RĂZBOI ȘI APĂRARE ÎN SPAȚIUL VIRTUAL

WAR AND DEFENSE IN VIRTUAL SPACE

Colonel (ret.) prof. univ. dr. Gheorghe BOARU*

Rezumat: *În societatea informaţională, informaţia - ca armă, ţintă şi materie primă strategică stă la baza tuturor deciziilor.*

Războiul informaţional a devenit o zonă de cercetare şi dezvoltare excepţională, pentru care se acordă o atenţie sporită dar şi resursele necesare pentru cercetare şi implementare, datorită progreselor rapide ale tehnologiei informaţiei din ultimele decenii.

Conflictul din mediul cibernetic sau războiul cibernetic a devenit un fenomen la confluenţa mai multor forme de confruntare dintre aceşti actori, cum ar fi războiul imagistic, războiul psihologic, războiul informaţiilor/contra-informaţiilor, terorismul cibernetic, războiul bazat pe reţea, războiul electronic, criminalitatea informatică etc.

Spaţiul virtual a devenit a cincea dimensiune a confruntării militare, astfel încât în cadrul războiului informaţional putem defini, în funcţie de stările de pace, criză, conflict (război) sau perioada postconflict, anumite faze specifice ale confruntării cibernetice.

Caracteristica comună a confruntărilor din spaţiul cibernetic este raportul antagonic continuu stabilit între ameninţările care se manifestă în spaţiul cibernetic (terorism, spionaj, sabotaj, subversiune şi crimă organizată) şi securitatea informaţională.

NATO a dezvoltat politici şi strategii, a înfiinţat organisme şi instituţii, în domeniul apărării cibernetice. România a acţionat în conformitate cu măsurile europene şi ale NATO elaborând documente similare şi creând structuri naţionale specifice de securitate cibernetică.

Cuvinte-cheie*: războiul informaţional; războiul cibernetic; spaţiul virtual; securitatea cibernetică; terorismul cibernetic; războiul electronic; securitatea informaţională.*

Abstract: *Within the information society, information - as a weapon, target and strategic raw material is the starting point from which all decisions are made.*

Information warfare has therefore become an area of exceptional research and development, generating a lot of interest and attention as well as involving a lot of resources needed for research and implementation, due to the rapid advances in information technology in recent decades.

The conflict in cyberspace or cyber warfare has become a phenomenon at the confluence of several forms of confrontation between these actors, such as imagistic warfare, psychological warfare, information / counter-information warfare, cyber-terrorism, network-based warfare, electronic war, cybercrime, etc.

* Membru corespondent al Academiei Oamenilor de Ştiinţă din România, Membru al Academiei de Ştiințe ale Securității Naționale, e-mail: boarugheorghe@yahoo.com

Cyberspace has become the fifth dimension of the military confrontation so that in the information warfare, we can define, depending on the states of peace, crisis, conflict (war) or the post-conflict period, some specific phases of cyber confrontation.

The common feature in the cyber-space confrontations is the continual antagonistic ratio established between cyber threats (terrorism, espionage, sabotage, subversion and organized crime) and information security.

NATO has developed policies and strategies, set up bodies and institutions in the field of cyber defense. Romania has acted in accordance with European and NATO measures by developing similar documents and creating specific national cyber security structures.

Keywords: *information warfare; cyber war; virtual space; cyber security; cyber terrorism; electronic warfare; information security.*

În ***era informaţională***, războiul nu mai ţine exclusiv de domeniul militar. În cadrul competiţiei informaţionale, care este la fel de veche ca şi conflictul uman, statele, instituţiile şi indivizii încearcă să-şi mărească şi să protejeze propria bază de informaţii, în paralel cu încercarea de a o limita pe cea a adversarului. În societatea informaţională, informaţia - ca armă, ţintă şi materie primă strategică stă la baza tuturor deciziilor.

De altfel, este evident faptul că, în era informaţională, informaţia a devenit parte integrantă a competiţiei umane. Actorul care posedă abilităţi mai bune de culegere, înţelegere, de control şi de utilizare a informaţiei va deţine superioritatea şi, în final, va obţine avantaje substanţiale faţă de ceilalţi competitori.

