INFLUENŢA ACŢIUNILOR CIBERNETICE OFENSIVE ASUPRA CONFLICTELOR MILITARE

Căpitan-comandor Vasile-Cristian ONESIMIUC

Doctorand, Universitatea Naţională de Apărare „Carol I", Bucureşti

Dezvoltarea accelerată a infrastructurii digitale afectează în mod direct aproape toate aspectele vieţii, având un important efect asupra Forţelor Armate şi a dezvoltării acestora. Operaţiile cibernetice au fost deja utilizate în conflictele militare şi este evident faptul că, în viitor, rolul operaţiilor cibernetice în activităţile Forţelor Armate va fi din ce în ce mai important. Pentru a fi în măsură să-şi îndeplinească cu succes misiunile încredinţate, Forţele Armate trebuie să se adapteze noului mediu de securitate, în care ameninţările cibernetice vor fi o prezenţă constantă. Adaptarea la noul mediu de securitate reprezintă, aşadar, o provocare continuă pentru Forţele Armate şi va necesita timp şi alte resurse aflate mai mult sau mai puţin la dispoziţie.

Cuvinte-cheie: Forţe Armate, operaţii cibernetice ofensive, securitate, risc, capabilităţi.

INTRODUCERE

Dezvoltarea accelerată la nivel mondial a tehnologiei digitale influenţează în mod direct dezvoltarea forţelor militare, având un impact considerabil şi asupra fizionomiei conflictelor militare. Această dezvoltare a tehnologiei digitale aduce beneficii evidente forţelor militare, eficientizând procesele desfăşurate atât pe timp de pace, cât şi pe timp de criză şi război, dar, în acelaşi timp, are un efect destabilizator prin crearea de noi vulnerabilităţi ce pot fi exploatate de diferiţi actori interesaţi să perturbe buna desfăşurare a activităţilor forţelor militare ale unui stat.

Ritmul din ce în ce mai rapid de desfăşurare a conflictelor conduce la un consum mai mare de resurse, din toate domeniile, direct implicate sau conexe. Integrarea tehnologiei digitale moderne în sprijinul desfăşurării activităţilor curente poate optimiza şi reduce costurile asociate, dar cursa înarmării şi susţinerea acesteia sunt din ce în ce mai costisitoare şi mai greu de suportat de către dezvoltarea economică, având în vedere costurile ridicate ale tehnologiilor militare de vârf.

Ritmul din ce în ce mai rapid de desfăşurare a conflictelor conduce la un consum mai mare de resurse, din toate domeniile, direct implicate sau conexe. Integrarea tehnologiei digitale moderne în sprijinul desfăşurării activităţilor curente poate optimiza şi reduce costurile asociate, dar cursa înarmării şi susţinerea acesteia sunt din ce în ce mai costisitoare şi mai greu de suportat de către dezvoltarea economică, având în vedere costurile ridicate ale tehnologiilor militare de vârf.

FORŢELE ARMATE ŞI NOUL MEDIU DE SECURITATE

Progresul tehnologic, însoţit de schimbările doctrinare impuse de către introducerea noilor tipuri de sisteme de armament, nu diminuează importanţa războiului convenţional. Forţele armate sunt constituite şi înzestrate pentru a putea fi angajate în orice tip de război, dar, în acelaşi timp, se are în vedere şi dezvoltarea unor capabilităţi care să fie în măsură să asigure un răspuns adecvat la tendinţele complexe de evoluţie a mediului de securitate global.

De exemplu, unul dintre sistemele de arme sofisticate utilizate de către SUA în conflictele din Irak şi Afganistan, dronele aeriene, a fost penetrat[1] cu succes de către insurgenţi, folosind un program disponibil pe internet, pentru o sumă modică (26 de dolari).

[1] https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked, accesat la 09.09.2019.

Imaginile video erau transmise necriptat între dronele aparţinând Forţelor Aeriene americane şi staţiile de control de la sol. Programul a permis accesarea imaginilor video de către insurgenţi, putând, potenţial, permite determinarea locaţiilor viitoarelor ţinte şi luarea unor măsuri de evitare a lovirii acestora.

Conducerea militară americană cunoştea lipsa criptării pentru imaginile transmise, dar a apreciat interceptarea datelor ca fiind peste capabilităţile tehnice disponibile ale insurgenţilor. Ca urmare a descoperirii unor cantităţi mari de imagini în posesia insurgenţilor, a fost luată decizia de criptare a datelor transmise de către drone, pentru eliminarea vulnerabilităţii identificate. Deşi oficialii americani au bănuit implicarea Iranului în furnizarea tehnologiei utilizate pentru interceptarea imaginilor, autorul articolului evaluează că problema interceptării imaginilor video putea fi rezolvată în mod foarte simplu, posibil accidental, prin acordarea unui televizor pe frecvenţa emisă de dronă.

