-au desfășurat în urma analizării a 40 de articole și de 12 lucrări științifice, selecționat din 78.439 de publicații identificate pe această temă (Den Boer, Lambrechts și Krikke 2020, 1-11).

Deși autorii argumentează potențialul sustenabil al acestei tehnologii pentru evitarea rupturilor în lanțurile de aprovizionare-livrare, provocări, precum costurile mari, asociate cu achiziția și mentenanța imprimantelor 3D, identificarea surselor de energie, a colaboratorilor din plan local, este nevoie de cercetări suplimentare pentru a putea susține aspecte care țin de: externalizarea serviciului de producție sau de asigurarea acestuia prin intermediul specialiștilor militari, depozitarea și transportul materiei prime, securitatea informațiilor, disponibilitatea informațiilor referitoare la caracteristicile produselor, obținerea certificărilor pentru fabricarea pieselor de schimb și respectarea drepturilor de proprietate intelectuală (Den Boer, Lambrechts și Krikke 2020, 5-10).

Întrucât studiile analizate au arătat că cele mai mari probleme legate de implementarea tehnologiei AM țin de disponibilitatea producătorilor de a dezvălui informațiile legate de caracteristicile produselor și ținând cont că autorii nu susțin această soluție pentru producția de nivel industrial, ci doar în cantități reduse și în situații operaționale complexe, rezultă că o posibilă soluție ar putea veni din modul în care sunt creionate clauzele contractuale, aspect care este menționat ca o posibilă direcție pentru cercetările viitoare. Din această perspectivă, studiul accentuează nevoia de digitalizare în domeniul logisticii militare și de cooperare cu producătorii, deschizând calea către alternativa achizițiilor sustenabile din domeniul militar (Den Boer, Lambrechts și Krikke 2020, 7-10).
Exceptând studiile analizate, în domeniul militar mai există alte câteva preocupări axate pe subelemente ale logisticii sustenabile, însă acestea nu pot fi considerate relevante, dat fiind faptul că nu au fost utilizate la elaborarea altor lucrări.

Concluzii

Ținând cont de analiza efectuată asupra studiilor din domeniul civil al logisticii sustenabile, se poate concluziona că viitoarele cercetări trebuie să aibă caracter interdisciplinar și să vizeze maximizarea posibilităților de abordare integratoare a

celor cinci arii tematice identificate. La acest moment, două elemente se conturează ca indispensabile progresului pe această linie, respectiv digitalizarea proceselor logistice și implementarea tehnologiilor care facilitează tranziția către sustenabilitate. Din acest punct de vedere, viitoarele cercetări ar trebui să se axeze pe identificarea impedimentelor (provocărilor) care îngreunează acest parcurs. Chiar dacă beneficiile abordării sustenabile a logisticii sunt scoase în evidență, nu același lucru se poate afirma și despre consecințele acestei transformări. Drept urmare, viitoarele studii ar trebui să abordeze fiecare provocare, în paralel cu efectele generate prin integrarea sustenabilității.
Rezultatele acestor studii ar putea susține transformările menționate la nivelul procesului decizional, decidenții având posibilitatea să ia decizii informate, care țin cont atât de reflectarea, la nivel logistic, a celor trei dimensiuni ale dezvoltării durabile, cât și de implicațiile adoptării tehnologiilor adecvate și de efectele scontate.

Insuficient explorată de studiile anterioare, latura socială a logisticii sustenabile trebuie să aibă parte de cercetări care să vizeze atât beneficiile angajaților logisticieni, cât și cele ale comunităților. Un domeniu insuficient explorat în acest sens s-a conturat a fi cel al logisticii umanitare. Această linie tematică asigură și puntea dintre logistica civilă și cea militară, recomandările desprinse din cercetările anterioare axându-se pe identificarea modalităților de acțiune sustenabilă, similar celei adoptate de structurile militare. Însă indisponibilitatea unor studii care să ateste modul de abordare la nivel militar nu face decât să întărească nevoia de cercetări în această arie de activitate. Concret, viitoarele studii ar putea fi axate pe identificarea unor lecții rezultate din acțiunile umanitare la care au participat structurile militare, care ar putea avea potențialul de a facilita procesul de integrare a sustenabilității atât în sfera civilă, cât și în cea militară.
De asemenea, aspecte mai puțin studiate, precum cele referitoare la transporturi, producție, achiziție și depozitare sustenabile, ar trebui să se bucure mai mult de atenția cercetătorilor.

Din perspectiva studiilor militare analizate, se poate spune că publicațiile din domeniul logisticii militare sustenabile sunt puține, nu sunt interconectate și sunt axate pe elemente disparate din sfera logisticii sustenabile economice. Aducând în discuție doar două dintre cele cinci arii tematice identificate în cazul logisticii din sfera civilă (nevoia de digitalizare a logisticii militare, pentru facilitarea integrării unor tehnologii performante, și utilizarea unor criterii decizionale bazate pe cele trei dimensiuni ale dezvoltării durabile), cercetarea din domeniul logisticii militare sustenabile este în stadiu incipient. Rezultă astfel că fiecare dintre activitățile circumscrise celor cinci arii tematice abordate de logistica civilă ar putea reprezenta o viitoare direcție de certare la nivelul logisticii militare. În plus, pentru facilitarea adoptării soluțiilor logistice sustenabile, viitoarele cercetări ar putea să se axeze pe identificarea modalităților de operaționalizare a conceptului de achiziții sustenabile.

Nu în ultimul rând, o altă concluzie desprinsă din analiza publicațiilor militare este necesitatea definirii conceptului de logistică militară sustenabilă. Chiar dacă

prezentul studiu aduce în atenție o serie de dimensiuni și subdimensiuni ale acestui concept, în special prin prisma studiilor din sfera logisticii civile, cercetarea acestor componente, în cazul logisticii din domeniul militar, trebuie să aibă la bază studii de impact care să nu pună în pericol succesul operațiilor militare.

Mențiuni speciale

Acest studiu conține părți din Raportul de cercetare nr. 2, aferent tezei de doctorat cu titlul „*Managementul integrat al resurselor de apărare în contextul dezvoltării durabile*", susținută public în septembrie 2024.

Referințe

Alazzawi, Ali și Jacek Żak. 2020. "MCDM/A Based Design of Sustainable Logistics Corridors Combined with Suppliers Selection. The Case Study of Freight Movement to Iraq." *Transportation Research Procedia* (Elsevier) (47): 577-584. https://www.sciencedirect.com/science/article/pii/S2352146520303331.

Awwad, Mohamed, Abhijeet Shekhar și Abhishek Sundaranarayanan Iyer. 2018. "Sustainable Last-Mile Logistics Operation in the Era of E-Commerce." *Proceedings of the International Conference on Industrial Engineering and Operations Management*. Washington DC, SUA. 584-591. http://ieomsociety.org/dc2018/papers/179.pdf.

Belcher, Oliver, Patrick Bigger, Ben Neimark și Cara Kennelly. 2019. "Hidden Carbon Costs of the „everywhere war": Logistics, geopolitical ecology, and the carbon bootprint of the US military." *Transactions of the Institute of British Geographers* 45 (1): 65-80. https://rgs-ibg.onlinelibrary.wiley.com/doi/10.1111/tran.12319.

Best, Katharina Ley, Scott R. Stephenson și alții. 2023. "Research Report: Climate and Readiness. Understanding Climate Vulnerability of U.S. Joint Force Readiness." https://www.rand.org/pubs/research_reports/RRA1551-1.html.

Blewitt, John. 2018. *Understanding Sustainable Development.* Ediția a treia. Londra, New York: Routledge, Taylor & Francis Group.

Comisia Europeană. 2025. "Joint White Paper for European Defence Readiness 2030." Bruxelles, 1-23. https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf.

Cooper, Bradley. 2019. "Precision Logistics: Sustainment for Multi-Domain Operations." Institute of Land Warfare, The Association of United States Army, 1-8. https://www.ausa.org/sites/default/files/publications/SL-19-4-Precision-Logistics-Sustainment-for-Multi-Domain-Operations.pdf.

Den Boer, Jelmar, Wim Lambrechts și Harold Krikke. 2020. "Additive manufacturing in military and humanitarian missions: Advantages and challenges in the spare parts supply chain." *Journal of Cleaner Production* (Elsevier). https://www.sciencedirect.com/science/article/abs/pii/S0959652620303486.

Grigore, Dan Radu. 2021. „Evaluare și scientometrie." https://mepopa.com/Pdfs/dgrig21apr.pdf.

Grzybowska, Katarzyna, Anjali Awasthi și Rapinder Sawhney. 2020. "Sustainable Logistics and Production in Industry 4.0. New Opportunities and Challenges." https://link.springer.com/content/pdf/bfm:978-3-030-33369-0/1.

Harrington, Kent. 2016. ”US Navy Green Fleet Makes Biofuels the New Normal.” https://www.aiche.org/chenected/2016/01/us-navy-green-fleet-makes-biofuels-new-normal.

Jafari, Niloofar, Mathew Azarian și Hao Yu. 2022. ”Moving from Industry 4.0 to Industry 5.0: What Are the Implications for Smart Logistics?” *Logistics* (MDPI) 6 (26): 1-27. https://www.mdpi.com/2305-6290/6/2/26.

Katiraee, Niloofar, Nicola Berti, Ilaria Isolan, Martina Calzavara și Daria Battini. 2024. ”A sustainable joint economic lot size model for supplier selection under carbon emissions: A case study.” *Cleaner Logistics and Supply Chain* (Elsevier) 13: 1-14. https://doi.org/10.1016/j.clscn.2024.100187.

Khan, Muhammad, Muhammad Sarmad, Sami Ullah și Junghan Bae. 2020. ”Education for sustainable development in humanitarian logistics.” *Journal of Humanitarian Logistics and Supply Chain Management* (Emerald Publishing Limited) 1-30. https://www.emerald.com/insight/content/doi/10.1108/JHLSCM-03-2020-0022/full/html.

Kumar, Ranjit. 2011. *Research Methodology. A Step-by-step Guide for Beginners.* Ediția a treia. Sage Publications.

Mosher, David E., Beth E. Lachman, Michael D. Greenberg, Tiffany Nichols, Brian Rosen și Henry H. Willis. 2008. ”Green Warriors: Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict.” https://www.rand.org/pubs/monographs/MG632.html.

NATO. 2016. ”Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council.” Warsaw. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

___. 2020. ”NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General.” https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-reflection-group-final-report-uni.pdf.

___. 2021. ”NATO Climate Change and Security Action Plan.” https://www.nato.int/cps/en/natohq/official_texts_185174.htm?selectedLocale=en.

NATO Standardization Office. 2022. ”AAP-06, Glosar de termeni și definiții NATO.” 1-440. https://www.unap.ro/ro/news/aap6.pdf.

Pezzey, John. 1992. ”Sustainable Development Concepts: An Economic Analysis.” *World Bank Environment Paper* (The World Bank) (2): 1-92. https://documents1.worldbank.org/curated/en/237241468766168949/pdf/multi-page.pdf.

Prunet, Thibault, Nabil Absi, Valeria Borodin și Diego Cattaruzza. 2024. ”Optimization of human-aware logistics and manufacturing systems: A comprehensive review of modeling approaches and applications.” *EURO Journal of Transportation and Logistics* (Elsevier) 13: 1-25. https://www.sciencedirect.com/science/article/pii/S2192437624000116?via%3Dihub#sec9.

Qaiser, Fahham Hasan, Karim Ahmed, Martin Sykora, Alok Choudhary și Mike Simpson. 2017. ”Decision support systems for sustainable logistics: a review and bibliometric analysis.” *Industrial Management & Data Systems* 117 (7): 1376-1388. https://eprints.whiterose.ac.uk/115817/1/05042017%20IMDS%20SI%20on%20KB-DSS%20-%20IMDS-09-2016-0410%20-%20Final%20draft.pdf.

Remida, Aimen. 2015. ”A Systemic Approach to Sustainable Humanitarian Logistics.” În *Humanitarian Logistics and Sustainability, Lecture notes in Logistics*, de Matthias Klumpp, Sander De Leeuw, Alberto Regattieri și Robert De Souza. Springer.

Ren, Rui, Wanjie Hu, Jianjun Dong, Bo Sun, Yicun Chen și Zhilong Chen. 2019. "A Systematic Literature Review of Green and Sustainable Logistics: Bibliometric Analysis, Research Trend and Knowledge Taxonomy." *International Journal of Environmental Research and Public Health* 17 (261): 1-20. https://www.mdpi.com/1660-4601/17/1/261.

Stroufe, Robert P. 2018. *Integrated Management – How Sustainability Creates Value for Any Business.* Ediția întâi. Emerald Publishing Limited.

Sun, Xu, Hao Yu, Wei Deng Solvang, Yi Wang și Kesheng Wang. 2022. "The application of Industry 4.0 technologies in sustainable logistics: a systematic literature review (2012–2020) to explore future research opportunities." *Environmental Science and Pollution Research* (29): 9560–9591. https://link.springer.com/article/10.1007/s11356-021-17693-y.

Trstenjak, Maja, Tihomir Opetuk, Goran Đukić și Hrvoje Cajner. 2022. "Logistics 5.0 Implementation Model Based on Decision Support Systems." *Sustainability* (MDPI) 14 (11): 1-19. https://www.mdpi.com/2071-1050/14/11/6514.

United Nations. 1987. *Report of the World Commission on Environment and Development: Our Common Future.* Oslo: Oxford University Press, 1-300. https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf.

___. 2015. "Transforming our world: the 2030 Agenda for Sustainable Development." New York, 1-35. https://www.unfpa.org/sites/default/files/resource-pdf/Resolution_A_RES_70_1_EN.pdf.

Uniunea Europeană. 2022. "A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security." https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

Vie, Loryana L., MAJ Eric V. Trivette și Adam D. Lathrop. 2021. "Department of the Army Career Engagement Survey. First Annual Report." https://talent.army.mil/wp-content/uploads/2021/11/DACES-Annual-Report_JUNE2021.pdf.

Wichaisri, Sooksiri și Apichat Sopadang. 2017. "Trends and Future Directions in Sustainable Development." *Sustainable Development* (Wiley) 26 (1): 1-17. https://onlinelibrary.wiley.com/doi/10.1002/sd.1687.

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

Contraterorismul Statelor Unite ale Americii și Programul de detenție și interogare al CIA – între constrângere legislativă și permisivitate excepțională

USA Counterterrorism and the CIA Detention and Interrogation Program – between Legislative Constraint and Exceptional Permissiveness

Dr. Lucian BUCIU*
*Ministerul Afacerilor Interne, București
e-mail: buciu.lucian@yahoo.com

Abstract

Prin metoda calitativă a analizei Programului de detenție și interogare al CIA, prezenta cercetare științifică își propune să evalueze gradul de eficiență al tehnicilor de interogare intensificată, dezvoltate de CIA, bazându-se concomitent pe o dublă analiză de conținut: pe de-o parte, analiza primelor zece concluzii din Raportul Comisiei senatoriale, alese de comunitatea de informații a SUA cu privire la Programul de detenție și interogare al CIA, iar pe de altă parte, analiza elementelor puse la dispoziție de decidenți politici de vârf și de foști operativi din seviciile de intelligence americane. Caracterul de noutate al temei articolului științific de față pentru peisajul literaturii de specialitate din România, dedicate contraterorismului american, constă în faptul că, pentru a maximiza gradul de obiectivitate în evaluarea eficienței tehnicilor de interogare intensificată ale Agenției, acesta pune față în față dimensiunea legislativă, reliefată de Raportul Comisiei, cu cea informativ-operativă, susținută prin elemente factuale, selectate de la actanți importanți din cadrul comunității de informații americane.

Through the qualitative method of the USA counterterrorism and the CIA detention and interrogation program, this research aims to assess the effectiveness of the enhanced interrogation techniques developed by the CIA, simultaneously relying on a dual content analysis: on the one hand, an analysis of the first 10 findings of the Report of the US Senate Select Committee on Intelligence on the CIA's Detention and Interrogation Program and, on the other hand, an analysis of the evidence provided by top policy makers and former US intelligence operatives. The novelty of the subject of this scientific contribution for the Romanian literature on American counterterrorism resides in the fact that, in order to maximize the degree of objectivity in assessing the effectiveness of the Agency's enhanced interrogation techniques, it confronts the legislative dimension highlighted by the Commission Report and the information-operational dimension supported by factual elements selected from key actors within the American intelligence.

Cuvinte-cheie:
CIA; SUA; contraterorism; interogare intensificată; intelligence; legislație; excepționalitate.

Keywords:
CIA; USA; counterterrorism; enhanced interrogation; intelligence; legislation; exceptionality.

Info articol
Primit: 13 mai 2025; Evaluat: 2 iunie 2025; Acceptat: 11 iunie 2025; Disponibil online: 27 iunie 2025

Citare: Buciu, L. 2025. „Contraterorismul Statelor Unite ale Americii și Programul de detenție și interogare al CIA – între constrângere legislativă și permisivitate excepțională". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(2): 21-30. https://doi.org/10.53477/2065-8281-25-09

1. Delimitări conceptuale și instrumentar metodologic

Având în vedere multitudinea de definiții existente ale conceptului de terorism la nivelul cercetării din domeniul științelor politice, fără ca „niciuna să fie recunoscută unanim" (Bourdillon 2007, 45), prezentul articol științific va opera cu semnificatul terorism, în accepție saussuriană, prin raportare la patru elemente definitorii, reținute de la Bourdillon – o tehnică foarte bine elaborată care se folosește de violență pentru a genera frică în rândul unui număr semnificativ de persoane. Terorismul este, astfel, asimilat unui război atipic, asimetric: „Este vorba despre un război fără război, adică fără front identificat, fără reguli, fără prizonier, la care toată lumea ia parte, indiferent dacă vrea sau nu" (Bourdillon 2007, 50).

În același timp, este de notat că motivațiile politico-religioase care stau la baza acțiunii practicanților acestui război atipic plasează mai degrabă terorismul sub semnul unei „utopii politico-religioase" (Cusson 2018, 21). De aceea reușita unui atac terorist va fi dependentă de măiestria lingvistică cu care teroristul va reuși să verbalizeze revendicarea victoriei politico-religioase, având astfel de-a face cu un terorism „secret în acte și prolific în vorbe" (Pascallon 2018, 46).

În ceea ce privește complexitatea tipologiei terorismului, demersul de cercetare științifică se va focusa asupra terorismului de proveniență fundamentalist islamică, aliniindu-se cercetărilor din domeniul studiilor de securitate care atrag atenția asupra unei nepotriviri terminologice între religia islamică și terorism: „De menționat că, în esență, religia islamică și terorismul sunt doi termeni care se contrazic. Islamul condamnă și respinge toate formele de teroare. Astfel, nu este fezabilă utilizarea anumitor sintagme, cum ar fi cea de terorism islamic. Încercările de a pune semnul egalității între religia islamică și terorism nu sunt doar lipsite de fond și eronate, ci și pur propagandistice și rău intenționate" (Barna și Popa 2021).

Contraterorismul sau ceea ce ar putea fi antidotul împotriva terorismului de proveniență fundamentalist islamică va fi înțeles pe parcursul întregului demers științific în accepția propusă de *Legea nr. 535 din 25 noiembrie 2004 privind prevenirea și combaterea terorismului, cu modificările și completările ulterioare*, în art. 4, drept „ansamblul măsurilor ofensive realizate, în cazul unui act de terorism, în scopul eliberării ostaticilor, capturării ori anihilării teroriștilor, neutralizării dispozitivelor utilizate de aceștia, eliberării obiectivelor atacate sau ocupate, precum și restabilirii ordinii legale."

Din punctul de vedere al instrumentarului metodologic utilizat, articolul de față este rezultatul unei cercetări cu precădere calitative, alegând să folosească metoda analizei documentului.
Cercetarea va face apel la tehnica analizei de conținut atât calitative, cât și cantitative, aplicată în cazul primelor 10 concluzii din Raportul Comisiei, pentru a realiza o inventariere a principalelor argumente pe baza cărora Comisia a măsurat mai degrabă ineficiența tehnicilor de interogare intensificată, dezvoltate de CIA.

Pledoariilor foștilor decidenți de vârf și operativilor din intelligence-ul american, implicați direct sau indirect în acțiunile contrateroriste ale Agenției, le va fi consacrată o analiză de conținut calitativă pentru a identifica principalele caracteristici care îi îndeamnă pe aceștia să susțină mai degrabă eficiența tehnicilor de interogare intensificată ale Agenției.

Scopul primordial al cercetării va fi reprezentat astfel de stabilirea gradului de eficiență al contraterorismului american, operaționalizat de CIA, în condiții excepționale, imediat după episodul 9/11.
În acest sens, analiza propusă de cercetarea științifică de față se va cristaliza pe fondul tensiunii a două dimensiuni – pe de-o parte, dimensiunea legislativă, în registrul căreia se înscrie Raportul Comisiei, iar pe de altă parte, dimensiunea informativ-operativă, căreia i se circumscrie selecția de elemente relevante, oferite de foști decidenți de vârf și operativi din comunitatea americană de informații.
Așadar, gradul de eficiență al tehnicilor de interogare intensificată ale Agenției va fi evaluat în funcție de măsura în care acestea au produs sau nu intelligence, în urma aplicării lor, și dacă, în final acestea, au adus sau nu succese contrateroriste.

2. Contextul elaborării Raportului Comisiei senatoriale alese de comunitatea intelligence a SUA cu privire la Programul de detenție și interogare al CIA

Atacurile teroriste, din 9/11, din SUA au reprezentat un t_0 în ceea ce privește resetarea contraterorismului american, în sensul în care CIA, în condiții excepționale și sub presiunea timpului, va operaționaliza o serie de așa-zise tehnici de interogare intensificată în războiul declarat împotriva terorismului, pe fondul unei puternici emoții sociale: „Acest sfidător atac a ucis aproape 3.000 de oameni și a șocat publicul american, care era mistuit de o dorință arzătoare de răzbunare" (Petraeus și Roberts 2025, 227).

Resetarea contraterorismului american aduce cu sine și o reformă din temelii a comunității americane de intelligence, odată cu *Legea privind reforma serviciilor secrete și prevenirea terorismului din 2004 (Intelligence Reform and Terrorism Prevention Act of 2004)*, atunci când „Congresul mandatase culegerea de informații interne" (Hayden 2018, 190), fiind, totodată, înființată funcția de *Director of National Intelligence (DNI)* care o va înlocui pe cea de *Director of Central Intelligence (DCI).*

După ce jurnalista Dana Priest de la Washington Post a început, în 2005, o așa-zisă „paradă Pulitzer, cu o demascare a programului de detenție și interogare al CIA" (Hayden 2018, 195), fostul director CIA, Michael Hayden, va decide doi ani mai târziu, în 2007, să pună la dispoziția membrilor Comisiei senatoriale, alese de comunitatea de intelligence a SUA, înregistrările video ale deținuților Abu Zubaydah și Abd al-Rahim al Nahiri, la sediul CIA (MacArthur și Horton 2015, 77). În 2009, Comisia demarează o anchetă referitoare la maniera în care au fost utilizate tehnicile

de interogare intensificată de către CIA în războiul dus de SUA împotriva terorismului: „în data de 5 martie 2009, cu un vot de 14 contra 1, Comisia a aprobat ordinul de misiune al unei anchete privind Programul de detenție și de interogare al CIA (MacArthur și Horton 2015, 77).

În decembrie 2012, la 3 ani de la demararea anchetei și în urma unei intense activități analitice, consacrate Programului de detenție și interogare, operaționalizat de CIA, raportul, care include 20 de constatări și concluzii, este aprobat cu majoritate de voturi de Comisia prezidată de Dianne Feinstein. În 2014, cu majoritate de voturi, Comisia prezintă președintelui „varianta revizuită a constatărilor și concluziilor, precum și sinteza raportului, în vederea declasificării lor și comunicării publice" (MacArthur și Horton 2015, 80).
Așadar, „competențele excepționale în lupta împotriva amenințării teroriste" (Rodriguez Jr. 2014, 164), de care CIA se va folosi, vor fi analizate punctual în prezentul demers științific.

Totodată, analiza primelor 10 constatări și concluzii din Raportul Comisiei senatoriale, alese de serviciile de intelligence ale SUA cu privire la Programul de detenție și interogare al CIA, se arată oportună și din perspectiva deliberării referitoare la tensiunea dintre constrângere legislativă/etică versus permisivitate excepțională, în numele luptei duse de SUA împotriva terorismului.

3. Concluziile Raportului Comisiei senatoriale alese de comunitatea de intelligence a SUA cu privire la Programul de detenție și interogare al CIA[1]

3.1. „Utilizarea de către CIA a tehnicilor de interogare intensificată nu a fost un mijloc eficient de a dobândi informații sau de a obține cooperarea deținuților" (United States Senate 2014, 12).
Prin folosirea de șapte ori a cuvântului „intelligence" în conținutul primei concluzii din Raport, Comisia încearcă gradual să încline balanța mai degrabă înspre ineficiența tehnicilor de interogare intensificată ale Agenției. Principalul element pe care Comisia își consolidează argumentația se referă la faptul că tehnicile au fost aplicate de Agenție pe un număr de șapte dintre cei 39 de deținuți, eșuând în a obține informații relevante.
Generalizarea ineficienței tehnicilor de interogare intensificată pe un eșantion nesemnificativ de șapte, din totalul celor 39 de deținuți ai Agenției trădează mai degrabă o intenție vădit politică a Comisiei, de a dicta, încă de la prima concluzie, o abordare care pare a se creiona înspre respingerea eficienței Programului CIA.
Comisia apreciază că ineficiența tehnicilor de interogare intensificată ale CIA este justificată la nivel psihologic prin faptul că deținuții, supuși

[1] Prezentul demers științific va analiza primele 10 concluzii din raportul Comisiei.

regulat unor tratamente brutale, coercitive, aleg adesea să comunice informații false sau parțial veridice, menite a-l deruta pe intervievator și a-l persuada asupra autenticității celor relatate.
Din analiza conținutului paragrafelor acestei prime concluzii a Comisiei, nu au rezultat elemente concrete care să susțină ineficiența tehnicilor Agenției din punct de vedere psihologic și din cel al informațiilor false sau parțial veridice.

În schimb, din argumentația fostului director CIA, Michael Hayden, care abundă în date concrete, va fi reținut faptul că, pe baza instrumentarului contraterorist, operaționalizat de CIA, au fost întocmite aproape 8.000 de rapoarte, cu relevanță directă în direcția consolidării securității SUA și descifrării rețelei complexe a teroriștilor (Hayden 2018, 427). Din analiza argumentației foarte precise, chiar matematice a fostului director CIA, reiese o evidentă respingere a ineficienței tehnicilor de interogare intensificată ale Agenției.

Calitatea excepțională a informațiilor obținute pe baza interogatoriilor intensificate ale Agenției este susținută, totodată, cu date din teren și de către Jose A. Rodriguez Jr, fostul șef al contraterorismului din cadrul CIA: „Informațiile obținute de la KSM, ca și cele aflate mai înainte de la AZ, s-au dovedit neprețuite. 441 dintre cele 1.700 de note de subsol din Raportul Comisiei 11 septembrie au provenit din interogatoriile luate liderilor Al-Qaeda" (Rodriguez Jr. 2014, 134).

Însă apogeul valorii inestimabile a informațiilor obținute prin tehnicile de interogare intensificată ale Agenției va duce, la 2 mai 2011, la uciderea lui Osama bin Laden, reprezentând *de facto* „punctul culminant al muncii de peste un deceniu a serviciilor de informații care în sfârșit îl localizaseră" (Petraeus și Roberts 2025, 255).

3.2. „Justificarea CIA pentru utilizarea tehnicilor sale de interogare intensificată s-a bazat pe afirmații inexacte cu privire la eficacitatea lor" (United States Senate 2014, 12-13).
Enumerarea, în conținutul celei de-a doua concluzii a cinci dintre cele mai importante instituții ale statului american – Casa Albă, Consiliul Securității Naționale, Departamentul de Justiție, Biroul Inspectorului General al CIA și Congresul –, consolidează pledoaria Comisiei în privința ineficienței tehnicilor de interogare intensificată ale Agenției și, totodată, îmbracă textual forma unei acuze directe aduse CIA de către Comisie, în ceea ce privește legalitatea îndoielnică a instrumentarului contraterorist, operaționalizat în condiții excepționale.

Tensiunea textuală se accentuează gradual, Comisia mergând până într-acolo încât să afirme că „soluția CIA era simplă – să mintă" (MacArthur și Horton 2015, 20), pentru a nu fi împiedicată din punct de vedere juridic să își pună în aplicare instrumentarul de tehnici de interogare intensificată.
Cu toate acestea, argumentele punctuale, evocate de Jose A. Rodriguez Jr., șeful Centrului pentru Combaterea Terorismului al CIA, de după perioada 9/11, traduc eficiența indubitabilă a tehnicilor de interogare intensificată ale Agenției: „După ce a

început să coopereze, informațiile furnizate de AZ de bunăvoie au fost unele dintre cele mai importante informații culese după 11 septembrie" (Rodriguez Jr. 2014, 109).

3.3. „Interogatoriile deținuților CIA au fost brutale și mult mai rele decât ceea ce CIA a prezentat decidenților politici și altora" (United States Senate 2014, 13-14).
Din folosirea predilectă a termenilor din câmpul semantic al brutalității în conținutul concluziei (ca, de exemplu, „coercitiv", „nociv fizic", „leziuni fizice", „privarea de somn", „tehnica simulării înecului"), se poate observa intenția Comisiei de a întări ineficiența tehnicilor de interogare intensificată ale Agenției.
În contrapartida celor de mai sus, din analiza argumentației lui Jose A. Rodriguez Jr., fostul șef al contraterorismului din cadrul CIA, va fi reținut exemplul concret al tehnicii peretelui, care traduce prin excelență o respingere categorică a așa-zisei brutalități a interogatoriilor, acesta probând cu date din teren că „multe dintre tehnici sunt, în esență, niște cacealmale" (Rodriguez Jr. 2014, 103).

