DE LA RĂZBOIUL CIBERNETIC LA PACEA CIBERNETICĂ

FROM CYBER WARFARE TO CYBER PEACE

Colonel (rtr.) prof. univ. dr. Gheorghe BOARU*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania, email: secretariat@aosr.ro)

Rezumat: *În problemele actuale de pace și securitate s-a produs o schimbare de paradigmă în sensul că a crescut exploziv rolul progresului tehnologic și științific, în special dezvoltarea rapidă a tehnologiei informației (TI) și inteligenței artificiale (IA).*

Comunicarea științifică abordează semnificația, potențialul TI, precum și provocările pe care le prezintă în ceea ce privește pacea și securitatea.

Din punct de vedere militar, ritmul rapid al progreselor tehnologice, impune imperativ să urmărim și să ne adaptăm la peisajul în continuă evoluție și să se producă de asemenea, ajustări în structura și pregătirea forțele militare.

Argumentul central pentru care războiul cibernetic trebuie prevenit și strategiile cibernetice ofensive ale armatei și serviciilor secrete trebuie oprite, este că armele cibernetice sunt, în multe privințe, la fel de periculoase și inumane ca armele biologice și chimice, pe care comunitatea internațională le consideră deja interzise.

Problemele războiului cibernetic și păcii cibernetice sunt deschise discuțiilor, deoarece disputele privind definițiile termenilor cruciali, cum ar fi armele cibernetice sau spațiul cibernetic, sunt nerezolvate. În consecință, în vremuri de militarizare crescândă a spațiului cibernetic, aplicarea dreptului internațional la acesta este încă o provocare.

Cuvinte cheie: *război cibernetic, pace cibernetică, securitate cibernetică, arme cibernetice, spațiu cibernetic, inteligența artificială, dreptul internațional.*

Abstract: *In current peace and security issues, a paradigm shift has occurred in the sense that the role of technological and scientific progress has increased explosively, especially the rapid development of information technology (IT) and artificial intelligence (AI).*

Scientific communication addresses the significance, potential of IT, as well as the challenges it presents in terms of peace and security.

From a military point of view, the rapid pace of technological progress makes it imperative to follow and adapt to the constantly evolving landscape and also to make adjustments in the structure and training of military forces.

The central argument for preventing cyberwarfare and halting the offensive cyber strategies of the military and intelligence services is that cyberweapons are, in many ways, as dangerous and inhumane as biological and chemical weapons, which the international community already considers prohibited.

* Membru titular al Academiei Oamenilor de Știință din România; Membru titular al Academiei de Ştiinţe ale Securităţii Naţionale; E-mail: boarugheorghe@yahoo.com.

The issues of cyberwarfare and cyberspace are open to discussion, as disputes over the definitions of crucial terms such as cyberweapons or cyberspace remain unresolved. Consequently, in times of increasing militarization of cyberspace, the application of international law to it remains a challenge.

***Keywords**: cyber warfare, cyber peace, cybersecurity, cyber weapons, cyberspace, artificial intelligence, international law.*

INTRODUCERE

Progresul tehnologic și științific, în special dezvoltarea rapidă a tehnologiei informației (TI) și a inteligenței artificiale (IA), joacă un rol crucial în chestiunile legate de pace și securitate. Avansul rapid al acestor tehnologii influențează semnificativ modul în care conflictele apar, evoluează și sunt abordate în contextul global actual.

Acest articol științific abordează semnificația, potențialul TI, precum și provocările pe care le prezintă în ceea ce privește pacea și securitatea, îl introduce pe cititor în conceptele de cercetare în domeniul păcii, conflictului și securității, concentrându-se în special pe perspectivele științifice naturale, tehnice și informatice, pune în lumină conflictele cibernetice, războiul și pacea, controlul armelor cibernetice, atribuirea cibernetică, infrastructurile, inteligența artificială, precum și TIC[1] în pace și conflict.

În domenii dinamice, multe se pot schimba într-o perioadă scurtă de timp, așa cum este cazul **tehnologiilor informaționale pentru pace și securitate**. Au apărut numeroase evoluții tehnologice în domeniul securității cibernetice și al inteligenței artificiale.

Deciziile politice au afectat posibilitățile de control al armelor, de exemplu, Tratatul privind Forțele Nucleare cu Rază Intermediară de Acțiune (Tratatul INF)[2] a fost retras la scurt timp în 2019.

În ultimii ani, am văzut numeroase războaie, inclusiv invazia Rusiei în Ucraina în 2022, în urma anexării Crimeei în 2014, unde armele semi-autonome sunt din ce în ce mai des utilizate. În plus, vedem războiul Israel-Hamas, urmat de un atac condus de Hamas asupra Israelului în octombrie 2023, și politici restrictive de moderare a conținutului de către Meta pentru a reduce punctele de vedere pro-palestiniene pe Instagram și Facebook.

