INTEGRAREA OPERAȚIILOR CIBERNETICE

CYBER OPERATIONS INTEGRATION

CSII dr. Mihai-Ștefan DINU*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania)

Rezumat: *Lucrarea se axează pe identificarea elementelor cheie care pot facilita integrarea operațiilor cibernetice, în special defensive în cadrul operațiilor multi-domeniu. Analiza comparativă a abordărilor unor state aliate NATO (SUA) dar și ale Rusiei și Chinei conduc către identificarea nevoii de reglementare comportamentală a statelor în spațiul cibernetic, reglementare care nu poate fi impusă decât prin implementarea unui cadru legislativ care să ia în calcul dezvoltarea noilor tehnologii și multitudinea aplicațiilor acestora. Din punct de vedere militar sunt identificate elemente de comandă și control care să dezvolte domeniul cibernetic ca parte a operațiilor multi-domeniu prin dezvoltarea unei planificări, coordonări, executări și evaluări integrate astfel încât procesele și practicile specifice spațiului cibernetic să beneficieze de informații coordonate în sprijinul realizării unei reziliențe efective.*

Cuvinte cheie: *operații cibernetice, spațiu cibernetic, juridic, integrare, atribuire.*

Abstract*: The paper focuses on identifying key elements that can facilitate the integration of cyber operations, especially defensive ones within multi-domain operations. The comparative analysis of the approaches of some NATO allied states (USA) but also of Russia and China lead to the identification of the need for behavioral regulation of states in cyberspace, regulation that can only be imposed by implementing a legislative framework that takes into account the development of new technologies and their multitude of applications. From a military point of view, the elements of command and control to develop the cyber domain as part of multi-domain operations have to develop integrated planning, coordination, execution and assessment so that cyberspace-specific processes and practices benefit from coordinated information in support of achieving effective resilience.*

Keywords*: cyber operations, cyber space, legal, integration, attribution.*

1. Introducere

De mai bine de un deceniu problema unei consolidări conceptuale în domeniul cibernetic suscită un interes major, rezultatele dezbaterilor, atât a celor academice cât și ale celor din industrie, fiind în mod continuu în atenția specialiștilor din domeniul militar. Acest interes a sporit odată cu recunoașterea spațiului cibernetic ca mediu operațional militar[1], alături de

* Membru asociat al Academiei Oamenilor de Știință din România, Secția de Științe Militare, CS II în cadrul Departamentului sisteme informaționale și acțiuni cibernetice din Facultatea de Securitate și Apărare a Universității Naționale de Apărare CAROL I, București, email:mihaistdinu@yahoo.co.uk.

[1] Department Of Defense - USA, *Department of Defense Strategy for Operating in Cyberspace*, disponibil la https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf, accesat la 05.11.2023.

cel terestru, naval, aerian și al spațiului cosmic. Această abordare a spațiului cibernetic apare menționată oficial în *Strategia pentru operarea în spațiul cibernetic* a Departamentului Apărării din SUA, care, în prima dintre cele cinci inițiative strategice propuse, afirmă că *Departamentul Apărării va trata spațiul cibernetic ca pe un domeniu operațional pentru a se organiza, instrui și echipa*[2]. Abordarea declarată a spațiului cibernetic, din punct de vedere militar, ca și cel de al cincilea mediu operațional, nu a fost lipsită de contestări care prevesteau o nouă eră, a militarizării spațiului cibernetic și extinderii domeniilor de supraveghere tehnică de tip *big brother, eye in the sky*, cu atât mai mult cu cât agențiile de informații păreau a fi găsit în acest spațiu un teren în care informațiile puteau fi culese mai facil. În plus, timpul a dovedit că limita dintre consolidarea securității naționale și integritatea unor drepturi precum dreptul la viață privată și intimitate, a fost pe cât de fragilă, pe atât de flexibilă. Unele tipuri de comportament ale acestui tip de agenții, sau chiar a unor companii doritoare de extinderea pieţelor comerciale a dus la adoptarea de către state sau organizații internaționale guvernamentale a unor norme legislative care să protejeze dreptul la viață privată și intimitate nu numai în spațiul cibernetic ci și în domeniul comunicațiilor electronice. Reglementarea protecției datelor personale de către Consiliul Uniunii Europene a fost un alt pas înainte care alături de Directiva NIS au adus o consolidare[3] în sensul obținerii unui comportament licit al tuturor actorilor care desfășoară activități în și prin intermediul spațiului cibernetic.