3.4. „Condițiile de detenție ale deținuților CIA au fost mult mai rele decât ceea ce CIA a prezentat decidenților politici și altora" (United States Senate 2014, 14).
Din analiza conținutului acestei concluzii, se degajă folosirea predilectă de către Comisie a unor termeni circumscriși câmpului semantic al detenției (ca, de exemplu, „sărac", „întuneric complet", „celule izolate", „temniță", „lipsa contactului uman"), care ar putea fi interpretat, în cheia unei acuze directe la adresa Agenției din partea Comisiei, reproșându-i-se CIA faptul că a recurs la ascunderea adevărului cu privire la condițiile reale de detenție și la pregătirea psihologică îndoielnică a intervievatorilor care reprezentau un pericol extrem pentru viața deținuților.

De cealaltă parte a baricadei, din analiza pledoariei lui Jose A. Rodriguez Jr., se desprinde gradual falsitatea acestei concluzii a Comisei, întărită de fostul operativ prin exemplul concret al controlului medical: „(…) li se făcea un control medical amănunțit, pentru a vedea dacă aveau vreo afecțiune care ar fi împiedicat, în cazul lor, aplicarea în condiții de siguranță a tehnicilor" (Rodriguez Jr. 2014, 104).

3.5. „CIA a furnizat în mod repetat informații inexacte Departamentului de Justiție, împiedicând o analiză juridică adecvată a Programului de detenție și interogare al CIA" (United States Senate 2014, 14-15).
Predilecția Comisiei pentru utilizarea unor termeni din câmpul semantic al legalității (ca, de exemplu, „justiție", „incorect", „verificare", „tortură", „interdicție", „memorandum") în textul argumentat al acestei concluzii evidențiază o dată în plus acuza Comisiei față de legalitatea îndoielnică a Programului CIA.

Ca urmare a probelor desprinse din analiza documentelor oficiale avute la dispoziție, membrii Comisiei senatoriale alese de comunitatea de intelligence a SUA cu privire la Programul de detenție și interogare al CIA aduc o serie de argumente incriminatorii la adresa Agenției, susținând că „juriștii CIA au mințit de fiecare dată ca să îi înșele pe juriștii Departamentului de Justiție, aparent pentru a obține avizele de care aveau nevoie" (MacArthur și Horton 2015, 17).

În schimb, din argumentația fostului operativ Jose A. Rodriguez Jr., fundamentată pe elemente legislative concrete, se desprinde înclinarea balanței în favoarea legalității Programului Agenției, acesta dezvăluind că „aprobarea tehnicilor de interogare ne-a parvenit sub forma unui memoriu de la Biroul de Consiliere Juridică din cadrul Departamentului de Justiție" (Rodriguez Jr. 2014, 104).

3.6. „CIA a evitat activ sau a împiedicat supervizarea programului de către Congres" (United States Senate 2014, 15-16).
Folosirea insistentă de patru ori în penultimul paragraf, din conținutul acestei concluzii, a termenului „inexact" nu face decât să traducă acuzele Comisiei referitoare la legalitatea îndoielnică a instrumentarului operaționalizat de CIA, în cadrul Programului de detenție și interogare a deținuților, aprobat de fostul președinte american George W. Bush.

Prin utilizarea formelor verbale negative (ca, de exemplu, „CIA nu a informat", „CIA nu a răspuns"), precum și a termenilor care pot fi grupați ca aparținând câmpului semantic al respingerii („s-a împotrivit", „refuzând", „a declinat răspunsul"), în conținutul acestei concluzii, Comisia reușește să își consolideze și mai evident acuzele la adresa Agenției privind cadrul legal neclar care planează asupra tehnicilor de interogare intensificată.

În opoziție cu Comisia, va fi reținută, din analiza pledoariei lui Jose A. Rodriguez Jr., menționarea decretului prezidențial MON, prin care fostul președinte Bush acordă competențe excepționale CIA, după cele întâmplate la 9/11, pentru a duce războiul împotriva terorismului (Rodriguez Jr. 2014, 164). În același timp, fostul director CIA Hayden, prin întrebuințarea textuală a unei construcții prezentative nu face decât să reliefeze importanța excepționalității instrumentalizării tehnicilor de interogare intensificată, care este mai presus de orice acuză referitoare la calitatea îndoielnică a cadrului legislativ, având în vedere cele întâmplate la 9/11: „Acesta nu este programul președintelui. Acesta este programul Americii."

3.7. „CIA a împiedicat efectiv supervizarea de către Casa Albă și luarea deciziilor" (United States Senate 2014, 16-17).
Prin folosirea simetrică, în primul și în ultimul paragraf, a termenilor „inexact" și „incomplet" din conținutul acestei concluzii, se conturează o tensiune textuală graduală care traduce de facto un fel de rechizitoriu al Comisiei, îndreptat împotriva Agenției, căreia îi reproșează o informare incompletă și inexactă a Casei Albe, în ceea ce privește eficiența tehnicilor de interogare intensificată.

Și această concluzie a Comisiei ar putea fi contrazisă prin raportare la argumentația lui Jose A. Rodriguez Jr., din care va fi reținut exemplul referitor la autorizarea prezidențială, venită dinspre Casa Albă, care traduce o întărire a legalității instrumentarului contraterorist, operaționalizat de CIA, în condiții excepționale, după episodul 9/11: „La mai puțin de o săptămână după atentatele din 11 septembrie,

președintele ne-a autorizat în mod oficial să capturăm, să extrădăm și să interogăm teroriști" (Rodriguez Jr. 2014, 71).

3.8. „Operarea și gestionarea de către CIA a programului au complicat și, în unele cazuri, au împiedicat misiunile de securitate națională ale altor agenții ale ramurii executive" (United States Senate 2014, 17-18).
Din analiza conținutului acestei concluzii, se desprinde gradual constituirea unui câmp semantic al constrângerii („a complicat", „a împiedicat", „a limitat", „a respins", „a blocat"), care traduce poziția de critică vehementă a Comisiei în ceea ce privește competențele excepționale cu care CIA a fost înzestrată de fostul președinte Bush, pentru a lupta împotriva terorismului, punând în practică instrumentarul tehnicilor de interogare intensificată. Comisia se poziționează împotriva excepționalității de acțiune, acordate Agenției, evidențiind că și FBI este componentă a comunității de informații a SUA și, în consecință, poate îndeplini cu succes misiuni contrateroriste, în numele SUA.

Din analiza argumentelor factuale ale fostului șef al contraterorismului din CIA Jose A. Rodriguez Jr., se desprinde opoziția fermă a acestuia față de pledoaria de mai sus a Comisiei, acesta arătându-se vizibil în favoarea competențelor excepționale acordate Agenției în războiul împotriva terorismului: „Mentalitatea FBI este de a strânge informații care să poată fi folosite pentru a face dovada unei infracțiuni în fața instanței. Ofițerii CIA se axează pe culegerea de informații care să prevină comiterea unor noi acte de terorism" (Rodriguez Jr. 2014, 93).

3.9. „CIA a împiedicat supervizarea de către Biroul Inspectorului General al CIA" (United States Senate 2014, 18).
Constituirea graduală a unui câmp semantic al reticenței („a evitat", „s-a împotrivit", „a împiedicat"), precum și folosirea repetată a termenului „inexact" în cel de-al doilea paragraf surprind textual poziția acuzatorie a Comisiei, prezidate de Dianne Feinstein, referitoare la legalitatea tehnicilor de interogare intensificată ale CIA, invocând inexistența unei supervizări a Programului Agenției de către Biroul Inspectorului General al CIA.

Din analiza pledoariei lui Jose A. Rodriguez Jr., se conturează poziționarea acestuia în antiteză cu cele susținute de Comisie, fostul operativ din CIA oferind argumente punctuale în favoarea legalității tehnicilor de interogare intensificată ale CIA: „La mai puțin de o săptămână după atentatele din 11 septembrie, președintele ne-a autorizat în mod oficial să capturăm, să extrădăm și să interogăm teroriști" (Rodriguez Jr. 2014, 71).

3.10. „CIA a coordonat difuzarea de informații clasificate către mass-media, inclusiv informații inexacte, referitoare la eficacitatea tehnicilor de interogare intensificată ale CIA" (United States Senate 2014, 18-19).
Folosirea repetitivă a termenului „inexact" în ultimul paragraf al concluziei accentuează poziția ferm incriminatoare a Comisiei la adresa Agenției, căreia îi sunt

aduse acuze dure privind scurgeri de informații clasificate false în mass-media, vădit intenționat pentru a întări succesele notabile în materie de contraterorism american, înregistrate prin operaționalizarea tehnicilor de interogare intensificată ale CIA, aprobate în circumstanțe excepționale de la nivel prezidențial.

Din analiza argumentației lui Jose A. Rodriguez Jr., reiese maniera foarte directă și dură prin care acesta respinge cu fermitate faptul că Agenția ar fi responsabilă de o posibilă scurgere de informații clasificate în mass-media și admite că asemenea speculații prejudiciază grav imaginea CIA (Rodriguez Jr. 2014, 227), poziție la care pare vizibil a adera și fostul director CIA Hayden, așa după reiese din analiza argumentelor punctuale, menționate de acesta: „Le-am relatat jurnaliștilor că o avalanșă recentă de articole ne costase cinci surse antiteroriste și antiproliferare promițătoare, care se temeau că nu le puteam garanta securitatea. (…) Când o prezență CIA sub acoperire, dintr-o zonă interzisă a fost dezvăluită în mass-media, două surse locale au fost arestate și executate" (Hayden 2018, 137).

Concluzii

În scopul maximizării obiectivității în evaluarea gradului de eficiență al tehnicilor de interogare intensificată, operaționalizate de CIA, după episodul 9/11, prezenta cercetare științifică s-a concentrat concomitent pe realizarea unei duble analize: pe de-o parte, analiza primelor zece concluzii din Raportul Comisiei, prezidate de Diane Feinstein, iar pe de altă parte, analiza argumentațiilor foștilor actanți importanți de la vârful conducerii CIA.

Pe fondul tensiunii textual-discursive dintre dimensiunea politico-legislativă, în registrul căreia se înscriu concluziile din Raportul Comisiei senatoriale, și dimensiunea informativ-operativă, care cuprinde argumentațiile foștilor actanți importanți din CIA, evaluarea gradului de eficiență al tehnicilor de interogare intensificată ale CIA a condus, în urma analizei effectuate, la evidențierea a două tabere polarizate: cei din Comisia senatorială, prezidată de Feinstein, care susțin ineficiența tehnicilor de interogare intensificată ale CIA, cărora li se opun foștii actanți importanți și operativi, care pledează pentru eficiența contraterorismului operaționalizat de CIA după 9/11.

Fără a neglija sub nicio formă deficiențele de natură procedurală din punct de vedere legislativ, în ceea ce a presupus operaționalizarea tehnicilor de interogare intensificată ale CIA, în condiții excepționale, contracronometru, și având în vedere că, în urma interogatoriilor, derulate de Agenție, au fost obținute informații extrem de utile care, ulterior, au fost valorificate și au dus la uciderea lui Osama bin Laden la data de 2 mai 2011, se poate concluziona că tehnicile de interogare intensificată ale CIA s-au dovedit a fi, în cele din urmă, eficiente, atingându-și obiectivul final.

Referințe

Barna, Cristian și Adrian Popa. 2021. *Forme de manifestare a terorismului în societatea contemporană.* București: Editura Top Form.

Bourdillon, Yves. 2007. *Terrorisme de l'Apocalypse. Enquête sur les idéologies de destruction massive.* Paris: Ellipses.

Congress.gov. 2004. „Legea privind reforma serviciilor secrete și prevenirea terorismului din 2004." https://www.congress.gov/bill/108th-congress/senate-bill/2845.

Cusson, Maurice. 2018. *L'antiterrorisme à l'âge du djihadisme.* Paris: L'Harmattan.

Hayden, Michael V. 2018. *Pe muchie de cuțit. Serviciile secrete americane în epoca terorii.* București: Editura Meteor Press.

MacArthur, John R. și Scott Horton. 2015. *La CIA et la torture.* Paris: Les Arènes.

Parlamentul României. 2004. „Legea nr. 535 din 25 noiembrie 2004 privind prevenirea și combaterea terorismului, cu modificările și completările ulterioare." *Monitorul Oficial* nr. 1.161 din 8 decembrie 2004. https://legislatie.just.ro/Public/DetaliiDocumentAfis/57494.

Pascallon, Pierre. 2018. *Rendre le renseignement plus efficace dans la lutte contre le terrorisme.* Paris: L'Harmattan.

Petraeus, General David și Andrew Roberts. 2025. *Conflict. Evoluția războiului din 1945 până la luptele din Gaza.* București: Litera.

Rodriguez Jr., Jose A. 2014. *Măsuri extreme. Cum au salvat măsurile dure adoptate de CIA după 11 septembrie viețile cetățenilor americani.* București: Editura RAO.

Șandor, Sorin Dan. 2013. *Metode și tehnici de cercetare în științele sociale.* București: Editura Tritonic.

United States Senate. 2014. "Report of the Senate Select Committee on Intelligence. Committee Study of the Central Intelligence Agency's Detention and Interrogation Program together with Foreword by Chairman Feinstein and Additional and Minority Views." https://www.intelligence.senate.gov/sites/default/files/publications/CRPT-113srpt288.pdf.

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

Abordarea vulnerabilităților cibernetice în sectoarele critice: sectorul sănătății

On Cyber Vulnerabilities Management in Critical Sectors: the Health Sector

Dr. Irina-Delia NEMOIANU*
*Directoratul Național de Securitate Cibernetică
e-mail: irina.nemoianu@dnsc.ro
ORCID: 0009-0000-3276-9656

Abstract

Digitalizarea sectorului sănătății din România a cunoscut o accelerare semnificativă, în special în urma pandemiei de COVID-19, însă această tranziție a amplificat riscurile de securitate cibernetică, expunând infrastructurile critice și datele pacienților la amenințări persistente. Acest studiu analizează vulnerabilitățile tehnice și nontehnice ale sectorului medical, bazându-se atât pe cercetare documentară, cât și pe un sondaj realizat în rândul reprezentanților instituțiilor de sănătate. Rezultatele evidențiază provocări importante, de la utilizarea de software învechit, deficit de personal specializat în securitate cibernetică și variații semnificative în nivelul de maturitate a protecției cibernetice între organizațiile publice și cele private. Având în vedere diversitatea provocărilor identificate, reziliența sectorului medical necesită o strategie integrată de securitate cibernetică, fundamentată pe investiții tehnologice, formare continuă și politici coerente de gestionare a riscurilor.

The digitalisation of the Romanian health sector has accelerated significantly, especially in the aftermath of the COVID-19 pandemic, but this transition has amplified cybersecurity risks, exposing critical infrastructures and patient data to persistent threats. This study analyses the technical and non-technical vulnerabilities of the medical sector, based on both documentary research and a survey conducted among representatives of health institutions. The results highlight important challenges, ranging from the use of outdated software, shortages of specialised cybersecurity staff and significant variations in the level of maturity of cyber protection between public and private organisations. Given the diversity of challenges identified, the resilience of the health sector requires an integrated cybersecurity strategy, underpinned by technological investments, continuous training and coherent risk management policies.

Cuvinte-cheie:
securitate cibernetică; atacuri cibernetice; vulnerabilități; sectorul sănătății; reziliență; factorul uman.

Keywords:
cybersecurity; cyber-attacks; vulnerabilities; the health sector; resilience; the human factor.

Info articol
Primit: 31 martie 2025; Evaluat: 29 aprilie 2025; Acceptat: 6 mai 2025; Disponibil online: 27 iunie 2025
Citare: Nemoianu, I.D. 2025. „Abordarea vulnerabilităților cibernetice în sectoarele critice: sectorul sănătății". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(2): 31-40. https://doi.org/10.53477/2065-8281-25-10

Într-un context global marcat de avansul tehnologic, digitalizarea sistemului de sănătate a devenit o prioritate strategică pentru România, vizând îmbunătățirea calității și eficienței serviciilor medicale. Acest demers a fost accelerat de pandemia de COVID-19, care a evidențiat necesitatea adaptării rapide a sectorului medical la noile realități. Cu toate acestea, sectorul se confruntă cu provocări semnificative în ceea ce privește securitatea cibernetică, legate atât de infrastructură, cât și de expertiza resurselor umane.

Creșterea gradului de digitalizare a dus la extinderea suprafeței de atac a amenințărilor cibernetice, fapt evidențiat de creșterea numărului de atacuri cibernetice asupra sistemului de sănătate din România. Proiectul RO-CCH, finanțat de Uniunea Europeană și implementat de Directoratul Național de Securitate Cibernetică (DNSC), a abordat provocările de securitate cibernetică din sectorul sănătății, cu scopul de a reduce riscurile de securitate cibernetică și de a crește gradul de conștientizare în instituțiile de sănătate din România (RO-CCH 2025a).

Pornind de la activitatea desfășurată în cadrul proiectului, acest articol prezintă o analiză a vulnerabilităților de securitate cibernetică ce pot afecta sectorul sănătății din România, evidențiind dimensiunile sociotehnice. Aceste dimensiuni reflectă interacțiunile dintre componentele tehnice – infrastructură hardware, software și de rețea – și factorii sociali – precum comportamentul uman, cultura organizațională, cadrul de reglementare și necesitatea unei abordări integrate pentru obținerea rezilienței sectorului. Studiul integrează, de asemenea, rezultatele unui sondaj, realizat cu reprezentanți ai spitalelor, evidențiind percepția acestora asupra amenințărilor cibernetice și asupra capacității actuale a organizațiilor de a gestiona vulnerabilitățile.

Atacuri cibernetice asupra sistemului de sănătate

Sistemul de sănătate din România se confruntă cu o creștere semnificativă a amenințărilor cibernetice, în special a atacurilor de tip ransomware, care vizează atât infrastructurile IT ale spitalelor, cât și furnizorii de servicii informatice din domeniu. Aceste tendințe sunt în acord cu tendințele europene sau globale (ENISA 2023), unde 8% din atacurile ransomware din 2023-2024 au vizat sectorul sănătății, al treilea cel mai afectat sector (ENISA 2024, 15). În România atacurile au demonstrat existența unor vulnerabilități atât în protecția datelor, cât și în continuitatea operațiunilor medicale, subliniind necesitatea unor măsuri robuste de securitate cibernetică, dar și a unor planuri de recuperare, în caz de incident.

În iulie 2021, Spitalul Clinic nr. 1 Witting din București a fost victima unui atac ransomware cu malware-ul Phobos, care a criptat datele de pe serverele instituției, atacatorii solicitând o răscumpărare pentru decriptare (SRI 2021). Acest ransomware (Cisco Systems Inc. 2023), distribuit prin exploatarea vulnerabilităților Remote Desktop Protocol (RDP) de acces la distanță în sistemele de operare Windows,

funcționează ca o platformă Ransomware-as-a-Service (RaaS). Astfel de platforme permit colaborarea dintre dezvoltatori și afiliați pentru extinderea atacurilor. Caracterul descentralizat al modelului îngreunează identificarea atacatorilor și aplicarea măsurilor de combatere, iar deși Serviciul Român de Informații (SRI) a oferit recomandări pentru securizarea infrastructurii IT, amploarea daunelor nu a fost făcută publică. Un incident similar a avut loc, în 2023, la Spitalul de Recuperare „Sfântul Gheorghe" din Botoșani, unde atacatorii au criptat baza de date a instituției, perturbând grav activitatea și solicitând o răscumpărare de trei bitcoini (aproximativ 50.000 de dolari) (ProTV 2023). Acest atac, intens mediatizat, a evidențiat impactul sever al amenințărilor cibernetice asupra sistemului de sănătate din România.

Cel mai recent atac ransomware de amploare a avut loc între 11 și 12 februarie 2024, afectând Romanian Soft Company, furnizorul platformei informatice Hippocrates, utilizată de numeroase spitale publice din România (DNSC 2024). Incidentul a perturbat grav activitatea a 26 de spitale care depindeau de această platformă pentru gestionarea datelor și coordonarea serviciilor medicale. Malware-ul utilizat a fost Backmydata, o variantă a ransomware-ului Phobos, similar cu cel folosit în atacul asupra Spitalului Clinic nr. 1 Witting, din 2021. La momentul redactării acestui articol, cauza exactă a incidentului nu a fost dezvăluită public, însă DNSC a menționat că nu au fost identificate dovezi de exfiltrare a datelor. Astfel, rămâne incert dacă atacul a exploatat o vulnerabilitate a platformei, o configurație eronată a RDP sau alte erori umane.

Creșterea frecvenței și complexității atacurilor ransomware asupra infrastructurii IT din sectorul medical românesc subliniază riscurile asociate atât deficiențelor în securitatea cibernetică, cât și a vulnerabilităților datorate lanțului de aprovizionare. Atacurile recente evidențiază necesitatea implementării unor strategii de protecție a rețelelor spitalicești, inclusiv implementarea unor politici stricte de backup și de recuperare a datelor pentru a preveni pierderile cauzate de atacurile ransomware, protejarea serviciilor informatice expuse la internet sau conectarea la rețele interne prin conexiuni Virtual Private Network (VPN) securizate. Alte măsuri care asigură reziliența, în caz de atacuri materializate, pot fi creșterea investițiilor în soluții avansate de securitate cibernetică și în planuri de răspuns rapid la incidente cibernetice, precum și instruirea personalului IT și a celui medical pentru a detecta și a preveni amenințările cibernetice comune, începând cu phishingul.

Vulnerabilități cibernetice

În securitatea cibernetică, vulnerabilitățile reprezintă deficiențe structurale sau erori în logica computațională, identificate în componente software sau hardware, care, atunci când sunt exploatate, pot compromite confidențialitatea, integritatea și disponibilitatea datelor și sistemelor informatice. Aceste slăbiciuni pot rezulta din deficiențe de proiectare, implementare sau configurare și constituie puncte de acces pentru atacatori.

Atenuarea acestor vulnerabilități implică, de obicei, una sau mai multe dintre următoarele măsuri:

- aplicarea de patch-uri pentru remedierea erorilor din cod;
- modificarea specificațiilor tehnice astfel încât să reducă expunerea la potențiale exploatări;
- deprecierea sau eliminarea completă a funcționalităților sau protocoalelor care prezintă vulnerabilități.

Conform Programului Common Vulnerabilities and Exposures (CVE) (The MITRE Corporation, fără an; SecurityScorecard, fără an), gestionat de MITRE Corporation, fiecare vulnerabilitate este înregistrată sub un CVE ID unic, care permite asocierea acesteia cu versiuni specifice ale software-ului sau ale bibliotecilor partajate, oferind astfel un sistem de referință care să ajute la procesul de gestionare a vulnerabilităților.

Scorul Common Vulnerability Scoring System (CVSS) oferă o metrică pentru evaluarea gravității vulnerabilităților de securitate cibernetică, pe baza mai multor criterii, precum impactul și exploatabilitatea acestora (NIST, fără an). Acesta poate fi transpus într-o reprezentare calitativă (scăzut, mediu, ridicat și critic) pentru a ajuta organizațiile să evalueze și să prioritizeze vulnerabilitățile în cadrul proceselor de management. CVSS este un standard public, dezvoltat de Special Interest Group (SIG) și utilizat pe scară largă de organizații din întreaga lume, cea mai recentă versiune fiind CVSS 4.0.
Sistemele IT din spitale se pot confrunta cu numeroase vulnerabilități cibernetice, multe dintre ele afectând diverse produse hardware, software și de rețea, utilizate pe scară largă și în alte sectoare, care pot compromite securitatea datelor pacienților și funcționarea infrastructurii critice de asistență medicală.

În urma cercetării documentare, dar și din discuțiile cu experți de securitate cibernetică ce colaborează cu entități din domeniul sănătății, printre cele mai frecvente probleme identificate se numără utilizarea software-ului și hardware-ului învechit, expus riscurilor, din cauza lipsei actualizărilor și a suportului tehnic adecvat. De asemenea, protocoalele slabe de securitate a rețelei, configurările defectuoase și măsurile inadecvate de control al accesului pot facilita accesul neautorizat la sistemele informatice. În plus, nivelul insuficient de instruire a personalului medical și a celui administrativ crește vulnerabilitatea instituțiilor sanitare în fața atacurilor de tip phishing, care rămân una dintre principalele metode de compromitere a infrastructurii IT. Aceste deficiențe expun spitalele unor amenințări semnificative, precum încălcări ale securității datelor, atacuri ransomware și acces neautorizat la informații sensibile, subliniind necesitatea implementării unor măsuri eficiente și proactive de securitate cibernetică.

Raportul prezintă o serie de vulnerabilități cibernetice legate de hardware, software, echipamente de rețea sau echipamente de securitate cibernetică, pe care organizațiile din domeniul sănătății pot să le aibă în vedere în strategiile lor de securitate (RO-CCH 2025b). În acest context, anumite vulnerabilități, identificate prin

CVE-urile corespondente, fie istorice, fie recent descoperite, prezintă un scor CVSS ridicat (High) sau critic (Critical), care necesită o abordare urgentă și măsuri de atenuare eficiente, având în vedere potențialul impact asupra continuității serviciilor medicale și asupra protecției infrastructurii critice din sectorul sănătății. În același timp, noi vulnerabilități sunt făcute public frecvent, o strategie adecvată de securitate cibernetică incluzând urmărirea alertelor diverșilor producători sau furnizori, informările diverselor agenții de securitate naționale sau achiziționarea/colaborarea cu organizații pentru obținerea de servicii de tip CERT privind vulnerabilitățile exploatate în mod activ de atacatori.

O abordare tot mai relevantă în managementul vulnerabilităților o reprezintă integrarea soluțiilor de inteligență artificială (IA) în soluțiile existente (AI-driven vulnerability management) prin utilizarea de algoritmi de învățare automată, pentru a îmbunătăți procesele de detecție, de prioritizare și de remediere a vulnerabilităților (Wan și alții 2024). Astfel, soluțiile IA pot analiza în timp real volume mari de date, de la jurnale de sistem și de rețea la fluxuri de threat intelligence, pentru a identifica tipare care sugerează posibile puncte slabe de securitate în infrastructură. Platforme comerciale de management al vulnerabilităților, precum Qualys VMDR, Tenable.io, Rapid7 InsightVM sau Darktrace, au integrat algoritmi de învățare automată pentru a corela vulnerabilitățile cunoscute cu nivelul lor de exploatare activă în mediul real (Tod-Răileanu și alții 2024). Inteligența artificială poate fi utilizată și în predicția vulnerabilităților, prin care se anticipează probabilitatea ca o vulnerabilitate recent descoperită să fie exploatată, pe baza comportamentului istoric al atacatorilor și al vectorilor de atac asociați.

Digitalizarea sectorului sănătății presupune integrarea și a tehnologiilor specifice, a sistemelor și protocoalelor, precum sisteme de gestionare a farmaciilor, a serviciilor de ambulanță și de urgență, sisteme informatice de laborator. Printre cele mai importante, se numără dosarele electronice de sănătate (Electronic Health Records), care integrează istoricul pacienților, folosind standarde, precum HL7 (Health Level 7) pentru schimbul de informații între sisteme, cum ar fi sistemele informatice de radiologie (Radiology Information Systems) și sistemele informatice de laborator (Laboratory Information Systems). Sistemele Picture Archiving and Communication Systems (PACS), de arhivare și comunicare a imaginilor, sunt utilizate pentru stocarea și gestionarea imagisticii medicale, în timp ce standardul Digital Imaging and Communications in Medicine (DICOM) permite interoperabilitatea dintre dispozitivele de imagistică și sistemele de stocare. Aceste tehnologii reprezintă o suprafață suplimentară de atac care trebuie avută în vedere de organizațiile din sectorul medical, atât pentru spitale, clinici, cât și pentru centre de imagistică medicală, laboratoare de analize medicale, cabinete stomatologice.

Vulnerabilități în dispozitive medicale

Dispozitivele medicale moderne, precum monitoarele cardiace, ventilatoarele și pompele de insulină, sunt din ce în ce mai integrate în infrastructura digitală a spitalelor prin Internetul Lucrurilor Medicale (Internet of Medical Things – IoMT).

Această conectivitate permite monitorizarea în timp real a pacienților și transmiterea automată a datelor către sistemele de gestionare a informațiilor clinice, îmbunătățind astfel eficiența actului medical. Dispozitivele comunică utilizând protocoale standard, precum Wi-Fi și Bluetooth, dar și protocoale proprietare, dezvoltate de producătorii de echipamente medicale. Această conectivitate, deși benefică din punct de vedere operațional, ridică provocări în ceea ce privește securitatea cibernetică, în special în protejarea confidențialității, integrității și disponibilității datelor pacienților.

Pentru a asigura securizarea transmisiunilor, peste protocoalele de rețea tradiționale, precum TCP/IP, care permit comunicarea între dispozitive, sunt utilizate și tehnologii de protecție suplimentare, cum ar fi VPN-urile și criptarea TLS/SSL. Aceste mecanisme reduc riscul de interceptare a informațiilor sensibile și protejează împotriva atacurilor cibernetice care vizează infrastructura medicală. Cu toate acestea, numeroase dispozitive IoMT rămân vulnerabile, din cauza configurărilor nesigure, a lipsei actualizărilor software sau a standardelor de securitate care variază între diferiți producători.

Un studiu asupra dispozitivelor medicale (Cynerio 2023) a analizat securitatea dispozitivelor medicale din 14 trusturi NHS (organizații din sistemul de sănătate din Regatul Unit), reprezentând 6,4% din totalul trusturilor NHS. Aceste instituții au fost selectate pentru a reflecta diversitatea spitalelor din punctul de vedere al dimensiunii, numărului de paturi și nivelului de finanțare. Studiul a utilizat un instrument de analiză anonimizată pentru a identifica principalele riscuri, vulnerabilități și amenințări active, asociate dispozitivelor IoMT. Constatările au evidențiat probleme critice, inclusiv posibilitatea exploatării vulnerabilităților nepatch-uite în peste 40% din dispozitive, configurații de rețea nesigure sau risc de acces neautorizat. În același timp, peste 36,7% dintre dispozitive s-ar confrunta cu riscuri reduse prin implementarea unei microsegmentări adecvate la nivel de rețea.