Natura acţiunilor cibernetice, modul ascuns în care se acţionează, poate să ofere un avantaj militar semnificativ atacatorului şi, în acelaşi timp, până la descoperirea acestora, prin lipsa acţiunilor vizibile împotriva sistemelor de armament vizate/atacate, să creeze un sentiment de siguranţă forţelor militare evident superioare.

Exemplul de mai sus prezintă unul dintre modurile prin care investiţiile majore în programe avansate de armament ale unui stat puternic sunt contracarate de un adversar mult mai modest din punct de vedere tehnologic. Una dintre lecţiile învăţate este aceea că orice stat poate să fie o potenţială ţintă, iar dezechilibrul major din punct de vedere convenţional al forţele militare angajate în conflicte militare poate să fie semnificativ micşorat prin executarea de acţiuni cibernetice ofensive sau defensive. Natura acţiunilor cibernetice, modul ascuns în care se acţionează, poate să ofere un avantaj militar semnificativ atacatorului şi, în acelaşi timp, până la descoperirea acestora, prin lipsa acţiunilor vizibile împotriva sistemelor de armament vizate/atacate, să creeze un sentiment de siguranţă forţelor militare evident superioare.

Comandamentul cibernetic al SUA (USCYBERCOM) a conştientizat schimbările profunde apărute în domeniul cibernetic de la înfiinţarea structurii, afirmând[2]: *„Superioritatea în domeniile fizice depinde, în mare parte, de superioritatea în spaţiul cibernetic”.*

Modul întrunit de executare a acţiunilor militare convenţionale şi obţinerea superiorităţii asupra adversarului sunt în mod esenţial legate de componenta cibernetică, dar, pentru a atinge această superioritate, a fost identificată necesitatea unei noi abordări, care să fie aliniată cu noua

[2] https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf, p. 1, accesat la 08.09.2019.

Sursa: Command-Vision-for-USCYBERCOM-23-Mar-18

realitate strategică. Unul dintre elementele importante recunoscute în cadrul documentului (vezi imaginea), dar care este valabil şi pentru alte state, putem afirma chiar că este o afirmaţie general valabilă, este aceea că acţiunile cibernetice ofensive se desfăşoară sub nivelul la care ar putea fi considerate ca făcând parte dintr-un conflict militar. Lipsa depăşirii acestui prag, după care acţiunile cibernetice pot fi clasificate ca fiind acţiuni militare, conduce la întârzierea sau chiar lipsa executării unei riposte din partea celui atacat. SUA au conştientizat importanţa deţinerii unor capabilităţi cibernetice puternice, în măsură să oprească atacurile adversarilor înainte ca acestea să producă prejudicii, dar, în acelaşi timp, capabile să determine influenţarea comportamentului adversarului şi inducerea unui sentiment de nesiguranţă în acţiunile întreprinse. Deţinerea unor capabilităţi cibernetice puternice va putea extinde opţiunile militare de răspuns aflate la dispoziţia conducătorilor statului şi a liderilor militari, dar superioritatea cibernetică dorită nu este asigurată implicit, ea fiind contestată în mod constant de alţi actori care posedă capabilităţi cibernetice.

SUA au conştientizat importanţa deţinerii unor capabilităţi cibernetice puternice, în măsură să oprească atacurile adversarilor înainte ca acestea să producă prejudicii, dar, în acelaşi timp, capabile să determine influenţarea comportamentului adversarului şi inducerea unui sentiment de nesiguranţă în acţiunile întreprinse.

În document sunt identificate cinci condiţii esenţiale în sprijinul îndeplinirii obiectivelor urmărite. Condiţia numărul doi[3] identificată – *„Crearea avantajelor în spațiul cibernetic pentru a îmbunătăți operațiile în toate domeniile. Dezvoltarea avantajelor în pregătirea şi în timpul operațiilor întrunite, atât în cazul conflictului, cât şi în cazul acțiunilor sub pragul conflictului armat. Integrarea capabilităților cibernetice şi a forțelor în planuri şi operații în tot spectrul de domenii."* – este o declaraţie clară a intenţiilor urmărite de către SUA de a folosi operaţiile cibernetice în acelaşi mod în care sunt utilizate

[3] *Ibidem*, p. 8, accesat la 08.09.2019.

acestea de către adversari, sub limita definirii acestora ca fiind parte a unui conflict militar, dar integrate de la bun început în cadrul acţiunilor militare.

Aşa-numita militarizare a spaţiului cibernetic[4] este o consecinţă a acţiunilor desfăşurate în spaţiul cibernetic, eforturile SUA de apărare activă a intereselor şi a aliaţilor fiind o consecinţă a acţiunilor agresive ale adversarilor.

