LOCUL SPAȚIULUI CIBERNETIC ÎN CADRUL PROCESULUI DE PLANIFICARE A OPERAȚIILOR

Locotenent-colonel Nicolae-Sorin MACOVEI

Academia Forțelor Terestre „Nicolae Bălcescu", Sibiu

Asigurarea securității cibernetice a căpătat o importanță din ce în ce mai mare și a culminat cu recunoașterea spațiului cibernetic ca fiind un mediu operațional, alături de sol, apă, aer și spațiu.

Operațiile desfășurate în mediul cibernetic trebuie să fie planificate, integrate și sincronizate cu operațiile derulate în celelalte medii operaționale. Forțele armate desfășoară operații în spațiul cibernetic și activități de sprijin în acest domeniu, ca parte a operației întrunite.

Superioritatea în mediul cibernetic asigură, în războiul modern, un avantaj decisiv comandanților de la toate eșaloanele. Aceasta se obține printr-o combinație umană, tehnologică și procedurală. Militarii sunt obișnuiți să vadă efectul acțiunilor lor în câmpul de luptă, într-un mediu fizic. Operațiile cibernetice se desfășoară însă într-un mediu virtual, iar efectele acestora sunt, uneori, greu de identificat.

Cuvinte-cheie: spațiul cibernetic, proces de planificare, operații cibernetice, nivel tactic, mediul operațional.

INTRODUCERE

Progresul tehnologic este cel care a determinat schimbări majore în fizionomia conflictelor militare și continuă să fie principalul factor de schimbare atât în ceea ce privește spectrul amenințărilor, cât și dezvoltarea unor noi sisteme de armament.

Progresul tehnologic duce aproape întotdeauna la modificări majore în modul de acțiune și concepție, iar legile luptei armate, care fac referire la dependența structurilor organizatorice, formelor și procedeelor, confirmă faptul că progresul tehnologic determină modificări substanțiale în concepțiile de ducere a luptei armate în aproape toate domeniile. Mai mult decât atât, progresul tehnologic a determinat apariția unor noi medii operaționale, iar un exemplu concret este spațiul cibernetic. Astfel că, în acest spațiu lipsit de limite fizice, se impune adoptarea de noi forme și procedee de acțiune în concordanță cu noile capabilități tehnologice și tactice. Aceste capabilități determină transformări și din punct de vedere organizațional, prin crearea unor structuri mai suple, cu mobilitate crescută, precum și apariția unor noi structuri și specialități militare.

Progresul tehnologic, atât pentru componentele sistemelor informatice, cât și pentru dispozitivele hardware utilizate în rețelele de comunicații, a avut o evoluție exponențială în ultimul timp *(Legea lui Moore și viitorul matematicii)*. Acest progres aduce beneficii mari pentru comandanți și stat major, deoarece sunt puse la dispoziție aplicații cu caracter funcțional, situațiile operative sau tactice pot fi vizualizate în timp aproape real, iar schimbul de informații, care se realizează în timp foarte scurt, contribuie la optimizarea actului de decizie. Totuși, odată cu aceste beneficii, sistemele moderne de comunicații și informatică, prin tehnologia utilizată și configurarea acestora, prezintă vulnerabilități, ca orice alt sistem informatic. Cu cât un sistem de comandă și control (C2) este mai informatizat, cu atât el este mai vulnerabil, iar securitatea sistemelor de comunicații și informatică reprezintă o preocupare continuă și majoră pentru personalul de specialitate.