Factorul uman în securitatea cibernetică

Sistemele informatice din cadrul unităților medicale sunt susceptibile la o serie de vulnerabilități care au ca origine factorul uman. Aceste deficiențe, deși nu se corelează întotdeauna cu vulnerabilități și expuneri comune sau CVE-uri specifice, reprezintă un vector critic în evaluarea riscului cibernetic. Analiza acestor vulnerabilități impune o abordare contextuală, având în vedere fluxurile de lucru și interacțiunile umane din domeniul medical.

Vectori de atac și erori umane în contextul spitalicesc – unul dintre vectorii de atac predominanți îl reprezintă campaniile de tip phishing, prin care personalul este indus în eroare prin intermediul unor mesaje electronice care imită surse legitime. Această manipulare are ca rezultat compromiterea datelor de autentificare sau instalarea de software malițios. În paralel, practicile deficitare de gestionare a credențialelor, cum ar fi utilizarea unor parole slab configurate sau reutilizarea acestora pe multiple platforme, facilitează accesul neautorizat.

Amenințări interne și ingineria socială – amenințările interne, provenind din partea angajaților cu intenții răuvoitoare sau nemulțumiri, reprezintă un risc semnificativ, aceștia putând abuza de privilegiile de acces pentru a exfiltra date sensibile sau a perturba operațiunile. În plus, tehnicile de inginerie socială, care manipulează personalul pentru a divulga informații confidențiale sau pentru a efectua acțiuni care compromit securitatea, subliniază importanța conștientizării și formării continue.

Gestionarea inadecvată a datelor și deficiențe în formarea personalului – manipularea necorespunzătoare a datelor sensibile prin transmiterea accidentală a informațiilor pacientului prin canale nesecurizate sau expunerea neintenționată a acestora reprezintă o altă categorie de risc. Deficiențele în programele de formare în domeniul securității cibernetice contribuie la această vulnerabilitate, personalul nefiind adesea familiarizat cu cele mai recente amenințări și practici de securitate.

Deficiențe în controlul accesului și nerespectarea protocoalelor de securitate – o gestionare deficitară a accesului utilizatorilor, manifestată prin neactualizarea drepturilor de acces, în urma modificării rolurilor sau părăsirii organizației, creează puncte de intrare pentru atacatori. Nerespectarea protocoalelor de securitate, precum ignorarea actualizărilor software sau ocolirea rețelelor private virtuale (VPN), expune suplimentar sistemele la vulnerabilități cunoscute.

Riscuri asociate dispozitivelor mobile și divulgării neintenționate – pierderea sau furtul dispozitivelor mobile care conțin date sensibile reprezintă un risc considerabil de exfiltrare a informațiilor. De asemenea, divulgarea neintenționată a datelor prin transmiterea eronată sau lăsarea ecranelor nesupravegheate reprezintă riscuri suplimentare, care pot fi atenuate prin implementarea unei culturi organizaționale, orientate spre securitate.

Percepția reprezentanților din sector asupra nivelului de securitate cibernetică

În ultimii ani, pe lângă atacurile cu ransomware care au afectat activitatea unităților spitalicești din România, organizațiile au fost expuse unei varietăți de atacuri cibernetice, evidențiind un peisaj de amenințări din ce în ce mai sofisticat. Unul dintre sondajele realizate în cadrul proiectului cu reprezentanți IT și din managementul a 30 de organizații cu profil medical din România a generat date care oferă indicii cu privire la nivelul de pregătire al acestor organizații în fața amenințărilor cibernetice, precum și la percepția subiecților asupra stadiului actual al securității cibernetice în sector.

Conform răspunsurilor obținute de la reprezentanți din sector, în ultimii trei ani phishingul și spear-phishingul au constituit cea mai mare parte a incidentelor raportate, fiind urmate de atacurile de tip Distributed Denial of Service (DDoS) care vizează indisponibilizarea infrastructurilor IT, și de atacurile de tip brute force, folosite pentru compromiterea credențialelor de acces. De asemenea, o categorie semnificativă

de amenințări a fost reprezentată de distribuirea de malware și spyware, indicând o diversificare a metodelor utilizate de atacatori. Această ierarhizare a incidentelor subliniază natura dinamică și adaptabilă a amenințărilor cibernetice, precum și necesitatea implementării unor măsuri de securitate multilaterale. În mod particular, prevalența atacurilor de tip phishing justifică necesitatea considerării vulnerabilităților umane ca un vector de exploatare în cadrul sistemelor de securitate cibernetică.

În ceea ce privește evaluarea și prioritizarea vulnerabilităților cibernetice în cadrul organizațiilor, participanții au oferit răspunsuri variate privind existența unor cadre sau metodologii specifice utilizate pentru determinarea nivelului de risc asociat fiecărei vulnerabilități. Dintre cei 30 de respondenți, 12 au declarat că nu dispun de un astfel de program structurat pentru gestionarea vulnerabilităților. Cu toate acestea, aproximativ jumătate dintre participanți folosesc instrumente de scanare a vulnerabilităților, sisteme de detectare a intruziunilor (IDS) sau alte instrumente automatizate, menite să identifice riscurile și amenințările. Aceste rezultate indică o abordare eterogenă a securității cibernetice în sector, în care, deși există eforturi pentru monitorizarea amenințărilor, un număr semnificativ de organizații nu implementează încă un proces formalizat de evaluare și gestionare a vulnerabilităților.

Nivelul scăzut de securitate cibernetică și capacitatea redusă de gestionare a incidentelor în cadrul organizațiilor sunt atribuite unei combinații de factori tehnici, organizaționali și umani. Conform datelor obținute, 28 din 30 de respondenți au indicat drept cauze principale utilizarea unor sisteme informatice învechite sau nesigure, implementarea controalelor de securitate inadecvate și resursele limitate alocate pentru protecția infrastructurii IT. Acești factori nu doar că sporesc riscul de compromitere a datelor și infrastructurilor critice, dar și îngreunează implementarea unor măsuri proactive de securitate.

Un aspect secundar, dar semnificativ, identificat în cadrul analizei, este lipsa de conștientizare, în rândul angajaților, a problemei privind securitatea cibernetică, ceea ce contribuie la vulnerabilități suplimentare în fața atacurilor bazate pe inginerie socială, cum ar fi phishingul. Aceste deficiențe reflectă probleme sistemice mai profunde, în special subfinanțarea și investițiile insuficiente în infrastructura de securitate cibernetică. În plus, acestea sunt amplificate de factori umani, inclusiv de deficitul de personal specializat, care limitează capacitatea organizațiilor de a detecta, de a preveni și de a răspunde eficient la incidente cibernetice. De asemenea, lipsa unui angajament strategic pentru dezvoltarea unei culturi organizaționale orientate spre securitate agravează și mai mult riscurile, subliniind necesitatea unor măsuri urgente pentru consolidarea rezilienței cibernetice la nivel instituțional.

Concluzii

România a făcut progrese semnificative în digitalizarea sectorului de sănătate, accelerate de pandemia de COVID-19, însă această transformare a crescut riscurile

cibernetice, expunând rețelele informatice și datele pacienților la amenințări. În acest articol, am evidențiat vulnerabilitățile tehnice și nontehnice ale sectorului, obținute atât din cercetare documentară, cât și din chestionarele cu reprezentanți din sector. Problemele evidențiate ale sectorului, de la utilizarea de software învechit la lipsa personalului instruit în securitate cibernetică atât din sectorul public, cât și din cel privat subliniază necesitatea unor măsuri mai stricte pentru protejarea infrastructurii IT din sănătate împotriva amenințărilor în creștere.

Pentru a proteja infrastructura critică din sănătate și datele pacienților, este necesară o gestionare eficientă a vulnerabilităților, actualizarea software-ului și modernizarea infrastructurilor IT. Date fiind nivelurile diferite de maturitate a securității cibernetice ale organizațiilor din sistem, reziliența sistemului de sănătate necesită o strategie națională coerentă, bazată pe investiții în tehnologie, pe formare în domeniul securității cibernetice și pe politici eficiente de gestionare a riscurilor.

Pe măsură ce tehnologia avansează, integrarea inteligenței artificiale ar putea avea un rol decisiv în abordarea proactivă a riscurilor cibernetice atât în sectorul sănătății, cât și în alte sectoare critice. Prin automatizarea proceselor de identificare a riscurilor și amenințărilor, de prioritizare a vulnerabilităților, soluțiile bazate pe IA pot îmbunătăți considerabil capacitatea de reacție și eficiența operațională. Adoptarea unei strategii naționale care să includă astfel de tehnologii ar putea reprezenta un atu pentru România în protejarea infrastructurilor critice și în creșterea rezilienței cibernetice la nivel național.

Referințe

Cisco Systems Inc. 2023. ”Understanding the Phobos affiliate structure and activity.” https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/.

Cynerio. 2023. ”The State of NHS Trust IoT Device Security 2023.” https://www.cynerio.com/nhs-trusts-iot-security-report-cynerio-only.

DNSC. 2024. ”Backmydata Ransomware (Alert).” https://www.dnsc.ro/vezi/document/alert-backmydata-ransomware-eng-pdf.

ENISA. 2023. ”Enisa Threat Landscape: Health Sector.” https://www.enisa.europa.eu/publications/health-threat-landscape.

___. 2024. ”ENISA Threat Landscape 2024.” doi:10.2824/0710888.

NIST. fără an. ”CVSS – Vulnerability Metrics.” Accesat decembrie 2024. https://nvd.nist.gov/vuln-metrics/cvss.

ProTV. 2023. „Spital din Botoșani, atacat de hackeri. Le-au criptat baza de date și cer 50.000 de dolari răscumpărare.” https://stirileprotv.ro/stiri/ilikeit/spital-din-botosani-atacat-de-hackeri-le-au-criptat-baza-de-date-si-cer-50-000-de-dolari-rascumparare.html.

RO-CCH. 2025a. ”About RO=CCH.” https://rocch.ro/en/about-ro-cch.

___. 2025b. ”Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1).” https://rocch.ro/en/dissemination/deliverables/d2-1/download.

SecurityScorecard. fără an. ”CVE Details.” Accesat decembrie 2024. https://www.cvedetails.com/.

SRI. 2021. „Atac ransomware asupra Spitalului Clinic Witting din București.” https://www.sri.ro/articole/atac-ransomware-asupra-Spitalului-Clinic-Witting-din-Bucuresti.html.

The MITRE Corporation. fără an. ”CVE® Program Mission.” Accesat decembrie 2024. https://www.cve.org/.

Tod-Răileanu, Gabriela, Ana-Maria Dincă, Sabina-Daniela Axinte și Ioan C. Bacivarov. 2024. ”Enhancing Vulnerability Management with Artificial Intelligence Algorithms.” *International Conference on Cybersecurity and Cybercrime.* 96–101. doi:10.19107/CYBERCON.2024.13.

Wan, Shengye, Joshua Saxe, Craig Gomes, Sahana Chennabasappa, Avilash Rath, Kun Sun și Xinda Wang. 2024. ”Bridging the Gap: A Study of AI-based Vulnerability Management between Industry and Academia.” *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S).* IEEE Computer Society. 80-87.

INFORMAȚII PRIVIND FINANȚAREA

Această cercetare a fost posibilă parțial prin sprijinul proiectului RO-CCH, care a furnizat date directe despre managementul vulnerabilităților cibernetice în instituțiile medicale din România, prin raportul *Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1)*. Autorul își exprimă aprecierea față de organizațiile din domeniul sănătății și față de experții care au contribuit prin participare la sondaje și prin furnizarea de perspective valoroase.

Direcția Națională de Securitate Cibernetică Română (DNSC) este beneficiarul unei finanțări nerambursabile pentru implementarea proiectului „Romanian Cyber Care Health – RO-CCH”, în temeiul acordului de grant nr. 101101522. Proiectul este finanțat prin autoritatea de finanțare: CNECT.H – Digital Society, Trust, and Cybersecurity, în cadrul apelului DIGITAL-2022-CYBER-02-SUPPORTHEALTH.

DECLARAȚIE PRIVIND CONFLICTUL DE INTERESE

Autorul declară că nu există potențiale conflicte de interese cu privire la cercetarea, paternitatea și/sau publicarea acestui articol.

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

Combaterea amenințării bombelor planor în conflictul din Ucraina

Countering the Glide Bombs Threat in the Ukrainian Conflict

Lt.col.Dr. Adrian MIREA*

*Universitatea Națională de Apărare „Carol I", București
e-mail: mirea.adrian@yahoo.com

Abstract

Conflictul din Ucraina asigură contextul readucerii la viață și întrebuințării inovative a sistemelor de armament și a muniților clasice, pentru a satisface necesitățile forțelor aflate în conflict. Lucrarea de față abordează o astfel de utilizare adaptată a bombelor clasice de aviație, în varianta echipată cu kit de planare, aspect ce a permis, practic, forțelor aeriene ruse să-și îndeplinească misiunile de bază într-o manieră nouă. Într-o primă fază, atenția lucrării este concentrată pe descrierea amenințării reprezentate de bombele planor și pe impactul potențial al acestora asupra desfășurării acțiunilor militare, iar ulterior, în cea de-a doua fază, am abordat posibile modalități de combatere a bombelor planor, aducând în atenție efortul forțelor ucrainene și al aliaților săi de a limita numărul de atacuri cu astfel de mijloace. În realizarea lucrării, am explorat surse deschise de informare prin metoda analizei documentare, pentru a sintetiza cele mai relevante aspecte privind întrebuințarea și contracararea bombelor planor în conflictul din Ucraina. Rezultatul investigațiilor făcute subliniază interesul forțelor ucrainene și al aliaților lor pentru identificarea celor mai eficiente metode de adaptare a acțiunilor militare la noua realitate a mediului operațional și pentru combaterea acestei amenințări reprezentate de utilizarea în masă a atacurilor cu bombe planor.

The conflict in Ukraine provides the context for the revival and innovative use of classic weapon systems and munitions to meet the needs of combat forces. This paper deals with such an adapted use of classic aviation bombs in a gliding kit version, which has practically enabled the Russian Air Force to perform its basic missions in a new way. In the first phase, the focus of the paper is on describing the threat posed by glide bombs and their potential impact on the conduct of military actions, and in the second phase, I have presented possible ways of countering glide bombs, emphasizing the efforts of the Ukrainian forces and its allies to limit the number of glide bomb attacks. In carrying out the paper, I explored open sources of information through the method of documentary analysis in order to synthesize the most relevant aspects of the use and counteraction of glide bombs in the Ukrainian conflict. The results of the investigations emphasize the interest of the Ukrainian forces and their allies in identifying the most effective methods of adapting military actions to the new reality of the operational environment while also countering the threat posed by the mass use of glide bomb attacks.

Cuvinte-cheie:
bombe planor; bombe de aviație; kit de planare; apărare antiaeriană; conflictul din Ucraina.

Keywords:
glide bombs; aviation bombs; gliding kit; air defense; Ukrainian conflict.

Info articol
Primit: 15 mai 2025; Evaluat: 30 mai 2025; Acceptat: 4 iunie 2025; Disponibil online: 27 iunie 2025
Citare: Mirea, A. 2025. „Combaterea amenințării bombelor planor în conflictul din Ucraina".
Buletinul Universității Naționale de Apărare „Carol I", 14(2): 41-50. https://doi.org/10.53477/2065-8281-25-11

În anul 2023 era raportată întrebuințarea de către armata rusă a bombelor de aviație UPAB-1500 (de 1500 kg) într-o variantă echipată cu kit de planare și având posibilitatea ghidării GPS la țintă. Aceste bombe au fost prezentate de armata rusă pentru prima dată în anul 2019, la expoziția MAKS (Gheja 2023), iar caracteristicile lor tehnice deschid noi posibilități de atac al țintelor de suprafață adăpostite în conflictul din Ucraina, în special datorită încărcăturii explozive de 1.010 kg și a capacității de lansare precisă de la o distanță de 40 km. În ciuda avantajelor asigurate de aceste caracteristici, armata rusă a subestimat, înainte de invazia Ucrainei din februarie 2022, nevoia de astfel de bombe planor, dar și nevoia de alte tipuri de muniții ghidate cu precizie, după cum a recunoscut chiar comandantul Forțelor Aeriene ruse (Hardie 2024).

Pentru realizarea acestui articol, am analizat surse deschise de informații, în general publicații, diverse site-uri și lucrări de autor, surse care detaliază aspecte relevante privind folosirea bombelor planor în conflictul din Ucraina, precum și modalitățile de combatere a acestora. Având ca fundament metoda analizei documentare (Okoko, Tunison și Walker 2023, 140), am avut în vedere colectarea, analiza și interpretarea sistematică a datelor obținute din sursele menționate, având ca scop înțelegerea și sintetizarea elementelor principale de interes pentru lucrarea de față.

Conceptul de utilizare a bombelor planor nu este unul nou, primele atacuri reușite cu astfel de muniții fiind atribuite forțelor armate naziste (Fritz-X) în Cel de-Al Doilea Război Mondial. Proiectarea bombei a început în anul 1939sub conducerea doctorului Max Kramer, iar testele finale de acceptare au fost desfășurate lângă orașul Foggia din Italia, la începutul anului 1942 (Australian War Memorial 2025). Utilizarea operațională a început la mijlocul anului 1943, iar cel mai mare succes obținut prin atacul cu astfel de bombe planor a fost înregistrat în septembrie 1943, când trei bombe Fritz-X au lovit și au scufundat cuirasatul italian Roma.

Actualmente, bombele planor sunt lansate de platforme aeriene cu aripă fixă, de regulă avioane cu reacție. Viteza și altitudinea la care aeronavele lansează aceste bombe sunt cele care asigură kitului de planare, montat pe ele, energia necesară angajării țintelor la distanțe considerabile. Totodată, sistemele de ghidare integrate în kit – sisteme inerțiale și GPS – permit ajustarea traiectoriei bombelor planor în timpul zborului, astfel încât angajarea țintelor să se facă cu o precizie caracteristică în mod normal altor muniții de precizie mult mai costisitoare. Având în vedere raza de acțiune a bombelor planor și precizia cu care pot angaja țintele terestre, lansarea acestor muniții poate fi făcută din zone sigure pentru platformele aeriene, în afara bătăii sistemelor de apărare antiaeriană ale inamicului.

Amenințarea reprezentată de bombele planor

În fazele inițiale ale conflictului din Ucraina, armata rusă nu a reușit să distrugă majoritatea sistemelor de rachete sol-aer ucrainene cu rază de acțiune medie și

lungă. Acest aspect, împreună cu reaprovizionarea constantă a Ucrainei cu sisteme portabile de apărare antiaeriană, a constituit un risc ridicat pentru platformele aeriene rusești destinate să bombardeze ținte aflate în apropierea liniei frontului, dar și în zone mai îndepărtate de pe teritoriul Ucrainei. Din această cauză, până în luna aprilie 2022, armata rusă a limitat încercările de pătrundere în dispozitivul de luptă inamic pe cale aeriană. În conflictul din Ucraina, forțele aeriene ruse se confruntă cu un adversar care dispune de o multitudine de sisteme de apărare antiaeriană terestre care formează o apărare de tip stratificat împotriva platformelor aeriene. Așa după cum am precizat, armata rusă nu a reușit să distrugă majoritatea acestor sisteme de apărare antiaeriană, în special sistemele ucrainene de rachete sol-aer cu rază medie și lungă de acțiune S-300 și, respectiv, Buk-M1. Drept consecință, aeronavele rusești, care încearcă să sprijine prin foc forțele terestre, trebuie să zboare la altitudini mici și foarte mici atunci când se aventurează în apropierea liniei frontului, însă acest lucru le face vulnerabile la sistemele de tip MANPAD și le împiedică să utilizeze eficient bombele neghidate.

Insuficiența loviturilor de precizie a făcut ca sprijinul forțelor terestre ale armatei ruse să se realizeze cu proiectile neghidate și, implicit, cu riscuri foarte mari pentru platformele aeriene angajate în lansarea acestora. Această nevoie tot mai mare de muniții de precizie a determinat dezvoltarea kitului de planare UMPK în ianuarie 2023. Este un kit ieftin care poate echipa bombele convenționale de aviație cu aripi și sisteme de ghidare, permițând astfel folosirea acestora asupra țintelor fixe din afara razei de acțiune a apărării antiaeriene ucrainene. Apariția și întrebuințarea bombelor planor au readus practic „la viață" forțele aeriene ruse, acestea fiind acum în măsură să angajeze ținte terestre din dispozitivul inamic, fără a fi nevoite să dețină superioritatea aeriană în prealabil sau să se aventureze prin pătrunderi în interiorul dispozitivului de luptă al forțelor ucrainene.

Kitul de planare UMPK este versiunea rusească a kitului de producție americană JDAM (Joint Direct Attack Munition), mai precis a kitului JDAM-ER (Extended Range), folosit de armata ucraineană. Trebuie menționat că, similar UMPK, JDAM este un kit folosit pentru a transforma bombele simple sau standard neghidate, în muniții „inteligente" de precizie, pentru a fi întrebuințate asupra țintelor terestre, inclusiv în condiții meteorologice nefavorabile. Prin adăugarea unei noi secțiuni de coadă, care conține un sistem de navigație inerțială și o unitate de ghidare prin GPS, kitul JDAM îmbunătățește precizia bombelor neghidate de uz general, indiferent de condițiile meteorologice. O versiune a kitului JDAM-ER folosit de armata ucraineană este cel atașat bombelor Mark 82 de 500 de livre (230 kg), lansate de avioane de tip Su-27, pentru a lovi ținte la distanțe de 72 km, cu o eroare circulară de maximum 11 m (Kushnikov 2023).

Potrivit purtătorului de cuvânt al Forțelor Aeriene ucrainene Yuriy Ihnat, kitul de planare UMPK permite bombelor să angajeze ținte la distanțe de 43 de mile (Hardie 2023). El a declarat că acest lucru asigură avioanelor rusești de tip Su-35S sau Su-34 posibilitatea lovirii țintelor fixe la distanțe de până la 12-18 mile în interiorul

Figura 1 JDAM-ER (Newsweek 2023)

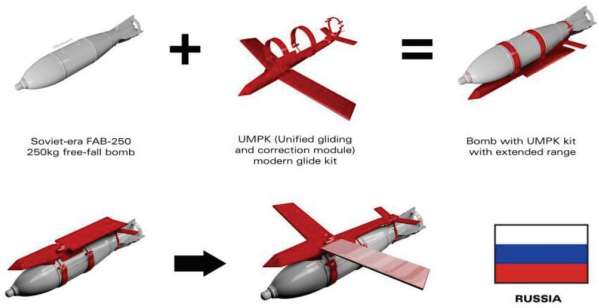

Figura 2 UMPK (Al-Rifai 2024)

dispozitivului de luptă al forțelor ucrainene, rămânând, totodată, în afara razei de acțiune a sistemelor de apărare antiaeriană ucrainene, care stau, de regulă, mai departe de linia frontului, din motive de siguranță. Un răspuns la acest tip de acțiuni a fost apropierea sistemelor de apărare antiaeriană de linia frontului, sporindu-le astfel vulnerabilitatea la loviturile de artilerie și la munițiile de tip loitering – Lancet.

Astăzi, utilizarea *noilor* muniții este calificată de partea ucraineană drept o amenințare extremă (Vesti din Rusia 2025), forțele armate ucrainene având dificultăți în interceptarea sau în bruiajul acestor muniții. Bombele planor sunt muniții convenționale, lansate din aer, care au fost echipate cu aripi și navigație asistată prin satelit pentru a le extinde raza de acțiune și precizia în angajarea de ținte. Acestea reprezintă o variantă ieftină de lovire a țintelor, în raport cu rachetele balistice și de croazieră, pe care forțele ruse le lansează cu regularitate asupra Ucrainei. Bombele planor, cu greutăți între 500 kg și 3.000 kg (Peleschuk 2024), sunt în număr mare în dotarea armatei ruse, ele provenind inclusiv din perioada sovietică, și pot fi purtate de platforme aeriene pentru a fi lansate din afara zonelor de acțiune a apărării antiaeriene a forțelor ucrainene.

Dacă un proiectil de artilerie de calibrul 152 mm conține 6,5 kg de material exploziv, o bombă planor de mărime mică conține peste 200 kg de material exploziv (Inwood și Kharchenko 2024). Lovirea pozițiilor defensive ale forțelor ucrainene cu astfel de muniții face aproape imposibilă rezistența acestora, indiferent de gradul de amenajare și adăpostire a elementelor de dispozitiv. Dispunerea de cantități suficiente, asociată cu posibilitatea lansării lor de la distanță, permite forțelor ruse să bombardeze, practic, și să anihileze orice poziție defensivă, indiferent de nivelul ei de fortificare prealabilă. Mai mult decât atât, aceste atacuri cu bombe planor permit anihilarea pozițiilor defensive ucrainene fără intervenția infanteriei ruse, ceea ce constituie, în sine, un avantaj considerabil pentru orice adversar.

Bombele planor au fost folosite cu succes de forțele ruse în special în atacuri asupra țintelor fixe de tip puncte de comandă, fortificații sau depozite de muniții, însă aceste muniții au fost folosite și împotriva populației civile prin lovirea centrelor urbane din localități, precum Sumî, Harkov și Zaporojie (Hodunova 2025). Efectul psihologic astfel obținut și potențialul de influențare a moralului trupelor ucrainene nu pot fi ignorate. Însăși puterea distructivă semnificativă a bombelor de aviație

convertite în bombe planor constituie un factor de descurajare pentru militarii ucraineni, deoarece inexistența sau imposibilitatea recuperării trupurilor celor uciși privează familiile sau aparținătorii acestora de compensațiile cuvenite (Watling și Reynolds 2025, 16).

Un alt aspect notabil privind utilizarea bombelor planor este, din punctul meu de vedere, exploatarea caracteristicilor acestor muniții – îndeosebi precizia și puterea lor distructivă – pentru lovirea pozițiilor de tragere ale artileriei ucrainene, bombele planor fiind, practic, integrate în focul de contrabaterie al forțelor ruse. Dronele „vânătoare de artilerie" au, de regulă, încărcături mici de explozivi și asigură efectul de neutralizare a țintei, însă bombele planor conțin încărcături de explozivi semnificativ mai mari, care asigură efectul de distrugere a gurilor de foc de artilerie.

Amenințarea bombelor planor este cu atât mai mare pentru partea ucraineană, dacă avem în vedere folosirea acestor muniții în combinație cu alte atacuri „convenționale" – cu rachete standard sau cu rachete de croazieră –, creând un efect de suprasaturație a posibilităților sistemelor de apărare antiaeriană. Un factor care a sporit dificultatea contracarării atacurilor cu bombe planor a fost reprezentat de întârzierile ajutoarelor partenerilor europeni și amânările în livrări ale Statelor Unite ale Americii, în ceea ce privește armamentul și muniția destinate apărării antiaeriene ucrainene (Di Mizio și Barrie 2024).

Creșterea semnificativă a numărului de bombe planor de la 40.000 de unități în anul 2024 la 70.000 de unități, estimate în 2025 (Watling și Reynolds 2025, 7), are un impact direct asupra numărului de victime în rândul trupelor ucrainene, aflate în poziții defensive în apărarea obiectivelor importante. Puterea distructivă mare, caracteristică bombelor planor, a determinat nevoia de adaptare a modului de amenajare a pozițiilor de apărare ale forțelor de manevră ucrainene, în sensul că punctele de sprijin de pluton sau de companie cuprind rețele mai mari de comunicații subterane, pentru a diminua riscul îngropării militarilor, în cazul lovirii unor secțiuni de tranșee cu astfel de bombe planor. Efectele amenințării crescânde a acestor bombe planor s-au resimțit inclusiv la nivelul armelor și serviciilor structurilor de forțe ucrainene care operează în raza lor de acțiune, acestea fiind nevoite să ia măsuri suplimentare de protecție fie prin dispersie, fie prin camuflare și adăpostire, în raport cu posibilitățile de observare ale inamicului.

Caracteristicile tehnico-tactice și disponibilitatea bombelor planor în cantități suficiente au permis exploatarea efectelor lor în acțiunile structurilor de manevră, ajungând a fi întrebuințate inclusiv pentru sprijinul prin foc al asalturilor unor grupe sau plutoane (Watling și Reynolds 2025, 8). Identificarea pozițiilor de apărare ale forțelor ucrainene prin asalturi succesive este urmată de lovirea cu artilerie, cu drone și cu bombe planor de diferite dimensiuni.
Am prezentat mai jos, sub formă tabelară, posibilitățile distructive ale bombelor de aviație de diferite dimensiuni, disponibile forțelor ruse.

TABEL NR. 1
Efecte ale bombelor de aviație folosite de armata rusă

Tipul de bombă	Probabilitatea efectului letal 100%	Probabilitatea efectului letal 10%
FAB-100	7,75 m	31 m
FAB-250	10,12 m	40 m
FAB-500	12,75 m	51 m
FAB-1500	18,78 m	75 m
FAB-3000	24 m	167 m
FAB-9000	35 m	245 m

Sursa: (Miler 2024)

Eficiența utilizării bombelor planor de către forțele ruse în distrugerea de poziții fortificate ale apărătorilor ucraineni în orașe, precum Avdiivka, a determinat unii analiști din mass-media să se întrebe dacă bombele planor reprezintă arma supremă a Rusiei sau un semn al echipării deficitare a Ucrainei – *"Glide bombs: Russia's 'ultimate weapon' or a sign of Ukraine's under-equipment?"* (Lefief 2024).

Modalități de combatere a amenințării bombelor planor

Întrebuințarea bombelor planor în Ucraina a asigurat lovirea cu precizie a țintelor de suprafață la distanțe mari, în condiții de siguranță din punct de vedere antiaerian pentru platformele aeriene destinate lansării acestora. În ceea ce privește forțele ruse, dispunerea de stocuri generoase de bombe de aviație a permis lansarea în număr tot mai mare de astfel de atacuri, aspect ce a determinat armata ucraineană și aliații săi să caute soluții viabile pentru combaterea acestei amenințări.