NATO a evaluat ameninţarea cibernetică[5] şi a sesizat necesitatea adoptării unor capabilităţi în măsură să apere Alianţa împotriva atacurilor cibernetice; astfel, în anul 2008, a fost adoptată prima politică a NATO de apărare cibernetică. Ulterior, în 2014, apărarea cibernetică a devenit un element al apărării comune, Alianţa declarând că un atac cibernetic poate conduce la invocarea articolului 5 din tratatul NATO, clauza apărării colective.

NATO a evaluat ameninţarea cibernetică şi a sesizat necesitatea adoptării unor capabilităţi în măsură să apere Alianţa împotriva atacurilor cibernetice. Astfel, în anul 2008, a fost adoptată prima politică a NATO de apărare cibernetică. Ulterior, în 2014, apărarea cibernetică a devenit un element al apărării comune, Alianţa declarând că un atac cibernetic poate conduce la invocarea articolului 5 din tratatul NATO, clauza apărării colective.

Evoluţia rapidă a ameninţării cibernetice a determinat, în anul 2016, recunoaşterea spaţiului cibernetic ca domeniu al operaţiilor militare şi, ca măsură firească, a condus la necesitatea întăririi cu prioritate a apărării cibernetice a reţelelor şi infrastructurii naţionale. De asemenea, NATO a adoptat noi politici în domeniul apărării cibernetice (2017), care reafirmă rolul important al apărării cibernetice în cadrul apărării colective, confirmă aplicarea legilor internaţionale în spaţiul cibernetic şi urmăresc dezvoltarea unor capabilităţi, atât la nivelul NATO, cât şi la nivelul statelor membre, scopul principal urmărit fiind protejarea reţelelor deţinute şi utilizate de către NATO.

Declaraţia NATO după Summit-ul din Bruxelles[6] (2018), articolul 20, prezintă cât se poate de clar obiectivul dorit de către Alianţă în spaţiul cibernetic: *„Trebuie să putem opera cu aceeaşi eficacitate în spaţiul cibernetic ca şi în plan aerian, terestru şi maritim, respectiv să consolidăm şi să sprijinim postura de ansamblu a Alianţei”.* Această postură defensivă se realizează prin integrarea capacităţilor cibernetice ale statelor membre ale Alianţei, puse la dispoziţie în mod voluntar. O problemă ridicată doctrinei cibernetice a NATO este cum influenţează capacitatea de descurajare sau de apărare lipsa capabilităţilor ofensive cibernetice puternice[7], o întrebare care se loveşte de reticenţa statelor

[4] *Ibidem*, p. 10, accesat la 08.09.2019.
[5] https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 07.09.2019.
[6] https://www.mae.ro/node/46405, accesat la 07.09.2019.
[7] https://www.atlanticcouncil.org/blogs/natosource/the-role-of-offensive-cyber-operations-in-nato-s-collective-defense, accesat la 08.09.2019.

membre ale Alianţei de a declara capabilităţile cibernetice ofensive deţinute. Recunoscând problema complexă a atribuirii autorului unui atac cibernetic, Alianţa admite că responsabilitatea atribuirii unui atac cibernetic este o prerogativă absolut naţională.

Problema atribuirii atacului cibernetic este cu atât mai mare, cu cât, la momentul de faţă, nu există norme legale sau comportamente unanim aprobate, drept urmare, toţi actorii care acţionează în mediul cibernetic (state, organizaţii etc.) au posibilitatea de a alege dacă să execute un atac sau să creeze un incident cibernetic, să stabilească nivelul de complexitate al acestora sau modul de răspuns în situaţia în care se aplică metode de apărare cibernetică.

Un alt element care complică utilizarea acţiunilor cibernetice ofensive este lipsa unor delimitări clare în ceea ce priveşte pragurile de răspuns între diferite tipuri de atacuri cibernetice, de la cele curente până la ameninţarea persistentă avansată (Advanced Persistent Threat). De asemenea, multitudinea de definiţii utilizate pentru definirea termenilor şi expresiilor din domeniul cibernetic, fără a fi general recunoscute, nu ajută la clarificarea problematicii din domeniu şi conduce la acceptarea aparentă a unor termeni şi expresii utilizaţi frecvent, dar al căror înţeles poate să fie diferit pentru utilizator.

Strategia de securitate cibernetică a României[8] defineşte termenii utilizaţi în domeniul cibernetic, astfel:

Spațiu cibernetic: „mediu virtual, generat de infrastructuri cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta”.

Securitate cibernetică: „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, 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 infrastructurii cibernetice, managementul identității, managementul consecințelor”.