2. Factori ce influențează utilizarea operațiilor cibernetice

Trebuie să fim conștienți că, în ciuda progresului tehnologic major ce a permis dezvoltarea și diversificarea acțiunilor diverșilor actori în spațiul cibernetic, din punct de vedere al actorilor statali, nu fiecare actor statal și-a dezvoltat capabilități de acțiune în spațiul cibernetic, iar printre cei care le-au dezvoltat există diferențe de abordare și punere în practică. Dintre factorii majori care au influențat adoptarea și desfășurarea de operații cibernetice menționăm în succinta noastră analiză:

- Abordarea națională a domeniului cibernetic și a digitalizării;
- Gestionarea amenințărilor și vulnerabilităților de tip cibernetic;
- Postura strategică;
- Integrarea operațiilor cibernetice defensive în operațiile multi-domeniu;
- Aspectele juridice privind desfășurarea operațiilor cibernetice;
- Abordarea privind capacitatea de reziliență cibernetică.

[2] *Ibidem*, p. 5.

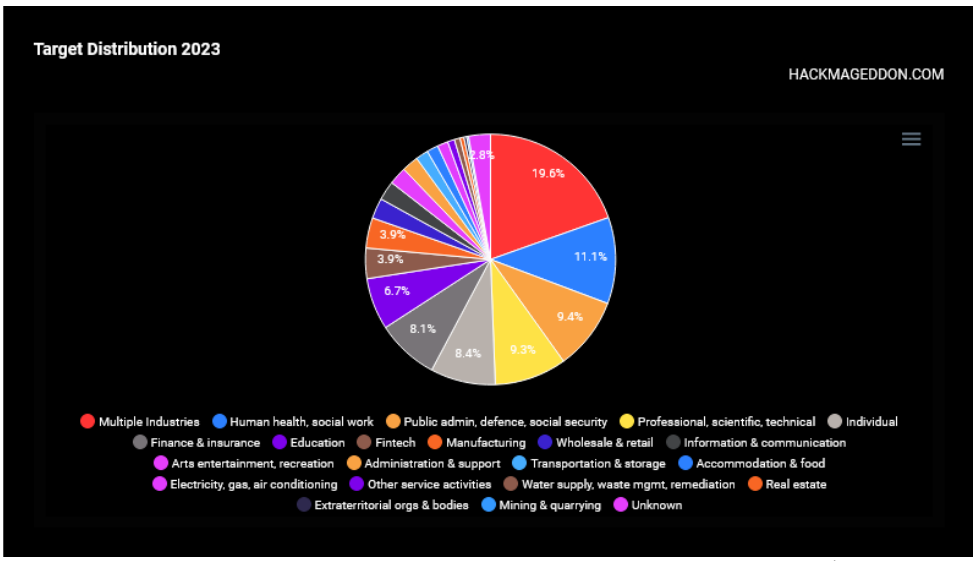
[3] The NIS2 Directive: A high common level of cybersecurity in the EU, disponibilă la https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333, accesat la 14.03.2024.

3. Abordarea domeniului cibernetic și a digitalizării de către actorii statali

Diversificarea acțiunilor în spațiul cibernetic pe fondul tendinței de creștere a nivelului de digitalizare, a condus la schimbarea mediului de securitate, amenințărilor și vulnerabilităților tradiționale adăugându-li-se amenințările și vulnerabilitățile de natură cibernetică. Mai mult, modul în care diverșii actori statali au ales să reacționeze față de acestea au condus la apariția unui context strategic modificat, dezvoltarea capabilităților cibernetice dovedindu-se un avantaj în scopul obținerii superiorității strategice. Astfel, la nivel național din ce în ce mai multe state au realizat și promovat propria strategie de securitate cibernetică, strategii care au permis direcțiile de dezvoltare ulterioare ale acțiunilor diverșilor actori în spațiul cibernetic.