Amenințarea reprezentată de bombele planor este recunoscută inclusiv la nivel de Alianță (NATO 2025), acestea fiind greu de combătut din punct de vedere aerian, din cauza caracteristicilor bombei (precum viteza, semnătura termică sau acustică) și a volumului mare de lansări care poate satura sistemele de apărare antiaeriene din zonele (sau intervalul de timp) vizate de astfel de atacuri. Un alt aspect avut în vedere la nivel NATO este raportul de costuri favorabil atacurilor cu bombe planor, în detrimentul resurselor implicate și consumate cu apărarea antiaeriană și cu anihilarea acestor muniții. Ca un element suplimentar al provocării bombelor planor, caracteristicile menționate ale acestora determină ca o parte din mijloacele de apărare antiaeriană să fie ineficiente în combaterea lor. Menționez, aici, munițiile care folosesc senzori în spectrul infraroșu, precum rachetele AIM-9 Sidewinder și FIM-92 Stinger (Hodunova 2025).

Cele mai practice metode de combatere a atacurilor cu bombe planor vizează, potrivit unor experți (Hoehn și Courtney 2024) și oficiali ucraineni, distrugerea platformelor aeriene destinate lansării acestor atacuri. Lovirea de către forțele ucrainene a unor

ținte terestre, reprezentate de aeronave la sol, folosind atât drone, cât și rachete tactice ATACMS (Army Tactical Missile System) lansate de HIMARS (High Mobility Artillery Rocket System), s-a dovedit a fi o primă metodă eficientă de combatere a atacurilor cu bombe planor. Cu toate că necesită o perioadă mai îndelungată pentru a produce efecte, menționez, aici, și reducerea în timp a numărului de zboruri sau de ieșiri ale platformelor aeriene purtătoare, prin afectarea oricărui domeniu al segmentului aviatic rusesc, ca fiind o metodă eficientă de reducere a numărului de atacuri cu bombe planor.

Distrugerea platformelor aeriene destinate lansării bombelor planor pe timpul zborului ar fi o a doua metodă eficientă de combatere a atacurilor cu bombe planor. Acest efect poate fi obținut fie folosind capabilitățile de atac aerian, precum rachetele AMRAAM (Advanced Medium-Range Air-to-Air Missile) purtate de avioanele F-16 ucrainene, fie prin dispunerea de suficiente capabilități de apărare antiaeriană cu rază lungă de acțiune de tip PATRIOT sau SAMP/T (Peck 2024).

O a treia metodă de combatere a atacurilor cu bombe planor este prin intermediul echipamentelor de război electronic. Bruiajul semnalului GPS necesar sistemelor de ghidare a bombelor planor va determina ca angajarea țintelor terestre să se facă în baza sistemelor secundare inerțiale, ceea ce va influența precizia. Erorile probabile de lovire a țintelor cresc direct proporțional cu distanța de zbor a bombelor planor fără asistența sistemelor GPS. Un exemplu de echipament de război electronic, eficient împotriva sistem bombelor planor pare a fi sistemul Lima, dezvoltat de echipa Night Watch în Ucraina (Axe 2025). Acesta acționează pe mai multe planuri asupra sistemelor de navigație, folosind o combinație de bruiaj, spoofing și atac cibernetic asupra receptoarelor GPS ale bombelor planor, determinând astfel abateri semnificative de la țintele vizate și, implicit, ineficiența atacurilor cu bombe planor.

Perturbarea aprovizionării cu bombe planor prin lovirea facilităților de producție, dar și a locațiilor de depozitare a acestora, înainte de a fi încărcate pe platforme aeriene reprezintă o altă metodă eficientă de combatere a atacurilor cu astfel de bombe. În anul 2024, mai multe atacuri ucrainene, întrebuințând drone cu rază lungă de acțiune, au pătruns în zonele de acțiune ale apărării antiaeriane ruse și au distrus depozite mari de muniție, inclusiv depozite de bombe planor, situate în proximitatea aerodromurilor cu aeronave purtătoare. Avem ca exemplu atacul și distrugerea unui astfel de depozit mare de muniții în Tikhoretsk (Al-Rifai 2024). Și în acest scop au fost solicitate insistent de către partea ucraineană muniții cu rază lungă de acțiune, pentru sistemele HIMARS, și aprobarea administrației americane să lovească ținte în adâncimea teritoriului Federației Ruse.

O altă metodă de a combate atacurile cu bombe planor este prin distrugerea respectivelor bombe pe traiectorie în timpul zborului, folosind tactici dovedite eficiente împotriva dronelor rusești de tip Shahed 136 (Hambling 2025). Aceste tactici se bazează pe amplasarea de senzori și de mijloace de lovire în apropierea liniei frontului în poziții de așteptare, având ca scop detecția și interceptarea bombelor

planor care sunt lansate din zonele ocupate de inamic. Sistemul integrează atât elemente de inteligență artificială pentru creșterea probabilității ratei de succes, cât și tunuri antiaeriene sau drone de interceptare pentru distrugerea bombelor planor.

Indiferent care dintre măsurile de contracarare a atacurilor cu bombe planor își vor demonstra viabilitatea și eficiența în timp, aspectul constant rămâne nevoia de adaptare la noua realitate a mediului operațional pentru forțele aflate în conflict, nevoie ce se poate răsfrânge în orice domeniu. Asistăm astfel la schimbări, implementate de forțele armate ale ambelor părți beligerante, în ceea ce privește strategia aplicată în conflict, doctrina de întrebuințare a forțelor terestre sau a forțelor aeriene, modul de înzestrare și de echipare a structurilor de forțe, modul de amenajare și de ocupare a pozițiilor defensive sau modul de asalt al acestora etc.

Concluzii

Folosirea bombelor planor pentru atacul diverselor ținte terestre și susținerea acțiunilor militare, în general, nu reprezintă astăzi un element de noutate. Aceste mijloace au fost exploatate în multe alte conflicte în trecut, originile lor fiind identificate încă din anii războaielor mondiale din secolul trecut. Aspectul inedit al reiterării întrebuințării bombelor planor în operație constă în exploatarea acestor mijloace în număr mare, datorită, în principal, costurilor reduse. Dezvoltarea și rafinarea kiturilor de planare, asociate cu sisteme eficiente de ghidare la țintă oferă, astăzi, un avantaj substanțial forțelor ruse în conflictul din Ucraina, asigurând posibilitatea utilizării platformelor aeriene într-o manieră nouă, diferită de cea de la debutul conflictului, fără a fi nevoite să câștige supremația sau superioritatea aeriană.

Efectele obținute prin folosirea în masă a bombelor planor se manifestă atât în plan fizic, precum distrugerea oricăror poziții defensive aflate pe direcțiile de înaintare ale forțelor ruse, cât și în plan psihologic, ceea ce are un impact semnificativ asupra moralului apărătorilor ucraineni și asupra populației civile afectate de aceste atacuri. Necesitatea eliminării sau diminuării potențialului devastator al bombelor planor a determinat căutarea de soluții de către armata ucraineană și aliații săi, astfel încât bombele planor să nu devină în timp un veritabil *game changer* în conflictul din Ucraina.

În cadrul acestei lucrări, am adus în atenție caracteristicile determinante ale bombelor planor și impactul atacurilor cu astfel de mijloace, pentru a sublinia potențialul pericol asupra operației militare, în ansamblul său. Totodată, am avut în vedere diverse soluții viabile, analizate atât la nivelul armatei ucrainene, cât și la nivelul aliaților săi, pentru a contracara eficient amenințarea reprezentată de bombele planor. Un lucru cert rămâne necesitatea adaptării structurilor de forțe, aplicabilă ambelor părți beligerante, la noua realitate a mediului operațional în conflictul din Ucraina.

Referințe

Al-Rifai, Nizar. 2024. "The Glide Bomb War: Evolving Aerial Combat Over the Ukrainian Battlefield." https://offbeatresearch.com/2024/11/the-glide-bomb-war-tracking-the-proliferation-of-glide-bombs-in-ukraine/.

Australian War Memorial. 2025. "Fritz X Guided Missile." https://www.awm.gov.au/collection/C152869.

Axe, David. 2025. "Ukraine Has Been Jamming Russian Glide Bombs. Now We Know How." https://www.forbes.com/sites/davidaxe/2025/03/17/ukraine-has-been-jamming-russian-glide-bombs-now-we-know-how/.

Di Mizio, Giorgio și Douglas Barrie. 2024. "Russian glide bombs add pressure on Ukraine's diminishing air defences." https://www.iiss.org/online-analysis/military-balance/2024/03/russian-glide-bombs-add-pressure-on-ukraines-diminishing-air-defences/.

Gheja, Victor. 2023. „Rusia folosește bombe planante de 1.500 kg în Ucraina: «Este echipată cu sistem de navigație prin satelit»." https://www.aktual24.ro/rusia-foloseste-bombe-planante-de-1-500-kg-in-ucraina-este-echipata-cu-sistem-de-navigatie-prin-satelit/.

Hambling, David. 2025. "A Ukrainian Mystery Weapon Is Shooting Down Russian Glide Bombs." https://www.forbes.com/sites/davidhambling/2025/02/13/a-ukrainian-mystery-weapon-is-shooting-down-russian-glide-bombs/.

Hardie, John. 2023. "Can Russia's New Guided Glide Bombs Help Blunt Ukraine's Counteroffensive?" https://www.fdd.org/analysis/2023/05/30/russias-new-guided-glide-bombs/.

___. 2024. "Photos offer insights on Russia's new UMPB D-30SN glide bomb." https://www.longwarjournal.org/archives/2024/06/photos-offer-insights-on-russias-new-umpb-d-30sn-glide-bomb.php.

Hodunova, Kateryna. 2025. "Russia's primitive glide bombs are still outmatching Ukraine's air defenses, killing more civilians." https://kyivindependent.com/russias-primitive-glide-bombs-are-still-outmatching-ukraines-air-defenses-killing-more-civilians-2/.

Hoehn, John și William Courtney. 2024. "How Ukraine Can Defeat Russian Glide Bombs." https://www.rand.org/pubs/commentary/2024/06/how-ukraine-can-defeat-russian-glide-bombs.html#:~:text=The%20most%20practical%20counter%20to,air%20capabilities%2C%20and%20electronic%20warfare.

Inwood, Joe și Tania Kharchenko. 2024. "Russia's glide bombs devastating Ukraine's cities on the cheap." https://www.bbc.com/news/articles/cz5drkr8l1ko.

Kushnikov, Vadim. 2023. "Ukrainian Su-27s are using JDAM-ER standoff bombs." https://militarnyi.com/en/news/ukrainian-su-27s-are-using-jdam-er-standoff-bombs/.

Lefief, Jean-Philippe. 2024. "Glide bombs: Russia's «ultimate weapon» or a sign of Ukraine's under-equipment?" https://www.lemonde.fr/en/international/article/2024/04/25/glide-bombs-russia-s-ultimate-weapon-or-a-sign-of-ukraine-s-under-equipment_6669544_4.html.

Miler, Sergio. 2024. "FAB 3000 Glide Bomb: Threat or Stunt?" https://wavellroom.com/2024/09/13/fab-3000-glide-bomb/.

NATO. 2025. ”Harnessing Innovation to Counter Glide Bombs.” https://www.act.nato.int/article/harnessing-innovation-counter-glide-bombs/.

Newsweek. 2023. ”U.S. Winged JDAM Smart Bombs Operational in Ukraine—Air Force General.” https://www.newsweek.com/us-winged-jdam-smart-bombs-ukraine-air-force-1786238.

Okoko, Janet Mola, Scott Tunison și Keith D. Walker. 2023. *Varieties of Qualitative Research Methods.* Saskatoon: Springer Texts in Education.

Peck, Michael. 2024. ”Glide Bombs: The Russian Wonder Weapon?” https://cepa.org/article/glide-bombs-the-russian-wonder-weapon/.

Peleschuk, Dan. 2024. ”Key facts about Russia’s highly destructive «glide bombs».” https://www.reuters.com/world/europe/russian-guided-bombs-wreaking-havoc-ukraine-2024-09-25/.

Vesti din Rusia. 2025. ”Asia Times: Bombele de tip planor ale Rusiei au pus Ucraina în impas.” https://www.vestidinrusia.com/2023/04/25/asia-times-bombele-cu-planare-ale-rusiei-au-pus-ucraina-in-impas/.

Watling, Jack și Nick Reynolds. 2025. *Tactical Developments During the Third Year of the Russo–Ukrainian War.* London: Royal United Services Institute.

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: 27 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.

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

Pragmatismul decizional în contextul agresiunii tip hibrid

Decision-making Pragmatism in the Context of Hybrid-type Aggression

Cpt. Diana-Elena CHIRILĂ*
*Direcția Instruire și Doctrină, Statul Major al Apărării
e-mail: chirila_diana92@yahoo.com

Abstract

Pragmatismul decizional joacă un rol crucial în gestionarea agresiunii hibride, un tip de conflict complex care combină tehnici convenționale cu atacuri cibernetice, cu manipularea informațiilor și cu presiuni economice. În fața unei astfel de amenințări, liderii trebuie să ia decizii rapide și flexibile, adaptându-se constant la schimbările rapide ale situației. Pragmatismul decizional implică utilizarea unor soluții inovative și eficiente, care integrează tehnologia, resursele informaționale și colaborarea dintre autoritățile civile și cele militare. Este esențială, de asemenea, cooperarea internațională și adaptarea legislativă pentru a combate efectele acestui tip de conflict, având în vedere interdependența globală. Abordarea pragmatică se axează pe anticiparea amenințărilor și răspunsul rapid la acestea, consolidând reziliența națională și internațională. Conflictul din Ucraina reprezintă un exemplu relevant al aplicării acestor principii, demonstrând importanța pragmatismului în răspunsul eficient la agresiunea hibridă și la provocările contemporane.

Decision-making pragmatism plays a crucial role in managing hybrid aggression, a complex type of conflict that combines conventional techniques with cyberattacks, information manipulation, and economic pressure. In the face of such a threat, leaders must make swift and flexible decisions, constantly adapting to rapidly changing circumstances. Decision-making pragmatism involves using innovative and effective solutions that integrate technology, informational resources, and collaboration between civilian and military authorities. International cooperation and legislative adaptation are also essential in countering the effects of this type of conflict, given global interdependence. The pragmatic approach focuses on anticipating and responding quickly to unpredictable threats, thereby strengthening both national and international resilience. The conflict in Ukraine serves as a relevant example of the application of these principles, demonstrating the importance of pragmatism in effectively responding to hybrid aggression and contemporary challenges.

Cuvinte-cheie:
pragmatism decizional; agresiune hibridă; conflicte moderne; securitate cibernetică; manipulare informațională; tehnologie și război; cooperare internațională; reziliență națională.

Keywords:
decision-making pragmatism; hybrid aggression; modern conflicts; cybersecurity; information manipulation; technology and warfare; international cooperation; national resilience.

Info articol
Primit: 6 mai 2025; Evaluat: 2 iunie 2025; Acceptat: 6 iunie 2025; Disponibil online: 27 iunie 2025
Citare: Chirilă, D.E. 2025. „Pragmatismul decizional în contextul agresiunii tip hibrid"
Buletinul Universității Naționale de Apărare „Carol I", 14(2): 69-79. https://doi.org/10.53477/2065-8281-25-13

În ultimele decenii, pe fondul evoluției rapide a tehnologiilor informaționale, al globalizării și al schimbărilor în structurile geopolitice, conflictele moderne au devenit din ce în ce mai complexe, iar natura lor a evoluat considerabil. Astfel, războaiele convenționale, așa cum le cunoșteam în trecut, au lăsat loc unor forme mult mai sofisticate de agresiune, care nu se limitează la confruntări directe între armate. Una dintre cele mai semnificative transformări în acest sens este apariția agresiunii hibride – un tip de conflict care integrează simultan metode tradiționale de luptă cu acțiuni de război informațional, atacuri cibernetice, presiuni economice și chiar manipularea opiniei publice (Grigore 2015, 187-191).

Această schimbare semnificativă în dinamica conflictelor impune noi provocări pentru procesul decizional al statelor și organizațiilor internaționale implicate în gestionarea crizelor. În fața unei amenințări hibride, deciziile trebuie să fie luate într-un context caracterizat de incertitudine, de rapiditate și complexitate. Astfel, pragmatismul decizional devine un factor cheie, în special în situațiile de criză, unde fiecare alegere are potențialul de a influența evoluția conflictului.

În această eră a războiului hibrid, deciziile nu mai sunt doar o simplă chestiune de opțiuni strategice pe câmpul de luptă, ci implică și domenii precum securitatea cibernetică, protecția infrastructurilor critice, gestionarea relațiilor internaționale și coordonarea eforturilor de informare și de mobilizare a populației. Astfel, autoritățile trebuie să adopte abordări inovative și flexibile, care să permită răspunsuri rapide și adaptabile în fața unui inamic imprevizibil și multiplicat pe mai multe fronturi.

În acest context, procesul de luare a deciziilor devine esențial nu doar în strategia militară, ci și în protejarea integrității sociale și economice a statului. Agresiunea hibridă pune, în fața liderilor politici, instituțiilor guvernamentale și armatei, dileme complexe, legate de resursele disponibile, de coordonarea acțiunilor și de prioritizarea obiectivelor.

Astfel, analiza pragmatismului decizional în fața agresiunii hibride trasează mai multe dimensiuni fundamentale conflictului modern. Răspunsul la această provocare nu se limitează doar la soluții tehnice sau militare, ci impune integrarea unei game largi de resurse – de la strategii economice și politice, la gestionarea informațiilor și implicarea societății civile. În acest sens, pragmatismul decizional reprezintă nu doar o alegere de eficiență, ci o necesitate absolută pentru a asigura securitatea și stabilitatea unui stat în fața unui atac complex și adesea neprevăzut.

Agresiunea hibridă – o nouă paradigmă a conflictului

Agresiunea hibridă reprezintă o formă sofisticată și complexă de război, caracterizată printr-o combinație sinergică între mijloacele convenționale și cele neconvenționale, între actorii statali și cei nonstatali, între operațiuni deschise și tactici disimulate (Ștefănescu 2024). Accentul militar în cadrul agresiunii hibride este unul subtil,

dar extrem de eficient, deoarece implică utilizarea forțelor armate într-o manieră indirectă și strategică, deseori sub acoperirea unor acțiuni civile sau nonmilitare.

Una dintre cele mai elocvente caracteristici ale agresiunii hibride este utilizarea forței militare sub pragul războiului convențional, astfel încât să nu provoace o reacție internațională directă. Spre exemplu, în cazul anexării Crimeei, forțele armate ruse au operat fără însemne oficiale, ceea ce a dus la etichetarea lor drept „omuleții verzi". Această tehnică a permis Rusiei să mențină o formă de negare plauzibilă și să evite o confruntare militară deschisă cu NATO.
În plus, mijloacele militare folosite într-un conflict hibrid sunt adesea însoțite de campanii intense de dezinformare, de destabilizare psihologică și război informațional, menite să slăbească moralul forțelor armate ale statului țintă și să creeze confuzie în rândul populației. Tacticile de tip "shock and awe" nu mai presupun bombardamente masive, ci atacuri cibernetice asupra infrastructurii critice, afectând rețelele electrice, comunicațiile și logistica militară.

Forțele speciale joacă un rol crucial în cadrul agresiunilor hibride. Aceste unități bine antrenate pot desfășura misiuni de recunoaștere, de sabotaj, de infiltrare și de influențare a populației locale. Operațiunile acestora sunt, în general, rapide, eficiente și greu de atribuit direct unui actor statal. De asemenea, aceste forțe sunt sprijinite logistic de o infrastructură civilă paralelă, care le permite să opereze sub acoperire într-un mediu aparent pașnic.

Tehnologia are un impact decisiv în componenta militară a războiului hibrid. Dronele, sateliții de observație, tehnologiile de recunoaștere facială și software-urile de analiză a datelor mari (big data) sunt folosite pentru a obține un avantaj strategic, fără a implica o desfășurare masivă de trupe. Astfel, în loc de o confruntare clasică pe câmpul de luptă, avem o bătălie invizibilă, dar letală, purtată pe multiple fronturi simultan.

O altă dimensiune importantă a agresiunii hibride cu accent militar este utilizarea conflictelor locale sau a tensiunilor etnice pentru a legitima intervenții „umanitare" sau „de protecție a minorităților". Sub această umbrelă, forțele armate ale agresorului sunt dislocate în teritorii străine, cu scopul aparent de a menține pacea, dar în realitate, acestea contribuie la ocuparea teritoriului și la influențarea structurii de putere locală.

Pe lângă toate acestea, importanța doctrinelor militare moderne nu poate fi subestimată. Statele care sunt potențiale victime ale agresiunilor hibride trebuie să își adapteze strategiile militare, să își modernizeze forțele armate și să investească în formarea unităților specializate de răspuns rapid, de luptă în medii urbane și de apărare cibernetică. Flexibilitatea doctrinară și capacitatea de reacție sunt esențiale pentru contracararea efectelor agresiunii hibride.

Așadar, dimensiunea militară a agresiunii hibride nu se manifestă prin invazii clasice, ci printr-o prezență subtilă, persistentă și multidimensională. Pentru a face

față acestui tip de amenințare, este necesară o reconfigurare profundă a modului în care sunt concepute și utilizate capacitățile militare, într-o manieră integrată cu celelalte domenii ale securității naționale.

Fundamentele pragmatismului decizional în situații de criză

În contextul agresiunii hibride, procesul decizional este supus unor presiuni fără precedent, întrucât liderii politici și militari trebuie să gestioneze un tip de conflict care nu urmează tiparele clasice. În acest cadru, pragmatismul decizional nu reprezintă doar o opțiune eficientă, ci o necesitate imperativă. Pragmatismul înseamnă orientarea deciziilor în funcție de rezultate concrete, de eficiență, de adaptabilitate și flexibilitate, evitând capcanele ideologizării sau ale deciziilor rigide, bazate exclusiv pe precedent.

În situații de criză, caracterizate de incertitudine, de presiune temporală și de un flux informațional dezechilibrat, factorii decizionali trebuie să adopte o abordare bazată pe analiza continuă a riscurilor și oportunităților (Dumitru 2022, 24-34). Elementele fundamentale ale unui astfel de pragmatism includ:

1. Evaluarea contextuală în timp real – pragmatismul decizional presupune adaptarea constantă la dinamica amenințării. În cazul agresiunii hibride, caracterul imprevizibil al evenimentelor necesită o monitorizare permanentă a mediului operațional, utilizând surse multiple de informații: intelligence militar, canale diplomatice, mass-media și analize open-source.

2. Flexibilitatea strategică – un principiu esențial este evitarea planificării rigide. În condiții de agresiune hibridă, în care tacticile adversarului se schimbă rapid, strategiile de răspuns trebuie să fie modulare, scalabile și reversibile. Acest lucru presupune existența unor scenarii predefinite, dar și capacitatea de a le ajusta în timp real.

3. Luarea deciziilor pe baza datelor – în locul reacțiilor impulsive sau al deciziilor bazate pe intuiție, pragmatismul promovează folosirea analizelor bazate pe date: modele predictive, simulări, algoritmi de învățare automată. Aceste instrumente sprijină o decizie rațională, redusă la esențial, dar informată și ancorată în realitate.

4. Decizii rapide și asumate – în contextul unui atac hibrid, amânarea deciziei poate produce efecte devastatoare. Pragmatismul implică o viteză crescută în procesul decizional, dar și o cultură instituțională, în care asumarea responsabilității este încurajată. Liderii eficienți trebuie să acționeze în condiții de incertitudine și să fie pregătiți să corecteze direcția, dacă situația o impune.

5. Colaborarea interinstituțională și multidisciplinară – deciziile nu mai pot fi luate izolat. În fața unei agresiuni hibride, unde dimensiunile militară, economică, informatică și socială sunt toate vizate simultan, este esențială colaborarea dintre instituții: armată, servicii de informații, guvern, mediul academic și sectorul privat.

6. Gândirea adaptativă și leadershipul anticipativ – un lider pragmatic anticipează scenariile de criză și pregătește organizația pentru reacție și reziliență. Aceasta înseamnă dezvoltarea unei culturi a învățării, în care lecțiile învățate din crize anterioare sunt documentate și transformate în politici viabile.

Pe lângă aceste elemente de natură operațională și strategică, pragmatismul decizional este influențat și de trăsăturile individuale ale decidenților: inteligență emoțională, capacitatea de a gestiona stresul, empatie și abilități de comunicare. Într-un climat marcat de haos informațional și de panică socială, capacitatea liderului de a transmite calm și coerent devine un vector esențial al stabilității. Fundamentele pragmatismului decizional în situații de criză sunt profund ancorate în realitatea complexă a secolului XXI, în care agresiunile hibride impun o reconfigurare profundă a mecanismelor de luare a deciziilor. Această paradigmă modernă nu poate fi redusă la simple manuale sau doctrine, ci trebuie să devină parte integrantă a culturii organizaționale, a educației liderilor și a arhitecturii instituționale. Doar printr-un astfel de efort coerent și multidimensional se poate asigura un răspuns eficient, legitim și sustenabil la amenințările hibride contemporane.

Instrumente decizionale și managementul agresiunii hibride

Gestionarea agresiunii hibride presupune un set complex de instrumente decizionale, capabile să răspundă provocărilor diverse ale unui conflict modern. Aceste instrumente trebuie să îmbine dimensiunile strategice, operaționale și tactice, într-un cadru de acțiune coordonat și adaptativ (Dojan 2016). În acest context, rolul decidentului pragmatic este de a selecta și de a operaționaliza instrumentele cele mai potrivite, în funcție de natura agresiunii, de gradul de acoperire al amenințării și de capacitățile interne disponibile (Cullen 2017).

1. Sistemele integrate de avertizare timpurie (SIAT) – acestea reprezintă prima linie de apărare împotriva agresiunii hibride (Botea 2019). Captarea și analiza timpurie a semnalelor slabe de criză din surse multiple – sociale, economice, militare, cibernetice – permit activarea mecanismelor de răspuns, înainte ca efectele să devină critice. Pragmatismul decizional presupune utilizarea eficientă a acestor instrumente în timp real, evitând paralizia decizională.

2. Celulele de criză interinstituționale – în fața unei amenințări hibride, răspunsul eficient implică o abordare multisectorială. Crearea unor celule de criză cu reprezentanți ai structurilor de apărare, ordine publică, informații, comunicare strategică și din mediul privat asigură un proces decizional colectiv, bazat pe partajarea rapidă a informației și pe capacitatea de a acționa simultan pe mai multe fronturi.

3. Simulările și jocurile de război (wargaming) – aceste instrumente permit testarea scenariilor de agresiune hibridă într-un mediu controlat. Ele contribuie la identificarea punctelor slabe, la testarea deciziilor, în condiții de

stres și la optimizarea răspunsului instituțional. Decidenții pragmatici folosesc aceste exerciții nu doar pentru pregătire, ci și pentru dezvoltarea unei culturi organizaționale orientate spre anticipare și adaptare.

4. Platformele decizionale asistate de inteligență artificială (IA) – în era digitală, IA poate procesa volume uriașe de date pentru a oferi suport decizional rapid și precis. Algoritmii de învățare automată pot detecta modele de comportament, pot anticipa mișcările actorilor hibrizi și pot sugera opțiuni de răspuns. Implementarea acestor platforme trebuie făcută cu prudență, asigurând un control uman permanent al deciziilor critice.

5. Comunicarea strategică și contranarațiunile – agresiunea hibridă include de cele mai multe ori un puternic component informațional. Combaterea dezinformării și manipulării presupune existența unor mecanisme clare de comunicare strategică prin care statul poate transmite mesaje coerente, credibile și sincronizate. Decidenții pragmatici trebuie să înțeleagă importanța acestei dimensiuni și să o integreze în arhitectura de răspuns.

6. Mecanismele de reziliență societală – un răspuns eficient la agresiunea hibridă nu poate exclude populația civilă. Pragmatismul decizional include și investiția în educație civică, în alfabetizare digitală, în voluntariat și infrastructuri comunitare, toate menite să reducă vulnerabilitatea la manipulare și să sprijine coeziunea socială (Buica 2022).

7. Instrumentele juridico-normative – reacția la o agresiune hibridă necesită un cadru legal care să permită intervenții rapide, fără a sacrifica valorile democratice. Deciziile pragmatice trebuie să fie legal sustenabile, iar cadrul normativ trebuie revizuit periodic pentru a ține pasul cu natura evolutivă a amenințărilor.

Instrumentele decizionale utilizate pentru gestionarea agresiunii hibride trebuie să reflecte o abordare holistică și integratoare, astfel încât să fie corelate între ele printr-un proces decizional clar, coordonat și pragmatic. Liderii eficienți sunt cei care înțeleg complexitatea acestor instrumente, le selectează, în funcție de context și le aplică într-o manieră flexibilă, dar fermă. Numai astfel se poate asigura un răspuns coerent și eficient într-un peisaj geopolitic din ce în ce mai fluid și mai provocator.

Pragmatismul decizional în contextul conflictului din Ucraina

Conflictul din Ucraina, care a început în 2014 și care a escaladat în 2022 prin invazia acesteia de către Federația Rusă, reprezintă un exemplu relevant al aplicării pragmatismului decizional într-un context de agresiune hibridă. Războiul din Ucraina combină tehnici de război convențional cu operațiuni cibernetice, cu război informațional, cu presiuni economice și cu manipularea opiniei publice. În fața acestei amenințări hibride complexe, autoritățile ucrainene au fost nevoite să adopte decizii rapide și eficiente pentru a proteja teritoriul național și pentru a menține stabilitatea internă, demonstrând capacitatea de a da un răspuns flexibil, menit să se adapteze unui mediu fluid și imprevizibil (Lesenciuc 2023, 64-85).