Apărare cibernetică: „acțiuni desfășurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării

Problema atribuirii atacului cibernetic este cu atât mai mare, cu cât, la momentul de faţă, nu există norme legale sau comportamente unanim aprobate, drept urmare, toţi actorii care acţionează în mediul cibernetic (state, organizaţii etc.) au posibilitatea de a alege dacă să execute un atac sau să creeze un incident cibernetic, să stabilească nivelul de complexitate al acestora sau modul de răspuns în situaţia în care se aplică metode de apărare cibernetică.

[8] https://lege5.ro/Gratuit/gm3demzrgq/strategia-de-securitate-cibernetica-a-romaniei-hotarare-271-2013?dp=gy2dsnjugu4ts, secțiunea 3, (1), accesat la 07.09.2019.

agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice specifice apărării naționale".

Atac cibernetic: „acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică".

De exemplu, Manualul Tallinn 2.0[9] definește atacul cibernetic astfel: *„Atacul cibernetic este o operație cibernetică, fie ofensivă, fie defensivă, care are ca rezultat așteptat rănirea, decesul persoanelor sau avarierea ori distrugerea bunurilor materiale".*

Este foarte uşor de observat cât de complexă este problema definirii atacului cibernetic din perspectiva a doar două entităţi diferite care folosesc acelaşi termen. Definirea aceluiaşi termen în diferite moduri are implicaţii ulterioare atât asupra înţelegerii aspectelor la care se referă definiţia, dar mai ales asupra acţiunilor concrete executate în spaţiul cibernetic. Lipsa unor definiţii unanim recunoscute la nivel internaţional ridică probleme în stabilirea unui cadru legal pentru reglementarea operaţiilor din spaţiul cibernetic, similar celui adoptat pentru operaţiile militare convenţionale executate în mediul terestru, naval şi aerian. Cu toate acestea, spre deosebire de acţiunile militare convenţionale, în care executarea unui atac este apanajul forţelor militare ale acelui stat, în spaţiul cibernetic, executarea unui atac cibernetic nu necesită aprobarea executării sau susţinerea acestuia din partea acelui stat.

Atacul cibernetic este o „acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică".

Conflictele militare au evoluat pe măsura evoluţiei sistemelor de arme aflate în dotarea forţelor militare angajate în conflict. Raza de acţiune a sistemelor de armament a permis angajarea adversarului de la momentul când acestea se află în raza vizuală până la limita maximă de bătaie a sistemelor utilizate, de la sute de metri la mii de km distanţă[10]. Această evoluţie a sistemelor de armament a trebuit să fie urmată îndeaproape de schimbarea modului de gândire atât al strategilor militari, cât şi al celor care utilizează armamentul în vederea integrării cât mai complete a noilor sisteme de armament în strategiile şi tacticile militare.

Efectul sistemelor de armament aflate în dotarea forţelor armate (sisteme artileristice, aeronave, sisteme de rachete etc.) are,

[9] Tallinn *Manual 2.0 on the International Law Applicable to Cyber Operations*, ediția a II-a, p. 415.

[10] https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2018/Blythe-Operational-Art/, accesat la 08.09.2019.

printre altele, un element comun, care le diferenţiază de efectul acţiunilor cibernetice ofensive, şi anume, necesită un timp variabil pentru realizarea efectului la ţintă, timp cu atât mai mare, cu cât distanţa faţă de ţintă este mai ridicată. Pe de altă parte, interconectarea la nivel global a tehnologiei digitale conduce la un efect aproape instantaneu, fără a fi influenţat de distanţa faţă de ţintă a acţiunilor cibernetice, dar care, în acelaşi timp, poate avea efecte asupra unor domenii care, la prima vedere, nu sunt în conexiune directă cu ţinta vizată.

Deşi, în mod tradiţional, mediul de securitate, cu ameninţările, riscurile şi vulnerabilităţile asociate, este evaluat şi tratat în principal din punct de vedere militar, mediul actual de securitate trebuie tratat într-un cadru mai larg, care înglobează elemente din diferite domenii, în afara cadrului strict militar.

Strategia Naţională de Apărare a Ţării[11] identifică faptul că *„mediul de securitate va continua să fie influenţat de provocări multiple, unele cu manifestări previzibile şi liniare, reprezentând consecinţe ale unor strategii urmărite de diverşi actori statali şi non-statali pe termen lung, iar altele, dimpotrivă, cu caracter impredictibil, nonliniar şi profund perturbator, care pot genera surprize strategice”.* Este evidentă provocarea uriaşă ridicată de mediul de securitate, aflat într-o continuă dinamică, asupra factorilor de decizie, care trebuie să asigure, prin mijloacele aflate la dispoziţie, dezvoltarea capacităţilor militare şi nu numai, în vederea asigurării securităţii statului şi a locuitorilor acestuia.