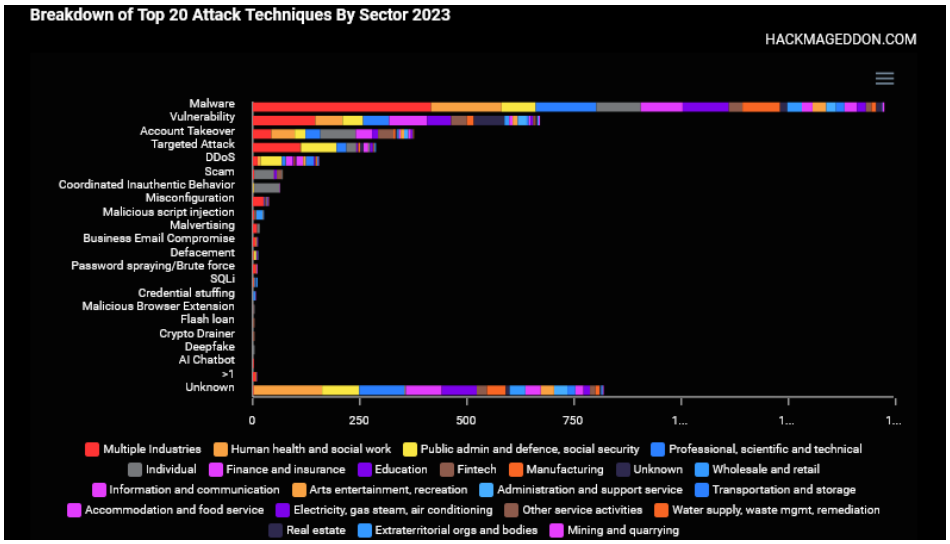
Știrile despre amenințări sau atacuri cibernetice au început să semnaleze frecvent că de la nivelul utilizatorului individual și până la nivel guvernamental vulnerabilitățile cibernetice pot fi exploatate rapid, uneori anonim, iar consecințele pot fi dezastruoase. Dintre țintele predilecte ale atacatorilor (*grafic nr. 1*), menționăm aici:

- Rețelele publice de utilități (alimentare energie electrică, apă, gaze);
- Instituții financiar-bancare;
- Industria (cu precădere aspecte care țin de inovare și cele legate de industria de apărare);
- Campanii electorale/alegeri;
- Sectorul de sănătate.



Grafic nr. 1: Ținte predilecte ale atacurilor cibernetice în 2024[4]

[4] Paolo Passeri, 2024 Cyber Attacks Statistics, disponibil la https://www.-hackmageddon.com/2024/03/26/2024-cyber-attacks-statistics/, acccesat la 05.04.2024.



Grafic nr. 2: Modalităţi de exploatare a vulnerabilităţilor[5]

În ultimele două decenii frecvenţa şi diversitatea atacurilor cibernetice au cunoscut o creştere progresivă, de multe ori obligând statele să gestioneze efecte majore ale unor segmente de infrastructură critică, ceea ce a condus la adoptarea unor măsuri pentru a preveni şi contracara eficient aceste atacuri. Nevoia de adoptarea a unor măsuri eficiente de contracarare a atacurilor cibernetice a rezultat în adoptarea unor politici naţionale desprinse din strategiile naţionale de securitate cibernetică, în special din cauza faptului că domeniul cibernetic evoluează continuu prin noi tehnici şi/sau tehnologii. În acest context de progres tehnologic în creştere, strategiile şi politicile modelează contextul strategic şi de securitate, factorul esenţial fiind acela al nivelului de cultură strategică, acesta influenţând direct atitudinea şi nivelul de folosire a operaţiilor cibernetice.