Contextul agresiunii hibride în Ucraina

Invazia rusă din 2022 a adus agresiunea hibridă într-o formă mult mai intensă, în care Federația Rusă a combinat tactici convenționale cu atacuri cibernetice, cu campanii de dezinformare și cu manipularea opiniei publice, cu presiuni economice și cu tentative de destabilizare socială (Stancu 2019, 12-43). Federația Rusă a folosit mai multe mijloace hibride pentru a destabiliza Ucraina și pentru a obține un avantaj strategic, iar răspunsul Ucrainei a fost marcat de pragmatism decizional. Mijloacele hibride utilizate de Rusia și răspunsurile Ucrainei sunt analizate mai detaliat în următoarele secțiuni (Giurgea 2024).

Mijloacele hibride utilizate de Federația Rusă

Federația Rusă a recurs la o combinație complexă de mijloace hibride pentru a destabiliza Ucraina și pentru a submina guvernul acesteia:

- **Atacuri cibernetice:** înainte și după invazia din 2022, Rusia a desfășurat o serie de atacuri cibernetice asupra infrastructurii critice ucrainene, inclusiv asupra sistemelor de alimentare cu energie, rețelelor de comunicații și sistemelor bancare. Aceste atacuri aveau scopul de a paraliza funcționarea instituțiilor statului și de a crea panică în rândul populației.
- **Războiul informațional și dezinformarea:** un alt mijloc hibrid folosit de Rusia a fost campania masivă de dezinformare. Purtătorii de cuvânt ai Kremlinului și agențiile de știri afiliate regimului au lansat campanii de propagandă pentru a manipula opinia publică din Ucraina și din mediul de afaceri internațional, inclusiv prin răspândirea de știri false, teorii ale conspirației și mesaje care subminau încrederea în autoritățile ucrainene.
- **Presiuni economice:** Rusia a impus sancțiuni economice și blocaje comerciale pentru a încerca să submineze economia ucraineană. În paralel, Rusia a blocat porturile ucrainene și a perturbat lanțurile de aprovizionare cu resurse vitale.
- **Subminarea structurilor politice interne:** Federația Rusă a utilizat tactici de destabilizare internă pentru a crea haos în rândul populației ucrainene. Acestea au inclus încercări de a cultiva conflicte etnice și sectare, alimentând nemulțumirile interne și disensiunile dintre diverse grupuri de cetățeni ucraineni.

Răspunsul pragmatic al Ucrainei la mijloacele hibride ale Rusiei

Răspunsul Ucrainei la agresiunea hibridă rusească a fost marcat de pragmatismul decizional. Autoritățile ucrainene au adoptat rapid măsuri eficiente pentru a contracara mijloacele hibride utilizate de Rusia:

- ✓ **Răspunsul cibernetic:** în fața atacurilor cibernetice, Ucraina a colaborat strâns cu parteneri internaționali, inclusiv cu NATO și cu companii de securitate cibernetică, pentru a întări infrastructura cibernetică națională. Ucraina a implementat măsuri rapide pentru a restabili sistemele afectate și pentru a proteja infrastructurile critice, având în vedere vulnerabilitățile în fața atacurilor cibernetice. Astfel, autoritățile ucrainene au demonstrat un pragmatism decizional rapid și flexibil în protejarea securității naționale.

✓ **Campaniile de combatere a dezinformării:** Ucraina a implementat strategii de război informațional, folosind rețelele sociale și mass-media pentru a informa corect populația și pentru a combate propaganda rusă. De asemenea, au fost întreprinse măsuri de identificare și de eliminare a surselor de dezinformare, colaborând cu platformele internaționale de socializare pentru a limita răspândirea de știri false. Președintele Ucrainei a jucat un rol central în aceste campanii, având o prezență activă pe rețelele sociale și comunicând direct cu cetățenii ucraineni și cu comunitatea internațională.

✓ **Sprijin internațional și alianțe strategice:** Ucraina a solicitat rapid ajutor din partea partenerilor internaționali, cum ar fi NATO, Uniunea Europeană și Statele Unite. Acest sprijin a inclus nu doar furnizarea de armament, dar și ajutor financiar și asistență economică pentru a sprijini economia ucraineană în fața presiunilor economice din partea Rusiei. Pragmatismul decizional al Ucrainei s-a văzut în diplomația activă, care a facilitat un răspuns unitar la nivel internațional, izolând Rusia și consolidând sprijinul global pentru Ucraina.

✓ **Mobilizarea resurselor interne și externe:** Ucraina a mobilizat rapid resurse interne, inclusiv armata, forțele teritoriale și voluntarii civili, pentru a apăra teritoriul național. În paralel, autoritățile ucrainene au apelat la implicarea civililor în diverse activități, inclusiv în producția de echipamente de apărare și în logistică, ceea ce a întărit reziliența națională. Mobilizarea rapidă a rezerviștilor și integrarea comunității locale în eforturile de apărare au constituit un exemplu clar de pragmatism decizional eficient.

✓ **Protejarea infrastructurii vitale și adaptarea rapidă a sistemului economic:** Ucraina a implementat măsuri rapide pentru a proteja infrastructura energetică și economică, inclusiv prin reorganizarea distribuției resurselor și găsirea unor soluții alternative pentru aprovizionarea cu energie electrică și cu gaze naturale. În plus, autoritățile ucrainene au implementat politici economice flexibile pentru a menține stabilitatea financiară, în ciuda sancțiunilor economice, impuse de Rusia.

✓ **Dezvoltarea rapidă a aplicației „Diia”**, un instrument digital esențial în gestionarea crizei: această aplicație a fost un element cheie în asigurarea unui flux constant de informații și de asistență pentru cetățenii ucraineni, oferind un mijloc eficient de comunicare guvernamentală și de coordonare a resurselor. Aplicația permite cetățenilor să aibă acces rapid la documente oficiale, să primească alerte în timp real privind situațiile de criză și să participe la procesele de mobilizare.

✓ **Campaniile de recrutare online**: într-un timp foarte scurt, autoritățile ucrainene au activat platforme online prin care cetățenii, inclusiv cei din diaspora, au fost încurajați să se alăture eforturilor de apărare națională. Aceste platforme au fost un exemplu de adaptare rapidă a autorităților la nevoile imediate ale conflictului.

✓ **Folosirea aplicațiilor de localizare și siguranță pentru civili:** autoritățile au lansat rapid aplicații și platforme care să permită localizarea în siguranță a civililor, coordonarea evacuărilor și informarea privind adăposturile sigure.

Aceste măsuri au demonstrat pragmatismul decizional al Ucrainei, permițând o

reacție rapidă și adaptivă la fiecare fază a agresiunii hibride. Aceste acțiuni au fost esențiale pentru menținerea unei coeziuni interne și pentru a garanta că resursele interne și externe erau folosite eficient.

Pragmatismul decizional al Ucrainei s-a reflectat și în capacitatea societății ucrainene de a rezista și de a se adapta la agresiunea hibridă. Populația a demonstrat o reziliență remarcabilă în fața atacurilor rusești și a presiunilor interne, fiind activ implicată în eforturile de apărare națională. Campaniile de informare, de educare a cetățenilor și de susținere a civililor care s-au implicat activ în protejarea teritoriilor lor au fost esențiale pentru menținerea moralului și coeziunii sociale. Spiritul civic și implicarea activă a populației în diverse domenii ale apărării naționale au fost factori cheie care au contribuit la succesul inițial al Ucrainei în contracararea agresiunii hibride rusești.

Pragmatismul decizional al autorităților ucrainene, combinat cu sprijinul internațional și cu implicarea activă a populației, a fost fundamental în contracararea agresiunii hibride rusești și în menținerea unui răspuns coerent și eficient pe termen lung. Acest studiu de caz subliniază importanța flexibilității și adaptabilității deciziilor într-un mediu de securitate extrem de volatil, cum este cel al agresiunii hibride.

Concluzii

În era actuală, marcată de instabilitate geopolitică, de proliferarea tehnologiilor emergente și de volatilitatea actorilor nonstatali, agresiunea hibridă reprezintă o amenințare complexă, adaptativă și persistentă. În acest peisaj, decizia nu mai poate fi un proces izolat, birocratic sau liniar, ci trebuie să se transforme într-un exercițiu continuu de pragmatism și anticipare. Astfel, pragmatismul decizional devine un criteriu de supraviețuire strategică în fața agresiunii hibride, iar într-un mediu dominat de ambiguitate și ambivalență, capacitatea decidentului de a acționa rapid, flexibil și pe baza unei evaluări continue a riscurilor este crucială. Pragmatismul în acest context înseamnă renunțarea la dogmatism și adaptarea permanentă la realitățile schimbătoare ale mediului operațional, decizia devenind un act de echilibru între ceea ce este posibil, fezabil și acceptabil într-un anumit moment.

Interoperabilitatea instituțională, inteligența artificială, analiza big data și simulările strategice sunt pilonii centrali ai infrastructurii decizionale moderne. Într-un conflict hibrid, unde timpul de reacție este esențial, abilitatea de a integra surse multiple de informații și de a extrage în timp real patternuri relevante din volume mari de date poate face diferența dintre succes și eșec. De asemenea, interoperabilitatea dintre structurile civile și cele militare, naționale și internaționale este fundamentală pentru evitarea disfuncționalităților și suprapunerilor, care pot fi exploatate de adversar.

Un alt element critic în peisajul conflictului hibrid este reprezentat de leadershipul adaptiv, reflexiv și proactiv, astfel încât liderii trebuie să fie nu doar buni strategi,

ci și empatici, deschiși la feedback și capabili să gestioneze tensiuni între priorități concurente. Aceștia trebuie să decidă în condiții de stres intens, să-și mobilizeze echipa și să mențină coeziunea organizațională în fața incertitudinii, iar formarea lor trebuie să includă nu doar pregătire militară, ci și dezvoltarea inteligenței emoționale, a gândirii critice și a competențelor de comunicare strategică.

Dimensiunea societală a răspunsului implică o viziune integrată asupra securității naționale. Cetățenii bine informați, educați în spiritul rezilienței și conștienți de mecanismele agresiunii hibride devin parteneri activi în apărarea țării. Combaterea manipulării informaționale, promovarea gândirii critice și întărirea încrederii în instituțiile democratice sunt acțiuni esențiale pentru limitarea succesului tactic al actorilor hibrizi. În plus, comunicarea guvernamentală trebuie să fie transparentă, coerentă și adaptată canalelor moderne pentru a consolida încrederea publicului.

Nu în ultimul rând, cadrele normative și mecanismele democratice trebuie modernizate, astfel încât să ofere atât flexibilitate operațională, cât și garanții de protecție a drepturilor cetățenești. Pragmatismul decizional cere un echilibru fin între viteza de reacție și respectarea principiilor statului de drept. Reformele legislative ar trebui să prevadă scenarii de urgență clar definite, proceduri rapide de activare a mecanismelor de apărare și protocoale de colaborare public-privat, mai ales în domeniile critice, precum infrastructura cibernetică, mass-media și sectorul financiar.

În concluzie, succesul în contracararea agresiunii hibride nu depinde exclusiv de resurse sau de tehnologie, ci și de calitatea procesului decizional. O abordare pragmatică, informată și bine articulată strategic poate transforma vulnerabilitatea într-un avantaj competitiv, iar criza, într-un catalizator al reformei. Într-o lume în care granițele conflictului devin din ce în ce mai difuze, rămâne esențial ca procesul decizional să fie ancorat în realitate, dar orientat spre viitor.

Referințe

Botea, M. 2019. „Despre războiul hibrid și contracararea efectelor acestuia." *Gândirea Militară Românească* nr. 2. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/GMR-2_2019.pdf.

Buica, D. 2022. *Dezinformarea, componentă a războiului hibrid.* București: Editura Universității Naționale de Apărare „Carol I".

Cullen, P. 2017. "Understanding Hybrid Warfare." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

Dojan, M. 2016. *Rusia și războiul hibrid. Cazul Ucraina.* București: Editura Universității Naționale de Apărare „Carol I".

Dumitru, I.R. 2022. „Evoluția conceptului de război hibrid în strategiile naționale de apărare ale României." *Buletinul Universității Naționale de Apărare „Carol I"* 11 (3): 24-34. https://revista.unap.ro/index.php/revista/article/view/1484/1435.

Giurgea, N. 2024. „Războiul hibrid: Tehnici şi strategii.” https://www.geopolitic.ro/2024/11/razboiul-hibrid-tehnici-si-strategii/.

Grigore, L. 2015. „Viitorul războiului – Războiul hibrid.” *Buletinul Universității Naționale de Apărare „Carol I”* 2 (2): 187-191. https://revista.unap.ro/index.php/revista/article/view/135.

Lesenciuc, A. 2023. „Războiul hibrid în vreme de război – încercare de operaționalizare conceptuală și acțională.” *Gândirea Militară Românească* nr. 1: 64-85. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2023%20gmr/gmr%201/LESENCIUC.pdf.

Stancu, M.C. 2019. „Războiul hibrid și forme de manifestare ale acestuia în criza din Ucraina.” *Gândirea Militară Românească* nr. 2: 12-43. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/stancu.pdf.

Ştefănescu, M. 2024. „Războiul hibrid: O abordare complexă a confruntărilor moderne.” https://www.ziarultricolorul.ro/razboiul-hibrid-o-abordare-complexa-a-confruntarilor-moderne/.

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

Confidențialitate, loialitate și responsabilitate: triada etică în managementul sistemelor informaționale în domeniul securității naționale

Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security

Conf.univ.Dr. Florentina-Loredana DRAGOMIR*
*Universitatea Națională de Apărare „Carol I", București
e-mail: Dragomir.Loredana@unap.ro

Abstract

Prezentul articol analizează triada etică formată din confidențialitate, loialitate și responsabilitate în managementul sistemelor informaționale din domeniul securității naționale, subliniind nevoia unei guvernanțe informaționale adaptate complexității actuale. În centrul analizei se află rolul sistemelor informaționale inteligente (SII), care, prin integrarea tehnologiilor de inteligență artificială, învățare automată și analiză comportamentală, oferă un suport decisiv în modernizarea arhitecturilor de securitate și în consolidarea unei culturi organizaționale etice. În acest sens, articolul susține că integrarea SII nu mai reprezintă o alegere tehnologică opțională, ci o necesitate strategică pentru organizațiile care gestionează informații clasificate și resurse critice. Prin abordarea sa multidisciplinară și prin argumentele fundamentate teoretic și normativ, studiul contribuie la delimitarea unui cadru conceptual robust privind guvernanța etică a informației în instituțiile de securitate națională.

This article analyzes the ethical triad of confidentiality, loyalty, and responsibility in the management of information systems in the field of national security, highlighting the need for information governance adapted to the current complexity. At the heart of the analysis is the role of intelligent information systems (IIS), which, by integrating artificial intelligence, machine learning, and behavioral analysis technologies, provide decisive support in modernizing security architectures and strengthening an ethical organizational culture. In this sense, the article argues that the integration of IIS is no longer an optional technological choice, but a strategic necessity for organizations that manage classified information and critical resources. Through its multidisciplinary approach and theoretically and normatively grounded arguments, the study contributes to the delimitation of a robust conceptual framework regarding the ethical governance of information in national security institutions.

Cuvinte-cheie:
sisteme informatice inteligente; securitate națională; guvernanță etică; decizii strategice; confidențialitate.

Keywords:
Intelligent Information Systems; National Security; Ethical Governance; Strategic Decision-Making; Confidentiality.

Info articol
Primit: 30 aprilie 2025; Evaluat: 28 mai 2025; Acceptat: 30 mai 2025; Disponibil online: 27 iunie 2025
Citare: Dragomir, F.L. 2025. „Confidențialitate, loialitate și responsabilitate: triada etică în managementul sistemelor informaționale în domeniul securității naționale". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(2): 80-93. https://doi.org/10.53477/2065-8281-25-14

Gestionarea etică a sistemelor informaționale în domeniul securității naționale a devenit o provocare strategică majoră. Instituțiile militare și de securitate se confruntă cu necesitatea de a echilibra transparența proceselor operaționale cu protecția informațiilor sensibile într-un mediu în care confidențialitatea, loialitatea și responsabilitatea constituie parametrii esențiali ai încrederii instituționale. În actualul climat strategic, profund marcat de digitalizare accelerată și volatilitate geopolitică, protejarea informațiilor sensibile reprezintă un obiectiv prioritar pentru organizațiile din domeniul securității naționale. În paralel, exigențele privind transparența proceselor și responsabilitatea instituțională devin din ce în ce mai pregnante, inclusiv în sectorul militar. Astfel, se conturează o dilemă etică fundamentală: cum poate fi asigurat un echilibru sustenabil între nevoia de transparență operațională și imperativele confidențialității?

Confidențialitatea nu mai este doar o chestiune tehnică, ci o dimensiune etică fundamentală în arhitectura sistemelor informaționale strategice. Studiile recente evidențiază că eficiența securității informaționale este influențată de factori instituționali și culturali, iar integrarea acestor aspecte în strategiile de securitate este esențială pentru protejarea datelor sensibile (Metin și alții 2024, 4226). Cercetările subliniază că performanța sistemelor de securitate informațională depinde în mod semnificativ de contextul instituțional și de valorile culturale, iar încorporarea acestor factori în politicile de securitate este crucială pentru asigurarea protecției datelor sensibile (Xu și alții 2025, 6). Loialitatea personalului cu acces la informații clasificate este un alt element critic. Comportamentele deviante, cum ar fi încălcarea politicilor de securitate, pot avea consecințe grave asupra integrității sistemelor informaționale. Analizele comportamentale subliniază importanța unei culturi organizaționale solide și a unei conduceri etice pentru prevenirea acestor riscuri (Metin și alții 2024, 4226). Totodată, loialitatea personalului cu acces la informații clasificate se afirmă ca o verigă esențială în lanțul de securitate. Fenomenele de abatere de la normele etice și riscurile asociate factorului uman rămân printre principalele vulnerabilități ale sistemelor informaționale. Prevenirea acestor riscuri presupune cultivarea unei culturi organizaționale solide, înrădăcinată în valori, precum devotamentul instituțional și disciplina profesională. Responsabilitatea atât la nivel individual, cât și instituțional este esențială în guvernanța sistemelor informaționale. Implementarea unor politici clare și a unor mecanisme de audit eficiente contribuie la asigurarea integrității și disponibilității informațiilor, aspecte cruciale pentru funcționarea optimă a organizațiilor strategice (Almomani și alții 2023, 4467). Pe de altă parte, responsabilitatea în materie de guvernanță informațională implică atât mecanisme formale de control (audit, trasabilitate, reglementări), cât și asumarea conștientă a consecințelor deciziilor luate la toate nivelurile structurale. Implementarea unui cadru de responsabilitate distribuită contribuie la întărirea rezilienței instituționale și la consolidarea încrederii publice (Almomani și alții 2023, 4467).

În acest context, articolul de față își propune să exploreze triada etică, formată din confidențialitate, loialitate și responsabilitate, analizând modul în care aceste valori pot fi integrate în managementul sistemelor informaționale din domeniul

securității naționale. Prin intermediul unei abordări multidisciplinare, vom examina provocările și soluțiile etice care pot contribui la consolidarea securității informaționale în organizațiile strategice.

1. Confidențialitatea în arhitectura sistemelor informaționale strategice

1.1. Definirea conceptului de confidențialitate în contextul securității naționale

Confidențialitatea, alături de integritate și disponibilitate, constituie una dintre cele trei dimensiuni esențiale ale securității informaționale, cunoscută sub denumirea de triada CIA. În sens operațional, confidențialitatea implică protejarea datelor împotriva accesului neautorizat, asigurând că doar persoanele sau entitățile autorizate pot vizualiza, manipula sau distribui informații sensibile. În cadrul organizațiilor de securitate națională, această componentă capătă o importanță critică. Protejarea informațiilor strategice, militare sau diplomatice de compromitere nu este doar o cerință tehnică, ci o obligație instituțională, care susține suveranitatea statului și funcționarea sistemului de apărare. Informațiile clasificate, dacă sunt divulgate sau accesate în mod neautorizat, pot conduce la vulnerabilități operaționale, la afectarea relațiilor internaționale sau chiar la pierderi de vieți omenești în teatrele de operații.

Unul dintre modelele conceptuale fundamentale pentru implementarea confidențialității este modelul Bell–LaPadula. Acesta a fost conceput pentru mediile militare, unde nivelurile de clasificare sunt riguroase. Aceste reguli au drept scop prevenirea accesului la informații de nivel superior de către utilizatori cu autorizații inferioare, respectiv blocarea transferului neautorizat de informații de la niveluri înalte către cele inferioare. Aplicarea acestui model contribuie la menținerea unei ierarhii riguroase de securitate, în care fluxul informațional este strict controlat și documentat. Astfel, confidențialitatea în arhitectura sistemelor informaționale strategice trebuie înțeleasă nu doar ca o măsură tehnologică de protecție, ci și ca o responsabilitate etică și instituțională, ancorată în cadrul normativ național și internațional privind securitatea informației.

1.2. Instrumente tehnologice și procedurale pentru asigurarea confidențialității

Protejarea informațiilor sensibile în cadrul sistemelor informaționale strategice presupune implementarea unui ansamblu de măsuri tehnologice și procedurale, menite să prevină accesul neautorizat, interceptarea sau compromiterea datelor. Aceste măsuri sunt integrate într-o arhitectură de securitate cuprinzătoare, care funcționează atât la nivelul infrastructurii informatice, cât și în cadrul structurilor organizaționale.

Criptarea datelor reprezintă unul dintre cele mai eficiente mijloace tehnologice de protejare a confidențialității. Algoritmii criptografici avansați, precum Advanced Encryption Standard (AES), asigură confidențialitatea informațiilor atât în tranzit, cât și în repaus, împiedicând accesul la conținutul acestora, în absența unei chei valide. În mediile militare, unde datele circulă prin rețele distribuite și adesea vulnerabile,

criptarea este însoțită de protocoale robuste de autentificare și de semnături digitale, care contribuie la validarea identității utilizatorilor și a integrității mesajelor.

O altă modalitate de protejare a confidențialității îl constituie politicile de control al accesului. Acestea sunt reglementate de mecanisme, precum controlul bazat pe roluri (Role-Based Access Control – RBAC) și controlul bazat pe atribute (Attribute-Based Access Control – ABAC), care asigură accesul la informații în funcție de responsabilitățile funcționale și de nivelul de autorizare al fiecărui utilizator. În instituțiile strategice, unde gradul de clasificare al datelor este ridicat, aceste mecanisme sunt completate de politici obligatorii de acces (Mandatory Access Control – MAC), care impun restricții rigide și ierarhizate, în conformitate cu legislația privind informațiile clasificate.

Pe lângă componentele tehnologice, instrumentele procedurale joacă un rol esențial în garantarea confidențialității. Auditarea sistematică a activităților informatice, monitorizarea în timp real a accesului la date și analiza comportamentului utilizatorilor contribuie la identificarea rapidă a posibilelor breșe de securitate (Kent și Souppaya 2006). În paralel, formarea continuă a personalului, derulată prin programe instituționale de conștientizare și de instruire, vizează reducerea riscurilor asociate erorii umane, care rămâne una dintre cele mai frecvente cauze ale compromiterii informațiilor clasificate.

Prin urmare, asigurarea confidențialității nu se limitează la implementarea unor tehnologii performante, ci presupune o guvernanță integrată a riscului informațional, în care procesele, politicile și comportamentele individuale se află într-o relație de interdependență strategică.

1.3. Riscuri asociate divulgării sau pierderii datelor clasificate

Divulgarea neautorizată sau pierderea informațiilor clasificate reprezintă una dintre cele mai grave vulnerabilități în arhitectura sistemelor informaționale strategice, cu implicații directe asupra securității naționale, stabilității geopolitice și capacității operaționale a instituțiilor militare. Aceste incidente pot compromite planuri tactice, pot dezvălui capabilități tehnice sau pot afecta alianțe și parteneriate strategice, generând un efect de domino în lanțurile decizionale și operaționale. În primul rând, compromiterea informațiilor clasificate poate conduce la pierderea avantajului strategic. Cum într-un mediu operațional asimetria informațională este decisivă, accesul adversarilor la date sensibile poate favoriza acțiuni de anticipare, de disuasiune sau de sabotaj, care subminează eficiența și siguranța misiunilor militare. Cazurile documentate în literatura de specialitate relevă faptul că scurgerile de informații din cadrul instituțiilor de apărare au condus în mod repetat la reevaluarea structurilor de comandă, la suspendarea temporară a operațiunilor și la diminuarea încrederii interinstituționale. În al doilea rând, pierderea controlului asupra datelor clasificate afectează sever relațiile internaționale și cooperarea în materie de securitate. Partenerii strategici își bazează schimbul de informații pe premisele confidențialității reciproce și pe existența unor măsuri echivalente de protecție

informațională. O breșă în acest sistem de încredere poate conduce la restrângerea accesului la informații critice, la suspendarea colaborărilor sau la reevaluarea poziției geopolitice a statului afectat.

Din perspectivă instituțională, astfel de incidente generează costuri semnificative atât din punct de vedere logistic, cât și reputațional. Reconfigurarea sistemelor afectate, inițierea anchetelor interne, măsurile de remediere și investițiile suplimentare în securitate implică alocarea unor resurse bugetare considerabile. Mai mult, în rândul opiniei publice, pierderea de informații sensibile poate eroda încrederea cetățenilor în capacitatea statului de a-și proteja interesele fundamentale, alimentând percepția de vulnerabilitate instituțională.

Pentru a limita aceste riscuri, organizațiile strategice trebuie să adopte o abordare proactivă, bazată pe evaluări continue de risc, pe teste de penetrare, pe simulări de incident și pe audituri independente. Aceste mecanisme trebuie susținute de un cadru normativ coerent și de o cultură organizațională orientată spre conformitate, responsabilitate și vigilență informațională. În absența acestor măsuri, protecția datelor clasificate rămâne expusă unor amenințări persistente, sofisticate și cu impact sistemic.

2. Responsabilitatea instituțională și individuală în guvernanța sistemelor informaționale

2.1. Cadre normative și obligații legale privind protecția informațiilor (legi naționale, tratate internaționale)

Responsabilitatea în materie de guvernanță a informației este strâns corelată cu respectarea unui cadru normativ complex, care reunește reglementări naționale, directive internaționale și tratate multilaterale privind protecția datelor clasificate și a infrastructurilor critice. În România, Legea nr. 182/2002 privind protecția informațiilor clasificate, împreună cu normele metodologice aferente, stabilește obligațiile instituțiilor publice și ale personalului autorizat în ceea ce privește clasificarea, manipularea și stocarea datelor sensibile. Aceste prevederi sunt armonizate cu cerințele NATO și UE privind interoperabilitatea în domeniul informațiilor securizate.

La nivel internațional, instrumente precum Tratatul de Securitate Informațională al NATO și Regulamentul General privind Protecția Datelor (GDPR) – în cazul în care interacțiunea implică și componente civile sau dual-use – impun standarde clare privind confidențialitatea, trasabilitatea și responsabilitatea procesării informațiilor. De asemenea, convenții precum Convenția de la Budapesta privind criminalitatea informatică conturează obligații statale în prevenirea și combaterea accesului ilegal la sisteme și date.

Respectarea acestor norme nu este opțională, ci face parte din responsabilitatea instituțională de a garanta securitatea informațională ca parte integrantă a securității

naționale. Această responsabilitate presupune existența unor structuri funcționale de control intern, audit periodic și actualizare continuă a procedurilor, în conformitate cu evoluțiile tehnologice și cu amenințările emergente (Dragomir-Constantin 2025c, 99-108).

2.2. Mecanisme de responsabilizare: trasabilitate, audit, răspundere penală sau disciplinară

În contextul sistemelor informaționale utilizate de organizațiile strategice, responsabilitatea nu poate fi redusă la un principiu teoretic sau la o valoare abstractă; ea trebuie să fie exprimată concret printr-un ansamblu de mecanisme instituționalizate care să permită atât prevenirea, cât și remedierea incidentelor care afectează confidențialitatea informațiilor clasificate. Această responsabilitate este dublă: individuală, în sensul asumării deciziilor de către fiecare utilizator autorizat, și instituțională, prin existența unor structuri și proceduri care asigură trasabilitatea acțiunilor, auditarea sistemelor și aplicarea de sancțiuni, în caz de abatere.

Trasabilitatea este condiția fundamentală pentru orice formă de responsabilizare. Prin implementarea unor mecanisme tehnice de monitorizare – precum logarea activităților, sistemele de jurnalizare criptografică și platformele de analiză comportamentală –, organizațiile pot asigura o vizibilitate continuă asupra interacțiunilor utilizatorilor cu sistemele critice. Astfel, fiecare accesare, modificare sau transmitere de date este înregistrată și asociată unei identități digitale, eliminând premisele anonimatului și reducând riscul de impunitate (Dignum 2019). Acest sistem de urmărire a acțiunilor individuale este indispensabil pentru identificarea sursei unui incident, dar și pentru stabilirea proporțională a răspunderii.

Auditul, ca instrument formal de verificare a conformității și eficienței, contribuie la menținerea unui climat instituțional transparent și predictibil. Evaluările periodice ale politicilor de securitate informațională, realizate de entități interne sau externe, permit nu doar corectarea abaterilor, ci și anticiparea unor vulnerabilități structurale. În mediile militare, auditul are o dimensiune strategică suplimentară: el validează capacitatea sistemelor informaționale de a susține operațiuni, în condiții de adversitate informațională și cibernetică (Kent și Souppaya 2006).

Sancțiunile disciplinare și juridice completează acest cadru, asigurând un răspuns instituțional proporțional la încălcările normelor de securitate. Fără mecanisme sancționatorii clare, responsabilitatea devine iluzorie, iar organizația se expune riscului ca normele să fie percepute ca pur formale. Aplicarea consecventă a măsurilor – de la retragerea accesului, la suspendarea temporară sau definitivă din funcție, până la urmărirea penală în cazurile grave – contribuie la consolidarea unei culturi instituționale bazate pe respectarea reglementărilor și pe conștientizarea consecințelor individuale ale neglijenței sau intenției malițioase (Metin și alții 2024).