Strategia Naţională de Apărare a Ţării identifică faptul că „mediul de securitate va continua să fie influenţat de provocări multiple, unele cu manifestări previzibile şi liniare, reprezentând consecinţe ale unor strategii urmărite de diverşi actori statali şi non-statali pe termen lung, iar altele, dimpotrivă, cu caracter impredictibil, nonliniar şi profund perturbator, care pot genera surprize strategice”.

Statutul de membru al Uniunii Europene şi al NATO necesită construirea şi adaptarea mediului de securitate în vederea alinierii la standardele aflate în vigoare în cadrul acestor organizaţii, dar care să menţină în atenţie evoluţia mediului regional de securitate. Este evident faptul că securitatea naţională nu poate fi asigurată în mod individual, colaborarea în cadrul structurilor de cooperare internaţională din care facem parte poate contribui la menţinerea unui climat de securitate, dar nu trebuie neglijată consolidarea forţelor militare şi civile naţionale la standarde care să permită apărarea împotriva unor acţiuni ostile.

Strategia Naţională de Apărare a Ţării[12] identifică direcţiile de acţiune pentru dezvoltarea capacităţii de răspuns la noile provocări

[11] *Strategia Națională de Apărare a Țării pentru perioada 2015-2019, O Românie puternică în Europa și în lume*, București, 2015, Cap. II, Evaluarea mediului internațional de securitate, aln. 27, p. 11.

[12] *Ibidem*, Cap. IV, Direcții de acțiune și principalele modalități pentru asigurarea securității naționale a României, aln. 72-75, pp.18-19.

ale mediului de securitate, pentru consolidarea capacităţii naţionale de apărare, inclusiv prin utilizarea eficientă a mecanismelor existente în cadrul NATO: dezvoltarea capabilităţilor necesare pentru a reacţiona la ameninţări asimetrice, adaptarea industriei de securitate la cerinţele de înzestrare ale forţelor armate, dar şi asigurarea mecanismelor de prevenire şi contracarare a atacurilor cibernetice la adresa infrastructurilor informaţionale de interes strategic. Direcţiile de acţiune identificate mai sus au un caracter defensiv, reactiv la ameninţările la adresa securităţii naţionale.

Analiza mediului de securitate actual trebuie să conducă la *„realizarea unei armate moderne, flexibile şi eficiente, capabile să execute întreaga gamă de misiuni, de la cele de management al crizelor până la acţiuni de luptă de mare intensitate”*[13].

Analiza mediului de securitate actual trebuie să conducă la „realizarea unei armate moderne, flexibile şi eficiente, capabile să execute întreaga gamă de misiuni, de la cele de management al crizelor până la acţiuni de luptă de mare intensitate”.

Necesitatea deţinerii unor forţe militare credibile, în măsură să apere teritoriul naţional şi să descurajeze acţiunile militare ale unui eventual agresor, este din ce în ce mai stringentă, dar nu în toate situaţiile este suficientă pentru îndeplinirea obiectivelor. Simpla deţinere a unor mijloace de luptă avansate, care, teoretic, ar fi în măsură să descurajeze un eventual agresor, nu este o garanţie a eliminării potenţialelor ameninţări din partea acestuia.

Autorii articolului *Cyber and deterrence*[14] afirmă că: *„În scopul realizării descurajării şi/sau apărării eficiente într-un astfel de conflict sau într-o situaţie conflictuală potenţială, în special împotriva adversarilor avansaţi din punct de vedere cibernetic, este necesar ca autorităţile civile şi militare, furnizorii şi operatorii de reţele să conlucreze atât în perioada premergătoare, cât şi pe timpul conflictului”*.

În opinia mea, devine din ce în ce mai importantă această colaborare dintre forţele militare şi entităţile civile care au atribuţii în asigurarea sprijinului acţiunii forţelor militare proprii, mai ales în ceea ce priveşte adversarii cu capabilităţi avansate de acţiune în mediul cibernetic. Posibilitatea redusă de succes în cazul declanşării unor acţiuni convenţionale împotriva forţelor militare ale unui stat, cel mai probabil, va accentua posibilitatea executării de acţiuni asupra unor domenii conexe, dar care vor putea avea consecinţe directe asupra ducerii acţiunilor de luptă de către forţele militare proprii. Este evident

[13] *Strategia Militară a României*, aprobată prin Hotărârea nr. 708 din 28 septembrie 2016, publicată în *Monitorul Oficial al României*, Partea I, nr. 789 din 7 octombrie 2016.

[14] Franklin D. Kramer, Robert J. Butler şi Catherine Lotrionte, *CYBER AND DETERRENCE*, accesat la 07.09.2019pe link http://www.atlanticcouncil.org/images/publications/Cyber_and_Deterrence_web_0103.pdf, p. 1.

faptul că entităţile civile şi forţele militare trebuie să desfăşoare încă de pe timp de pace acţiuni active pentru asigurarea securităţii sectoarelor cu utilizare dual, civilă şi militară.