SPAȚIUL CIBERNETIC – DE LA CONCEPT LA MEDIU OPERAȚIONAL

Asigurarea *securității cibernetice* a căpătat, cu timpul, la nivelul NATO, precum și al UE, o importanță din ce în ce mai mare. Summitul din 2002, de la Praga, a fost considerat primul moment în care securitatea cibernetică a Alianței a fost abordată la nivel strategic, în rândul statelor aliate, și a fost subliniată necesitatea protecției

sistemelor informatice utilizate. La Summitul de la Riga, din 2006, nu a întârziat să apară prima strategie a Alianței în domeniul securității cibernetice, strategie concretizată în *„Policy on Cyber Defence".* Odată cu recunoașterea, în cadrul Summitului de la Varșovia, din anul 2016, ca mediu operațional, alături de sol, aer și apă, spațiului cibernetic i s-a acordat importanța cuvenită. Apărarea cibernetică a devenit, astfel, parte a cerințelor de bază ale NATO în apărarea colectivă. Alianța trebuie să fie pregătită să-și apere rețelele și operațiile împotriva amenințărilor și atacurilor cibernetice din ce în ce mai sofisticate și mai numeroase. Începând cu 2016, Alianța a definit domeniul apărarea cibernetică ca fiind unul prioritar.

În anul 2018, la Summitul de la Bruxelles, Alianța a fost de acord cu înființarea unui Comandament pentru Operații Cibernetice ca parte a structurii de comandă întărită a NATO, proiectat să devină total operațional în anul 2023 (Emmott, 2018). În luna februarie 2019, Alianța a avizat un ghid NATO care stabilește un set de instrumente cu scopul de a consolida și mai mult capacitatea NATO de a răspunde la activitățile malițioase în domeniul cyber.

În România, anul 2013 a fost cel în care au apărut *Strategia de securitate cibernetică a României* și *Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*, prin care *„România își propune asigurarea stării de normalitate în spațiul cibernetic, reducând riscurile și valorificând oportunitățile, prin îmbunătățirea cunoștințelor, a capabilităților și a mecanismelor de decizie".* (Hotărârea nr. 271, 2013, p. 11).

În *Strategia de securitate* au fost stabilite patru direcții de acțiune pentru realizarea acestui scop, astfel:

- stabilirea cadrului conceptual, organizatoric şi acţional necesar asigurării securităţii cibernetice;
- dezvoltarea capacităţilor naţionale de management al riscului în domeniul securităţii cibernetice şi de reacţie la incidente cibernetice în baza unui program național;
- promovarea şi consolidarea culturii de securitate în domeniul cibernetic;
- dezvoltarea cooperării internaţionale în domeniul securității cibernetice (Ibid., p. 11).

Armata Statelor Unite ale Americii, precum și celelalte armate din statele membre ale NATO și-au actualizat doctrinele și manualele la noul concept de spațiu cibernetic. Astfel, în iunie 2018, a fost republicată *Doctrina operațiilor întrunite pentru operații cibernetice (Joint Publication 3-12)*, care sprijină planificarea, executarea și evaluarea operațiilor cibernetice.

Tacticile și procedurile pentru coordonarea și integrarea operațiilor din spațiul cibernetic și război electronic pentru sprijinul operațiilor terestre și întrunite au fost publicate în Field Manual (2017) – *Cyberspace and electronic warfare operations*. În acest manual sunt prezentate, pe lângă fundamentele operațiilor cibernetice, termenii și definițiile specifice domeniului, precum și rolul, resursele comandanților și modul de evaluare a operațiunilor.

În *Army Doctrine Publication* (2019), este integrat spațiul cibernetic ca mediu informațional, alături de celelalte componente ale spațiului de luptă (terestru, aerian, maritim, cosmic).

Armata Română s-a aliniat la tendințele NATO. În acest context strategic, la 1 decembrie 2018 a fost înființat Comandamentul Apărării Cibernetice, autoritatea competentă a Ministerului Apărării Naționale în domeniile securității cibernetice, apărării cibernetice și tehnologia informației, iar în august 2020, a fost elaborată *„Doctrina operațiilor în spațiul cibernetic”.*

SPAȚIUL CIBERNETIC ÎN DESFĂȘURAREA OPERAȚIILOR

Mediul de desfășurare a operațiilor se caracterizează prin complexitate și dinamism și poate fi extins în toate mediile operaționale, devenind, astfel, unul multidimensional. Aceste caracteristici sunt rezultatul interacțiunilor, relațiilor, condițiilor, circumstanțelor și influențelor a diferite variabile existente în câmpul de luptă.