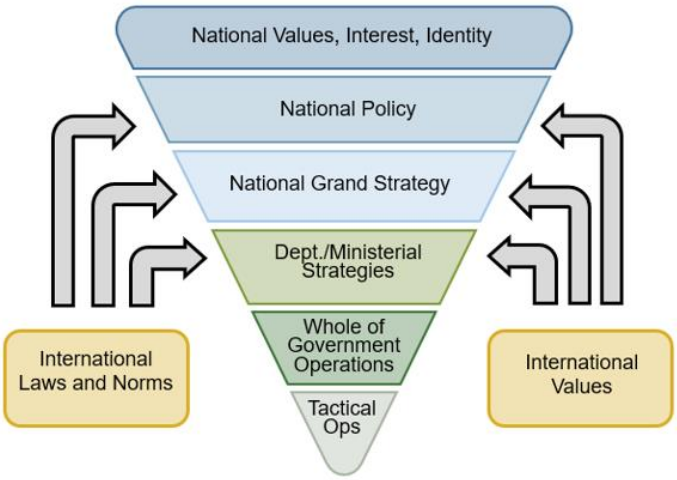
5. Operaţiile cibernetice şi postura strategică

Operaţiile cibernetice pot fi definite general drept acele măsuri adoptate de state, proiectate în scopul apărării, atacului, exploatării sau distrugerii prin intermediul computerelor, reţelelor de computere, instrumente software şi hardware şi a personalului uman instruit în acest scop. Astfel spaţiul cibernetic, care este un domeniu global alcătuit din reţele interconectate şi date stocate sau care circulă în interiorul acestor reţele (internet, reţele telecom, computere etc), devine un spaţiu de luptă, alături de spaţiul cosmic, aerian, maritim şi terestru, permiţând desfăşurarea de operaţii cibernetice separat sau întrunit cu alt tip de operaţii. Tipurile de operaţii cibernetice sunt: defensive, ofensive şi de tip exploit. Atunci când contextul cibernetic permite, operaţiile cibernetice pot deschide calea către acţiuni ale căror efecte pot varia de la accidente până la sabotaje, efecte care dincolo de latura materială pot submina încrederea în asigurarea unei stări

[5] *Ibidem.*

de securitate stabilă de către forțele armate controlate de guvernele diverșilor actori statali.

De aceea este foarte importantă postura strategică a respectivului actor statal deoarece influențează direct translatarea politicilor din strategia națională în politici către implementarea doctrinei naționale, astfel politicile și elementele componente devin un cadru în care resursa umană își asumă roluri în scopul operaționalizării forțelor în spațiul cibernetic (grafic nr. 3).



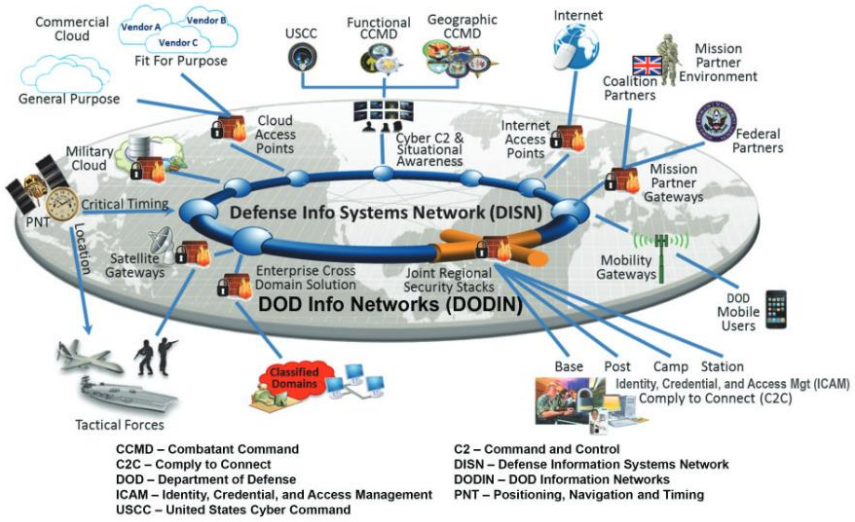
Grafic nr. 3: Translarea de la strategie la operaționalizare[6]

Postura strategică a diverșilor actori statali poate avea implicații de securitate în sensul unui nivel extins al digitalizării și, prin urmare un nivel mai mare de încredere acordat tehnologiei informației în domeniul apărării.