Autorii articolului propun[15] un posibil plan de acţiune la nivelul SUA, care cuprinde următorii paşi:

- crearea de planuri de rezervă pentru entităţile implicate (autorităţi militare şi civile), dezvoltate în concordanţă cu procesele de planificare aflate în uz şi exersate pe timpul unor situaţii de urgenţă simulate;
- crearea unor lanţuri de comandă clare, atât în ceea ce priveşte colaborarea civil-militară, cât şi în interiorul autorităţilor militare cu competenţe în domeniu, cu scopul final de a crea un cadru legal pentru executarea de acţiuni cibernetice unificate;
- efectuarea de analize în vederea stabilirii măsurilor de protecţie efectivă, rezilienţă şi refacere a capacităţii operaţionale a obiectivelor atacate;
- dezvoltarea şi clarificarea rolului fiecărui element din cadrul echipelor de răspuns la atacurile cibernetice semnificative;
- asigurarea fondurilor necesare pentru rezilienţă şi refacerea capacităţii operaţionale a infrastructurii critice supuse la atacuri cibernetice;
- utilizarea acţiunilor ofensive pentru perturbarea planificării şi executării acţiunilor cibernetice ale adversarului.

Planul de acţiune propus pentru forţele militare americane poate fi folosit ca model de urmat în cadrul procesului de adaptare al forţelor militare proprii, dar necesită efectuarea unor ajustări. Aceste ajustări sunt necesare din următoarele considerente: dacă, la nivelul obiectivului urmărit, ca urmare a aplicării planurilor de acţiune, nu apar diferenţe, obiectivul fiind asigurarea unui grad cât mai ridicat de protecţie a forţelor proprii, diferenţele de mărime ale forţelor alocate, precum şi posibilităţile financiare disponibile se reflectă în nivelul diferit de adaptare la provocările ridicate de către operaţiile cibernetice.

Unul dintre elementele importante ale procesului de adaptare este identificarea tuturor acelor sectoare din domeniul civil care au potenţialul de a produce efecte disruptive asupra posibilităţilor

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Autorii articolului Cyber and deterrence propun un posibil plan de acţiune la nivelul SUA, care cuprinde următorii paşi: crearea de planuri de rezervă pentru entităţile implicate; crearea unor lanţuri de comandă clare; asigurarea fondurilor necesare pentru rezilienţă şi refacerea capacităţii operaţionale a infrastructurii critice supuse la atacuri cibernetice; utilizarea acţiunilor ofensive pentru perturbarea planificării şi executării acţiunilor cibernetice ale adversarului.

[15] *Ibidem*, p. 2.

de acţiune ale elementelor sistemului militar. Pentru aceasta, este necesară recunoaşterea faptului că operaţiile cibernetice împotriva unor facilităţi civile au fost deja executate în cadrul unor conflicte mai mult sau mai puţin convenţionale şi, cel mai probabil, probabilitatea utilizării operaţiilor cibernetice ofensive asupra unei serii largi de obiective civile în viitor va creşte.

Imposibilitatea identificării cu exactitate a obiectivelor susceptibile a fi atacate va determina realizarea procesului de adaptare având la bază ipoteze eronate, ca urmare, se impune desfăşurarea de măsuri active pentru realizarea unor analize pertinente, care să identifice măsurile de protecţie efectivă, rezilienţă şi refacerea capacităţii operaţionale a obiectivelor atacate.

Similar modului în care sunt pregătite misiunile de bază ale forţelor militare, prin respectarea paşilor de planificare, asigurarea mijloacelor necesare pentru desfăşurarea activităţilor, repetarea secvenţială a misiunii şi, ulterior, repetarea acesteia ca parte a unei operaţii întrunite, este necesară regândirea tuturor acestor elemente prin prisma integrării operaţiilor cibernetice, atât a operaţiilor defensive, cât şi a celor ofensive.

Deşi este un prim pas important, identificarea corectă a obiectivelor care prezintă un risc crescut de atac cibernetic nu garantează identificarea unor masuri de protecţie viabile, care să fie în măsură să asigure rezilienţa şi, ulterior, refacerea capacităţii operaţionale. Similar modului în care sunt pregătite misiunile de bază ale forţelor militare, prin respectarea paşilor de planificare, asigurarea mijloacelor necesare pentru desfăşurarea activităţilor, repetarea secvenţială a misiunii şi, ulterior, repetarea acesteia ca parte a unei operaţii întrunite, este necesară regândirea tuturor acestor elemente prin prisma integrării operaţiilor cibernetice, atât a operaţiilor defensive, cât şi a celor ofensive.