Operațiile desfășurate în spațiul cibernetic trebuie să fie planificate, integrate și sincronizate cu operațiile întrunite. Forțele armate desfășoară operații în spațiul cibernetic și activități de sprijin în acest domeniu ca parte a operației întrunite. Superioritatea în spațiul cibernetic asigură, în războiul modern, un avantaj decisiv comandanților de la toate eșaloanele.

Pentru a crea efectele specifice acestui mediu operațional, misiunile desfășurate în spațiul cibernetic necesită angajarea unor variate tipuri de acțiuni. Acestea constau în acțiuni de apărare, acțiuni de atac, acțiuni de culegere de informații, supraveghere și recunoaștere/ISR – Intelligence, Surveillance and Reconnaissance, acțiuni de pregătire operațională a mediului/OPE – Operational Preparation of the Environment și acțiuni de securitate, toate raportate la spațiul cibernetic (Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition, 2020). Pentru a planifica, desfășura și evalua aceste acțiuni, este important să înțelegem diferențele între ele și scopul fiecăreia.

Militarii sunt obișnuiți să vadă efectul acțiunilor lor în câmpul de luptă, într-un mediu fizic. Operațiile în spațiul cibernetic se desfășoară însă într-un mediu virtual,

iar efectele sunt, uneori, greu de identificat de către personalul nespecializat sau, câteodată, sunt identificate prea târziu.

Modalitatea prin care un adversar poate ataca infrastructura hardware și software, având ca efect destabilizarea Sistemului de comandă și control, sunt atacurile cibernetice, care au loc, bineînțeles, în spațiul cibernetic. *Atacul cibernetic* este definit ca o *„acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică”* (Hotărârea nr. 271, p. 7), iar pentru reducerea suprafeței de atac, pot fi duse o serie de operații.

Acțiunile de *apărare cibernetică* sunt acele *„acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale”.* (Ibid., p. 7). Aceste tipuri de acțiuni sunt critice pentru asigurarea funcționării sistemelor de comunicații și informatice și sunt luate, de regulă, de către specialiștii care planifică, organizează și operează sistemele și rețelele de comunicații și informatice.

Acțiunile de culegere de informații, supraveghere și recunoaștere (ISR) sunt desfășurate în spațiul cibernetic cu scopul de a culege informațiile necesare pentru sprijinul desfășurării viitoarelor acțiuni de atac sau de apărare cibernetică. Aceste acțiuni sprijină planificarea și executarea operațiilor curente și viitoare desfășurate în spațiul cibernetic (*figura nr. 1*).

Figura nr. 1: Tipuri de acțiuni în spațiul cibernetic (FM 3-12, p. 1-19)

Acțiunile de pregătire operațională a mediului (OPE) sunt activități desfășurate în scopul planificării și pregătirii unor potențiale operații militare, dar care nu țin de mediul informațional (Ibid.). Acestea includ identificarea datelor și informațiilor, configurațiilor de sistem/rețea sau a structurii fizice care conectează o rețea sau un sistem (aplicațiile utilizate, porturi, asignarea adreselor de rețea sau alți identificatori) în scopul determinării vulnerabilităților sistemului. Tot în această categorie sunt cuprinse și acțiunile întreprinse pentru a asigura accesul și/sau controlul asupra sistemului, rețelei sau datelor în timpul unor potențiale ostilități.

Acțiunile de securitate au drept scop atingerea *„stării de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor salvate sau în tranzit, a resurselor și serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive și reactive pot include politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor”.* (Hotărârea nr. 271, p. 7). Securitatea cibernetică se realizează prin măsuri de ordin tehnic, procedural și uman. Cel care îmbină toate măsurile de securitate este factorul uman. Astfel, pentru a asigura securitatea cibernetică, trebuie ca provocările și amenințările din noul mediu operațional (cibernetic) să fie cunoscute de către toți utilizatorii/operatorii de sisteme informatice. Se simte nevoia formării, dezvoltării și antrenării unei culturi de securitate cibernetică. Majoritatea utilizatorilor de sisteme informatice nu au cunoștințe despre acest fenomen și se identifică nevoia dezvoltării unei culturi de securitate cibernetică în rândul acestora.