Acţiunile militare moderne se prezintă ca un proces dinamic cu două componente care se condiţionează reciproc: componenta energetică şi componenta informaţională. Acţiunea componentei energetice are ca obiectiv distrugerea ori neutralizarea unui sistem fizic advers.

Componenta informaţională își propune procurarea, prelucrarea şi transmiterea informaţiilor, în scopul asigurării eficacităţii acţiunii energetice.

Comparativ cu cea distructivă, componenta informaţională se caracterizează printr-un consum mult mai mic de energie. De aceea, se apreciază că informaţia reprezintă o adevărată armă de luptă, a patra armă[42].

În literatura de specialitate, informaţia este abordată atât ca *„o armă puternică, precum şi ca o ţintă preferată”*[43] , sau se afirmă că *„informaţia poate fi cea mai de temut armă în cadrul evoluţiilor tehnologice din spaţiul de luptă...”*[44].

Asigurarea informaţională, în mediul militar, este dependentă strict de tehnologia informaţiei şi a comunicaţiilor, iar componentele de comunicaţii şi informatice moderne

[42] Stan Petrescu, *Informaţiile a patra armă*, Editura Militară, Bucureşti, 1999, p. 18.
[43] *Cornerstones of Information Warfare,* Department of the Air Force, Washington DC, 1995, p. 2.
[44] Peter Grier, *„Information Warfare”,* Air Force Magazine, No. 3, March 1995, p. 23.

au devenit suportul principal al sistemelor militare, în special al sistemelor informaţionale specifice pentru comandă şi control (C4I, C4I2, C4ISR, C4ISTAR etc.).

Revoluţia informaţională a condus la apariţia unui nou tip de război în care nici dimensiunea forţelor şi nici mobilitatea acestora nu pot decide rezultatul. Acest fapt se datorează în primul rând noilor tehnologii, modului de colectare, stocare, procesare, transmitere şi prezentare a informaţiilor, iar în al doilea rând modului în care organizaţiile sunt pregătite să folosească avantajul cantităţii uriaşe de informaţii disponibile în sistemele informatice şi de comunicaţii.

Tehnologia informaţiei şi comunicaţiilor (TIC), în special Internetul, au fost un aspect tot mai important al vieţii sociale politice şi economice, timp de două decenii, la nivel mondial şi sunt coloana vertebrală a societăţii informaţionale globale de astăzi. Evoluţia şi dezvoltarea acestora au adus multe beneficii pentru persoane fizice, precum şi pentru o serie de instituţii şi actori publici şi privaţi, dar, în același timp, ne-au permis să fim martori al impactului pozitiv a reţelelor sociale în revoltele din primăvara arabă din 2011, sau la utilizarea sporită a comerţului electronic în rândurile oamenilor de afaceri şi persoanelor fizice.

Cu toate acestea, TIC a adus, de asemenea, ameninţări grave de atacuri cibernetice, demonstrate în ultimii ani, prin acte de spionaj cibernetic şi criminalitatea informatică în reţelele virtuale, în cadrul ecosistemului în care trăim.

Vulnerabilităţile sistemelor care folosesc TIC depind de mai mulţi factori dintre care consider că numărul şi calitatea utilizatorilor (cultura de securitate) sunt foarte importante. În această idee am analizat câteva date statistice care să-mi permită a trage câteva concluzii, astfel:

- la 31 decembrie 2017 din 7 515 560,214 locuitori ai globului[45] existau 4 156 932,140 utilizatori de Internet[46] ceea ce înseamnă peste 55% din populaţia globului;
- distribuţia utilizatorilor de Internet pe glob arată că toate continentele (zonele geografice), utilizează acest serviciu în procente diferite[47], astfel: Asia:48,7%; Europa: 17,0%; Africa:10,9%; America Latină:10,5%; America de Nord:8,3%; Orientul Mijlociu: 3,9%; Oceania/Argentina: 0,7%.

Cel mai recent raport al Uniunii Internaţionale pentru Telecomunicaţii **(UIT) arată că din peste patru miliarde de oameni care folosesc Internetul în lume, opt din primele zece ţări din topul statelor cu cei mai mulţi utilizatori sunt europene.**

[45] *Statisticile lumii în timp real*, [http://www.worldometers.info/ro/].
[46] *Internet World Stats*, [http://www.internetworldstats.com/stats.htm].
[47] *Idem.*

Potrivit clasamentului realizat de ITU, Danemarca este cea mai *„conectată”* ţară din lume, clasamentul în Top 10 fiind completat de Coreea de Sud, Suedia, Islanda, Marea Britanie, Norvegia, Olanda, Finalnda, Hong Kong şi Luxemburg.