Nu trebuie pierdută din vedere şi natura dual a activităţilor din mediul cibernetic, care au o componentă legitimă şi una desfăşurată cu rea intenţie. Dezvoltarea tehnologică se manifestă şi în cazul tehnologiei, care are efecte disruptive, ca urmare poate furniza celor interesaţi noi oportunităţi. Atacarea unor obiective civile cu utilizare dual va produce acelaşi efect pentru forţele militare ale unor state diferite din punctul de vedere al ordinului de mărime al forţelor, dar potenţialul impact al operaţiilor cibernetice va fi mai mare pentru forţele militare care dispun de mijloace de luptă moderne şi mai numeroase. Potenţiala indisponibilizare a mijloacelor de luptă, chiar şi temporară, poate determina creşterea riscului de neutralizare a acestor mijloace încă din fazele incipiente ale unui conflict militar.

Se conturează, astfel, posibilitatea utilizării operaţiilor cibernetice ofensive pentru a executa acţiunile de lovire a acelor elemente de infrastructură critică, de comunicaţii şi de transport, care, de regulă,

sunt lovite la începutul unui conflict militar, în scopul destabilizării sau chiar al paralizării apărării adversarului. Astfel, acţiunile din mediul cibernetic pot deveni un substitut pentru mijloacele clasice de lovire, iar rezultatele dorite pot fi obţinute cu mult mai puţine riscuri pentru mijloacele clasice de lovire utilizate în realizarea acestor misiuni (cu precădere mijloacele aeriene sunt supuse unui risc ridicat pe timpul executării misiunilor de lovire a unor obiective situate în adâncimea teritoriului adversarului).

Cu toate că, la prima vedere, utilizarea acţiunilor cibernetice ofensive pare a avea mult mai multe avantaje comparativ cu executarea unei misiuni convenţionale de lovire a unui obiectiv, trebuie luate în calcul şi aspectele mult mai puţin evidente ale obiectivelor cu utilizare dublă, precum şi eventualele daune colaterale rezultate în urma executării acţiunilor cibernetice. Unul dintre aceste aspecte este greutatea crescută de identificare a acestor obiective ca fiind ţinte militare legitime, din cauza incertitudinii privind modul de utilizare preponderent, militar sau civil. Dificultatea identificării cu un grad crescut de certitudine a legitimităţii unei ţinte, cu siguranţă, va avea implicaţii şi asupra evaluării efectelor rezultate în urma lovirii acesteia, prioritatea acordată efectele pur militare vizate putând scăpa din atenţie efecte nebănuite în sectorul civil.

În situaţia în care mijloacele de lovire convenţionale sunt angajate pentru executarea unor acţiuni de lovire a unei ţinte, efectele produse asupra acesteia sunt permanente, iar modificările fizice aduse acesteia nu mai pot fi anulate.

În situaţia în care mijloacele de lovire convenţionale sunt angajate pentru executarea unor acţiuni de lovire a unei ţinte, efectele produse asupra acesteia sunt permanente, iar modificările fizice aduse acesteia nu mai pot fi anulate. În cazul acţiunilor cibernetice ofensive, în funcţie de nivelul vizat, se pot lua măsuri pentru calibrarea efectelor urmărite în urma executării atacurilor, pentru neutralizarea temporară a ţintei sau distrugerea acesteia.

În cazul acţiunilor cibernetice ofensive, în funcţie de nivelul vizat, se pot lua măsuri pentru calibrarea efectelor urmărite în urma executării atacurilor, pentru neutralizarea temporară a ţintei sau distrugerea acesteia.

Acţiunile cibernetice ofensive oferă posibilitatea dozării mult mai precise a efectelor asupra ţintei, sub rezerva evaluării pertinente a efectelor lovirii în toate domeniile în care ar putea avea implicaţii directe. Utilizarea, chiar şi limitată, a acţiunilor cibernetice ofensive urmăreşte scoaterea din luptă sau, cel puţin, perturbarea activităţii adversarului, drept urmare, din punctul de vedere al subiectului acţiunii cibernetice ofensive, aceste activităţi sunt catalogate ca fiind ostile.

Acţiunile militare sunt reglementate din punct de vedere legal, lunga istorie a conflictelor militare permiţând dezvoltarea şi aplicarea

unui cadru legal general acceptat. Spre deosebire de cadrul legal aplicabil conflictelor militare, cel pentru spaţiul cibernetic nu este la fel de dezvoltat, acesta fiind în stadii incipiente. Limitările din punct de vedere legal sunt aplicabile doar statelor care decid să respecte aceste limitări, acolo unde există sau dacă sunt impuse în mod voluntar forţelor militare proprii. Limitările voluntare nu se aplică altor actori din mediul cibernetic, care au posibilitatea să execute acţiuni cibernetice ofensive după bunul plac, ca urmare, pentru menţinerea unei capabilităţi de descurajare eficiente, în opinia mea, este necesară adăugarea, în arsenalul forţelor proprii, a unor capabilităţi cibernetice ofensive credibile, care să permită executarea unor riposte suficient de puternice împotriva unui actor cibernetic ostil. Acţiunile cibernetice ofensive vor modela câmpul de luptă în viitor[16], acestea vor putea fi utilizate atât de state, cât şi de alţi actori, pentru a executa acţiuni de lovire cu ajutorul mijloacelor cibernetice.