Este evident că TIC-urile, inclusiv rețelele sociale, exercită o influență semnificativă și joacă un rol proeminent în mediile afectate de conflicte.

Ca urmare a acestor războaie violente din întreaga lume, oamenii își părăsesc țările și folosesc TIC pentru a-și coordona și planifica migrația (fuga). Mai mult, observăm din ce în ce mai mult o tendință crescândă de campanii de dezinformare direcționate în timpul alegerilor, așa cum s-a

[1] ***TIC*** se referă la ***Tehnologia Informației și Comunicațiilor***, un domeniu esențial care cuprinde toate tehnologiile folosite pentru a gestiona și transmite informații, cum ar fi hardware-ul, software-ul, internetul și rețelele de comunicații. Acest sector joacă un rol crucial în dezvoltarea economiilor moderne, în educație, în sănătate și în aproape orice alt domeniu.

[2] Intermediate-Range Nuclear Forces Treaty (**INF** Treaty).

văzut în Brazilia în 2022, și în timpul conflictelor, orchestrate de o gamă diversă de actori.

Aceste exemple subliniază importanța cercetării tehnice în domeniul păcii și securității pentru a analiza în mod cuprinzător fenomenele relativ noi printr-o prismă interdisciplinară.

Având în vedere ritmul rapid al progreselor tehnologice, este imperativ să urmărim și să ne adaptăm la peisajul în continuă evoluție.

Conexate cu tehnologia modernă sunt și studiile privind infrastructurile critice, inteligența artificială și armele cibernetice, despre consolidarea păcii digitale, precum și despre observațiile și reflecțiile științifice pe această temă din ultimii ani.

Aceste studii sunt susținute, în multe țări europene, de ministerele de resort privind educația, cercetarea științifică, …, cu scopul de a aprofunda și dezvolta contribuția la pacea și securitatea cibernetică.

1. UN MEDIU DIGITAL MAI RESPONSABIL, ETIC ȘI SUSTENABIL

Tendința generalizată de digitalizare și dependența pe scară largă de sistemele TI declanșează, de asemenea, ajustări în forțele militare atât ca structură cât mai ales ca inzestrare și pregătire.. Pe lângă îmbunătățirile necesare ale securității TI și măsurile defensive pentru spațiul cibernetic, un număr tot mai mare de state își stabilesc capabilități militare ofensive pentru acest domeniu.

Evoluțiile și transformările istorice datorate progreselor în tehnologiile militare, precum și progresele politice realizate și instrumentele dezvoltate, corespunzător etapelor respective, au contribuit la gestionarea provocărilor și limitarea amenințărilor la adresa securității internaționale. Având în vedere acest context, putem evalua o posibilă aplicare a acestor eforturi la evoluțiile privind spațiul cibernetic, precum și obstacolele care trebuie abordate pentru a reuși.

Este obligatoriu să ținem cont de progresele politice deja în curs de desfășurare, rolul inițiativelor sociale, cum ar fi campania pentru pace cibernetică a Forumului Informaticienilor pentru Pace și Responsabilitate Socială (FIfF)[3], precum și potențialele consecințe ale probabilității crescânde a unui război cibernetic, comparativ cu perspectivele păcii cibernetice.

Aceste tipuri de forumuri sunt de obicei create pentru a adresa dilemele etice și sociale legate de tehnologie și pentru a crea un cadru de dezbatere și soluționare a problemelor cu care se confruntă societatea în era digitală. Printre temele de discuție ar putea fi:

[3] **Forumul Informaticienilor pentru Pace și Responsabilitate Socială (FIfF)** este o organizație sau o platformă destinată profesioniștilor din domeniul informaticii care își propun să contribuie la dezvoltarea unui mediu digital mai responsabil, etic și sustenabil. Scopul principal al unui astfel de forum ar fi să promoveze utilizarea tehnologiilor informaționale în moduri care să susțină pacea, drepturile omului și responsabilitatea socială.

- **Etica în tehnologie** – cum pot programatorii și inginerii să dezvolte software care respectădrepturile și libertățile individului, cum ar fi protecția datelor și confidențialitatea;
- **Impactul social al tehnologiilor** – inclusiv întrebări legate de automatizare, inteligență artificială și ce înseamnă acestea pentru locurile de muncă, educație și Securitate;
- **Responsabilitatea socială** – cum să promovăm un utilizarea echitabilă și incluzivă a tehnologiilor, reducându-se excluziunea digitală și promovând accesul universal;
- **Tehnologii pentru pace** – cum pot fi folosite tehnologiile pentru a rezolva conflicte, pentru educație în domeniul păcii sau pentru a promova valori comune de înțelegere și colaborare.