Rețelele de calculatoare ale forțelor proprii și ale inamicului, sistemele de comunicații, calculatoare, sistemele de telefonie celulară, site-urile de socializare și infrastructurile tehnice sunt câteva dintre principalele componente ale spațiului cibernetic.

Deși spațiul cibernetic coexistă cu celelalte medii operaționale, acesta este un mediu separat. El pătrunde, prin intermediul rețelelor de comunicații și informatică interconectate prin diferite medii de transmisie, în mediile operaționale terestru, aerian, maritim și cosmic. Libertatea de manevră în spațiul cibernetic permite comanda misiunii și libertatea de manevră în celelalte domenii. Fiecare mediu operațional fizic are propriul său mediu cibernetic, iar luate împreună, acestea formează mediul cibernetic întrunit.

SPAȚIUL CIBERNETIC ÎN PROCESUL DE PLANIFICARE A OPERAȚIILOR

Având în vedere importanța pe care a căpătat-o spațiul cibernetic în desfășurarea operațiilor militare, se cuvine ca, și în procesul de planificare a operațiilor, acesta să joace un rol asemănător. Planificarea operațiilor în spațiul cibernetic este parte integrantă a procesului de planificare a operațiilor, având ca finalitate elaborarea anexei specifice la OPORD/OPLAN.

Comandanții de la toate eșaloanele trebuie să conștientizeze importanța spațiului cibernetic în realizarea obiectivelor și misiunii primite. Un atac cibernetic bine executat de inamic poate avea același efect ca și un foc de artilerie asupra punctului de comandă, respectiv scoaterea acestuia din funcțiune.

Operațiile desfășurate în spațiul cibernetic pot fi extrem de complexe, iar pentru a desfășura un proces de planificare eficient, este recomandat să fie luate în considerare patru niveluri de planificare a acestor operații: tehnic, tactic, operativ și strategic. Deci, comparativ cu procesul de planificare a operațiilor într-un mediu operațional tradițional, unde se desfășoară pe trei niveluri, în cazul planificării operațiilor cibernetice trebuie plecat de la un nivel tehnic. Încorporarea corespunzătoare a aspectelor tehnice are o importanța critică în desfășurarea unei planificări eficiente în spațiul cibernetic (*figura nr. 2*).

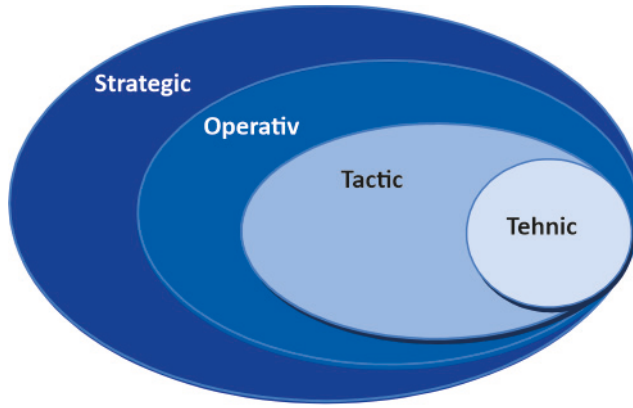

Figura nr. 2: Nivelurile planificării (Barber et. al., 2015, p. 3)

Detaliile tehnice asociate cu operațiile desfășurate în spațiul cibernetic nu sunt înțelese la fel de intuitiv de către comandanți și planificatori, așa cum sunt capabilitățile și limitările tehnicii de luptă (tancuri, nave maritime sau avioane). Natura complexă și dinamică a spațiului cibernetic, precum și caracteristica tehnică

a acestuia duc, de multe ori, analiza și planificarea operațiilor dincolo de acele practici și proceduri de planificare regăsite în doctrina tradițională.