Astfel, responsabilitatea într-un ecosistem informațional de tip strategic nu poate funcționa în absența unui cadru coerent de trasabilitate, audit și sancționare. Această

triadă instituțională asigură nu doar reziliența operațională, ci și legitimitatea internă și externă a organizației în fața provocărilor specifice mediului de securitate contemporan.

Trasabilitatea reprezintă o funcționalitate esențială în cadrul arhitecturii de securitate a sistemelor informaționale strategice, definind capacitatea sistemului de a înregistra, urmări și corela toate acțiunile desfășurate asupra resurselor informaționale de către utilizatorii autorizați. Această funcție nu are doar un rol tehnic, ci constituie fundamentul responsabilității individuale și instituționale, oferind suport probatoriu pentru evaluarea comportamentului utilizatorilor și conformității proceselor cu politicile și reglementările în vigoare. În mod operațional, trasabilitatea se realizează printr-un ansamblu de tehnologii și metode, precum loguri de acces detaliate, sisteme de jurnalizare criptografică și module de analiză comportamentală, care permit corelarea fiecărei acțiuni din sistem cu o identitate digitală univocă. În mediile militare și instituționale de înaltă securitate, aceste sisteme sunt configurate pentru a funcționa în regim de nonrepudiere, asigurând că nicio operațiune relevantă nu poate fi contestată ulterior de către actorul care a generat-o (Sulaiman și alții 2022).

Importanța trasabilității nu se limitează la dimensiunea investigativă postincident, deși aceasta este vitală pentru determinarea cauzelor și responsabilităților, în cazul compromiterii informațiilor. Ea joacă un rol preventiv și sistemic în procesul de guvernanță a riscului informațional, permițând instituțiilor să monitorizeze în timp real activitatea utilizatorilor, să detecteze anomalii comportamentale și să reacționeze prompt în fața abaterilor sau a potențialelor atacuri interne. Astfel, trasabilitatea contribuie la consolidarea capacității de reacție operațională și la menținerea unei culturi organizaționale bazate pe transparență și responsabilitate. În plus, trasabilitatea constituie o condiție esențială pentru auditul eficient al sistemelor informatice. În special în organizațiile strategice, logurile trebuie să fie protejate împotriva modificării sau ștergerii, întrucât acestea pot constitui probe juridice în anchete disciplinare sau penale. Din acest motiv, instituțiile militare implementează soluții care asigură integritatea logurilor prin mecanisme de sigilare digitală, de sincronizare temporală cu surse de timp externe și de replicare în sisteme redundante, garantând astfel că orice tentativă de alterare a înregistrărilor este detectabilă și sancționabilă.

Prin urmare, trasabilitatea nu este doar o componentă tehnologică, ci o dimensiune strategică a arhitecturii de securitate, integrată în ansamblul politicilor de conformitate, de control intern și de guvernanță informațională. Fără un mecanism robust de trasabilitate, instituțiile strategice riscă nu doar pierderea controlului asupra resurselor informaționale, ci și diminuarea capacității de a reacționa în mod legitim și eficient în fața abaterilor interne sau a atacurilor externe.

Urmează auditul, una dintre cele mai importante componente ale mecanismului de control instituțional în materie de securitate informațională, acesta având rolul de a evalua conformitatea, eficiența și robustețea proceselor, politicilor și infrastructurilor

informatice. În mediile strategice, auditul transcende dimensiunea pur procedurală, devenind un instrument esențial de guvernanță și anticipare a riscurilor, care contribuie la consolidarea integrității organizaționale și la menținerea capacității operaționale, în condiții de incertitudine sau amenințare.

Auditul de securitate informațională se desfășoară pe două planuri interdependente: cel tehnic și cel procedural. Auditul tehnic presupune examinarea sistemelor informatice din perspectiva configurațiilor de securitate, a nivelurilor de criptare, a sistemelor de detecție a intruziunilor, precum și a politicilor de acces și logare. Obiectivul este identificarea vulnerabilităților care ar putea fi exploatate de actori interni sau externi și evaluarea capacității sistemului de a rezista la atacuri cibernetice, inclusiv cele de tip avansat persistent (APT). În organizațiile militare, acest tip de audit este completat adesea prin simulări de penetrare (”red teaming”), în care echipe specializate încearcă să compromită sistemele în mod controlat pentru a evidenția punctele slabe din apărare.

Pe de altă parte, auditul procedural se concentrează asupra modului în care politicile și regulamentele de securitate sunt aplicate în practică. Acesta analizează compatibilitatea dintre fluxurile operaționale și cerințele normative, gradul de respectare a protocoalelor de acces și de manipulare a informațiilor clasificate, precum și nivelul de instruire al personalului. Discrepanțele dintre prevederile teoretice și comportamentul real al actorilor instituționali pot semnala deficiențe de comunicare, lipsa unei culturi organizaționale axate pe securitate sau chiar riscuri sistemice, generate de toleranța la abateri.

Un audit eficient presupune independența structurilor de control, accesul la date nefiltrate și capacitatea de a formula recomandări operaționale, nu doar constatări tehnice. De asemenea, este esențial ca rezultatele auditului să fie integrate într-un ciclu continuu de îmbunătățire, în care recomandările să fie transpuse în măsuri concrete, iar implementarea acestora să fie urmărită cu aceeași rigoare. În concluzie, auditul nu este doar o practică de verificare retrospectivă, ci și un element activ al sistemului de securitate informațională, menit să detecteze și să corecteze vulnerabilități, să valideze măsuri și să întărească responsabilitatea individuală și instituțională. În absența unei funcții de audit solid ancorate în arhitectura decizională a organizațiilor strategice, controlul riscurilor informaționale rămâne parțial și reactiv, ceea ce poate compromite reziliența întregului sistem.

Răspunderea juridică și disciplinară reprezintă dimensiunea sancționatorie prin care organizațiile strategice își consolidează mecanismele de control și previn comportamentele neconforme. În mediile cu grad ridicat de secretizare, precum cele militare, responsabilitatea individuală pentru protejarea informațiilor clasificate nu este doar o obligație profesională, ci și o exigență legală, reglementată prin norme interne, legislație națională și tratate internaționale în materie de securitate și apărare.

În cadrul instituțiilor militare, regimul sancționator este completat de regulamente interne care includ, pe lângă suspendarea temporară sau revocarea accesului la informații clasificate, și proceduri de retrogradare sau de excludere din sistem. Responsabilitatea penală se activează atunci când compromiterea informațiilor are loc prin fapte intenționate, din neglijență gravă sau în urma unor omisiuni culpabile. Astfel de fapte includ transferul neautorizat de date, accesul nepermis la sisteme clasificate, pierderea suporturilor fizice de stocare sau nerespectarea procedurilor operaționale. În aceste cazuri, autoritățile competente, inclusiv structurile specializate ale Ministerului Public sau serviciile de contrainformații declanșează anchete care pot conduce la trimiterea în judecată a persoanelor implicate (Metin și alții 2024).

Răspunderea disciplinară, deși distinctă de cea penală, joacă un rol complementar, având ca obiectiv menținerea ordinii interne și a conformității cu normele organizaționale. Aceasta poate fi aplicată inclusiv în situații în care fapta nu întrunește elementele constitutive ale unei infracțiuni, dar reflectă o conduită inacceptabilă din perspectiva obligațiilor de serviciu. Sancțiunile pot varia de la avertismente scrise și scăderea temporară a salariului, până la destituirea din funcție sau excluderea din structurile de securitate, în funcție de gravitatea încălcării și de poziția ocupată de persoana în cauză. În mediile strategice, eficiența acestor forme de răspundere depinde de trei factori: claritatea normelor, consecvența aplicării și transparența procedurilor. Lipsa unui cadru normativ bine definit sau aplicarea selectivă a sancțiunilor poate conduce la erodarea culturii organizaționale bazate pe etică și responsabilitate. Astfel, răspunderea juridică și disciplinară trebuie înțeleasă ca o verigă esențială a ecosistemului de securitate informațională, prin care comportamentul individual este corelat cu normele instituționale, iar protejarea informațiilor sensibile devine un act de conformitate, loialitate și respect față de interesul național.

3. Contribuțiile sistemelor informaționale inteligente la consolidarea responsabilității și eticii organizaționale

În era transformării digitale accelerate și a intensificării amenințărilor hibride, sistemele informaționale inteligente (SII) s-au impus ca elemente esențiale în arhitectura organizațiilor strategice, redefinind paradigmele de guvernanță, de securitate și de luare a deciziilor. Aceste sisteme, fundamentate pe inteligență artificială (IA), pe învățare automată (ML), pe analitică predictivă și pe procese de automatizare cognitivă, extind funcționalitățile infrastructurii informaționale tradiționale, oferind o capacitate crescută de adaptare și anticipare în medii operaționale volatile (Dignum 2019; Xu și alții 2024).

În mod particular, SII permit modernizarea proceselor decizionale prin reducerea incertitudinii și creșterea vitezei de reacție în fața amenințărilor informaționale.

Algoritmii de învățare automată pot analiza volume masive de date în timp real, identificând tipare relevante, anomalii și semnale slabe care ar putea indica o breșă de securitate sau un comportament deviant din partea unui utilizator intern. Această capacitate de detecție precoce, asociată cu mecanisme de răspuns automatizat, contribuie direct la consolidarea rezilienței informaționale și la prevenirea incidentelor cu impact sistemic (Grigaliunas și alții 2024). Mai mult, sistemele inteligente facilitează o guvernanță proactivă a riscurilor informaționale prin generarea de modele predictive și recomandări decizionale, bazate pe evaluarea probabilistică a amenințărilor. Aceste instrumente nu doar susțin procesele tactice de securitate, ci și permit alinierea deciziilor operaționale la standarde etice și juridice prestabilite. Astfel, SII devin instrumente de suport etic în medii în care deciziile rapide trebuie să fie compatibile cu reglementările naționale și internaționale privind protecția datelor și drepturile fundamentale (Dignum 2019; Tounsi și Rais 2018).

Un element esențial care diferențiază sistemele informaționale inteligente (SII) de infrastructurile clasice de securitate este capacitatea lor de a facilita o guvernanță proactivă a riscurilor informaționale, bazată pe anticipare, adaptare și conformitate normativă. Această abordare proactivă presupune depășirea paradigmei reactive, în care măsurile de securitate sunt implementate post-factum, și trecerea la un model predictiv, în care amenințările sunt identificate, evaluate și neutralizate înainte de a se materializa.

SII integrează algoritmi de învățare automată și modele de inteligență artificială care procesează volume mari de date din surse heterogene – inclusiv loguri de sistem, fluxuri de comunicație, profiluri comportamentale și indicatori de amenințare – pentru a genera evaluări probabilistice privind riscurile emergente. Prin aceste capabilități, sistemele pot detecta semnale slabe și pot corela evenimente aparent izolate, identificând tipare care indică activități anormale, potențial periculoase, înainte ca acestea să devină manifeste (Tounsi și Rais 2018). Acest tip de analiză predictivă oferă factorilor de decizie un avantaj temporal semnificativ, permițându-le să adopte măsuri de securitate cu caracter preventiv, nu doar corectiv.

Pe lângă dimensiunea tehnică, SII contribuie și la susținerea unui cadru decizional etic și juridic coerent. În organizațiile strategice, unde deciziile trebuie luate adesea în condiții de presiune și incertitudine, instrumentele inteligente oferă sprijin analitic obiectiv, reducând riscul de decizii arbitrare sau nealiniate cu reglementările în vigoare. De exemplu, prin integrarea unor reguli deontologice sau a unor criterii de conformitate cu legislația privind protecția datelor, sistemele pot evalua opțiunile decizionale nu doar din punctul de vedere al eficienței operaționale, ci și al respectării normelor legale și principiilor de drept (Dignum 2019). Această funcție de „asistență etică automatizată" devine crucială în domenii sensibile, precum apărarea națională, securitatea cibernetică sau protecția infrastructurilor critice, unde deciziile pot implica simultan consecințe tehnice, umane și politice. SII pot recomanda opțiuni care minimizează riscurile colaterale, protejează datele personale sau respectă drepturile fundamentale, chiar și în contexte operaționale în care astfel

de dimensiuni sunt ușor de neglijat. Astfel, aceste sisteme nu doar că optimizează răspunsul la amenințări, ci și instituționalizează un cadru de responsabilitate etică distribuită, în care principiile normative sunt încorporate în logica algoritmică a acțiunii. În acest sens, rolul SII transcende funcția de suport tehnologic, devenind parte integrantă a unui mecanism decizional responsabil, capabil să integreze în timp real criterii de securitate, de legalitate și de etică. Într-un ecosistem informațional complex și hiperconectat, în care granițele dintre operațional și normativ sunt din ce în ce mai fluide, această capacitate de a susține decizii compatibile, simultan cu imperativul de eficiență și cu exigențele morale și juridice reprezintă un avantaj strategic major.

Un alt beneficiu esențial al SII constă în sprijinirea culturii organizaționale etice. Prin monitorizarea continuă și imparțială a interacțiunilor utilizatorilor cu sistemele informaționale, aceste tehnologii oferă un cadru de responsabilitate distribuită, în care fiecare actor este conștient că acțiunile sale sunt supuse unui regim obiectiv de evaluare și trasabilitate. În acest sens, tehnologia funcționează nu doar ca un gardian al datelor, ci și ca un mecanism de conformitate morală, reducând spațiul pentru abateri sau comportamente oportuniste (Xu și alții 2024).

Sistemele informaționale inteligente contribuie la modernizarea arhitecturilor de securitate și la profesionalizarea deciziilor strategice, oferind un sprijin tehnologic indispensabil pentru atingerea unui echilibru durabil între eficiență operațională, responsabilitate și etică instituțională. Cum timpul de reacție este critic, iar erorile umane pot avea consecințe ireversibile, integrarea SII nu mai este o opțiune, ci o necesitate strategică pentru organizațiile care gestionează informații clasificate și resurse critice.

Unul dintre cele mai relevante beneficii ale sistemelor informaționale inteligente (SII) în cadrul organizațiilor strategice constă în capacitatea acestora de a susține și de a consolida o cultură organizațională etică, în care normele comportamentale, valorile instituționale și responsabilitatea individuală sunt în mod continuu promovate, verificate și întărite prin mecanisme tehnologice transparente și imparțiale. Spre deosebire de modelele tradiționale de conformitate, care se bazează preponderent pe supraveghere ierarhică și audituri periodice, SII oferă posibilitatea unei monitorizări constante, scalabile și neutre a interacțiunilor dintre utilizatori și resursele informaționale critice. Prin culegerea și analiza automată a datelor privind activitatea utilizatorilor – inclusiv accesarea fișierelor, modificarea configurațiilor, comunicarea prin canale interne sau activitatea în afara orelor de lucru –, aceste sisteme pot construi profiluri comportamentale care permit detectarea devierilor semnificative de la normele instituționale. Această formă de monitorizare nu vizează controlul represiv, ci cultivarea unui mediu în care actorii organizaționali devin conștienți că fiecare acțiune este supusă unei forme de evaluare obiectivă, nemijlocită de percepții sau interese subiective (Xu și alții 2024). În această configurație, tehnologia devine un catalizator al responsabilității individuale, contribuind la internalizarea normelor etice de către utilizatori. Conștientizarea faptului că activitatea profesională este vizibilă și trasabilă

nu doar descurajează comportamentele oportuniste, dar și încurajează adoptarea unor practici conforme, în care respectarea politicilor nu mai este percepută ca o obligație externă, ci ca o normă integrată în identitatea profesională a individului. Această responsabilitate distribuită – susținută de sisteme imparțiale și automate – are avantajul de a reduce spațiul de manevră pentru acțiuni distructive, consolidând, în același timp, încrederea în mecanismele instituționale de control.

Mai mult, SII pot contribui la dezvoltarea unui climat organizațional în care conformitatea morală nu este doar un rezultat al fricii de sancțiune, ci al înțelegerii și asimilării valorilor instituționale. Prin analiza comportamentelor colective și individuale, sistemele pot genera informații utile referitoare la tiparele dominante, vulnerabilitățile etice ale organizației și necesitatea unor intervenții de formare sau ajustare culturală. Acest tip de feedback analitic permite decidenților să adopte politici proactive de etică organizațională, fundamentate pe date, nu doar pe presupuneri sau incidente reactive (Tounsi și Rais 2018).

Prin capacitățile avansate de analiză predictivă, de detectare a anomaliilor, de automatizare a reacțiilor și de asistare a deciziilor, SII asigură un sprijin operațional care depășește sfera tehnică și care pătrunde în dimensiunile normative și organizaționale ale securității. Astfel, deciziile nu mai sunt adoptate exclusiv în baza intuiției sau experienței individuale, ci sunt susținute de date, corelate cu scenarii, evaluate în funcție de riscuri și filtrate prin constrângeri etice și juridice. Această recalibrare a procesului decizional permite nu doar minimizarea erorilor umane, ci și consolidarea legitimității și transparenței în interiorul instituțiilor strategice (Dignum 2019). În contextul operațional contemporan, în care timpul de reacție este comprimat, iar presiunea asupra liderilor instituționali este constantă, deciziile rapide, dar conforme devin un imperativ. În această ecuație, SII oferă un avantaj competitiv prin capacitatea lor de a furniza informații în timp real, de a învăța din incidente anterioare și de a genera soluții adaptive în fața unor amenințări dinamice (Tounsi și Rais 2018).

Mai mult, prin promovarea unei culturi organizaționale bazate pe transparență, trasabilitate și etică distribuită, aceste sisteme sprijină dezvoltarea unei instituții agile, capabile să funcționeze în medii volatile, fără a-și compromite valorile fundamentale. În acest sens, rolul SII nu este limitat la un instrument de securitate, ci se extinde către statutul de infrastructură critică pentru decizia responsabilă, guvernanța strategică și reziliența organizațională. Așadar, în mediile instituționale care gestionează informații clasificate, infrastructuri critice sau mize strategice naționale, implementarea sistemelor informaționale inteligente nu mai poate fi considerată un lux sau o alegere opțională. Ea reprezintă o necesitate pentru consolidarea securității, optimizarea deciziilor și asigurarea unei conduite instituționale conforme cu standardele internaționale de etică, legalitate și performanță.

Concluzii

În condițiile creșterii volumului de date strategice și accentuării amenințărilor hibride, protejarea informațiilor sensibile nu mai poate fi realizată eficient prin mecanisme tradiționale de securitate și de control instituțional. Articolul de față a argumentat că triada etică, formată din confidențialitate, loialitate și responsabilitate, nu poate fi susținută fără integrarea tehnologiilor emergente, în special a sistemelor informaționale inteligente (SII).

Aceste sisteme nu doar extind capabilitățile tehnice ale organizațiilor strategice, ci și transformă fundamental modul în care este înțeleasă și aplicată guvernanța informațională. Prin capacitatea de a monitoriza în timp real comportamentul utilizatorilor, de a genera evaluări predictive ale riscurilor și de a susține deciziile strategice prin recomandări conforme cu standardele etice și juridice, SII devin infrastructuri de responsabilitate distribuită. Ele oferă garanții suplimentare pentru integritatea proceselor și reduc semnificativ riscul de eroare umană, de abuz sau de neglijență instituțională.

Un alt aport esențial al acestor tehnologii constă în sprijinirea unei culturi organizaționale etice. Prin trasabilitate, imparțialitate în evaluare și capacitate de adaptare, SII contribuie la întărirea conștiinței profesionale a personalului și la internalizarea valorilor instituționale. Astfel, tehnologia funcționează nu doar ca un instrument de control, ci și ca un mecanism de cultivare a eticii instituționale, în care responsabilitatea nu este impusă extern, ci susținută prin infrastructură și proces decizional.

Integrarea sistemelor informaționale inteligente în arhitectura organizațiilor strategice trebuie să fie privită nu ca o opțiune tehnologică, ci ca o necesitate strategică. Sistemele informaționale inteligente oferă premisele unei guvernanțe robuste, conforme, proactive și orientate spre valori. Mediul informațional tot mai instabil, unde timpul de reacție este critic, iar costurile greșelilor sunt ireversibile, vizează SII, care se constituie într-un suport indispensabil pentru asigurarea securității, legitimității și rezilienței instituționale.

Referințe

Almomani, Iman, Aala Alkhayer și Walid El-Shafai. 2023. "E2E-RDS: Efficient End-to-End Ransomware Detection System Based on Static-Based ML and Vision-Based DL Approaches". *Sensors 23* (9): 4467. https://doi.org/10.3390/s23094467.

Bell, David Elliott și Leonard LaPadula. 1973. "Secure Computer Systems: Mathematical Foundations. Technical Report MTR-2547", Vol. I. https://websites.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf

Dignum, Virginia. 2019. "Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way". Springer. https://link.springer.com/book/10.1007/978-3-030-30371-6

Dragomir, Florentina-Loredana și Gelu Alexandrescu. 2017a. "Applications of Artificial Intelligence in Decision-Making Process". *Bulletin of "Carol I" National Defense University* 4(2): 56-61. https://cssas.unap.ro/en/pdf_periodicals/si63.pdf.

___. 2017b. "The Axiomatic Character of Decision". *Bulletin of "Carol I" National Defense University* 6 (1): 16-22. https://www.ceeol.com/search/article-detail?id=548274.

Dragomir, Florentina-Loredana, Gelu Alexandrescu și Florin Postolache. 2018. "Tools for hierarchical security ". *The 14 the International Scientific Conference "eLearning and Software for Education"*, Bucharest, Carol I" National Defence University, April 19 - 20, Advanced Distributed Learning Association, vol. 4, pp. 34-38.

Dragomir-Constantin, Florentina-Loredana. 2025a. "Information System for Macroprudential Policies." *Acta Universitatis Danubius. Œconomica* 21 (1): 48-57. https://dj.univ-danubius.ro/index.php/AUDOE/article/view/3254.

___. 2025b. "Thinking Patterns in Decision-Making in Information Systems". *New Trends in Psychology* 7 (1): 89-98. https://dj.univ-danubius.ro/index.php/NTP/article/view/3255.

___. 2025c. "Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making". *New Trends in Psychology 7* (1) 99-108. https://dj.univ-danubius.ro/index.php/NTP/article/view/3257.

Grigaliūnas, Šarūnas, Michael Schmidt, Rita Brūzgienė și Smyrli Panagiota. 2024. "Holistic Information Security Management and Compliance Framework". https://epubl.ktu.edu/object/elaba:209322117/.

Kent, Karen și Murugiah Souppaya. 2006. "Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology". https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

Metin, Bilgin, Fatma Gözde Özhan și Martin Wynn. 2024. "Digitalisation and Cybersecurity: Towards an Operational Framework." *Electronics* 13 (21): 4226. https://www.mdpi.com/2079-9292/13/21/4226.

Sulaiman, Nur Shafinas, Mohd Azlan Fauzi, Wendy Wider și Jasmine Rajadurai. 2022. "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review." *Social Sciences* 11 (9): 386. https://www.mdpi.com/2076-0760/11/9/386.

Tache, Florentina-Loredana, Postolache Florin, Nachila Cătălin și Ivan Maria Alexandra. 2010." Consulting in Electronic Commerce." *Acta Universitatis Danubius. Œconomica* 6 (3): 162-169. https://journals.univ-danubius.ro/index.php/oeconomica/article/view/707.

Tounsi, Wassim și Hassen Rais. 2018. "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attack". *Computers & Security* 72. https://www.sciencedirect.com/science/article/abs/pii/S0167404817301839?via%3Dihub.

Xu, Yao, Jixin Wei, Ting Mi și Zhihua Chen. 2024 "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics." *World Electric Vehicle Journal* 16 (1): 6. https://doi.org/10.3390/wevj16010006.

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

Utilizarea metodologiilor de proiect Agile în planificarea acțiunilor militare

Using Agile Project Methodologies in Military Action Planning

Lt.drd. Ionuț-Alexandru RADU*
*Universitatea Națională de Apărare „Carol I", București
e-mail: radu.alexandru@unap.ro

Abstract

Create inițial pentru dezvoltarea de programe informatice, abordările Agile oferă o modalitate nouă de a spori eficacitatea și eficiența planificării în contextul militar prin utilizarea managementului de proiect. Acest studiu analizează aplicarea conceptelor Agile – cum ar fi colaborarea, flexibilitatea și iterația – în planificarea operațiunilor militare, reliefând, totodată, avantajele și dificultățile punerii în practică a acestor concepte într-un cadru militar, dar și modul în care acestea pot îmbunătăți adaptabilitatea strategică și timpii de reacție rapidă. Studiul rezumă, de asemenea, ansamblul cercetărilor privind abordările Agile, concentrându-se, în principal, asupra modului în care cadrele Agile, precum Scrum și Kanban, pot fi adaptate pentru a fi utilizate în contexte militare.

Originally created for software development, Agile approaches offer a new way to increase the effectiveness and efficiency of planning in the military context through the use of project management. This study examines the application of Agile concepts - such as collaboration, flexibility, and iteration - to the planning of military operations. This study highlights the advantages and challenges of applying these concepts in a military setting, emphasising how they can improve strategic adaptability and rapid response times. Focusing on their development, fundamental ideas and various project management applications, the study summarises the body of research on Agile approaches. The main focus of the paper is on the way in which Agile frameworks such as Scrum and Kanban can be adapted for use in military contexts.

Cuvinte-cheie:
metodologii Agile; Scrum; Kanban; proiect; operațiuni militare; planificare.

Keywords:
Agile Methodologies; Scrum; Kanban; Project; Military Operations; Planning.

Info articol
Primit: 22 aprilie 2025; Evaluat: 5 mai 2025; Acceptat: 12 mai 2025; Disponibil online: 27 iunie 2025

Citare: Radu, I.A. 2025. „Utilizarea metodologiilor de proiect Agile în planificarea acțiunilor militare". *Buletinul Universității Naționale de Apărare „Carol I"*, 14(2): 94-109. https://doi.org/10.53477/2065-8281-25-15

Operațiunile militare se desfășoară în medii caracterizate prin volatilitate, incertitudine, complexitate și ambiguitate. Metodologiile de proiect Agile, concepute inițial pentru dezvoltarea de software, oferă abordări promițătoare pentru a spori eficiența planificării militare în aceste medii dinamice. Prezenta lucrare examinează modul în care cadrele Agile pot fi adaptate contextelor militare, furnizând dovezi empirice ale beneficiilor acestora, recunoscând, în același timp, provocările legate de implementarea lor. Cercetările arată că organizațiile militare care adoptă metodele Agile au obținut îmbunătățiri semnificative în ceea ce privește capacitatea de reacție, colaborarea și eficiența operațională. Proiectele de mărime medie care utilizează metode Agile au adus beneficii mai mari clienților decât abordările tradiționale, cu un succes notabil în implementările IT militare. Deși rezistența organizațională și preocupările legate de securitate reprezintă provocări, abordările strategice de punere în aplicare, care echilibrează structurile ierarhice militare cu principiile Agile sunt foarte promițătoare pentru îmbunătățirea capacităților operaționale militare.

1. Contextul istoric și evoluția planificării militare

1.1. Abordări tradiționale de planificare militară

Planificarea militară a utilizat, istoric, procese liniare, secvențiale, care pun accentul pe o planificare prealabilă cuprinzătoare și pe o execuție ierarhică strictă. Aceste abordări tradiționale, deși oferă structură și claritate de comandă, de multe ori nu reușesc să răspundă eficient la condițiile operaționale în schimbare rapidă. Organizațiile militare din întreaga lume au recunoscut această limitare în mediile operaționale contemporane în care amenințările evoluează rapid și informațiile circulă continuu.

Planificarea militară tradițională urmează, de obicei, o abordare de tip „waterfall", cu faze secvențiale care includ culegerea de informații, analiza misiunii, dezvoltarea cursului de acțiune, compararea, aprobarea și executarea. Această metodologie pune accentul pe analiza aprofundată și pe planificarea detaliată, înainte de începerea execuției (Tudose 2021, 95-112). Deși această abordare oferă o analiză cuprinzătoare a factorilor și o direcție clară, ea suferă de limitări semnificative în medii dinamice. Odată lansate, aceste planuri sunt dificil de modificat fără perturbări substanțiale, creând o rigiditate care poate fi exploatată de adversari mai agili.

Pe măsură ce liderii militari se confruntă cu medii operaționale din ce în ce mai complexe și imprevizibile, limitele abordărilor tradiționale de planificare au devenit mai evidente. Căutarea unei mai mari flexibilități în cadrul organizațiilor militare a devenit „ cerința momentului" în era digitală, acestea încercând să aplatizeze structurile organizaționale pentru a accelera procesul decizional și a îmbunătăți capacitatea de reacție. Această recunoaștere a dus la creșterea interesului pentru abordările alternative de planificare care pot acomoda mai bine incertitudinea și schimbarea.

1.2. Apariția metodologiilor Agile

Metodologiile Agile au apărut în industria de dezvoltare software în anii ’90, culminând cu „Manifestul Agile” în 2001. Acest manifest a stabilit patru valori fundamentale: indivizii și interacțiunile sunt mai importante decât procesele și instrumentele; software-ul funcțional este mai important decât documentația completă; colaborarea cu clienții este mai importantă decât negocierea contractelor; răspunsul la schimbare este mai important decât respectarea unui plan. Aceste valori au reprezentat o îndepărtare semnificativă de abordările tradiționale de dezvoltare „în cascadă”, care urmau un proces liniar, secvențial, similar planificării militare tradiționale (Agile Manifesto 2001).

Abordarea Agile a introdus mai multe inovații-cheie în gestionarea proiectelor, inclusiv dezvoltarea iterativă, echipele autoorganizate, feedbackul continuu al clienților și adaptarea la cerințele în schimbare. Aceste principii au fost aplicate, inițial, dezvoltării de software, dar de atunci, s-au extins la diverse domenii, inclusiv spre dezvoltarea de produse, marketing și managementul organizațional. Succesul Agile în gestionarea complexității și incertitudinii în mediile comerciale a stârnit interes pentru aplicarea sa în contexte militare.