Ca ţară europeană România a cunoscut o evoluţie exponenţială în domeniul TIC după 1989. Acum, în Europa, în topul ţărilor cu cei mai mulţi utilizatori de Internet România este în primele 60. Demn de evidenţiat este mai ales faptul că România ocupă locul 58 în topul Mondial, ce cuprinde 166 de state, fiindcă, deși viteza conexiunilor este printre cele mai bune, suntem „depunctaţi” la rata de penetrare[48],

România se află pe locul şase din 20 de ţări într-un clasament realizat trimestrial de compania americană Akamai Technologies[49] privind viteza de conectare la Internet, reușind să surclaseze SUA şi Marea Britanie în acest domeniu. Clasamentul, elaborat pentru perioada iulie - septembrie 2013, a fost realizat în funcţie de viteza maximă de conectare, în traficul realizat prin reţeaua globală a companiei[50].

Statele Unite ale Americii se afla doar pe locul 13, unul dintre motive fiind suprafaţa mare a ţării, care face dificilă instalarea pe întreg teritoriul a cablurilor din fibră optică.

Romania era devansată în ordine de Hong Kong, Coreea de Sud, Japonia, Singapore şi Israel. Pe poziţia a şaptea se afla Letonia, Akamai Technologies explicând că ţările mici reuşesc mai repede să instaleze tehnoloigia necesară Internetului de mare viteză.

Bulgaria era pe locul 12, cu o viteză de conectare de 37 megabiţi pe secundă, de peste două ori mai mare decât media globală, iar Marea Britanie se afla pe locul 16, cu o viteză de 35,7 megabiţi pe secundă, cu 3,9% mai scăzută faţă de trimestrul precedent, dar cu 27% mai rapidă faţă de acum un an.

Aproape 70% dintre persoanele cu vârste între 16 şi 74 de ani din România, echivalentul a 10,6 milioane de utilizatori, au folosit Internetul, în 2016, în creştere 1,2 puncte procentuale faţă de anul anterior, în timp ce 65% dintre gospodăriile din ţară au avut acces la reţeaua de Internet de acasă, potrivit datelor Institutului Naţional de Statistică (INS)[51].

Explicaţia acestor performanţe românești este că datorită faptului că în România Internetul a fost adoptat mult mai tarziu decât în unele ţări mai dezvoltate economic, aceasta a permis să se sară peste tehnologiile incipiente, care erau mai lente, şi au fost adoptate direct tehnologiile mai performante.

[48] hotnews.ro.
[49] Akamai Technologies este un operator american de reţea de Internet din Cambridge, Massachusetts - SUA, prin intermediul căruia are loc 15%-20% din traficul total de Internet la nivel mondial.
[50] https://www.bloomberg.com/.
[51] http://www.insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2016.pdf.

Numărul utilizatorilor de Internet, dar şi proporţia acestora din cadrul populaţiei totale mondiale, a crescut într-un ritm inimaginabil, ceea ce ne îndreptăţește să afirmăm că suntem în plină eră informaţională.

Securizarea spaţiului virtual a devenit una dintre provocările de securitate cele mai presante ale secolului al XXI-lea, prin importanţa sa pentru viaţa de zi cu zi, pentru guvern, securitate naţională, afaceri şi deopotrivă pentru cetăţeni. Lumea cibernetică şi tehnologiile asociate au creat, pe de o parte, mai multe oportunităţi sociale, culturale, economice şi politice pentru toţi, iar pe de altă parte, natura sa fără frontiere a adus cu ea ameninţări sub formă de atacuri cibernetice şi criminalitate informatică[52].