Planificarea operațiilor în spațiul cibernetic se desfășoară concomitent cu procesul de planificare a operației, urmând etapele și fazele acestuia. Produsele rezultate în urma planificării sunt, de regulă, cele prevăzute în *Manualul de planificare a operațiilor*.

Având în vedere că, la nivel tactic, nu există încă structuri specializate pentru operații în spațiul cibernetic[1], sarcinile pentru planificare sunt distribuite personalului din statul major al unității. Membrii statului major responsabili cu planificarea și integrarea operațiilor cibernetice participă la activitățile procesului de luare a deciziei.

Un rol important în procesul de planificare a operațiilor îl are structura de informații. Aceasta este cea care va desfășura activitatea de pregătire informativă a câmpului de luptă, cuprinzând în această analiză și spațiul cibernetic. Este o adevărată provocare pentru structura de informații, deoarece personalul implicat în această activitate trebuie să fie instruit și să cunoască particularitățile spațiului cibernetic. Pentru a îndeplini cât mai eficient această sarcină, este recomandat ca structura de informații să coopereze îndeaproape cu structura planificatoare a rețelelor informatice și de comunicații, respectiv structura de comunicații și informatică.

O analiză complexă oferă persoanelor implicate informațiile relevante pentru a înțelege, vizualiza și descrie mediul operațional, iar decizia luată poate fi pertinentă.

Spațiul cibernetic, ca parte a mediului operațional, trebuie analizat, în primă fază, din perspectiva mediului informațional. Mediul informațional este caracterizat de dimensiunile fizică, informațională și cognitivă.

Astfel, *dimensiunea fizică* a mediului cibernetic este reprezentată de elementele fizice de rețea care includ rețele de comunicații, sisteme informatice și infrastructuri de rețea. Dimensiunea fizică asigură accesul și controlul informațiilor și datelor de către utilizatori, reprezentați de persoane sau grupuri.

Dimensiunea informațională este reprezentată de informații care se pot regăsi într-una din cele două stări: în tranzit sau salvate pe disc. Această dimensiune este direct conectată cu spațiul cibernetic; datorită volumului de informații salvat sau în tranzit, el asigură colectarea, procesarea, păstrarea, diseminarea și afișarea textului, imaginilor sau datelor. Dimensiunea informațională asigură legătura dintre dimensiunea fizică și cea cognitivă.

[1] Notă: Noile ținte de capabilități NATO prevăd înființarea de elemente de reglementare și comandă la nivel strategic și operativ, respectiv structuri de execuție de nivel tactic, dotate și instruite corespunzător, capabile să execute acțiuni specifice în spațiul cibernetic.

Dimensiunea cognitivă cuprinde *„cunoașterea”* celor care transmit, primesc, răspund sau acționează la o informație. Dimensiunea cognitivă în spațiul cibernetic este reprezentată de indivizi, grupuri sau organizații. Spațiul cibernetic conectează datele și ideile celor care transmit, recepționează, răspund, acționează sau adaugă noi informații. (FM 3-12, p. 1-13)

Totodată, spațiul cibernetic este descris ca o însumare a trei straturi: stratul fizic, stratul logic și stratul *„cyber-persona”* (FM 3-12, Ibid.), straturi care permit înțelegerea contextului și crearea de oportunități operaționale.

Prin *stratul fizic* al spațiului cibernetic se înțelege acea componentă geografică ca parte a dimensiunii fizice. Componenta geografică, în situația de față, reprezintă localizarea elementelor de rețea într-unul din mediile operaționale terestru, aerian, maritim sau cosmic. Stratul fizic este alcătuit din componente hardware, aplicații de sistem și infrastructuri (fir, wireless, legături prin cablu, unde electromagnetice, satelit sau optice) care alcătuiesc rețeaua și din conexiunile fizice existente (fire, cabluri, frecvențe radio, switch-uri, servere și calculatoare).