Evoluția industriei software de la abordarea în cascadă la abordarea Agile reflectă provocările cu care se confruntă organizațiile militare. După cum a explicat, în 2017, generalul Ellen M. Pawlikowski, fost comandant al Air Force Material Command, Agile se referă la iterația continuă: „Îl planifici, îl construiești, îl lansezi, primești feedback. Și faci acest lucru în mod constant”. Această abordare iterativă oferă o potențială soluție la provocările legate de adaptabilitate cu care se confruntă operațiunile militare (U.S. Air Force 2019).

2. Cadrul teoretic pentru implementarea abordărilor Agile în mediul militar

2.1. Principiile fundamentale ale managementului de proiect Agile

Managementul Agile al proiectelor se bazează pe mai multe principii fundamentale care îl diferențiază de abordările tradiționale. În primul rând, acesta pune accentul pe dezvoltarea iterativă, împărțind proiectele în cicluri mici, ușor de gestionat, care produc valoare incrementală. În al doilea rând, prioritizează adaptabilitatea, încurajând schimbarea mai degrabă decât opunându-i rezistență. În al treilea rând, se concentrează pe colaborare, promovând autoorganizarea, echipele interfuncționale lucrând în strânsă colaborare. În al patrulea rând, se concentrează pe client, asigurând alinierea continuă la nevoile utilizatorului. În sfârșit, încurajează îmbunătățirea continuă prin reflectarea și adaptarea periodică a proceselor (Daraojimba și alții 2024, 190-218).

Aceste principii se manifestă în diverse practici în cadrul Agile. Întâlnirile zilnice de stand-up îmbunătățesc comunicarea și rezolvarea problemelor. Revizuirile

Sprint (în Scrum) oferă oportunități regulate pentru feedbackul părților interesate. Retrospectivele permit echipelor să învețe din experiență și să îmbunătățească procesele. Gestionarea vizuală a fluxului de lucru (în Kanban) sporește transparența și identifică blocajele. Împreună, aceste practici creează un cadru pentru a răspunde în mod eficient la cerințele în schimbare, menținând, în același timp, concentrarea pe furnizarea de valoare (Orlov și alții 2021, 693-700).

Natura iterativă a gestionării proiectelor Agile este deosebit de valoroasă în mediile incerte. În loc să încerce să prezică toate cerințele și să planifice totul în avans, abordările Agile recunosc incertitudinea și stabilesc mecanisme pentru reevaluarea și adaptarea periodică. Această abordare iterativă permite echipelor să învețe și să se adapteze pe măsură ce progresează, ceea ce o face potrivită pentru medii complexe și dinamice precum operațiunile militare.

2.2. Paralele între strategia militară și filozofia Agile

În mod surprinzător, multe principii Agile își găsesc paralele în strategia și tactica militară tradițională. Străvechiul strateg militar chinez Sun Tzu sublinia adaptabilitatea, răspunsul rapid și exploatarea circumstanțelor în schimbare – concepte care se aliniază îndeaproape cu filozofia Agile. Cercetările au explorat aceste conexiuni, evidențiind modul în care conceptele strategiei militare pot fi transpuse în principiile dezvoltării Agile. De exemplu, accentul pus de Sun Tzu pe adaptabilitate și pe ajustarea strategiilor, în funcție de situație se aliniază cu accentul pus de Agile pe răspunsul la schimbare (Tudose 2021, 95-112).

Doctrina militară a recunoscut de mult timp importanța adaptabilității în medii incerte. Conceptele de comandă a misiunii și de intenție a comandantului oferă unităților subordonate libertatea de a-și adapta abordarea, menținând, în același timp, alinierea la obiectivele generale. Acest echilibru între autonomie și aliniere reflectă accentul pus de Agile pe echipele autoorganizate care lucrează în vederea atingerii unor obiective comune (Tudose 2021, 95-112).

Legătura dintre strategia militară și Agile devine deosebit de evidentă atunci când se examinează abordarea militară a mediilor VUCA (Volatility, Uncertainty, Complexity, and Ambiguity) – un concept care a fost aplicat, de asemenea, contextelor de afaceri. Atât doctrina militară, cât și metodologiile Agile recunosc limitările predicției și ale planificării detaliate în astfel de medii, punând accentul, în schimb, pe adaptabilitate, învățare și descentralizarea procesului decizional (Supriyadi și alții 2023, 40-52).

2.3. Adaptabilitatea și capacitatea de reacție în contexte militare

Capacitatea de a se adapta rapid la circumstanțele în schimbare este crucială în operațiunile militare. Soldații operează, de obicei, în medii incerte, ostile și ambigue, în care scenariile care se schimbă rapid sunt norma. Abordările tradiționale de planificare au adesea dificultăți în a-și menține relevanța în astfel de medii dinamice, deoarece planurile pot deveni caduce înainte de a putea fi executate integral.

Adoptarea metodologiilor Agile le permite liderilor militari să exercite controlul, adaptându-se, în același timp, la condițiile schimbătoare care, altfel, ar putea perturba operațiunile. Prin divizarea operațiunilor în iterații mai mici, prin menținerea unor bucle de feedback continuu și prin abilitarea echipelor de a ajusta tacticile în funcție de realitățile din teren, abordările Agile pot spori capacitatea armatei de a răspunde eficient amenințărilor și oportunităților emergente.

Această adaptabilitate sporită poate oferi avantaje strategice în situații de conflict. Teoreticienii militari au recunoscut de mult timp că abilitatea de a executa bucla OODA (Observare, Orientare, Decizie, Acțiune) mai rapid decât adversarii oferă un avantaj semnificativ. Metodologiile Agile, cu accentul lor pe feedback și adaptare rapidă, pot accelera această buclă, permițând forțelor militare să depășească adversarii în medii dinamice (Toroi și Stanciu 2023, 20-45).

3. Cadrele Agile și aplicațiile lor militare

3.1. Cadrul Scrum în operațiunile militare

Scrum, unul dintre cele mai utilizate cadre Agile, oferă o abordare structurată, dar flexibilă a gestionării proiectelor, care poate fi adaptată contextelor militare. Cadrul organizează activitatea în iterații încadrate în timp, denumite sprinturi, care durează de obicei 1-4 săptămâni. Fiecare sprint începe cu planificarea, include reuniuni zilnice de sincronizare și se încheie cu sesiuni de revizuire și cu retrospective. Un proprietar de produs prioritizează munca pe baza valorii, în timp ce un maestru Scrum facilitează procesul și elimină impedimentele (Schwaber și Sutherland 2020).

În mediul militar, Scrum poate fi adaptat pentru a sprijini planificarea și execuția operațională. Sesiunile de planificare Sprint pot include analiza misiunii și dezvoltarea cursului de acțiune. Întâlnirile zilnice servesc drept reuniuni de sincronizare pentru echipele operaționale, asigurând alinierea și ridicând la suprafață provocările. Revizuirile Sprint oferă oportunități structurate de evaluare a progreselor și de ajustare a planurilor, în funcție de schimbarea condițiilor. Retrospectivele sprijină procesele de revizuire după acțiune și lecțiile învățate, consolidând învățarea organizațională.

Armata Statelor Unite a utilizat cu succes Scrum pentru a gestiona operațiunile logistice din Irak și din Afganistan, demonstrând aplicabilitatea sa dincolo de dezvoltarea de software. Organizând sprijinul logistic în sprinturi și menținând o sincronizare regulată, aceste operațiuni au obținut o mai mare capacitate de reacție la nevoile în schimbare, menținând, în același timp, coordonarea dintre unități. Această aplicație arată cum structura Scrum poate oferi un cadru suficient pentru a asigura coordonarea, permițând, în același timp, flexibilitatea necesară în medii dinamice (Orlov și alții 2021).

3.2. Implementarea Kanban pentru logistică și sprijin militar

Metoda Kanban oferă o abordare vizuală a gestionării fluxului de lucru care poate fi deosebit de valoroasă pentru funcțiile de logistică și sprijin militar. Metoda vizualizează elementele de lucru pe o tablă cu coloane reprezentând etapele fluxului de lucru, limitează lucrările în curs pentru a preveni supraîncărcarea și se concentrează pe optimizarea fluxului prin sistem. Această vizualizare face ca blocajele să fie imediat vizibile, permițând echipelor să abordeze problemele, înainte ca acestea să afecteze operațiunile (Kanban University 2021).

În contexte militare, Kanban poate gestiona eficient sarcinile operaționale, logistica și activitățile de sprijin. Marina SUA a utilizat Kanban pentru a gestiona dezvoltarea sistemelor software, demonstrând aplicabilitatea sa militară. Prin vizualizarea stadiului sarcinilor și prin limitarea lucrărilor în curs, echipele de logistică își pot concentra resursele asupra priorităților critice, în loc să disperseze prea mult eforturile pe mai multe sarcini (Abercrombie, Fullbright și Long 2016).

Accentul pus de Kanban pe limitarea lucrărilor în curs se aliniază cu principiul militar al concentrării forței, ceea ce sugerează o potrivire naturală între cele două abordări. Prin vizualizarea fluxurilor de lucru și identificarea blocajelor, unitățile militare se pot asigura că resursele sunt direcționate către sarcinile cele mai critice, sporind eficiența operațională generală.

3.3. Abordări hibride: Scrumban, Kanplan și gândirea de proiectare militară (MDT)

Recunoscând că nu există un cadru unic care să se potrivească tuturor contextelor, au apărut abordări hibride care combină elemente ale diferitelor metodologii Agile. Scrumban combină structura Scrum cu optimizarea fluxului Kanban, în timp ce Kanplan adaugă conceptele de backlog Scrum la Kanban, permițând echipelor care nu lucrează iterativ să beneficieze de pregătirea backlogului.

În mod similar, armata a dezvoltat abordări hibride care combină principiile Agile cu planificarea militară tradițională. Gândirea prin design militar (Military Design Thinking – MDT) adaptează principiile gândirii prin design la contextele militare, creând o metodă inovatoare și flexibilă de comandă și control (C2). Această abordare menține structurile militare necesare, încorporând, în același timp, iterația, centrarea pe utilizator și adaptabilitatea din abordările Agile și de gândire prin design (Alaidaros, Omar și Romli 2021).

Aceste abordări hibride oferă o flexibilitate valoroasă prin combinarea structurii cu adaptabilitatea. Ele recunosc realitatea că organizațiile militare nu pot abandona complet structurile ierarhice și procesele formale, dar le pot îmbunătăți cu ajutorul principiilor Agile. Această abordare echilibrată poate reprezenta cea mai practică direcție de urmat pentru organizațiile militare care doresc să devină mai adaptabile, menținând, în același timp, structurile de comandă necesare.

4. Dovezi empirice și studii de caz

4.1. Analiza transnațională a proiectelor IT militare

Studiile empirice ale proiectelor IT militare oferă informații valoroase cu privire la eficacitatea metodologiilor Agile în contexte militare. Un studiu transnațional al proiectelor IT din țările și agențiile NATO a constatat că proiectele care folosesc metode Agile au adus mai multe beneficii clienților decât cele care folosesc metode tradiționale. Proiectele de dimensiuni medii au avut rezultate mai bune decât proiectele mici și mari, iar implicarea clienților a avut un efect pozitiv asupra succesului proiectului. Specificarea clară a obiectivelor a avut, de asemenea, un efect pozitiv semnificativ din punct de vedere statistic asupra rezultatelor proiectului.

Această cercetare contestă ipoteza comună conform căreia abordările tradiționale sunt mai potrivite pentru proiectele militare. Dovezile empirice sugerează că metodele Agile pot oferi rezultate superioare, în special în ceea ce privește beneficiile și satisfacția clienților. Constatarea că proiectele de dimensiuni medii au avut cele mai bune rezultate indică faptul că metodele Agile pot fi mai eficiente atunci când sunt aplicate la o scară adecvată – nici prea mici, pentru a justifica cheltuielile generale, nici prea mari, pentru a fi gestionate eficient (Orlov și alții 2021).

Studiul a evidențiat, de asemenea, importanța implicării clientului – un principiu Agile de bază – în succesul proiectului. Proiectele informatice militare care au beneficiat de participarea activă a utilizatorilor finali au avut mai multe șanse de a aduce beneficii care să răspundă nevoilor operaționale reale. Această constatare susține accentul pus de Agile pe colaborarea dintre dezvoltatori și utilizatori pe tot parcursul ciclului de viață al proiectului.

4.2. Diggerworks: o poveste de succes Agile în domeniul militar

Unul dintre cele mai convingătoare cazuri de implementare Agile de succes într-un context militar este Diggerworks, organizația australiană de apărare responsabilă cu proiectarea, dezvoltarea și integrarea echipamentelor și îmbrăcămintei de luptă pentru soldați. În urma trecerii la Agile, Diggerworks a obținut rezultate remarcabile: productivitatea a crescut cu 400-600%, termenele de livrare a proiectelor au scăzut de la luni la săptămâni în multe cazuri, iar satisfacția angajaților a crescut semnificativ (Cebon și Samson 2012).

Cazul Diggerworks este deosebit de notabil, deoarece implică mai degrabă echipamente fizice decât software, demonstrând aplicabilitatea Agile dincolo de IT. Organizația a fost înființată în 2011, după ce audierile Senatului australian au identificat probleme critice în achizițiile și acordurile privind lanțul de aprovizionare pentru echipamente militare. Prin adoptarea abordărilor Agile, care pun accentul pe inovare și receptivitate, Diggerworks și-a îmbunătățit în mod semnificativ capacitatea de a furniza mai rapid echipamente mai bune.

Acest succes a determinat alte grupuri militare să ia în considerare adoptarea Agile, inclusiv grupurile de cercetare și dezvoltare ale armatei, gestionarea personalului și proiectele majore de achiziții. Chiar și Marina Regală Australiană și Forțele Aeriene și-au exprimat interesul, ceea ce sugerează o recunoaștere din ce în ce mai mare a beneficiilor potențiale ale Agile în toate domeniile militare.

4.3. Transformarea Agile de către Forțele Aeriene ale SUA

Forțele Aeriene ale SUA au adoptat metodologiile Agile pentru a face față provocărilor din domeniul dezvoltării și achiziționării de software. Urmând exemplul unor organizații, precum Defense Innovation Unit (DIU), Forțele Aeriene pun în aplicare o abordare mai modernă și mai puțin birocratică a dezvoltării, care urmărește să ofere capabilități luptătorilor mai rapid și la costuri mai mici (U.S. Air Force 2019).

Un exemplu notabil este inițiativa de dezvoltare software Kessel Run a Forțelor Aeriene, care utilizează metode Agile pentru dezvoltarea și implementarea rapidă a capacităților software. Prin adoptarea practicilor Agile, Kessel Run a redus semnificativ timpii de dezvoltare, permițând un sprijin mai receptiv nevoilor operaționale. Această inițiativă reprezintă o îndepărtare de „abordarea în cascadă", tradițională a Forțelor Aeriene, în ceea ce privește dezvoltarea de software, care urma, de obicei, un proces secvențial, cu cerințe lungi de documentare și revizuire (Budden și alții 2021).

Aceste inițiative ale Forțelor Aeriene demonstrează maniera în care chiar și organizațiile militare mari, tradițional ierarhice, pot adopta cu succes abordări Agile. Prin începerea cu proiecte specifice și prin demonstrarea succesului, aceste inițiative creează un impuls pentru o schimbare organizațională mai amplă, răspunzând, în același timp, nevoilor operaționale imediate.

5. Beneficiile Agile în operațiunile militare

5.1. Îmbunătățirea capacității de reacție la condițiile în schimbare

Unul dintre principalele beneficii ale metodologiilor Agile în contexte militare este capacitatea sporită de reacție la condițiile în schimbare. Procesele tradiționale de planificare militară pot lua mult timp și pot fi dificil de ajustat, odată puse în mișcare. Abordările Agile, care pun accentul pe iterație și adaptare, permit unităților militare să reacționeze mai rapid la schimbarea circumstanțelor, menținând eficiența operațională, în ciuda incertitudinii.

Cercetările privind proiectele militare care utilizează metode Agile au arătat îmbunătățiri semnificative în ceea ce privește durata ciclului și capacitatea de reacție. De exemplu, programul ISPAN a scurtat durata ciclului cu 45 de luni, demonstrând potențialul de economisire a timpului, în urma abordărilor Agile (Kniberg și Skarin 2010). În mod similar, experiența Diggerworks a arătat reduceri importante ale termenelor de livrare a proiectelor, de la luni la săptămâni (Cebon și Samson 2012).

Aceste îmbunătățiri ale capacității de reacție se traduc direct în avantaje operaționale. În situații de luptă, capacitatea de a se adapta rapid la circumstanțele în schimbare poate determina succesul sau eșecul. Prin adoptarea principiilor Agile, organizațiile militare își pot spori capacitatea de a răspunde eficient la mediile operaționale dinamice, păstrând inițiativa și profitând de oportunități, pe măsură ce acestea apar.

5.2. Îmbunătățirea colaborării și a schimbului de informații

Metodologiile Agile pun accentul pe colaborare și comunicare în cadrul și între echipe. În contexte militare, acest lucru poate duce la o coordonare mai eficientă și la schimbul de informații, abordând problema „țevii de sobă", adesea observată în organizațiile militare în care informațiile rămân izolate în unități sau sisteme separate (Tudose 2021, 95-112).

Studiile privind proiectele IT militare au constatat că implicarea clienților, un aspect-cheie al abordărilor Agile, a avut un efect pozitiv asupra succesului proiectului. Prin încurajarea unei colaborări mai strânse între dezvoltatori și utilizatori, metodele Agile garantează că soluțiile răspund nevoilor operaționale reale, mai degrabă decât cerințelor presupuse. Dincolo de proiectele IT, principiile Agile pot îmbunătăți colaborarea în planificarea și execuția operațională. Practici, precum reuniunile zilnice și revizuirile periodice, îmbunătățesc sincronizarea dintre unități și garantează că toate părțile interesate au o înțelegere comună a situației și a planului. Această colaborare îmbunătățită poate reduce fricțiunile, poate spori coordonarea și, în cele din urmă, poate îmbunătăți eficacitatea operațională (Alaidaros, Omar și Romli 2021).

5.3. Creșterea eficienței și eficacității operaționale

Metodologiile Agile pot îmbunătăți eficiența și eficacitatea operațiunilor militare prin concentrarea resurselor asupra sarcinilor prioritare, prin reducerea risipei și promovarea îmbunătățirii continue prin feedback și adaptare regulată. Accentul pus de Kanban pe vizualizarea lucrărilor și pe limitarea lucrărilor în curs ajută unitățile militare să identifice blocajele și să se asigure că resursele sunt alocate sarcinilor esențiale. Experiența Diggerworks, cu o creștere a productivității de 400-600%, demonstrează potențialele câștiguri de eficiență ale abordărilor Agile. Concentrându-se pe furnizarea de valoare incrementală, pe limitarea lucrărilor în curs și pe îmbunătățirea continuă a proceselor pe baza feedbackului, organizațiile militare pot realiza potențial mai mult cu resurse limitate, abordând provocarea perenă de a echilibra strategiile cu resursele disponibile (Agile Manifesto 2001).

Aceste îmbunătățiri ale eficienței sunt deosebit de valoroase în mediile cu resurse limitate. Prin eliminarea risipei, prin concentrarea asupra activităților de mare valoare și prin îmbunătățirea continuă a proceselor, abordările Agile permit organizațiilor militare să maximizeze impactul resurselor disponibile. Această eficiență poate crea avantaje strategice, permițând dezvoltarea și desfășurarea mai rapidă a capacităților.

5.4. Adaptabilitate strategică și învățare

La nivel strategic, metodologiile Agile oferă organizațiilor militare capacități sporite de adaptabilitate și învățare. Natura iterativă a abordărilor Agile creează oportunități regulate de evaluare a progreselor, de colectare a feedbackului și de ajustare a cursului, după caz. Acest lucru permite o învățare și o adaptare mai rapidă decât abordările tradiționale care se bazează pe o analiză postoperațională extinsă. Cercetările privind strategia militară sugerează că adaptabilitatea și învățarea sunt factori esențiali în succesul pe termen lung. Prin adoptarea principiilor Agile, organizațiile militare pot îmbunătăți aceste capacități, obținând avantaje strategice în fața adversarilor mai puțin adaptabili. Capacitatea de a învăța și de a se adapta mai rapid decât adversarii creează oportunități de a prelua și de a menține inițiativa în medii dinamice. Această adaptabilitate strategică sprijină, de asemenea, inovarea în dezvoltarea capacităților militare. Prin crearea unor bucle de feedback mai scurte între utilizatori și dezvoltatori, abordările Agile permit identificarea și implementarea mai rapidă a unor soluții inovatoare la provocările operaționale. Acest ciclu de inovare accelerat poate oferi avantaje semnificative în dezvoltarea și implementarea capacităților (Abercrombie, Fullbright și Long 2016).

6. Provocări și considerații privind punerea în aplicare

6.1. Bariere organizaționale și culturale

În ciuda beneficiilor sale potențiale, implementarea metodologiilor Agile în contexte militare se confruntă cu bariere organizaționale și culturale semnificative. Organizațiile militare au tradiții adânc înrădăcinate și moduri de lucru stabilite care pot fi dificil de schimbat. Natura ierarhică a structurilor militare poate părea să intre în conflict cu accentul pe care Agile îl pune pe echipe autoorganizate și pe luarea deciziilor distribuite. De exemplu, în contexte internaționale, diferențele culturale pot accentua incompatibilitățile dintre echipele Agile autoorganizate și structurile ierarhice rigide (Šmite, Gonzalez-Huerta și Moe 2018).

Cercetările privind adoptarea Agile în contexte guvernamentale și militare au identificat rezistența la schimbare drept un obstacol comun. Factorii culturali, inclusiv aversiunea față de risc și preferința pentru procesele stabilite pot împiedica adoptarea de noi abordări. Depășirea acestei rezistențe necesită un sprijin puternic din partea conducerii, o comunicare clară a beneficiilor și o punere în aplicare treptată și atentă care să respecte structurile de comandă militare necesare.

Accentul tradițional al armatei pe planificarea extensivă și pe documentația formală poate intra, de asemenea, în conflict cu preferința Agile pentru soluții funcționale, în detrimentul documentației complete. Găsirea unui echilibru adecvat care să mențină documentația necesară, eliminând, în același timp, birocrația inutilă reprezintă o provocare semnificativă pentru implementările militare Agile (Alaidaros, Omar și Romli 2021).

6.2. Preocupări legate de securitate și confidențialitate

Operațiunile militare implică informații sensibile și cerințe stricte de securitate care pot intra în potențial conflict cu accentul pus de Agile pe transparență și schimbul de informații. Echilibrarea nevoilor de securitate cu practicile de colaborare reprezintă o provocare semnificativă pentru implementările militare Agile.

Informațiile clasificate și accesul compartimentat creează bariere practice în calea fluxului liber de informații care sprijină colaborarea Agile. Este posibil ca echipele să nu poată împărtăși anumite informații dincolo de granițele organizaționale, limitând astfel eficiența practicilor de colaborare. De exemplu, procesul DIACAP, utilizat pentru evaluarea securității în proiectele DoD, introduce întârzieri semnificative care contravin ritmului rapid al metodologiilor Agile (Chung și Nixon 2013).

Organizațiile militare trebuie să dezvolte abordări modificate care să mențină controalele de securitate necesare, păstrând, în același timp, beneficiile principale ale Agile. În plus, sistemele militare funcționează adesea pe rețele izolate cu acces restricționat, ceea ce complică punerea în aplicare a instrumentelor digitale de colaborare care sprijină practicile Agile. Soluțiile creative care mențin securitatea, permițând, în același timp, colaborarea necesară sunt esențiale pentru implementările Agile militare de succes (Kniberg și Skarin 2010).

6.3. Scalarea Agile pentru operațiuni militare de amploare

Scalarea metodologiilor Agile la operațiuni militare mari și complexe prezintă provocări semnificative. În timp ce abordările Agile funcționează bine pentru echipele mici, aflate în același loc, acestea devin mai dificil de implementat în cadrul organizațiilor mari, distribuite, cu interdependențe multiple – exact mediul în care se desfășoară, de obicei, operațiunile militare. Cercetările privind extinderea Agile în organizații mari au identificat, ca probleme comune, dificultățile de coordonare, de aliniere și barierele de comunicare. Operațiunile militare, care pot implica mii de persoane din mai multe locații, se confruntă cu provocări similare, în ceea ce privește extinderea abordărilor Agile dincolo de unitățile mici sau de proiectele specifice.

Mai multe cadre pentru extinderea Agile au apărut în contexte comerciale, inclusiv SAFe (Scaled Agile Framework), LeSS (Large-Scale Scrum) și Nexus.
De exemplu, Saab a demonstrat succesul scalării Agile prin coordonarea a peste 100 de echipe Agile pentru dezvoltarea avionului Gripen, utilizând stand-upuri zilnice și sprinturi sincronizate. Astfel de exemple subliniază importanța adaptării cadrului Agile la complexitatea proiectelor militare, menținând alinierea între echipe și obiectivele strategice (Rigby, Sutherland și Noble 2018).

Deși aceste cadre oferă soluții potențiale, ele trebuie adaptate contextelor militare pentru a ține seama de structurile ierarhice de comandă și de cerințele operaționale specifice. Dezvoltarea unor abordări specifice militare pentru scalarea Agile reprezintă un domeniu important în cercetarea și inovarea viitoare.

6.4. Strategii de implementare pentru contexte militare

Implementarea cu succes a metodologiilor Agile în contexte militare necesită strategii bine gândite care să recunoască realitățile organizaționale, urmărind, în același timp, o schimbare semnificativă. Cercetările privind schimbarea organizațională sugerează că abordările progresive sunt adesea mai de succes decât transformările radicale, în special în organizațiile consacrate cu culturi puternice.

O abordare eficientă este aceea de a începe cu proiecte-pilot în domenii selectate, în care Agile are cele mai mari șanse de succes. Acestea ar putea include proiecte IT, gestionarea logisticii sau programe de formare, în care beneficiile adaptabilității și feedbackului rapid sunt cele mai evidente. Proiectele-pilot de succes servesc drept exemple și oportunități de învățare pentru o punere în aplicare mai largă, creând un impuls pentru schimbarea organizațională (Daraojimba și alții 2024, 190-218).
De exemplu, inițiative, precum Kessel Run din cadrul Forțelor Aeriene ale SUA, au utilizat metodologii Agile pentru dezvoltarea aplicațiilor critice, obținând economii semnificative de resurse și îmbunătățirea planificării operaționale (Budden și alții 2021).

Abordările hibride care combină elemente ale metodelor tradiționale și Agile oferă o altă strategie promițătoare. De exemplu, menținerea structurii proceselor tradiționale de planificare militară, încorporând, în același timp, practici Agile, precum iterația, feedbackul și adaptarea, poate oferi o punte de legătură între abordări. Aceste modele hibride recunosc realitatea că organizațiile militare nu pot abandona complet structurile ierarhice, dar le pot îmbunătăți cu ajutorul principiilor Agile. Sprijinul și implicarea conducerii sunt esențiale pentru succesul implementării Agile. Liderii nu trebuie doar să sprijine adoptarea Agile, ci și să modeleze comportamentele și mentalitățile care o susțin, inclusiv acceptarea unor niveluri adecvate de incertitudine, încurajarea experimentării și valorizarea învățării din eșec. Programele de educație și formare ar trebui să abordeze atât practicile tehnice Agile, cât și schimbarea de mentalitate care stă la baza acestora către adaptabilitate și îmbunătățire continuă (Tudose 2021).

7. Viitoare direcții și oportunități de cercetare

7.1. Tendințe emergente în adoptarea Agile în domeniul militar

Mai multe tendințe emergente sugerează creșterea interesului și inovației în aplicarea metodologiilor Agile în contexte militare. Acestea includ integrarea Agile cu inteligența artificială și cu sistemele autonome, extinderea dincolo de IT la domeniile operaționale și dezvoltarea de cadre Agile specifice armatei, adaptate cerințelor unice ale operațiunilor militare.

Pe măsură ce organizațiile militare utilizează din ce în ce mai mult inteligența artificială, învățarea automată și sistemele autonome, abordările Agile oferă cadre valoroase pentru gestionarea acestor tehnologii complexe, care evoluează rapid.

Natura iterativă și adaptivă a Agile se aliniază bine cu învățarea și îmbunătățirea continue, inerente acestor tehnologii.
În timp ce multe implementări militare Agile s-au axat pe proiecte IT și de achiziții, există un interes tot mai mare pentru aplicarea principiilor Agile la planificarea și executarea operațională. Concepte, precum comanda și controlul agile (C2), urmăresc să sporească adaptabilitatea în mediile operaționale, menținând, în același timp, structurile de comandă necesare. Aceste aplicații reprezintă domenii promițătoare pentru dezvoltarea și cercetarea în viitor (Orlov și alții 2021).

7.2. Nevoi de cercetare și formare

Există mai multe oportunități de cercetare în domeniul adoptării Agile în domeniul militar. Sunt necesare mai multe studii empirice ale implementărilor Agile militare pentru a înțelege mai bine rezultatele și factorii de succes în aceste contexte specifice. Dezvoltarea și validarea cadrelor Agile specifice mediului militar reprezintă un alt domeniu de cercetare important, la fel ca și investigarea factorilor culturali și organizaționali care influențează adoptarea Agile în mediul militar.

Programele de formare care abordează atât practicile tehnice Agile, cât și schimbarea de mentalitate care stă la baza acestora sunt esențiale pentru succesul implementării. Acestea ar trebui să fie adaptate contextelor militare, recunoscând provocările și cerințele unice ale operațiunilor militare, păstrând, în același timp, principiile Agile de bază. Elaborarea unor abordări eficiente pentru educația Agile în instituțiile militare de formare reprezintă un domeniu important de dezvoltare.