Conflictul cibernetic este strict determinat de cel informaţional şi cel bazat pe reţea şi reprezintă o formă concretă, particularizată pentru perioadele de criză şi război, a acestuia. Conflictul cibernetic nu trebuie confundat cu acţiunea hackerilor sau cu infectarea aleatoare a unor reţele de calculatoare cu viruși informatici. El se compune dintr-un sistem de acţiuni care vizează îndeosebi perturbarea sau *„orbirea“,* prin toate mijloacele, a reţelelor informaţionale adverse, protecţia celor proprii, dezinformarea adversarului şi intoxicarea informaţională a acestuia.

Dacă admitem că spaţiul cibernetic este un spaţiu în care poate avea loc o confruntare complexă, cu importanţi actori statali sau non-statali, ca în cazul terorismului internaţional sau criminalităţii transfrontaliere, atunci conflictul din mediul cibernetic, sau ***războiul cibernetic*** este un fenomen aflat la confluenţa mai multor forme ale confruntării dintre acești actori, astfel: război imagologic (mediatic); războiul psihologic; războiul informaţiilor/contrainformaţiilor; terorism cibernetic; război bazat pe reţea; război de comandă şi control; război electronic; criminalitate informatică etc.

Studiul mijloacelor şi metodelor de atac informatic, precum şi identificarea scopurilor acestor acţiuni ofensive ne permite analiza şi caracterizarea ameninţărilor din spaţiul cibernetic, pornind de la domeniile ameninţărilor clasice TESSO[53] proiectate în spaţiul cibernetic.

Odată cu apariţia războiului cibernetic, ca răspuns imediat la agresiunile informatice, specialiștii au căutat să definească noi soluţii de apărare cibernetică (*cyber defence*), care s-au concretizat într-un set complex de acţiuni ofensive şi defensive. În cadrul acestuia, cel mai bine s-au dezvoltat şi implementat atât la nivelul societăţii civile, cât şi în domeniul militar, acţiunile defensive pentru răspuns la incidentele de securitate IT, desfăşurate de structuri specializate cunoscute sub denumirea de *Computer Emergency Response Team (**CERT**).*

---

[52] Colonel (r.) prof. univ. dr. Gheorghe Boaru, *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Ştiinţe ale Securităţii Naţionale nr. 2/2017, p. 65.

[53] *TESSO - T*errorism, *E*spionage, *S*abotage, *S*ubversion, *O*rganized Crime.

La nivel european există agenţii cheie ale UE, inclusiv Agenţia Europeană de Apărare (***EDA*** - *European Defence Agency*), care funcţionează pentru dezvoltarea apărării cibernetice a UE.

Mai mult decât atât, este esenţial pentru UE, de a atinge obiectivele pe care le-a stabilit în Agenda digitală pentru Europa (2010), şi la fel de semnificativă, forţa motrice a unei astfel de agende - *Strategia Europa 2020*.

Strategia de securitate Cibernetică pentru Uniunea Europeană (*EUCSS*) recunoaște că *„este în principal sarcina a statelor membre de a face față provocărilor de securitate în spaţiul virtual"*[54], dar de asemenea şi că UE trebuie să joace un rol-cheie ca actor în sine în acest „joc".

În același spirit de abordare (*EUCSS*) precizează că *„Securitatea cibernetică poate fi solidă şi eficientă doar dacă se bazează pe drepturile şi libertăţile fundamentale așa cum sunt consacrate în Carta Drepturilor Fundamentale a Uniunii Europene "*[55].

În acest scop, este clar că UE poate fi un mediator care să ofere o platformă sau chiar o punte de legătură între diferitele domenii de securitate cibernetică, să creeze condiţiile necesare pentru implementarea eficientă a unei culturi a securităţii cibernetice în cadrul statelor membre.

La nivel naţional, în deplin acord cu acţiunile europene, a fost aprobată în februarie 2015 *Strategia Naţională privind Agenda Digitală pentru România 2020*[56], care definește patru domenii de acţiune dintre care amintesc doar primul domeniu, care este: e-Guvernare, Interoperabilitate, *Securitate Cibernetică*, Cloud Computing şi Social Media.

Acest document a preluat şi adaptat la specificul ţării noastre elementele Agendei Digitale pentru Europa. Agenda Digitală definește astfel rolul major pe care utilizarea TIC trebuie să-l joace în realizarea obiectivelor Europa 2020.