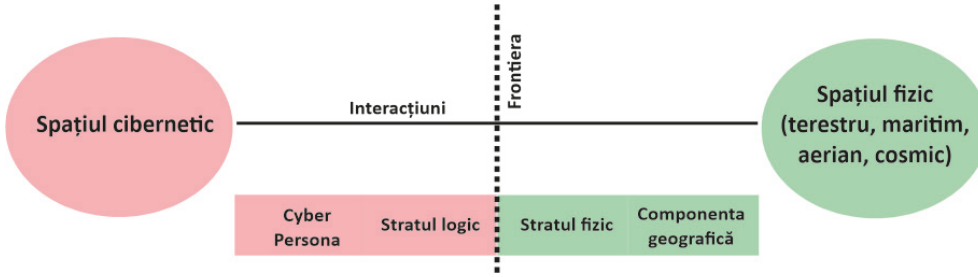

Figura nr. 3: Straturile spațiului cibernetic (Azmi, 2019, p. 25)

Stratul logic constă în interconectarea componentelor din rețeaua fizică într-un mod abstractizat. De exemplu, nodurile de rețea din stratul fizic se pot conecta logic între ele pentru a forma entități în spațiul cibernetic, dar, fizic, ele nu depind de un anumit nod, cale sau individ.

Stratul cyber-persona este o reprezentare digitală a unei identități individuale sau entități în spațiul cibernetic. Acest strat este reprezentat, de fapt, de utilizatorii sau consumatorii de servicii de rețea.

Se poate spune că spațiul cibernetic este reprezentat de rețelele de comunicații și calculatoare interconectate prin stratul logic, care permit ca informația să fie accesibilă din orice punct, utilizând stratul fizic format din conexiuni prin fir sau wireless cu viteze mari de transfer de date, care este accesat de persoane utilizînd stratul cyber-persona.

În analiza informativă a spațiului cibernetic, analiza acestor dimensiuni și straturi oferă o imagine de ansamblu, însă, pentru o imagine completă, trebuie avute în vedere și caracteristicile acestuia.

Pentru identificarea caracteristicilor spațiului cibernetic, trebuie plecat de la o rețea extinsă și complexă, formată din noduri de rețea care se regăsesc în fiecare domeniu operațional, conectate între ele prin diferite medii de transmisie. Așadar, prima caracteristică a spațiului cibernetic este *caracteristica de rețea.* Nucleul acestor rețele sunt infrastructurile tehnologice formate din mai multe enclave distincte, conectate într-o singură rețea logică, permițând transportul de date. Identificarea acestor infrastructuri și a operațiunilor se realizează prin analiza straturilor din spațiul cibernetic, a dimensiunilor mediului informațional, a variabilelor mediului operațional și a celorlalte aspecte tehnice specifice rețelelor de comunicații și informatică cu fir și fără fir. (FM 3-12, p. 1-15)

Deoarece spațiul cibernetic asigură interacțiunea între persoane, grupuri, organizații și state, o altă caracteristică a spațiului cibernetic este *caracteristica socială*. Sistemele informatice și rețelele de calculatoare fac posibilă crearea, stocarea, procesarea, manipularea și transportul rapid al datelor și informațiilor pentru un public restrâns sau unul foarte larg. Mesajele text, e-mail-ul, site-urile de socializare și alte forme interpersonale de comunicare sunt posibile datorită spațiului cibernetic.

Progresul tehnologic crește complexitatea componentelor și dispozitivelor hardware și software ale sistemului de comunicații și informatică, iar cum spațiul cibernetic este dependent de aceste componente, se poate afirma că progresul tehnologic influențează direct spațiul cibernetic. Cu alte cuvinte, o altă caracteristică a spațiului cibernetic este cea *tehnologică*. Mai mult decât atât, este o cerință ca personalul care operează aceste echipamente să fie unul cu abilități tehnice dezvoltate.

Interdependența și interrelaționarea sunt specifice, de asemenea, spațiului cibernetic, deoarece operațiile desfășurate în celelalte patru medii operaționale sunt dependente de spațiul cibernetic. În plus, există interdependență și interrelaționare între spațiul cibernetic și mediul informațional. Distribuirea informațiilor și a datelor, actualitatea și cantitatea acestora sunt dependente direct de capabilitățile și limitările infrastructurii de rețea.