Intersecția metodologiilor Agile cu strategia și doctrina militară oferă oportunități deosebit de bogate pentru cercetare și inovare. Explorarea modului în care principiile Agile pot îmbunătăți concepte militare, precum comanda misiunii, intenția comandantului și bucla OODA, ar putea oferi informații valoroase atât pentru operațiunile militare, cât și pentru gestionarea proiectelor Agile (Schwaber și Sutherland 2020).

7.3. Facilitatori tehnologici pentru Agile militar

Progresele tehnologice pot sprijini și îmbunătăți aplicarea metodologiilor Agile în contexte militare. Instrumentele digitale de colaborare care funcționează în cadrul constrângerilor de securitate pot permite aplicarea practicilor Agile în unități militare dispersate geografic. Sistemele avansate de analiză și de sprijinire a deciziilor pot oferi feedbackul rapid necesar pentru iterația și adaptarea eficientă în medii complexe. Capacitățile de simulare și de modelare pot sprijini experimentarea și învățarea, fără riscurile asociate cu operațiunile din lumea reală.

Adoptarea tot mai frecventă de către armată a cloud computing sprijină, de asemenea, implementarea Agile prin furnizarea de medii mai flexibile și scalabile pentru dezvoltare și implementare. Această trecere la cloud crește agilitatea organizațională prin reducerea dependenței de sisteme învechite cu flexibilitate limitată.

Acești facilitatori tehnologici, combinați cu schimbări organizaționale și formare adecvată, pot ajuta organizațiile militare să depășească unele dintre barierele practice în calea implementării Agile. Prin furnizarea infrastructurii și a instrumentelor care sprijină practicile Agile, tehnologia poate facilita tranziția către abordări mai adaptative ale planificării și execuției (Orlov și alții 2021).

Concluzii

Aplicarea metodologiilor de proiect Agile la planificarea acțiunilor militare reprezintă o abordare promițătoare pentru îmbunătățirea adaptabilității și capacității de reacție în medii operaționale dinamice. Dovezile din proiectele și inițiativele IT militare, precum Diggerworks, demonstrează că metodologiile Agile pot aduce beneficii tangibile în ceea ce privește viteza, calitatea și eficacitatea operațională. Prin adoptarea unor principii, precum colaborarea, iterația și adaptarea, organizațiile militare își pot îmbunătăți capacitatea de a răspunde eficient la complexitatea și incertitudinile operațiunilor contemporane.

Cu toate acestea, punerea în aplicare a metodologiilor Agile în contexte militare prezintă provocări semnificative, inclusiv rezistență organizațională, cerințe de securitate și probleme de scalare. Abordarea acestor provocări necesită strategii de implementare bine gândite, care să echilibreze nevoia de adaptare cu respectarea structurilor și proceselor militare necesare. Abordările hibride care combină elemente ale metodelor tradiționale și Agile oferă căi practice de urmat, recunoscând realitățile organizaționale și urmărind, în același timp, îmbunătățiri semnificative ale adaptabilității.

Pe măsură ce organizațiile militare continuă să exploreze și să adopte abordări Agile, există oportunități pentru continuarea cercetării, inovării și dezvoltării de cadre specifice sectorului militar. Învățând din experiențele dobândite în contexte atât militare, cât și nemilitare, organizațiile pot dezvolta abordări care să valorifice punctele forte ale Agile, abordând, în același timp, cerințele unice ale operațiunilor militare.

Într-o eră a schimbărilor tehnologice rapide și a evoluției amenințărilor, capacitatea de a se adapta rapid și eficient este din ce în ce mai esențială pentru succesul militar. Metodologiile Agile, care pun accentul pe adaptabilitate, colaborare și îmbunătățire continuă, oferă instrumente valoroase pentru îmbunătățirea acestei capacități, putând contribui la operațiuni militare mai eficiente și mai receptive în secolul XXI.

Călătoria către o planificare militară mai agilă este abia la început, dar primele rezultate sugerează că această cale este foarte promițătoare pentru îmbunătățirea eficacității militare în medii complexe și dinamice.

Referințe

Abercrombie, Erick, Patrick Fullbright și Seth Long. 2016. "Analysis of the Marine Corps Supply Management Unit's Internal Operations and Effect on the Warfighter." https://apps.dtic.mil/sti/tr/pdf/AD1030643.pdf.

Agile Manifesto. 2001. "Manifesto for Agile Software Development." https://agilemanifesto.org/.

Alaidaros, Hamzah, Mazni Omar și Rohaida BT Romli. 2021. "The State of the Art of Agile Kanban Method: Challenges and Opportunities." *Independent Journal of Management & Production* 12 (8). doi:10.14807/ijmp.v12i8.1482.

Budden, Phil, Fiona Murray, Isaac Rahamim, Dylan Brown și Nick Setterberg. 2021. "Kessel Run: An Innovation Opportunity for the U.S. Air Force." Mission Innovation Working Paper, Cambridge, MA: Massachusetts Institute of Technology. https://innovation.mit.edu/assets/Kessel-Run.pdf.

Cebon, Peter și Danny Samson. 2012. *Diggerworks: Driving Innovation and Effectiveness in the Defence Sector – A Study of Success Factors.* Melbourne: University of Melbourne.

Chung, Lawrence și Brian Nixon. 2013. *Mission-Oriented Agile Software Development.* Fort Belvoir, VA: Defense Technical Information Center.

Daraojimba, Emmanuel Chibuike, Chinedu Nnamdi Nwasike, Abimbola Oluwatoyin Adegbite și Chinedu Alex Ezeigweneme. 2024. "Comprehensive Review of Agile Methodologies in Project Management." *Computer Science & IT Research Journal* 5 (1): 190-218. doi:10.51594/csitrj.v5i1.717.

Kanban University. 2021. *The Official Kanban Guide.* Seattle, WA: Mauvius Group Inc. https://resources.kanban.university/wp-content/uploads/2021/06/The-Official-Kanban-Guide_A4.pdf.

Kniberg, Henrik și Mattias Skarin. 2010. "Kanban and Scrum: Making the Most of Both." https://www.agileleanhouse.com/lib/lib/People/HenrikKniberg/KanbanAndScrumInfoQVersionFINAL.pdf.

Orlov, Evgeniy Vladimirovich, Tatyana Mikhailovna Rogulenko, Oleg Alexandrovich Smolyakov, Nataliya Vladimirovna Oshovskaya, Tatiana Ivanovna Zvorykina, Victor Grigorevich Rostanets și Elena Petrovna Dyundik. 2021. "Comparative Analysis of the Use of Kanban and Scrum Methodologies in IT Projects." *Universal Journal of Accounting and Finance* 9 (4): 693-700. doi:10.13189/ujaf.2021.090415.

Rigby, Darrell, Jeff Sutherland și Andy Noble. 2018. „Agile at Scale." *Harvard Business Review.* https://hbr.org/2018/05/agile-at-scale.

Schwaber, Ken și Jeff Sutherland. 2020. "The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game." https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf.

Šmite, Darja, Javier Gonzalez-Huerta și Nils Brede Moe. 2018. "When in Rome, Do as the Romans Do: Cultural Barriers to Being Agile in Distributed Teams." https://doi.org/10.1007/978-3-030-49392-9_10.

Supriyadi, Arip, Moeljadi, Adi Kusumaningrum și Susilo. 2023. "The VUCA of Strategic Environment in the Defense Planning of Indonesian Marine Corps." *International Journal of Innovation, Creativity and Change* 17 (2): 40-52.

Toroi, George-Ion și Cristian-Octavian Stanciu. 2023. „Aspecte privind planificarea acțiunilor de inducere în eroare la nivel operativ." *Gândirea Militară Românească* nr. 3: 20-45.

Tudose, Cătălin. 2021. "Agile Methodology and War Strategies." *Journal of Systemics, Cybernetics and Informatics* 19 (8): 95-112. https://doi.org/10.54808/JSCI.19.08.95.

U.S. Air Force. 2019. "The Air Force is becoming more agile – one project at a time." https://www.afmc.af.mil/News/Article-Display/Article/1823609/the-air-force-is-becoming-more-agile-one-project-at-a-time/.

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

Aspecte privind procesul de pregătire a personalului participant la operațiile multinaționale

Aspects Concerning the Training Process of Personnel participating in Multinational Operations

Maior drd. Alice-Claudița MANDEȘ*
*Universitatea Națională de Apărare „Carol I", București
e-mail: mandesclaudita@gmail.com

Abstract

Căile și modalitățile prin care se organizează, se planifică și se execută pregătirea personalului participant la operațiile multinaționale influențează într-o mare măsură atingerea obiectivelor acțiunilor militare la care participă personalul militar român, indiferent dacă operația multinațională se desfășoară sub conducerea Organizației Națiunilor Unite (ONU), Organizației Tratatului Atlanticului de Nord (NATO), Uniunii Europene (UE) sau a Organizației pentru Securitate și Cooperare în Europa (OSCE).
Totodată, calitatea procesului de pregătire, adaptarea obiectivelor etapelor de selecție la specificul misiunii, la gradul de periculozitate a acțiunilor desfășurate și nu în ultimul rând la regiunea de desfășurare a operației multinaționale reprezintă întotdeauna repere sintetice prin care poate fi determinat succesul operației militare.

The ways and means by which the training of personnel participating in multinational operations is organized, planned and executed greatly influence the achievement of the objectives of the military actions in which Romanian military personnel participate, regardless of whether the multinational operation is conducted under the leadership of the United Nations (UN), the North Atlantic Treaty Organization (NATO), the European Union (EU) or the Organization for Security and Cooperation in Europe (OSCE).
At the same time, the quality of the training process, the adaptation of the objectives of the selection stages to the specifics of the mission, to the degree of danger of the actions carried out and, last but not least, to the region of deployment of the multinational operation always represent synthetic benchmarks through which the success of the military operation can be determined.

Cuvinte-cheie:
operații multinaționale; obiectivele misiunii; standarde de calitate; personal militar; planificare acțiuni militare; profesionalism; profesioniști.

Keywords:
multinational operations; mission objectives; quality standards; military personnel; military action planning; professionalism; professionals.

Info articol
Primit: 3 martie 2025; Evaluat: 9 aprilie 2025; Acceptat: 13 mai 2025; Disponibil online: 27 iunie 2025
Citare: Mandeș, A.C. 2025. „Aspecte privind procesul de pregătire a personalului participant la operațiile multinaționalel".
Buletinul Universității Naționale de Apărare „Carol I", 14(2): 110-117. https://doi.org/10.53477/2065-8281-25-16

Acțiunile militare desfășurate în cadru multinațional implică abilităţi care nu sunt în mod necesar o parte comună a pregătirii militare generale sau de specialitate. Multinaţionalitatea scoate în evidenţă nu numai necesitatea de a legitima acţiunile militare ale forţelor multinaţionale (Herciu 2019, 19). Din acest punct de vedere, atât NATO, cât și UE trebuie să fie în măsură să asigure cooperarea deplină nu numai dintre statele membre care participă la operația multinațională, ci și cu alte state contribuitoare cu trupe din afara sferei lor de responsabilitate.

De aceea pregătirea pentru acest gen de acţiuni este una specializată, care se situează, cumva, deasupra pregătirii militare obișnuite. Abilităţile de bază și principiile pentru operațiile multinaționale diferă de la misiune la misiune, ele nefiind similare pentru o misiune de tip Alianță sau una de tip coaliție de forțe, numai cu state membre sau și cu state nonmembre, respectiv una de menținere a păcii sau una de impunere a păcii, spre exemplu.

Alături de procesul de selecție, de modul în care este elaborat și transpus în practică procesul de pregătire a personalului participant la operațiile multinaționale depinde în mare măsură succesul misiunii desfășurate în context internațional, care impune în mod obligatoriu înțelegerea spațiului de angajare a forțelor și complexitatea operației multinaționale (Herciu 2019, 21). Altfel spus, cele două procese au o contribuție însemnată la cuantificarea rezultatelor operației multinaționale.

Cele două procese mai sus menționate, atât cel de selecție, cât mai ales cel de pregătire care are loc după finalizarea celui dintâi, se influențează reciproc, sunt complementare și se valorizează unul pe altul. Un proces de selecție bine gândit, eficient și eficace ne arată atât cum trebuie desfășurată selecția, cât și cum poate fi potențată mai bine. Ulterior, întregul proces de instruire asigură pregătirea militarilor selecționați pentru participarea la operația multinațională, la specificul misiunii, astfel încât aceștia să facă față rigorilor, riscurilor și amenințărilor identificate pentru operația respectivă (Alexandrescu și Băhnăreanu 2007, 39-40).

Organizarea procesului de pregătire

Procesul de pregătire a personalului care participă la operații multinaționale sub comanda organizațiilor internaționale de securitate conține un ansamblu complex de măsuri și activități care se organizează, se planifică și se execută pentru însușirea de către personalul militar a cunoștințelor necesare îndeplinirii misiunilor, pe timpul dislocării în teatrul de operații. De regulă, procesul de pregătire a personalului pentru participarea la operații multinaționale are un caracter intensiv, practic-aplicativ, pluridisciplinar, în scopul îndeplinirii misiunilor de către întregul efectiv de militari la standarde ridicate, în condiții de siguranță, pe cât posibil fără riscuri inutile, cu consumuri reduse de resurse. Corespunzător noii concepții de pregătire a militarilor (Stoica 2015, 38) participanți la operațiile multinaționale, considerăm că se impune planificarea și organizarea instruirii acestora pe baza unui plan perfect adaptat condițiilor de misiune.

Din *perspectivă temporală și a locului de desfășurare*, procesul de pregătire a personalului militar care ia parte la acțiuni militare în teatrele de operații vizează două perioade principale și anume *cea destinată pregătirii* misiunilor multinaţionale, care se execută, cu preponderență, în cadrul unității destinate a executa acțiuni militare de acest gen, prin programe și lecții de pregătire, unde se pune accentul pe cunoașterea procedurilor de operare standard din cadrul misiunii la care structura militară urmează să participe, pe cunoașterea condițiilor specifice din țara de misiune, prin cursuri de perfecționare și specializare, deci o pregătire cu caracter teoretic, precum și prin activități practic-aplicative, exerciții, diverse antrenamente de stat major, cu un profund caracter demonstrativ și metodic.

Materialele prezentate în cadrul pregătirii teoretice pot fi organizate sub formă de lecţii care vor avea atât prezentări, cât și ședințe practice, având în vedere, în permanență, ca informațiile necesare pentru misiune să fie obținute atât prin efortul fiecărui participant (studiu individual), cât și prin verificări cu privire la situații existente și posibile care pot să apară în teatrul de operații, în funcție de zona de dislocare. Rezultatul final trebuie să urmărească obținerea unui volum de cunoștințe care să asigure participanților la misiune îndeplinirea sarcinilor primite, reieșite din fișa postului.

Cea de-a doua vizează perioada petrecută în teatrul de operații, pe timpul executării misiunii multinaţionale, pregătirea personalului având o notă aparte, în sensul că toată această activitate se va desfășura descentralizat, având în vedere distanțele uneori mari care pot separa locațiile de dispunere a personalului din cadrul aceluiași contingent, aceasta desfășurându-se în funcţie de necesitate, de situaţie și de timpul avut la dispoziţie.

Considerăm ca fiind foarte important modul în care se derulează activitatea de instruire, în zona de dispunere, din teatrul de operații. În acest sens, procesul de instruire continuă ar trebui să ia în considerare ca ședințele de pregătire să aibă atât un caracter teoretic, cât și unul practic-aplicativ, cu prezentarea de informații și situații concrete, pentru care alocarea timpului să aibă în vedere aspectele nou apărute și, evident, eliminarea unor comportamente formale, generate de staționarea în teatrul de operații pentru o perioadă mai lungă de timp sau de unele evenimente care influențează modul de manifestare a personalului.

Datorită acestor particularități, este necesar ca, în timpul pregătirii misiunii, să se selecţioneze un număr minim de cadre care vor trebui să participe la un program de pregătire separată care să le asigure cunoștințele necesare conducerii pregătirii specifice atât din punct de vedere teoretic, practic, cât mai ales psihopedagogic.

Pe de altă parte, din perspectiva *modului de organizare și planificare a procesului de instruire*, pregătirea întregului personal care participă la operația multinațională este una de natură specială, ea trebuind să se desfășoare pe două coordonate. Astfel, *prima etapă* reprezintă nivelul de bază al pregătirii (etapa instruirii individuale) la

care trebuie să ajungă întregul personal, iar în cadrul acesteia, toţi militarii, indiferent de misiunea multinaţională la care participă, indiferent de specialităţi şi funcţiile ocupate. În această etapă se urmăreşte asigurarea cunoştinţelor necesare executării misiunilor multinaţionale.

În a *doua etapă* se urmăreşte realizarea unei pregătiri specifice (etapa instruirii colective), în funcţie de tipul de misiune în care unitatea este implicată. Dorim să evidenţiem faptul că toate temele de pregătire, cele destinate atât întregului personal, cât şi personalului care îndeplineşte diverse funcţii vor fi distribuite în mod progresiv în etapa instruirii individuale, dar şi în timpul instruirii colective, urmărindu-se acumularea cunoştinţelor de bază necesare desfăşurării misiunii, precum şi a celor specifice, adaptate condiţiilor zonei geografice de misiune şi teatrului de operaţii.

Elemente specifice procesului de pregătire

Pregătirea personalului selecţionat să participe la operaţii multinaţionale se desfăşoară diferenţiat, pe categorii de personal, în raport cu categoria din care acesta face parte şi luând în considerare funcţiile pe care sunt militarii încadraţi. Astfel, din perspectiva înțelegerii situației și a contextului în care se desfășoară operația multinațională, este avută în vedere o tematică, ce cuprinde, printre altele:

- cunoașterea principiilor și cerințelor doctrinei operațiilor multinaționale întrunite, a modului de organizare și funcționare a organizației de securitate aflate la comanda operației multinaționale și aplicarea acestora în vederea îndeplinirii obiectivelor generale și specifice;
- perfecţionarea cunoştinţelor referitoare la conducerea acţiunilor militare în cadrul multinaţional, cooperarea cu alte structuri prezente în teatrul de operaţiuni;
- manevra de forțe și mijloace a structurilor aflate în teatrul de operații, în raport cu misiunile primite, modalităţi de soluționare a problemelor apărute etc.;
- cunoașterea caracteristicilor tehnico-tactice, construcţiei, funcţionării, întreţinerii și reparării tehnicii din înzestrare, a echipamentelor primite de la diverși parteneri din teatrul de operații, inclusiv a principiilor de folosire eficientă a acestora;
- cunoașterea prevederilor actelor normative naționale și a celor cuprinse în SOP-urile operației multinaționale, referitoare la activitățile cu caracter general și specific;
- măsurile care se impun în timpul pregătirii, afluirii și desfășurării misiunii privind asigurarea acţiunilor și protecţiei personalului și echipamentelor, materialelor proprii, cunoașterea semnalelor de recunoaștere, realizarea sistemului informaţional etc;
- cunoașterea și aplicarea măsurilor specifice și a regulilor de securitate a muncii și supravegherea tehnică a instalațiilor sub presiune și de ridicat, a mijloacelor de măsurare, precum și a măsurilor de prevenire și stingere a incendiilor;

- modul de asigurare a legăturilor, de culegere a informațiilor, de pregătire și prezentare a rapoartelor de informare către țară, respectiv către comandamentul regional etc. (SMG/Ctr. 1 2008, 41-46).

Foarte important este modul în care conducerea structurii care urmează a se deplasa în teatrul de operații înțelege să asigure instruirea personalului raportat la specificul tuturor funcțiilor. Astfel, dacă pentru personalul tehnic, militarii care au în primire și care răspund de starea de operativitate a echipamentelor militare se organizează și desfășoară, de regulă, ședințe practic-aplicative referitoare la modalitățile concrete de executare a lucrărilor de întreținere, respectiv de reparații, cu personalul care răspunde de asigurarea serviciilor de campanie sau a sprijinului medical operațional, vor trebui avute în vedere inroducerea de ședințe de instruire care să evidențieze modul în care se realizează relaționarea cu structurile responsabile de sprijinul logistic din teatrele de oeprații, în timp ce cu militarii care încadrează structurile de manevră (plutoane, grupe etc.), se prezintă și se exersează modalitățile concrete de acțiune, de comunicare, de conlucrare și colaborare pe timpul executării acțiunilor militare cu caracter operațional.

Ședințele de pregătire teoretică și practic-aplicativă se organizează și se desfășoară, de regulă, atât în timpul alocat pregătirii de specialitate, cât și în perioadele destinate pregătirii exercițiilor sau altor activități specifice, în funcție de destinația structurilor din cadrul unității (subunității) care ia parte la operația multinațională.

În sensul celor prezentate, demn de remarcat este faptul că, pentru personalul care intră în compunerea unității (subunității) prin detașare, trebuie avute în vedere organizarea de ședințe de instruire separate pentru înțelegerea rolului, locului și misiunii structurii care urmează a se disloca în teatrul de operații. Din această perspectivă, ședințele pot fi derulate în mod diferențiat, în funcție de pozițiile deținute în statul de organizare de către militarii respectivi.

Tot aici, se cuvine a fi făcută următoarea remarcă. Apar destul de des situații, în care în structura unităților (subunităților) participante la operații multinaționale, sunt introduse noi categorii de tehnică și echipamente, chiar în timpul pregătirii pentru misiune. În acest caz, de regulă, pregătirea celor care vor exploata tehnica și aceste echipamente se execută atât în timpul pregătirii misiunii (în funcție de timpul rămas la dispoziție), cât și ulterior, după intrarea în teatrul de operații. În astfel de situații, se poate lua decizia pregătirii intensive a unora dintre militarii detașamentului, urmând ca experiența acumulată de ei să fie împărtășită ulterior și celorlalți.

Ținând cont de faptul că, în timpul celei de-a doua etape, se are în vedere pregătirea specifică la condițiile teatrului și zonei de misiune (etapa instruirii colective), în acest tip de instruire se poate pune accent nu numai pe antrenarea personalului prin exerciții în teren, dar și pe formarea, specializarea și perfecționarea militarilor în condițiile primirii de categorii noi de tehnică și echipamente, în conformitate cu prevederile reglementărilor elaborate la nivelul Statului Major al Apărării și al categoriilor de forțe, pentru situațiile nou apărute.

Comandanţii şi şefii structurilor care urmează a fi dislocate în zona de operaţii sunt responsabili de modul în care se organizează, se planifică și se execută procesul de pregătire în vederea cunoașterii exploatării noilor echipamente, respectiv pentru actualizarea materialelor utilizate în procesul de instruire.

Nu în ultimul rând, comandanţii și șefii structurilor (unități, subunități) care participă la operaţii multinaționale trebuie să ia în considerare faptul că procesul de instruire a personalului trebuie să asigure nu numai cunoştinţe generale privind natura misiunilor ce urmează a fi executate, dar şi să permită, printr-o abordare modernă, înţelegerea modului concret de executare a acestora. Astfel, întregul personal trebuie să obțină și să dețină, pe perioada executării misiunii, unele deprinderi care să îi permită să se comporte coerent într-o structură de forţe multinațională, care trebuie să acționeze bazându-se pe încrederea populației locale și pe acceptarea de către aceasta a modului său de acțiune (pe baza procedurilor de operare standard).

O mare răspundere revine, în contextul participării la operația multinațională a personalului de stat major și a unor structuri de forțe din România, structurilor specializate din cadrul Statului Major al Apărării și al categoriilor de forțe, respectiv al comandamentelor de sprijin pentru elaborarea de reglementări și instrucțiuni concrete cu privire la modul de instruire a militarilor români pentru astfel de operații multinaționale, la modul în care asigură monitorizarea și verificarea obținerii capacității inițiale, respectiv finale de acțiune. În acest sens, respectivele structuri vor trebui să se asigure că militarii participanți dețin, la finalul procesului de instruire, cunoştinţele necesare pentru îndeplinirea cu succes atât a misiunilor individuale, specifice posturilor ocupate, cât și a celor colective, în funcție de obiectivele forței multinaționale.

Astfel, întregul personal participant la operația multinațională va trebui să fie în măsură să înțeleagă și să aplice standardele organizației internaționale de securitate aflate la comanda operației multinaționale, procedurile existente la nivelul forței multinaționale, dar și pe cele naționale în activitățile care privesc organizarea, finanţarea și administrarea resurselor proprii și a celor puse la dispoziție de NATO, UE, ONU sau OSCE, respectiv modul concret de negociere și de încheiere a contractelor în teatrul de operaţii sau pentru a obține anumite resurse din ţara considerată națiune gazdă pentru forța multinațională (carburanţi, lubrifianți, apă potabilă sau pentru necesități menajere, facilități temporare de cazare și cartiruire, produse situate în clasa I de materiale NATO și UE, forță de muncă, alte servicii de campanie).

Concluzii

Prin cele prezentate, am dorit să facem o trecere în revistă a modului în care se derulează procesul de pregătire a militarilor care participă la operațiile multinaționale, ceea ce ne conduce către ideea conform căreia acest tip de demers are un caracter de generalitate destul de însemnat, adică poate fi foarte ușor aplicabil unor structuri militare (unități, subunități) cu specific și domeniu de activitate diferite.

Având în vedere că procesul de instruire nu face altceva decât vine să finalizeze, practic, procesul de selecție, considerăm că, pentru viitor, cele două procese ar trebui analizate integrat, fără a avea diferențe în ceea ce privește modul de abordare. Pe de altă parte, suntem de părere că organizarea și planificarea unui proces de instruire nu trebuie să scape din vedere modalitățile concrete prin care cunoștințele asimilate trebuie să fie reîmprospătate periodic. Această abordare ar veni în continuarea celor două procese, deja amintite, asigurând o serie de metode noi de instruire, propunând căi concrete de acțiune, precum și instrumente prin care cunoștințele dobândite sunt readuse periodic în atenția militarilor participanți la operația multinațională.

Organizarea, în timpul executării misiunii multinaționale, a unor ședințe de instruire, fără o durată prea mare, cu o anume intensitate, administrată în mod plăcut, poate contribui la readucerea în memoria militarilor a informațiilor și datelor, prezentate în perioada de pregătire în țară.

Din perspectiva lecțiilor identificate și, ulterior, a celor învățate, a reieșit foarte clar faptul că organizarea, planificarea și punerea în aplicare a unui proces de instruire judicios formulat poate veni în ajutorul militarilor participanți la operația multinațională, fiind nu numai o dovadă de profesionalism a organelor de conducere și a celor de execuție de la nivelul structurilor militare implicate, dar și o măsură prin care pot fi evitate o serie de evenimente care să implice atât personal, cât și tehnică și echipamente moderne.

Susținem această idee prin faptul că punerea în aplicare a unui program de instruire corespunzător nu numai că poate contribui la eliminarea sau minimalizarea unor minusuri în activitatea curentă, dar poate conduce la creșterea capacității combative a unităților care iau parte la operații multinaționale, la evitarea celor mai multe dintre scoaterile din funcțiune a tehnicii și echipamentelor proprii, precum și la creșterea mediei timpului de bună funcționare și, implicit, a gradului de folosire a tehnicii introduse în teatrul de operații.

Din perspectiva celor prezentate, devine evident faptul că succesul acțiunilor militare ale structurilor Armatei României participante la operații multinaționale în cadrul NATO și UE depinde în mare măsură atât de capacitatea lor de autosusținere în teatrele de operații, cât mai ales de potențialul de luptă, dobândit în urma finalizării proceselor de selecție și de instruire de către personalul militar care încadrează aceste structuri (Moldovan 2007, 50).

Referințe

Alexandrescu, Grigore și Cristian Băhnăreanu. 2007. *Operații militare expediționare.* București: Editura Universității Naționale de Apărare „Carol I".

Herciu, Alexandru. 2019. „Fizionomia operației întrunite multinaționale." *Buletinul Universității Naționale de Apărare „Carol I"* 6 (3): 14-21.

Moldovan, Dorinel-Ioan. 2007. „Priorităţi ale managementului integrat al resurselor de apărare privind misiunile internaţionale." *Managementul integrat al resurselor de apărare. Necesitate, actualitate, perspective (sesiune de comunicări ştiinţifice).* Braşov: Editura Departamentului Regional de Studii pentru Managementul Resurselor de Apărare.

Parlamentul României. 2011. „Legea 121 din 15 iunie 2011 privind participarea forţelor armate la misiuni şi operaţii în afara teritoriului statului român." *Monitorul Oficial* nr. 427, din 17 iunie 2011.

SMG/Ctr. 1. 2008. *Instrucţiuni privind evaluarea capacităţii unităţilor/detaşamentelor din forţele terestre participante la misiuni în afara teritoriului statului român.* Bucureşti.

Statul Major al Apărării. 2014. *Manualul sprijinului cu personal în operaţii.* Bucureşti.

Stoica, Viorel. 2015. „Rezerva de forţe şi mecanismul completării pierderilor în acţiunile militare." *Buletinul Universității Naționale de Apărare „Carol I"* 2 (3): 34-40.


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS
EXECUTIVE BUREAU OF ARACIS

Președinte
Președinte
Prof. univ. dr. Petrescu Iordan

Vicepreședinte
Vice Președinte
Prof. univ. dr. Ghipulică Cristina

Director Departament de Evaluare Externă a Calității
Director of the Evaluation Department
Conf. univ. dr. Bunoiu Mădălin

Director Departament de Acreditare
Director of the Accreditation Department
Prof. univ. dr. ing. Lache Simona

Secretar General
General Secretary
Prof. univ. dr. Cojocaru Bogdan

Data eliberării/Release date:
31.08.2021

Nr. 182/2021

EDITOR
Editura Universității Naționale de Apărare „Carol I"
(Editură cu prestigiu recunoscut de Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare)
Adresa: Șoseaua Panduri, nr. 68-72, sector 5, București
e-mail: buletinul@unap.ro
Tel. 319.48.80 / 0365; 0453

Bun de tipar: 26.06.2025
Lucrarea conține 118 pagini.

412/26.06.2025

C.159/2025