Efectele mult mai puţin vizibile la nivel internaţional ale acţiunilor cibernetice ofensive, comparate cu efectele rezultate în urma utilizării unei arme nucleare, pot tenta deţinătorii unor instrumente cibernetice ofensive să folosească arsenalul deţinut şi, prin aceasta, riscă să determine reacţia statului atacat, mai ales în condiţiile în care nu sunt definite cu claritate limitele de răspuns la acţiunea ostilă.

Generalul Paul M. Nakasone, comandantul USCYBERCOM, a făcut[17] o paralelă între descurajarea nucleară şi cea cibernetică, subliniind: *„Spre deosebire de domeniul nuclear, unde avantajul strategic sau puterea vin din posesia unei capabilități sau a unui sistem de armament, în spațiul cibernetic utilizarea capabilităților cibernetice este cea care are importanță strategică. Amenințarea cu utilizarea unei capabilități în spațiul cibernetic nu este atât de importantă ca utilizarea acesteia, deoarece aceasta este acțiunea adversarilor asupra noastră”.*

CONCLUZII

Devine evident că simpla deţinere a unor capabilităţi cibernetice puternice nu asigură statului care le deţine un mediu de securitate stabil şi sigur. Efectele mult mai puţin vizibile la nivel internaţional ale acţiunilor cibernetice ofensive, comparate cu efectele rezultate în urma utilizării unei arme nucleare, pot tenta deţinătorii unor instrumente cibernetice ofensive să folosească arsenalul deţinut şi, prin aceasta, riscă să determine reacţia statului atacat, mai ales în condiţiile în care nu sunt definite cu claritate limitele de răspuns la acţiunea ostilă. Utilizarea acţiunilor cibernetice ofensive la nivel de stat, pentru a testa în permanenţă capacităţile militare şi civile ale adversarilor, are o mare probabilitate de realizare încă de pe timp de pace.

[16] https://www.atlanticcouncil.org/blogs/natosource/the-role-of-offensive-cyber-operations-in-nato-s-collective-defense, accesat la 08.09.2019.

[17] https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf, p. 4, accesat la 09.09.2019.

Cu siguranţă, această probabilitate va deveni o certitudine pe timpul viitoarelor conflicte militare. Acţiunile cibernetice ofensive vor fi o constantă în spectrul ameninţărilor care, în viitor, vor afecta mediul de securitate. Dificultatea identificării şi atribuirii atacului, desfăşurarea acţiunilor cibernetice ofensive sub nivelul care să determine un răspuns militar, integrarea acţiunilor cibernetice încă de la începutul desfăşurării acţiunilor militare, neclaritatea legislativă şi inexistenţa unui set de reguli general acceptate, rapiditatea cu care sunt angajate ţintele, imposibilitatea asigurării apărării cibernetice pentru absolut toate obiectivele, posibilitatea calibrării acţiunilor cibernetice ofensive sunt doar câteva dintre elementele care ne arată modul în care conflictele militare vor putea fi influenţate în viitor.

BIBLIOGRAFIE:

1. ***, *Strategia Militară a României*, în *Monitorul Oficial al României*, Partea I, nr. 789 din 7 octombrie 2016.
2. ***, *Strategia Naţională de Apărare a Ţării pentru perioada 2015-2019, O Românie puternică în Europa şi în lume*, Bucureşti, 2015.
3. ***, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd Edition, 2017.

WEBOGRAFIE:

4. https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked;
5. https://assets.documentcloud.org/documents/4419681/Command-Vision-for-USCYBERCOM-23-Mar-18.pdf;
6. https://www.nato.int/cps/en/natohq/topics_78170.htm;
7. https://www.mae.ro/node/46405;
8. https://www.atlanticcouncil.org/blogs/natosource/the-role-of-offensive-cyber-operations-in-nato-s-collective-defense;
9. https://lege5.ro/Gratuit/gm3demzrgq/strategia-de-securitate-cibernetica-a-romaniei-hotarare-271-2013?dp=gy2dsnjugu4ts;
10. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/November-December-2018/Blythe-Operational-Art/;
11. http://www.atlanticcouncil.org/images/publications/Cyber_and_Deterrence_web_0103.pdf;
12. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf.