RĂZBOIUL RUSO-UCRAINEAN ȘI IMPACTUL SĂU ASUPRA SECURITĂȚII CIBERNETICE ÎN NATO ȘI ÎN UE

Căpitan-comandor drd. Claudiu-Cosmin RADU
Universitatea Națională de Apărare „Carol I”, București
10.55535/GMR.2023.4.1

Încă de la începutul anului 2022, înainte de declanșarea conflictului ruso-ucrainean, spațiul cibernetic a fost folosit intens, iar operațiile cibernetice au jucat un rol-cheie în disimularea informațiilor, în acțiunile de înșelare și de atac asupra infrastructurilor critice. Războiul s-a schimbat, devenind tot mai complex, iar acțiunile cibernetice, coroborate cu efectele „hard power”, devin tot mai disruptive. Acțiunile cibernetice s-au extins peste granițele Ucrainei, fiind afectate state vecine, membre ale NATO și ale UE. Astfel de incidente sunt pe cât de actuale, pe atât de periculoase pentru securitatea statelor din flancul estic al Alianței Nord-Atlantice. Articolul analizează nevoia de cooperare în cadrul alianțelor și de dezvoltare a capabilităților, doctrinelor și strategiilor cibernetice pentru a realiza un mediu propice securității la nivel regional. România, ca stat membru al NATO și al UE din flancul estic, trebuie să rămână un pilon al stabilității și un furnizor de securitate în regiune. În acest context, alianțele din care România face parte trebuie să se adapteze pentru a putea răspunde provocărilor respective.

Cuvinte-cheie: spațiu cibernetic, război ruso-ucrainean, operații cibernetice, securitate cibernetică, vector de stabilitate.

INTRODUCERE

Regiunea Mării Negre a devenit o zonă de interes global, caracterizată printr-un potențial de instabilitate ridicat odată cu izbucnirea conflictului dintre Federația Rusă și Ucraina. Viziunea statelor din regiune privind securitatea proprie este puternic afectată de agresivitatea Federației Ruse. În aceste circumstanțe, rolul României în realizarea securității Alianței Nord-Atlantice și a Uniunii Europene a devenit unul foarte important. Prezența forțelor militare străine pe teritoriul său și exercițiile comune cu Aliații au rolul de a liniști populația care trebuie să-și recapete mai rapid percepție pozitivă asupra securității proprii.

Dezideratul de a avea o prezență militară mai puternică este firesc, deoarece amenințarea vine de la o superputere care a avut o perioadă mare de timp influență asupra acestei regiuni. Din perspectiva unei Rusii agresive, această prezență militară suplimentară a aliaților la granița de est a NATO nu reprezintă îngrijorare semnificativă. Chiar dacă acțiunile conflictului sunt preponderent cinetice, există implicații din ambele tabere privind aspectele cibernetice. Acestea din urmă reprezintă, în general, operațiuni secrete sau de înșelăciune, care urmăresc constrângerea adversarului. Mai nou, operațiunile cibernetice acționează atât ca activități complementare în război, cât și ca acțiuni decisive de sine stătătoare. În esență, putem spune, eufemistic, că Federația Rusă folosește Ucraina ca pe un poligon de tragere cu scopul de a-și îmbunătăți capacitățile cibernetice prin testarea și operaționalizarea diferitelor metode noi. Mai mult, Federația Rusă recurge la metode hibride de atac testate și în alte conflicte, atacurile cibernetice devenind, așadar, mai sofisticate.

Ca și în cazul altor state, României îi revine un rol fundamental în securizarea frontierei estice a NATO și a UE. România și-a asumat un acord în cadrul NATO și își propune să devină un vector de stabilitate, democrație și valori euroatlantice în regiunea Mării Negre. De asemenea, România are ambiția să se transforme într-un pilon de securitate geopolitică regională și are oportunitatea de a se afirma ca un furnizor excelent de securitate. Ca membru activ al Alianței Nord-Atlantice și al Uniunii Europene, aceasta își asumă un angajament pe termen lung de a investi în securitate, în promovarea păcii și stabilității, în extinderea economiei de piață, a valorilor ce caracterizează o societate deschisă către Vest, către partenerii strategici.

Pe măsură ce războiul din Ucraina avansează, agențiile rusești își concentrează operațiunile de influență cibernetică asupra populației ucrainene cu scopul de a submina încrederea în voința și capacitatea țării de a rezista atacurilor rusești. În plus, vizată de propagandă este și populația rusă, deoarece este nevoie de sprijinul acesteia pentru a susține efortul de război. Statele susținătoare ale Kievului, de asemenea, au fost țintele unor atacuri cibernetice având scopul de a avertiza și descuraja. Cea mai mare parte a atenției asupra atacurilor cibernetice ca o componentă a războiului se concentrează pe potențialul de a perturba, degrada sau distruge obiective. Cu toate acestea, Federația Rusă are un istoric extins în ceea ce privește utilizarea intruziunilor în rețea pentru colectarea de informații, iar aceste operațiuni pot fi mult mai greu de detectat.

O lecție importantă extrasă din desfășurarea de forțe operaționale multidomeniu o reprezintă mobilizarea exemplară a celorlalte state în sprijinul Ucrainei. Aceasta poate duce, cu siguranță, la o mai bună cooperare interstatală în cadrul Alianței Nord-Atlantice și al Uniunii Europene, punând bazele unei noi forme de apărare colectivă. De asemenea, Ucraina a beneficiat de o susținere deosebită din partea entităților private: companii lider pe piața securității cibernetice, grupări renumite de hackeri, dar și grupări de hackeri patrioți voluntari. În general, atacurile cibernetice au capacitatea de a perturba, degrada sau distruge infrastructuri critice. Mai mult, Federația Rusă are o istorie vastă în utilizarea intruziunilor în rețele în scopul colectării de informații, al spionajului, degradării sau blocării sistemelor adverse. Aceste acțiuni pot avea efecte imediate sau pot fi lansate să producă efecte în timp, fără a fi detectate.

RĂZBOIUL INFORMAȚIONAL AL FEDERAȚIEI RUSE ÎNAINTE DE 2022

Pentru a înțelege mai bine operațiile din mediul cibernetic în cadrul acțiunilor militare ale Rusiei în Ucraina de la începutul anului 2022, ar trebui să menționăm modul unic în care Moscova percepe operațiile cibernetice și aplică doctrinele în scopul realizării succesului pe câmpul de luptă. Cu toate acestea, în acest articol, nu voi analiza aspectele doctrinare ale acțiunilor din domeniul cibernetic, ci mă voi concentra pe modul în care aceste acțiuni se desfășoară în mediul cibernetic. De asemenea, voi analiza și efectele pe care aceste acțiuni le generează, cu scopul de a identifica un tipar al utilizării acestor atacuri cibernetice de către Federația Rusă.

Unul dintre principalele rezultate ale dezvoltării rapide a tehnologiei informațiilor a fost extrapolarea confruntărilor clasice în mediul virtual, creându-se, astfel, spații

alternative realității. Spațiul cibernetic a devenit un nou câmp de luptă, caracterizat de viteza și eficiența sa, sporite în comparație cu metodele tradiționale de luptă. Un avantaj semnificativ al acestui mediu este că riscul de pierdere de vieți omenești este minim. Acest nou domeniu de confruntări a fost oficial recunoscut ca domeniu de operații militare de către membrii Alianței Nord-Atlantice, la summitul din Varșovia, Polonia, în anul 2016 (North Atlantic Treaty Organization, 2023).

Federația Rusă a utilizat acest mediu de confruntare mult mai devreme, însă, după cum putem vedea și astăzi, strategia sa constă în utilizarea războiului convențional combinat cu acțiuni noncinetice, de tipul propagandei, spionajului, terorismului cibernetic, operațiilor cibernetice și folosirea de malware. Aceste tipuri de atac utilizate asupra sistemelor informaționale și informatice au rolul de a induce populația în eroare, de a bloca activitățile economice, de a scoate din uz infrastructuri critice naționale, de a culege informații despre capabilitățile militare și de a vulnerabiliza securitatea statului țintă. Federația Rusă este cunoscută ca un actor capabil să desfășoare o gamă largă de operațiuni de spionaj cibernetic și sabotaj încă din anii ’90 (Aliyev, 2022). Aceasta dispune deja de o vastă experiență în mediul informațional, bazată pe campaniile de dezinformare coordonate chiar de guvern, cu care a reușit să mobilizeze populația de etnie rusă în anul 1999, în timpul celui de-al doilea război cu Cecenia, utilizând ca mijloc de propagandă mass-media.

O altă campanie de atacuri cibernetice, de această dată de o amploare și de o rezonanță mai mari, au reprezentat-o seriile de atacuri cibernetice din 2007 la adresa Estoniei, pe fondul unor neînțelegeri istorice dintre cele două state. Timp de mai multe zile s-au desfășurat operațiuni cibernetice împotriva mai multor ținte estoniene, precum: site-urile unor ministere, bănci, partide politice, mass-media și a unor servicii de telecomunicații. Efectele au fost surprinzătoare, deoarece Estonia era o țară destul de digitalizată la acel moment (Herzog, 2011, p. 51). Acele atacuri, care aveau să blocheze pentru o perioadă limitată de timp diferite ținte estoniene, au reconfirmat capabilitățile rusești din mediul informațional. Devenind prima țară care s-a confruntat cu un atac cibernetic de o astfel de amploare, Estonia a avut nevoie de ajutor extern din partea aliaților și a comunității internaționale. Un an mai târziu, Federația Rusă a folosit metode hibride de acțiune în războiul ruso-georgian. Acțiunile noncinetice au constat în atacuri cibernetice și informații psihologice, inclusiv propagandă și știri false.

Georgia, o țară care căuta succesul democrației în Vest, apropiindu-se tot mai mult de SUA și de NATO, a stârnit nemulțumiri din partea Rusiei. Aceasta a recurs la măsuri militare împotriva Georgiei, după summitul NATO de la București, din 2008,

unde aliații au discutat cu guvernul de la Tbilisi posibilitatea aderării la Alianța Nord-Atlantică. Deși discuțiile nu au condus la un rezultat concret, schimbarea ideologiei și a atitudinii față de Kremlin și apropierea de spațiul euroatlantic au sporit agresivitatea Rusiei asupra acestui mic stat.

Începând cu același an, sprijinul cetățenilor pentru integrarea europeană și euroatlantică a Georgiei a crescut foarte mult. Potrivit unui sondaj de opinie realizat de Institutul Național Democrat (NDI) în 2021, 80% dintre georgieni și-au exprimat sprijinul față de aderarea Georgiei la UE (față de 76%, în 2020), în timp ce 74% din populație a susținut integrarea în NATO (în creștere, de la 69%, în 2020) (Seskuria, 2021). La momentul respectiv, serviciile de securitate rusești au reușit, prin tehnici și mijloace de manipulare a informațiilor care au inclus propaganda, controlul informațiilor și campanii de dezinformare, să domine domeniul informațional. O parte din propaganda Kremlinului se concentra din ce în ce mai mult pe schimbarea opiniei publice, susținând că Federația Rusă este factorul determinant în ceea ce privește securitatea regională și încetarea conflictului, iar statele vestice nu au nici capacitatea, nici interesul de a face acest lucru. Răspândirea de știri antioccidentale prin intermediul actorilor locali a cultivat în mod activ și a sprijinit financiar partidele pro-ruse și a răspândit mesaje ultranaționaliste și xenofobe (Ib.). Prin intermediul televiziunilor și al interviurilor zilnice cu un purtător de cuvânt militar, Federația Rusă a controlat fluxul internațional de informații și a încercat să influențeze populațiile locale prin impunerea știrilor, diseminarea progreselor înregistrate de trupele rusești care protejau cetățenii ruși și evidențiind atrocitățile georgiene (Iasiello, 2017, p. 53). Mai mult, acțiunile din mediul informațional s-au derulat concomitent cu operațiile militare fizice, astfel încât au condus la defăimări de pagini web, refuz de servicii și atacuri distribuite de negare a serviciilor împotriva guvernului georgian, mass-mediei și instituțiilor financiare din Georgia, precum și alte acțiuni publice și private. Atacurile au reușit să interzică accesul cetățenilor la 54 de site-uri web legate de comunicații, finanțe și guvern (Ib., p. 52).

Mai târziu, între anii 2011 și 2013, protestele cauzate de alegerile controversate din Federația Rusă au demonstrat modul în care mass-media poate fi utilizată în manipularea populației cu scopul de a genera valuri de nemulțumiri publice. Acestea, alături de revoltele arabe, demonstrează eficiența rețelelor de socializare în schimbarea unor regimuri de guvernare. Mai mult, acestea au ajutat guvernul de la Kremlin să dezvolte capacități informaționale care au facilitat anexarea Crimeei în 2014. În acest context, tactici, tehnici și acțiuni cibernetice au avut ca rezultat dezorganizarea rețelelor informatice guvernamentale, paralizia sistemului

de comandă și control, perturbarea canalelor de comunicație și au servit drept instrumente pentru consolidarea strategiilor războiului hibrid. Operațiile psihologice au jucat un rol crucial, amplificând eficacitatea acestor strategii. Gradual, operațiunile psihologice au început prin încercarea de a câștiga credibilitate și convingere în rândul indivizilor, apoi s-au concentrat pe exercitarea presiunii asupra populației din Crimeea și Ucraina. În final, scopul a fost să se creeze condiții care să minimizeze imaginea Federației Ruse ca stat agresor. Răspunsul Ucrainei la acest conflict hibrid a fost caracterizat de reacții inadecvate și fragmentate, cu o dominanță în sfera informațională, mediatică virtuală și psihologică (Stanciu, 2016, p. 74).

În opinia mea, Federația Rusă a studiat conflictele anterioare și a aplicat lecțiile învățate, astfel că a sincronizat atacurile cinetice cu cele cibernetice. Acestea din urmă erau considerate lovituri esențiale, cu eficacitate maximă în special asupra infrastructurilor critice. Aceste operațiuni cibernetice rusești urmăreau incapacitarea infrastructurii digitale ucrainene, diseminarea propagandei pro-ruse și înfrângerea voinței de a lupta atât în rândul liderilor politici, cât și al celor militari și civili. De asemenea, acțiunile cibernetice aveau ca scop descurajarea aliaților ucraineni de a interveni în conflict. Actorii cibernetici statali și nonstatali ruși au coordonat o serie de atacuri de negare a serviciilor (Distributed Denial of Service/DDoS) asupra site-urilor web guvernamentale ucrainene, vizând, în special, politicieni considerați a avea opinii antirusești și site-uri web legate de alegeri. Mai mult decât atât, aceștia răspândesc în mod agresiv pe diverse platforme de socializare ucrainene propagandă pro-rusă și știri false (Salt, Sobchuk, 2021, p. 1). Putem afirma, în aceste condiții, că Federația Rusă a folosit acest conflict ca o oportunitate de a-și testa noile tehnici, tactici și proceduri din domeniul cibernetic, îmbunătățindu-și în continuare aceste capacități prin testarea și operaționalizarea diferitelor metode noi. Atacurile cibernetice împotriva Crimeei au oprit telecomunicațiile, au dezactivat principalele site-uri web ucrainene și au blocat telefoanele mobile ale principalilor oficiali ucraineni înainte ca forțele rusești să intre în peninsulă (Iasiello, p. 54). Odată cu acest conflict, atacurile cibernetice au evoluat de la propagandă la alterarea efectivă a infrastructurii fizice, cum ar fi destabilizarea rețelei electrice ucrainene și provocarea de pene de curent în întreaga țară. Astfel de atacuri cibernetice au avut loc la scară industrială, ajungând, uneori, la câteva mii pe lună. De asemenea, atacurile au vizat companii din sectorul privat cu programe malware, ceea ce a complicat și mai mult încercările ucrainenilor de apărare cibernetică, deoarece multe sisteme informatice ajungeau să fie infectate cu programe malware rusești fără a fi detectate.

Operațiunile cibernetice ale Federației Ruse au influențat luptele din teren chiar și la nivel tactic. Rușii au reușit să folosească diverse tehnologii cu ajutorul cărora au descoperit și transmis mesaje pe telefoanele mobile atât ale militarilor, cât și ale familiilor acestora, cu scopul de a-i determina să renunțe la luptă. Din cauza faptului că majoritatea computerelor personale și chiar ale companiilor aveau sisteme de securitate învechite, acestea deveneau vulnerabile. Aceste valuri de atacuri cibernetice rusești se aseamănă mai mult cu bombardamentele decât cu lovituri de precizie, acestea având rolul de a copleși orice apărare și contramăsuri din partea Ucrainei (Salt, Sobchuk, p. 2).

Experți americani în domeniul militar au afirmat că, fără îndoială, atacurile cibernetice au fost executate pentru a izola Crimeea și pentru a facilita mișcările de trupe pe teritoriul ucrainean. Însă, chiar și după terminarea conflictului, încheiat cu anexarea Crimeei la Federația Rusă, actorii statali și non-statali cu afinități pro-ruse au continuat activitățile în spațiul cibernetic și pe timp de pace. Aceste activități cibernetice aveau scopul de a testa vulnerabilitățile sistemelor ucrainene, în acest mod specialiștii cibernetici ruși antrenându-se pentru viitoarele atacuri cibernetice.

Federația Rusă desfășoară atacuri cibernetice și în absența unei acțiuni militare planificate, încercând să perturbe politica altor state, neurmărind să provoace un război armat. Alegerile, în general, pot fi extrem de vulnerabile, deoarece oferă actorilor externi șansa nu doar de a susține un candidat preferat, ci și de a ridica întrebări cu privire la integritatea candidaților și corectitudinea procesului electoral. Ingerința în alegerile prezidențiale din SUA, din 2016, este cel mai bun exemplu de utilizare de către Federația Rusă a tehnicilor informațional-tehnice și informațional-psihologice. Aceasta s-a manifestat sub forma colectării și, ulterior, a scurgerii de date din registrele partidelor, precum și a datelor personale ale unor candidați. De asemenea, s-au remarcat operațiuni specifice de colectare de date și incidente cibernetice legate de alegerile din Parlamentul European, Ucraina, Suedia, Franța, precum și din alte țări. Acestea sunt definite prin campanii de *spear phishing* de accesare a datelor, operațiuni de piratare și scurgeri de informații, atacuri disruptive asupra infrastructurii electorale, utilizarea mediului online pentru răspândirea de informații false și manipulare (Hakala, Melnychuk, 2021, p. 27).

Având în vedere cele prezentate, putem afirma că Federația Rusă folosește numeroase atacuri cibernetice care au rolul de a destabiliza, de a scoate din funcțiune sau de a îngreuna sistemele de comunicații și infrastructurile critice. Pe partea de propagandă și dezinformare, aceasta are sisteme foarte bine dezvoltate. Acțiunile din mediul informațional sunt fundamentate de numeroase strategii

și doctrine, dintre care amintim controversata *„Doctrină Gerasimov”*. Acțiunile Rusiei din spațiul cibernetic au rolul de a pregăti câmpul de luptă înainte de a introduce trupe sau de a folosi armament convențional. În esență, aceasta utilizează cele mai periculoase atacuri cibernetice asupra sistemelor critice ale țării pe care urmează să o atace, cu scopul de a o paraliza.

DINAMICA ATACURILOR CIBERNETICE ÎN CADRUL RĂZBOIULUI RUSO-UCRAINEAN (2022)

În ianuarie 2022, după o concentrare numeroasă de trupe la granița cu Ucraina, Federația Rusă a cerut garanții juridice din partea Statelor Unite și a țărilor membre ale NATO că Ucraina nu va fi acceptată să adere la Alianța Nord-Atlantică. După refuzul cererilor, o lună mai târziu, imaginile din satelit arătau o dislocare impresionantă de forțe terestre și de elicoptere rusești la granița cu Ucraina. Următoarea mișcare a fost de a-și retrage tot personalul diplomatic de pe teritoriul ucrainean, indicând pregătirea unei operații militare împotriva statului vecin. Astfel, armata rusă a trecut granița ucraineană la 24 februarie 2022, printr-o ofensivă combinată de trupe, tancuri, avioane și rachete de croazieră în ceea ce era denumită de către Kremlin o *„operație militară specială”*, demonstrând, astfel, că nu va permite ca Ucraina să fie în afara sferei de influență rusească.

O eventuală aderare a Ucrainei la alianța militară occidentală ar reprezenta o schimbare a situației geostrategice și de securitate la nivel regional și ar fi privită drept o amenințare la adresa intereselor și securității Rusiei, practic aceasta ar fi avut granița direct cu NATO! Această ofensivă militară rusească a condus la cea mai mare mobilizare pe câmpurile de luptă a personalului militar, a armelor și a echipamentelor militare din Europa, după cel de-Al Doilea Război Mondial (Guchua, Zedelashvili, Giorgadze, 2022, p. 30).

Cu toate acestea, primele *„proiectile”* au fost lansate pe 23 februarie, cu câteva ore înainte de apariția rachetelor sau de deplasarea tancurilor. Este vorba despre o nouă rundă de atacuri cibernetice ofensive și distructive îndreptate împotriva infrastructurii digitale a Ucrainei. Microsoft a detectat și anunțat oficialii ucraineni despre acest nou pachet malware, pe care l-a denumit *„Fox Blade”* (Orenstein, 2022). Federația Rusă dispune de o vastă experiență de luptă în domeniul cibernetic, iar infrastructura și echipamentele cibernetice rusești s-au dezvoltat continuu, astfel încât au favorizat punerea în practică a acțiunilor de tip hibrid. Dinamica atacurilor cibernetice a dovedit că acestea sunt utilizate ca acțiuni premergătoare oricăror forme de acțiune, iar pentru atingerea scopurilor propuse, acestea pot continua

la o intensitate mai mare sau pot reprezenta deschiderea pentru o nouă etapă a operației militare. *Modus operandi* al Federației Ruse s-a bazat pe experiențele acumulate din conflictele trecute cu Estonia, Georgia și Ucraina, ceea ce nu i-a surprins pe mulți specialiști. În noul context internațional, în care securitatea globală este volatilă, declarațiile belicoase provoacă neliniște și teamă chiar și pentru actorii statali neimplicați direct în acest conflict.

În contextul tensiunilor care se intensificau între cele două țări, agenția de informații militare rusești (GRU) lansa, la începutul lunii februarie 2023, o serie de atacuri DDoS împotriva site-urilor web ucrainene din domeniul bancar, guvernamental și al apărării. Potrivit unui raport al Microsoft, alte două entități rusești, precum Serviciul de informații externe (SVR) și Serviciul federal de securitate (FSB), *„au desfășurat atacuri distructive, operațiuni de spionaj sau ambele, în timp ce forțele militare rusești atacă țara pe uscat, în aer și pe mare”* cu scopul de a *„perturba sau degrada funcțiile guvernamentale și militare ucrainene și de a submina încrederea publicului în aceleași instituții”* (Orenstein).

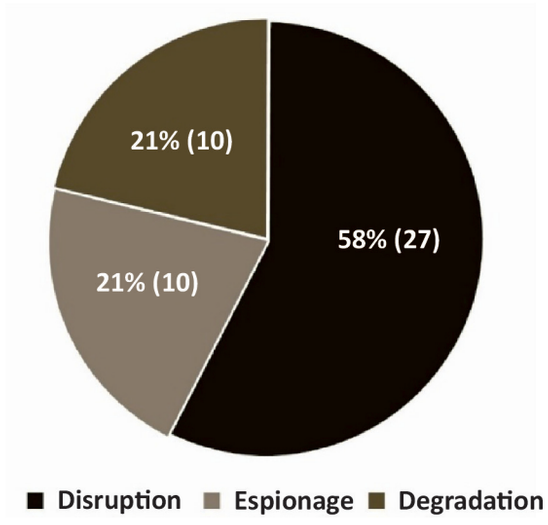

Figura 1: Obiectivele cibernetice rusești
(CSIS, 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war)

După analizarea activității cibernetice a Rusiei la începutul conflictului, s-a constatat că obiectivele sale în domeniul cibernetic s-au concentrat mai mult pe acțiuni disruptive decât pe cele degradante, ceea ce este evidențiat în *figura 1*. Potrivit aceleași surse, activitățile cibernetice rusești de după 2000 au vizat actori privați nestatali (57%), actori guvernamentali nemilitari (32%) și actori militari

guvernamentali (11%) (Mueller, Jensen, Valeriano&Mane, 2023). Acțiunile din mediul cibernetic au devenit mai periculoase odată cu coordonarea acțiunilor militare convenționale în încercarea de a crea dezechilibru, panică și confuzie în rândul populației. Federația Rusă a început pregătirea acestor acțiuni noncinetice încă din martie 2021, în timp ce trupele se cantonau la granița cu Ucraina.

Oficialii guvernamentali ucraineni au raportat în ianuarie 2022 că, în primele 10 luni ale anului 2021, au fost înregistrate aproximativ 288.000 de atacuri cibernetice, pe lângă cele 397.000 de atacuri înregistrate în 2020 (Office for Budget Responsibility, 2022). În cadrul unui interviu, Oleksandr Potii, vicepreședinte al Serviciului de stat pentru comunicații speciale și protecția informațiilor din Ucraina (SSSCIP), susținea că, în primele șase luni de război, s-au detectat peste 1.500 de atacuri cibernetice împotriva Ucrainei (Beecroft, 2022). Concomitent cu pregătirea și desfășurarea de exerciții militare la granița cu Ucraina, aceste atacuri aveau ca scop colectarea de informații de politică externă, militare și obținerea accesului la infrastructurile critice ucrainene. Multe dintre acestea au fost lansate după ce diverse discuții diplomatice dintre Federația Rusă, Ucraina, NATO și UE au eșuat. Moscova a utilizat aceste atacuri cibernetice fie ca un avertisment, fie ca o amenințare pentru a da mai multă seriozitate acțiunilor diplomatice (Orenstein).

Oficialitățile de la Kremlin au declarat că țările care vor ajuta Ucraina în această confruntare vor suporta consecințele. Într-adevăr, agențiile de informații rusești au intensificat activitățile de spionaj și penetrare a rețelelor de comunicații care vizează guvernele solidare Ucrainei. Microsoft a detectat acțiuni rusești de intruziune în rețele a 128 de organizații din 42 de țări. În topul țărilor vizate de aceste atacuri la nivel mondial se află SUA, în timp ce, în Europa, ținta prioritară a devenit Polonia, țară vecină Ucrainei, care coordonează o mare parte a sprijinului logistic militar și umanitar. Echipe rusești au utilizat ransomware-ul Prestige în această campanie malițioasă împotriva organizațiilor de logistică și transport din Polonia, o tactică ce nu a fost folosită frecvent împotriva țintelor ucrainene. În plus, atacurile par să urmeze un model similar cu activitățile anterioare de hacking susținute de Federația Rusă (Constantinescu, 2022, p. 23). Alte state care s-au confruntat cu un număr în creștere al incidentelor cibernetice asupra rețelelor informatice au fost Țările Baltice, Danemarca, Norvegia, Finlanda, Suedia și chiar Turcia.

O atenție deosebită trebuie acordată României, țară învecinată cu Ucraina, aflată la granița de est a NATO și a UE. Aceasta a fost ținta unor astfel de atacuri cibernetice de DDoS, vizate fiind mai multe instituții, între care Guvernul, Ministerul Apărării Naționale, Poliția de Frontieră, site-ul Căilor Ferate Române, bănci și alte

organizații publice și private. Potrivit unui comunicat al Directoratului Național de Securitate Cibernetică, site-urile acestor instituții au fost indisponibile o perioadă de timp, dar nu s-au înregistrat pagube însemnate (https://dnsc.ro/citeste/comunicat-site-uri-ro-afectate-de-un-atact-de-tip-ddos). Mai mult, aceste incidente au fost mai mult cu titlul de avertizare și descurajare, fiind asumate de hackerii pro-ruși de la Killnet. Atacurile au fost motivate de declarațiile de sprijin ale liderilor de la București pentru Ucraina, în contextul invaziei acestui stat de către Federația Rusă. România a fost printre primele țări care au acordat ajutor umanitar imigranților ucraineni fugiți din calea războiului și a continuat să ajute statul vecin prin diferite metode, în pofida intensificării incidentelor de securitate cibernetică.

Analizând pe scurt acțiunile rusești din mediul cibernetic, putem face o analogie cu ideile unor teoreticieni militari plecând de la Sun Tzu și continuând cu Clausewitz și alții, care au punctat necesitatea învingerii inamicului chiar și fără distrugerea fizică a acestuia. Prin intermediul războiului psihologic, dezinformare și propaganda răspândită în mediul virtual, Federația Rusă a dorit modelarea și incapacitarea componentelor esențiale fizice sau morale ale adversarului prin cucerirea lui fără luptă fizică. Acele elemente, pe care ulterior Clausewitz le-a numit centre de greutate ale unui adversar, au fost lovite mai târziu de aviație. Acest concept clausewitzian al centrului de greutate al inamicului a stat în centrul teoriilor lui J.F.C. Fuller, Liddell Hart, John Boyd sau John Warden. Conform acestor teorii, prin lovirea centrelor de greutate se putea realiza paralizia strategică, determinându-l, astfel, pe adversar să renunțe la luptă. Practic, câștigarea luptei nu se realiza prin distrugerea fizică a forțelor luptătoare, ci prin scăderea moralului în urma executării unor lovituri chirurgicale. Mai mult, puterea aeriană avea atributul de a lovi rapid și eficient centrele de comandă și control, comunicațiile, centrele industriale și elemente esențiale din adâncimea teritoriului inamic, cu eficiență maximă și cu costuri minime. Prin urmare, se observă că Federația Rusă, prin *„paralizia cibernetică”*, și-a propus aceleași efecte prin amplele sale atacuri cibernetice.

Pe de altă parte, reziliența rețelelor ucrainene a fost parțial legată de acțiunile întreprinse înainte de conflict pentru a sprijini dezvoltarea și punerea în aplicare a unei strategii cibernetice naționale. Ambele state dispun de forțe militare specializate în război informațional, dar au fost susținute și de grupări patriotice de hackeri care au intervenit în sprijinul acestor instituții fie pentru a lansa atacuri cibernetice, fie în scopul apărării cibernetice. În plus, acest nou mod de luptă a atras atenția și altor state care au oferit fără ezitare sprijin acestor țări, devenind o oportunitate de a-și testa în mod real posibilitățile de luptă din mediul cibernetic.

Atacurile cibernetice de amploare ale Rusiei asupra Ucrainei oferă o perspectivă a modului în care aceasta desfășoară atacuri cibernetice în conflicte armate și în războiul său hibrid împotriva Occidentului. După mai mult de un an și jumătate de război, putem concluziona că Federația Rusă folosește un amalgam de tehnici și tactici militare, o combinație între cele mai noi tactici și cele folosite în războaiele mondiale, utilizând, de asemenea, arme învechite simultan cu atacurile cibernetice sofisticate sau atacurile în care folosește drone, rachete hipersonice sau informații satelitare.

IMPACTUL RĂZBOIULUI RUSO-UCRAINEAN ASUPRA SECURITĂȚII CIBERNETICE ÎN NATO ȘI ÎN UE

Trebuie subliniat că Federația Rusă se opune vehement aderării Ucrainei la NATO, deoarece acest pas ar amplifica potențialul militar al Ucrainei și ar crea o situație regională precară. Este indiscutabil faptul că agresiunea militară a Federației Ruse împotriva Ucrainei a remodelat situația amenințărilor din NATO și UE, astfel că securitatea cibernetică a aliaților, o componentă a securității colective, a fost pusă la încercare. Odată cu escaladarea conflictului, state din NATO și din afara organizației au devenit ținte sau victime colaterale ale atacurilor cibernetice lansate de actori statali sau nonstatali ruși. Moscova are un mare potențial în ceea ce privește războiul cibernetic, iar datorită situației geopolitice, acesta a fost adaptat cu succes pentru a-și extinde interesele. Atacurile cibernetice lansate sunt, în cea mai mare parte, utilizate în condițiile unui conflict asimetric (Guchua, Zedelashvili, Giorgadze, 2022, p. 33). Potrivit unui raport Mandiant, în 2022 s-a înregistrat o creștere de 250% a tentativelor de phishing rusesc împotriva Ucrainei și o creștere de 300% a acelorași atacuri împotriva țărilor membre ale NATO (DeCloquement, 2023). Toate statele membre ale NATO sau ale UE care au oferit în mod activ sprijin politic, umanitar sau militar Ucrainei s-au confruntat cu valuri de atacuri cibernetice. Aceste operațiuni au avut ca scop perturbarea infrastructurilor naționale, dar și crearea unui factor de descurajare împotriva intervenției în război. Prin intermediul rețelelor de socializare și al atacurilor asupra site-urilor de știri și a posturilor de radio, s-au desfășurat operațiuni de dezinformare și știri false împotriva guvernului ucrainean și a NATO. Rușii au desfășurat operațiuni ofensive și împotriva SUA, Poloniei, Marii Britanii, Germaniei, Letoniei, României și a altor țări.

Înainte de începerea invaziei terestre, Federația Rusă a desfășurat malware care a perturbat sistemul de sateliți Viasat și a dus la întreruperea temporară a peste 30.000 de conexiuni de internet în Europa, inclusiv 5.000 de turbine

eoliene. Compania SpaceX susține că rețeaua Starlink a rezistat la multiplele atacuri cibernetice rusești de când au fost desfășurate în Ucraina. Uniunea Europeană și-a activat echipele de răspuns rapid la incidente de securitate cibernetică pentru a ajuta Ucraina să respingă atacurile cibernetice rusești (Mueller, et al.). Această nouă provocare cu care s-au confruntat statele europene și cele din NATO este una nouă, în care actorii rău intenționați urmăresc degradarea infrastructurii critice, extragerea de informații, furtul de proprietate intelectuală și perturbarea activitățile militare. Alianța a adoptat o politică globală de apărare cibernetică și a reafirmat valabilitatea articolului 5 din Tratatul Nord-Atlantic în spațiul cibernetic. În plus, la ultimele summit-uri, problema spațiului cibernetic a ocupat un loc important pe agenda discuțiilor șefilor de state și de guverne. De asemenea, sprijinul militar pentru Ucraina devine un imperativ al securității europene. Deși numai NATO îi poate oferi Ucrainei protecție împotriva atacurilor rusești, țările membre nu au reușit să ajungă la un acord asupra unei perspective concrete de aderare a acesteia, la summitul din iulie 2023, din Lituania, semn că nimeni nu dorește o confruntare directă și deschisă cu Federația Rusă. Porțile aderării Ucrainei la Alianța militară rămân deschise, dovadă fiind tratatul-cadru privind *„garanții de securitate pe termen lung și cuprinzătoare”* pentru Ucraina, pentru a ajuta țara să se *„apere acum”*, urmând ulterior să se concretizeze acordurile bilaterale. (North Atlantic Treaty Organization, 2023). NATO a mers atât de departe, încât a acceptat Ucraina ca participant contributor în cadrul Centrului de excelență NATO în domeniul cooperării pentru apărarea cibernetică (CCDCOE).

În ceea ce privește relația cu Uniunea Europeană, Ucraina a fost și este considerată un important aliat. Liderii UE au solicitat, încă din 2014, consolidarea capacității de protecție împotriva amenințărilor cibernetice atât pentru Ucraina, cât și pentru statele membre. De asemenea, în anul 2020, președintele Comisiei Europene, Ursula von der Leyen, a solicitat o mai mare *„suveranitate în domeniul tehnologiei”*, făcând referire la dependența de tehnologie din Asia. Mai mult, dependența de petrolul și gazul rusesc a făcut ca UE să realizeze planuri de tranziție pentru a renunța la dependența de gazele naturale rusești și de a consolida reziliența economică a UE. Costurile economice produse de activități rău-intenționate pun la grea încercare reziliența statelor și instituțiilor democratice, țintind direct la pacea și securitatea Uniunii Europene. Aceasta se concentrează pe acțiunile diplomatice în sprijinul securității cibernetice în ceea ce privește schimbul de informații și interoperabilitatea între statele membre sau între UE și state nemembre.

În ceea ce privește susținerea externă, Ucraina a beneficiat de o creștere substanțială a sprijinului cibernetic din partea unor guverne sau servicii ale unor companii digitale de renume, precum Microsoft și Amazon, aceste companii private având capacități analitice mult mai mari decât majoritatea țărilor occidentale. (DeCloquement).

Războiul ruso-ucrainean oferă câteva lecții de aplicat în viitoarele conflicte privind securitatea cibernetică. Atacurile cibernetice sunt inevitabile și pot avea loc atât înainte, cât și în timpul unui conflict. Statele trebuie să fie proactive în anticiparea acestor atacuri și să fie pregătite să le evalueze, să le gestioneze și să răspundă rapid la ele. Este esențial ca parteneriatele-cheie să fie stabilite în prealabil între forțele armate, aliați, industrie și agenții de securitate cibernetică angajați în operațiuni cibernetice defensive proactive. Aceste parteneriate sunt un element fundamental în această ecuație. Pentru a rezista în conflictele viitoare, statele membre ale NATO și ale UE ar trebui să înțeleagă faptul că operațiunile cibernetice defensive sunt cruciale. Astfel, armatele statelor membre trebuie să continue să studieze experiențele Ucrainei din trecut și din prezent, pentru a contribui la dezvoltarea viitoarelor capacități militare. Mai mult, se impune o strategie coordonată și cuprinzătoare pentru a consolida apărarea împotriva întregii game de operațiuni cibernetice distructive, de spionaj și propagandă. Strategiile defensive trebuie să ia în considerare coordonarea acestor operațiuni cibernetice cu operațiunile militare cinetice.

O altă lecție identificată în acest conflict este nevoia pregătirii unui număr mai mare de echipe de răspuns la incidente de securitate cibernetică sau utilizarea inteligenței artificiale în detectarea mai eficientă a incidentelor cibernetice și răspunsul rapid la acestea. De asemenea, conștientizarea populației statelor membre ale NATO și ale UE asupra riscurilor de securitate cibernetică prin creșterea igienei cibernetice poate duce la evitarea vulnerabilităților în sistemele informatice, mai ales în situații de criză sau război. Mai mult, sunt necesare actualizarea legislațiilor din domeniul cibernetic, precum și investițiile în tehnologii inovative pentru creșterea rezilienței cibernetice. Din experiența Ucrainei, mutarea datelor în cloud a fost o soluție pentru o protecție mai eficientă a datelor. Dat fiind faptul că guvernele nu pot realiza singure tehnologiile, softurile și specialiștii din domeniul cibernetic, cooperarea dintre serviciile publice și cele private ar trebui dezvoltată pe viitor, mai ales că firmele specializate în securitatea cibernetică pot ajuta la apărarea cibernetică în cazul unor atacuri cibernetice de amploare, așa cum s-a întâmplat în Ucraina. În plus, este indicată o creștere a interoperabilității în cadrul alianțelor,

dar și în afara lor, prin creșterea numărului de exerciții, de simulări de criză și jocuri cibernetice utilizate pentru a dezvolta o înțelegere comună a modului optim de a răspunde la incidente și de a atenua consecințele (Smith, 2022).

Agenția UE pentru Securitate Cibernetică (ENISA) acordă o atenție sporită securității cibernetice la nivelul Politicii Externe și de Securitate Comună (PESC) și promovează cooperarea între statele membre cu scopul de a implementa politicile de securitate cibernetică ale Uniunii. Spațiul cibernetic poate fi apărat eficient numai printr-o colaborare solidă. O cooperare mai strânsă între inițiativele cibernetice ale NATO și ale UE contribuie la îmbunătățirea bunăstării și securității cetățenilor, la protejarea infrastructurilor critice și la întărirea apărării cibernetice. Oficialii NATO și ai UE au discutat recent despre evoluțiile în politica cibernetică și au convenit să continue să colaboreze strâns pentru a îmbunătăți înțelegerea comună a situației, pentru a întări capacitățile cibernetice și pentru a preveni, descuraja și răspunde la amenințările cibernetice (North Atlantic Treaty Organization, 2023).

La summitul de la Vilnius, aliații au luat decizii semnificative pentru consolidarea apărării cibernetice ca parte a strategiei generale de descurajare și apărare a NATO. Aceasta include angajamentul de a întări apărarea cibernetică națională prin intermediul Angajamentului de apărare cibernetică consolidat al NATO. În plus, aliații au lansat o nouă capacitate virtuală de sprijinire a incidentelor cibernetice NATO, menită să ajute în eforturile naționale de reducere a efectelor acțiunilor cibernetice rău-intenționate semnificative. Acest instrument oferă aliaților o resursă suplimentară de asistență (North Atlantic Treaty Organization, 2023). Prin gestionarea apărării cibernetice prin intermediul structurilor multilaterale din cadrul NATO, statele membre pot comunica eficient și pot împărtăși experiențe, astfel încât să beneficieze de cele mai bune practici și colaborări în utilizarea eficientă a specialiștilor și a resurselor disponibile.

CONCLUZII

Sub paradigma războiului viitorului, atacurile din spațiul cibernetic vor fi, probabil, folosite pe scară largă în operații de mare amploare, încercând să conducă la paralizia strategică a adversarului. Utilizarea forțelor cibernetice în viitor amplifică și potențează efectele acțiunile din celelalte domenii de operații militare, un element vital în acțiunile multidomeniu despre care se vorbește tot mai mult. Acțiunile cibernetice sunt folosite în mod complementar sau de sine stătător.

Când toate sistemele avansate depind de senzori de înaltă performanță, transmiterea rapidă a unor cantități masive de date, precizia detectării țintelor,

implementarea targeting-ului, realizarea comunicărilor satelitare și dezvoltarea capacităților de proiecție a puterii prin intermediul mijloacelor spațiale de supraveghere, recunoaștere și comunicare, toate aceste aspecte devin vulnerabile la atacurile cibernetice. Însă, aceste sisteme nu pot fi la fel de vulnerabile ca orice rețea de calculatoare dacă nu este securizată la timp și în mod corect. Provocarea cea mai mare este de a reuși securizarea unor sisteme de comandă și control care pot deveni centre de greutate la diferite niveluri ale luptei armate (strategic, operativ și tactic).

Tendința este de a muta lupta armată în spațiul cibernetic, pentru a reduce pierderile de vieți omenești, dar să producă efectele dorite din punct de vedere politic și militar în timp scurt și cu costuri minime. De aceea, autoritățile responsabile pot oferi răspunsul privind adaptarea politicilor ce guvernează spațiul cibernetic la evoluțiile tehnologice și procedurale ofensive. Totodată, cea mai de preț resursă rămâne omul. Educarea lui privind igiena cibernetică reprezintă o resursă infinită, fie că este expert, fie că este un simplu utilizator al spațiului digital. Cu cât este mai educat, cu atât va ști cum să identifice, să se ferească și să acționeze oportun la valurile de incidente cibernetice pe care lumea întreagă le experimentează zilnic.

Acest conflict a creat o oportunitate de utilizare de către Federația Rusă a atacurilor cibernetice în timp de război. Totodată, le permite analiștilor să înțeleagă mai bine strategia Rusiei în materie de atacuri cibernetice. În plus, oferă experților din domeniul apărării lecții pentru viitor. Deși nimeni nu poate prezice cât va dura acest război, potențialul unei viitoare agresiuni rusești continuă să rămână o preocupare pentru Uniunea Europeană și Alianța Nord-Atlantică.

BIBLIOGRAFIE:

1. Aliyev, N. (24 noiembrie 2022). *Riddle*, preluat de pe https://ridl.io/cyber-operations-during-russia-s-invasion-of-ukraine-in-2022/, accesat la 12 septembrie 2023.
2. Bateman, J. (2022). *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications.* Carnegie Endowment for International Peace.
3. Beecroft, N. (3 noiembrie 2022). *Carnegie*, preluat de pe https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322, accesat la 12 septembrie 2023.
4. Constantinescu, V. (11 noiembrie 2022). *Bitdefender*, preluat de pe https://www.bitdefender.co.uk/blog/hotforsecurity/russian-military-threat-group-linked-to-ransomware-attacks-in-ukraine/, accesat la 22 august 2023.
5. CSIS (2023), https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war, accesat la 12 august 2023.

6. DeCloquement, F. (27 februarie 2023). *Cyber-bilan Ukraine*. *Atlantico*. Franța: Atlantico.
7. Guchua, A., Zedelashvili, T., Giorgadze, G. (2022). *Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats*. *Ukrainian Policymaker*, pp. 27-36.
8. Hakala, J., Melnychuk, J. (2021). *Russia's strategy in cyberspace.* Riga: NATO StratCom COE.
9. Herzog, S. (2011). *Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses*. În *Journal of Strategic Security*, vol. 4, nr. 2, pp. 49-60.
10. Iasiello, E.J. (2017). *Russia's Improved Information Operations: From Georgia to Crimea*. În *The US Army War College Quarterly*, pp. 51-63.
11. Isaacson, W. (7 septembrie 2023). *The Washington Post*, preluat de pe https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/, accesat la 22 septembrie 2023.
12. Lewis, J.A. (2022). *Cyber War and Ukraine.* Washington, D.C: Center for Strategic and International Studies.
13. Michta, A.A. (2015). *NATO's Eastern Front*. În *GLOBAL FORECAST*, pp. 45-47.
14. Mueller, B.G., Jensen, B., Valeriano, B., Mane, C.R. (13 iulie 2023). *Center for Strategic & International Studies*, preluat de pe https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war, accesat la 12 august 2023.
15. North Atlantic Treaty Organization. (22 septembrie 2023). *North Atlantic Treaty Organization*, preluat de pe https://www.nato.int/cps/en/natohq/news_218654.htm, accesat la 22 septembrie 2023.
16. North Atlantic Treaty Organization (14 septembrie 2023). *North Atlantic Treaty Organization*, preluat de pe https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 29 septembrie 2023.
17. North Atlantic Treaty Organization (2023). *Vilnius Summit Communiqué*, preluat de pe https://www.nato.int/cps/en/natohq/official_texts_217320.htm, accesat la 22 septembrie 2023.
18. Office for Budget Responsibility. (iulie 2022). *Office for Budget Responsibility,* preluat de pe https://obr.uk/frs/fiscal-risks-and-sustainability-july-2022/, accesat la 22 august 2023.
19. Orenstein, M. (7 iunie 2022). *Foreign Policy Research Institute*, preluat de pe https://www.fpri.org/article/2022/06/russias-use-of-cyberattacks-lessons-from-the-second-ukraine-war/, accesat la 22 septembrie 2023.
20. Pinko, E. (22 iunie 2023). *The Begin-Sadar Center for Strategic Studies*, preluat de pe https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/, accesat 15 septembrie 2023.
21. Salt, A., Sobchuk, M. (2021). *Russian Cyber-Operations in Ukraine and the Implications for NATO*. În *Canadian Global Affairs Institute*, pp. 1-7.
22. Seskuria, N. (2021). *Russia's "Hybrid Aggression" against Georgia: The Use of Local and External Tools.* Center for Strategic and International Studies .

23. Smith, B. (22 iunie 2022). *Microsoft*, preluat de pe https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/, accesat la 22 septembrie 2023.
24. Stanciu, C. (2016). *Viitorul conflictualității – operații asimetrice și hibride.* București: Editura Universității Naționale de Apărare *„Carol I"*.
25. Statista Research Department (16 ianuarie 2023). *Statista*, preluat de pe https://www.statista.com/topics/7335/information-security-and-cyber-crime-in-russia/#topicOverview, accesat la 21 septembrie 2023.
26. Umbach, F. (16 iunie 2022). *Reassessing Russia*, preluat de pe https://www.gisreportsonline.com/r/russia-cyber/, accesat la 22 august 2023.