Accesul facil, complexitatea rețelelor și a aplicațiilor, lipsa considerentelor de securitate în design-ul rețelelor și dezvoltarea aplicațiilor, activitatea inadecvată a utilizatorului dau spațiului cibernetic *caracteristica de vulnerabilitate*. Accesul la spațiul cibernetic al unui individ sau grup de indivizi care dețin un dispozitiv de rețea

este ușor, iar un individ având un singur dispozitiv poate fi capabil să dezactiveze o rețea întreagă. Vulnerabilitatea sistemelor care operează în spațiul cibernetic obligă la luarea unor măsuri de reducere a riscurilor și de protecție a spațiului cibernetic. Efectele generate în spațiul cibernetic pot avea un impact global asupra domeniilor fizice.

Înțelegerea vulnerabilităților și a componentelor mediului operațional permite ca decizia să fie pertinentă, legată de context. Aplicarea continuă a acestor cadre analitice le permite comandantului și personalului să analizeze spațiul cibernetic din diferite perspective, de-a lungul procesului operațional.

CONCLUZII

Spațiul cibernetic joacă un rol din ce în ce mai important în ducerea luptei armate. Unele acțiuni din spațiul cibernetic se desfășoară continuu, indiferent de starea de alertă existentă sau de prezența unui conflict. Acțiunile de apărare și de securitate în spațiul cibernetic trebuie să fie o preocupare continuă a structurilor de specialitate și, totodată, trebuie să fie în atenția comandanților de la toate structurile. Noile sisteme de armament, pe lângă faptul că oferă numeroase avantaje operaționale, prezintă, în același timp, vulnerabilități cauzate de interconectarea cu spațiul cibernetic.

Spațiul cibernetic are un rol marcant și în procesul de planificare, iar dacă este întrebuințat corespunzător, prin acțiunile planificate și desfășurate în acest mediu, se pot substitui unele efecte ale altor tipuri de acțiuni militare care implică un consum mare de resurse.

BIBLIOGRAFIE:

1. Azmi, R., Kautsarina, K. (2019). *Revisiting Cyber Definition*. ECCWS 2019 18th European Conference on Cyber Warfare and Security, https://books.google.ro/books/about/ECCWS_2019_18th_European_Conference_on_C.html?id=b8-hDwAAQBAJ&redir_esc=y, accesat la 22 septembrie 2020.
2. Barber E.D., Bobo T.A., Sturm P. K. (2015). *Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains în Military Cyber Affairs*. The Journal of the Military Cyber Professionals Association. Vol. 1, nr. 1, art. 3, https://core.ac.uk/download/pdf/71958458.pdf, accesat la 24 septembrie 2020.
3. Emmott, R. (2018). *NATO cyber command to be fully operational in 2023*, https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9, accesat la 24 septembrie 2020.
4. ADP 2-0, *Intelligence*, 2019.
5. Congressional Research Service (4 iunie 2020). *Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition*, https://crsreports.congress.gov, accesat la 12 septembrie 2020.

6. FM 3-12, *Cyberspace and electronic warfare operations*, aprilie 2017.
7. FM 3-38, *Cyber electromagnetic activities*, februarie 2014.
8. *Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică.* Guvernul României, 23 mai 2013.
9. Joint Publication 3-12, *Cyberspace Operations*, 8 iunie 2018.
10. *Legea lui Moore și viitorul matematicii*, https://rum.journal-headerpop.com/make-mine-double-moores-law-824535, accesat la 14 august 2020.

SURSE WEB:

1. https://www.cybercommand.ro, accesat la 15 septembrie 2020.
2. https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/, accesat la 13 septembrie 2020.
3. https://intelligence.sri.ro/evolutia-amenintarii-cibernetice/, accesat la 26 septembrie 2020.
4. https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9, accesat la 10 septembrie 2020
5. https://rum.journal-headerpop.com/make-mine-double-moores-law-824535, accesat la 21 septembrie 2020.