6. Integrarea operațiilor cibernetice defensive în operațiile multi-domeniu

Executarea cu succes a operațiilor cibernetice necesită integrarea și sincronizarea rețelelor informaționale cu misiunile care implică operații cibernetice.

[6] Esie Miller, The Next Frontier – Transforming Enterprise Ops to Multi-Domain Ops, disponibil la https://cdn.ymaws.com/www.alamoafcea.org/resource/resmgr/aace/2018/-doc_miller2018aace.pdf, accesat la 27.04.2024.



Grafic nr. 4: Digitalizarea mediului operațional[7]

Elementele importante ale integrării operațiilor cibernetice sunt constituite de:

- Capabilități cibernetice integrate în planul comandanților și sincronizate cu alte operații militare;
- Sprijinul adecvat oferit de operațiile cibernetice celorlalte tipuri de operații militare, care trebuie să crească proporțional cu extinderea nivelului de digitalizare;
- Implicare activă a specialiștilor în planificare operațională a acțiunilor din spațiul cibernetic în fiecare fază operațională.

Există, însă, o multitudine de cerințe tehnice, organizatorice și doctrinare care trebuie îndeplinite pentru integrarea eficientă a capabilităților cibernetice în cadrul operațiilor multi-domeniu, cum ar fi: realizarea unui mediu combinat de C2 și elemente de inteligență artificială, formațiuni de luptă multi-domeniu integrate cu elemente de comandă de tip cyber și nu în ultimul rând elemente de doctrină pentru conducerea misiunilor ce implică operații cibernetice. Adițional acestor elemente, cadrul integrat operațional trebuie să cuprindă roluri juridice, în domeniul dreptului internațional privind respectarea legii și a drepturilor omului, ca repere de dezvoltare a forțelor, în concordanță cu voința și cultura strategică națională. Astfel, metodologia schemei operaționale va trebui să demonstreze înțelegerea direcțiilor strategice, a mediului strategic, a mediului operațional, toate aceste fiind necesare pentru identificarea cerințelor strategice și operaționale.

[7] Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives, disponibil la https://www.dote.osd.mil/Portals/97/pub/reports/FY2022/-dod/2022dms.pdf?ver=eYBu_u4mMHS6qY5gCsl4CQ%3D%3D, accesat la 20.04.2024.

Concluzii

Din succinta noastră analiză putem avea câteva concluzii:

- spațiul cibernetic permite sprijinirea operațiilor din toate celelalte domenii operaționale precum spațiul cosmic, naval, aerian și terestru;
- elementele cheie în desfășurarea operațiilor cibernetice sunt determinate de strategie și obiectivele misiunii;
- directiva strategică și planificarea strategică în cadrul operațiilor cibernetice sunt influențate de beneficiarii direcți, diversele condiții și influențe ale mediului operațional afectând direct capacitatea de angajare;
- comanda și controlul forțelor ce desfășoară operații cibernetice este modelată de natura acestor operații (multi-domeniu);
- capacitatea de influențare a operațiilor cibernetice a celorlalte domenii operaționale necesită unitate de efort.

BIBLIOGRAFIE

MILLER E., The Next Frontier – Transforming Enterprise Ops to Multi-Domain Ops, disponibil la https://cdn.ymaws.com/www.-alamoafcea.org/resource/resmgr/aace/2018/doc_miller2018aace.pdf;

PASSERI P., 2024 Cyber Attacks Statistics, disponibil la https://www.-hackmageddon.com/2024/03/26/2024-cyber-attacks-statistics/;

Department Of Defense - USA, Department of Defense Strategy for Operating in Cyberspace, disponibil la https://csrc.nist.gov/-csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf;

The NIS2 Directive: A high common level of cybersecurity in the EU, disponibilă la https://www.europarl.europa.eu/thinktank/-en/document/EPRS_BRI(2021)689333;

Digital Modernization Strategy (DMS) - Related Enterprise Information Technology Initiatives, disponibil la https://www.dote.osd.-mil/Portals/97/pub/reports/FY2022/dod/2022dms.pdf?ver=eYBu_u4mMHS6qY5gCsl4CQ%3D%3D.