În România cadrul general de cooperare care reuneşte acele autorităţi şi instituţii publice cu responsabilităţi şi competenţe în domeniul securităţii cibernetice este reprezentat de Sistemul Naţional de Securitate Cibernetică (*SNSC*). Activitatea SNSC este coordonată la nivel strategic de Consiliul Suprem de Apărare a Ţării.

Coordonarea unitară a elementelor SNSC este asigurată de Consiliul Operativ de Securitate Cibernetică (*COSC*). În funcţie de competenţele specifice, în

[54] *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, p. 4, [http://eeas.europa.eu/ archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf], accesat la data 10.03.2018.

[55] *Cybersecurity Strategy of the European Union, op. cit.*

[56] *Strategia Națională privind Agenda Digitală pentru România 2020* a fost aprobată prin Hotărârea de Guvern nr. 245/7 aprilie 2015.

domeniul securităţii şi apărării naţionale, fiecare dintre instituţiile care au reprezentare în COSC cooperează cu organismele internaţionale ale UE, NATO, OSCE etc.

Guvernul României, prin Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - *CERT-RO*[57] – asigură, potrivit ariei sale de competenţă, elaborarea şi promulgarea politicilor publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice naţionale.

Ca element de specific naţional, în accepţiunea Strategiei de securitate cibernetică a României, *apărarea cibernetică* este definită ca fiind: *„acţiuni desfăşurate în spaţiul cibernetic în scopul oportun împotriva ameninţărilor asupra infrastructurilor cibernetice specifice apărării naţionale”*[58].

Este de evidenţiat faptul că, în acest domeniu al securităţii cibernetice, abordările românești sunt în deplin accord cu cele europene dar şi cu cerinţele NATO.

În formularea *strategiilor de apărare cibernetică* se au în vedere următoarele aspecte:

- multidisciplinaritatea domeniului INFOSEC: abordează aspecte privind securitatea personalului, fizică şi a documentelor, securitatea IT şi cea industrială;
- capacitatea de reacţie să fie aptă să răspundă la cele mai diverse şi imprevizibile forme de agresiune cibernetică;
- apărarea cibernetică reprezintă şi o formă complementară de cooperare între persoane, organizaţii, alianţe şi state pentru combaterea *criminalităţii cibernetice*.

Apărarea împotriva atacurilor cibernetice este deosebit de complexă şi presupune mult mai mult decât folosirea unor proceduri simple sau unui sistem de protecţie singular. Ca răspuns imediat la agresiunile informatice, specialiştii au căutat să definească noi soluţii de apărare cibernetică, care s-au concretizat într-un set complex de acţiuni ofensive şi defensive.

Dacă acţiunile ofensive ţin mai mult de domeniul militar, este recunoscut faptul că măsurile defensive sunt rezultatul unei colaborări eficiente a societăţii civile cu organizaţiile militare. Astfel, la ora actuală se poate afirma că cel mai bine s-au dezvoltat şi implementat atât la nivelul societăţii civile, cât şi în domeniul militar, acţiunile defensive pentru răspuns la incidentele de securitate IT.

În prezent, NATO şi statele membre sunt expuse riscului de atacuri cibernetice care pot afecta activele lor fizice sau informaţionale, acţiunile acestora

[57] *Hotărârea Guvernului nr. 494/2011* privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.

[58] *HG 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, Anexa nr. 1 la Strategia de Securitate Cibernetică a României.

derulate în plan internaţional sau imaginea publică a acestora. Astfel de atacuri se pot desfăşura în scopul dezinformării, spionajului electronic pentru obţinerea avantajului competitiv global, modificării clandestine a datelor sensibile din cadrul teatrelor de operaţii sau pentru alterarea sau întreruperea funcţionării unor infrastructuri critice naţionale, cum ar fi cele de energie, apă, combustibil, comunicaţii, bancare sau transport, care sunt esenţiale pentru funcţionarea societăţii şi economiei.

În plan militar acestea pot urmări sabotajul, subversiunea, spionajul sau terorismul şi sunt concretizate în exploatarea/provocarea de scurgeri de informaţii, împiedicarea desfășurării misiunilor, provocarea unor anomalii în cursul de desfășurare al operaţiilor etc.

De regulă, astfel de acte pot fi motivate de obţinerea unor câștiguri ilicite sau a unor avantaje politice şi pot fi comise de persoane, organizaţii sau state care au capabilitatea de a executa, induce, transporta, transmite sau susţine o ameninţare, desfășurând acţiuni şi folosind procese automate pentru a sprijini/dezvolta această capabilitate. În funcţie de actorii implicaţi, precum şi de motivaţia lor, atacurile cibernetice pot fi categorisite drept acte de criminalitate informatică, terorism cibernetic sau război cibernetic.

Pe scurt, infrastructurile noastre digitale au devenit active naţionale de nivel strategic, iar acum sunt expuse unor riscuri majore de securitate. Natura expediţionară a misiunilor armatelor moderne, desfășurarea operaţiunilor pe baza noii doctrine bazate pe capabilităţile facilitate de reţea NEC – *Network Enabled Capability*, pentru a permite interoperabilitatea coaliţiilor, aduce o nouă eră a ameninţărilor şi provocărilor la adresa securităţii operaţiilor militare.

Războiul cibernetic determină şi dezvoltarea unor strategii şi doctrine noi de organizare şi ducere a acţiunilor, în măsură să răspundă unor noi întrebări de genul: ce tipuri de forţe sunt necesare, unde şi cum se desfășoară, cum pot lovi inamicul, unde şi când se poziţionează sistemele informatice şi de comunicaţii, ce tip de computere, senzori, reţele şi baze de date se utilizează.

Ca inovaţie a războiului, războiul cibernetic a devenit pentru secolul XXI, ceea ce *„războiul fulger" (blitzkrieg)* a fost pentru secolul XX. Simplificând la minim, războiul cibernetic reprezintă o extensie a importanţei acordată în trecut acţiunilor pentru obţinerea informaţiilor în război: deţinerea superiorităţii cu ajutorul sistemelor de comandă şi control şi realizarea surprinderii adversarului prin descoperirea, localizarea şi inducerea în eroare a acestuia.

Caracteristica comună a confruntărilor din spaţiul cibernetic este raportul antagonic continuu stabilit între *ameninţările* care se manifestă în spaţiul cibernetic *– terorism, spionaj, sabotaj, subversiune şi crimă organizată, pe de o parte* şi *securitatea informaţională* pe de altă parte**.** Aceste ameninţări se manifestă într-un

mediu foarte larg, oferit de războiul informaţional, într-o accentuată interferenţă conceptuală şi acţională între *războiul electronic*, cel al *hackerilor*, cel *psihologic, economic* şi între o tipologie complexă a *atacurilor informatice*.

Dat fiind faptul că este o Alianţă pentru apărare, NATO a identificat şi a recunoscut, încă de la începutul deceniului trecut, gravitatea ameninţărilor cibernetice şi importanţa protecţiei reţelelor informaţionale.

Apărarea cibernetică a apărut pe agenda NATO la Summit-ul de la Praga din 2002 şi a fost ulterior confirmată ca prioritară la Summit-ul de la Riga, din 2006. O politică în domeniu a fost agreată, pentru prima dată, de şefii de state şi de guverne la Summit-ul de la Bucureşti, în aprilie 2008.

Evoluţia rapidă a atacurilor şi caracterul lor sofisticat au determinat plasarea temei în centrul agendei de securitate a NATO. Astfel, la Summit-ul de la Lisabona (2010) s-a adoptat un Concept Strategic care menţionează ameninţările din domeniul cibernetic, arătând că *„acestea pot viza direct securitatea infrastructurilor naţionale vitale şi pot atinge niveluri de natură a pune în pericol prosperitatea, securitatea şi stabilitatea naţională şi euro-atlantică”*[59].

În consecinţă, acest tip de provocări impune dezvoltarea de către Alianţă a capacităţii de prevenire, detectare şi apărare împotriva lor, de redresare în urma apariţiei lor, de consolidare şi coordonare a capabilităţilor naţionale de apărare cibernetică.

Analizând esenţa Summit-ului de la Lisabona constatăm că în timp ce Conceptul Strategic stabilea Strategia NATO în domeniu pentru următoarea decadă, Declaraţia Summit-ului prevedea revizuirea în profunzime a actualei politici aliate, vizând adaptarea acesteia la dinamica mediului de securitate.

Pasul următor s-a făcut la Summit-ul din Ţara Galilor (2014), unde şefii de state şi de guverne NATO au confirmat, împuternicit şi girat, noua Politică întărită în domeniul apărării cibernetice, care subliniază faptul că *apărarea cibernetică este parte a sarcinii de bază a NATO privind apărarea colectivă*.

Considerăm că deosebit de important, pentru domeniul abordat în acest articol, este Summit-ul NATO de la Varşovia (*8-9 iulie 2016)* la care şefii de stat şi de guvern participanţi la întrunirea Consiliului Nord-Atlantic, au elaborat o declaraţie comună cu 139 puncte dintre care unele (punctele 5, 47, 70) se referă chiar la tipurile de ameninţări, despre care am vorbit în acest articol, din partea unor actori statali, dar şi non-statali - din partea unor forţe militare, dar şi din partea atacurilor teroriste, cibernetice sau hibride.

Importanţa care s-a acordat acestei probleme la nivelul NATO este demonstrată şi de faptul că la Summit-ul de la Varşovia s-au reluat unele teme

[59] NATO, *Apărarea cibernetică*, [https://nato.mae.ro/node/435].

discutate la Summit-urile de la București (2008), Lisabona (2010), Chicago (2012) şi Ţara Galilor (2014).

Atacurile de natură cibernetică pot afecta direct fluxurile de informaţii care se vehiculează în cadrul sistemelor de comandă şi control militare şi în legătură cu acest aspect la Varșovia s-a afirmat că *„Este din ce în ce mai importantă abilitatea noastră de înţelegere, urmărire şi, în cele din urmă, anticipare a acţiunilor potenţialilor adversari, prin capacităţi de Informaţii, Recunoaştere şi Supraveghere (IRS) şi acorduri cuprinzătoare privind schimbul de informaţii. Acestea sunt esenţiale pentru a permite luarea unor decizii politice şi militare prompte şi informate. Am stabilit adecvarea capacităţilor necesare pentru a ne asigura viteza de răspuns, faţă de forţele noastre cu cel mai înalt grad de operativitate”*[60].

Oficialii NATO apreciază că atacurile cibernetice prezintă o provocare clară la adresa securităţii Alianţei şi ar putea fi la fel de dăunătoare pentru societăţile moderne ca şi atacurile convenţionale. Se reamintește, cu această ocazie, că NATO are un *mandat defensiv* şi că *„cyber-spaţiul este considerat ca un domeniu de operaţii în care NATO trebuie să se apere la fel de eficient ca şi în aer, la sol sau pe mare”*[61].

În același context participanţii la acest summit, care după opinia mea a fost cel mai relevant pentru domeniul apărării cibernetice, și-au exprimat susţinerea pentru acţiunile NATO de descurajare şi apărare pe scară mai largă, în care apărarea cibernetică va continua să fie integrată în planificarea operaţională şi operaţiunile şi misiunile Alianţei, şi că vor lucra împreună pentru a contribui la succesul acestora.

Declaraţiile făcute de participanţi subliniază acest lucru: *„Continuăm să implementăm Politica întărită în domeniul apărării cibernetice a NATO, şi să consolidăm capacităţile NATO în domeniul apărării cibernetice, beneficiind de tehnologii de ultimă generaţie. Ne reafirmăm angajamentul de a acţiona în conformitate cu dreptul internaţional, inclusiv Carta ONU, dreptul umanitar internaţional şi legislaţia privind drepturile omului, după caz”*[62].

Reuniunea miniștrilor apărării din statele membre ale NATO care a avut loc la Bruxelles pe 14 februarie 2018, au vizat şi implementarea deciziilor asumate anterior la Summit-urile de la Varşovia şi din Ţara Galilor referitoare la postura de apărare şi descurajare, discuţii pe dimensiunea proiectării stabilităţii şi a luptei împotriva terorismului precum şi pe cooperarea între NATO şi UE.

---

[60] *Declaratia Summit-ului din Varsovia*, adoptată de șefii de stat și de guvern participanți la reuniunea Consiliului Nord Atlantic din Varşovia (8-9 iulie 2016), pct. 47, [https://www.mae.ro/node/36635].
[61] *Idem.*, pct. 70.
[62] *Declaraţia Summit-Ului din Varşovia, op. cit.*

Analiştii militari apreciază că rezultatele discuţiilor vor contribui la conturarea cadrului abordării acestui subiect la Summit-ul NATO de la Bruxelles, din iulie 2018.

În cadrul discuţiilor, Președintele României a salutat progresele înregistrate în implementarea Prezenţei Înaintate (Forward Presence), subliniind necesitatea ca, *„prin deciziile care vor fi adoptate la Summitul de la Bruxelles, din acest an, să fie asigurate unitatea, coerenţa şi consolidarea măsurilor aliate pe Flancul Estic în cadrul posturii de descurajare şi apărare a NATO”*[63].

Considerăm şi sperăm că activitatăţile politico-militare care au avut loc şi care vor urma în cadrul NATO, UE dar şi la nivel naţional vor contribui la elaborarea unor norme și/sau reglementări internaţionale/naţionale care să ridice nivelul comportamentului responsabil al statelor şi a măsurile de sporire a încrederii în legătură cu spaţiul cibernetic.

Concluzii

Considerăm că specificul ameninţările la adresa securităţii cibernetice, care au devenit din ce în ce mai serioase în ultimii ani, este dat şi de faptul că ele nu sunt limitate de frontiere şi înregistrează o creştere permanentă a frecvenţei şi a gradului de sofisticare dar şi de apartenenţa universală a spaţiului cybernetic. Riscurile de securitate pe care le implică atacurile cibernetice şi caracterul global al efectelor lor impun eforturi comune de cooperare internaţională pentru asigurarea securităţii sistemelor informaţionale ale statelor membre ale Alianţei.

Documentele elaborate de ţările membre NATO reafirmă principiile indivizibilităţii securităţii Aliaţilor, precum şi ale prevenţiei, detectării, rezistenţei, recuperării şi apărării. Acestea reamintesc faptul că responsabilitatea fundamentală a NATO, în domeniul apărării cibernetice, este de a-şi apăra propriile reţele, precum şi faptul că asistenţa către Aliaţi trebuie abordată în concordanţă cu spiritul solidarităţii, cu sublinierea responsabilităţii Aliaţilor de a-şi dezvolta capacităţile relevante în vederea protejării propriilor reţele naţionale.

[63] http://www.amosnews.ro/iohannis-s-intalnit-cu-ministrii-apararii-ai-cele-noua-state-membre-nato-din-flancul.

BIBLIOGRAFIE

*** *Hotărârea de Guvern nr. 494/2011* privind înfiinţarea *Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO.*

*** *HG 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, Anexa nr.1 la Strategia de securitate cibernetică a României.

*** *Hotărârea de Guvern nr. 245/7 aprilie 2015* prin care se aprobă *Strategia Naţională privind Agenda Digitală pentru România 2020.*

*** *Cybersecurity Strategy of the European Union*, Brussels, 7.2.2013, JOIN (2013) 1 final, [http://eeas.europa.eu/ archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf].

*** *Declaraţia Summit-ului din Varşovia,* adoptată de şefii de stat şi de guvern participanţi la reuniunea Consiliului Nord Atlantic din Varşovia (8-9 iulie 2016), pct. 47, [https://www.mae.ro/node/36635].

*** *Cornerstones of Information Warfare*, Department of the Air Force, Washington DC, 1995.

BOARU G., *Securitatea cibernetică în Uniunea Europeană,* Revista Academiei de Ştiinţe ale Securităţii Naţionale nr. 2/2017.

GRIER P., *Information Warfare, Air Force Magazine*, No. 3, March 1995.

PETRESCU S., *Informaţiile a patra armă*, Editura Militară, Bucureşti, 1999.

NATO, *Apărarea cibernetică*, [https://nato.mae.ro/node/435].

http://www.amosnews.ro/iohannis-s-intalnit-cu-ministrii-apararii-ai-cele-noua-state-membre-nato-din-flancul.

Statisticile lumii în timp real, [http://www.worldometers.info/ro/].

Internet World Stats, [http://www.internetworldstats.com/stats.htm].

www.insse.ro/cms/sites/default/files/com_presa/com_pdf/tic_r2016.pdf.

hotnews.ro.

www.bloomberg.com/.