2. CÂTEVA EXEMPLE DE ATACURI CIBERNETICE

În iunie 2010, în Iran, un software rău intenționat (malware) a fost descoperit pe computerele specializate de control industrial ale unei instalații de îmbogățire a uraniului, care fusese folosit pentru a sabota instalația prin manipularea centrifugelor. Analizele programului, implementat de o unitate flash USB infectată, cunoscută acum sub numele de *Stuxnet*, au relevat că sabotajul se desfășura deja de câțiva ani și că hackerii trebuie să fi posedat abilități tehnice remarcabile și cunoștințe detaliate despre construcția instalației.

Din cauza costurilor ridicate de dezvoltare și a efortului pentru un astfel de malware capabil să atace o instalație industrială deconectată de la internet, s-a presupus că o agenție guvernamentală este forța motrice din spatele Stuxnet. Această presupunere a fost confirmată, iar Stuxnet este acum cunoscut ca fiind un proiect comun al serviciilor militare și de informații americane și israeliene[4].

Cu toate acestea, Stuxnet nu a fost primul malware despre care se presupune că a fost aplicat de un stat. De exemplu, în 2007, armata israeliană a fost acuzată de sabotarea sistemelor de apărare aeriană siriene[5]. În Estonia, serverele au fost atacate și dezactivate temporar, probabil de către activiști din Rusia cu sediul la Kremlin[6] - incidente despre care se

[4] Ellen Nakashima and Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say, The* Washington Post, June 2, 2012, disponibil la https://www.-washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, accesat la 25.08.2025; David E. Sanger, *Syria War Stirs New U.S. Debate on Cyberattacks*, New York Times, 2014; https://www.nytimes.com/2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html.

[5] David A. Fulghum, *Why Syria's Air Defenses Failed to Detect Israelis,* Aviation Week & Space Technology, October 5, 2007; disponibil la https://cyber-peace.org/wp-content/uploads/2016/11/IMRA-Friday-October-5-2007-Why-Syrias-Air-Defenses-Failed-to-Detect-Israelis.pdf, accesat la 25.08.2025.

[6] Arthur Bright, *Estonia Accuses Russia of „Cyber Attack",* Christian Science Monitor, May 17, 2007, disponibil la https://www.csmonitor.com/2007/0517/p99s01-duts.html, accesat la 25.08.2025.

spune că s-ar fi produs în timpul războiului din Caucaz din 2008, într-o formă similară[7].

Din 2010, astfel de evenimente au atras în mod repetat atenția publicului (a se vedea tabelul 1 pentru o listă extinsă de incidente rău intenționate), cum ar fi cazul din 2015, când sistemul de comunicare internă al Parlamentului Federal German, Parlakom, a fost spionat timp de luni de zile, iar documentele, detaliile de acces și comunicarea personală a deputaților și angajaților acestora au fost probabil furate. Atacul a împiedicat grav activitatea parlamentului și nu a putut fi oprit până când sistemul nu a fost închis complet în timpul pauzei de vară[8].

Alte cazuri includ atacuri de tip phishing împotriva membrilor Bundestagului german în 2021[9]. Un videoclip realizat de FIfF, în 2017, motivează discuția despre războiul cibernetic și pacea cibernetică introducând în ecuație conceptul de *„Informatica păcii”* legând studiile despre pace și conflict cu ajutorul informaticii. Argumentul lor central pentru care războiul cibernetic trebuie prevenit și strategiile cibernetice ofensive ale armatei și serviciilor secrete trebuie oprite este că armele cibernetice sunt, în multe privințe, la fel de periculoase și inumane ca armele biologice și chimice, pe care comunitatea internațională le consideră... deja interzise.

Prin urmare, armele cibernetice sunt programe malware (cum ar fi viruși, viermi și troieni), care funcționează doar atunci când se bazează pe breșe în securitatea sistemelor extraterestre, sisteme străine.

Prin urmare, armamentul cibernetic constă în principal în căutarea unor vulnerabilități potențiale în rețele, instituții și dispozitive străine sau ostile acestora sau în „crearea” acestora. Desigur, deoarece există o piață pentru orice, accesul la breșele de securitate și cunoașterea acestora pot fi, de asemenea, cumpărate, predominant în Darknet[10].

În războiul cibernetic, agresorii își folosesc controlul asupra sistemelor pentru a face rău sau a spiona partea adversă. În practică, aceasta înseamnă că orice conține un computer poate fi atacat. Astfel, fiecare PC, fiecare router și telefon și fiecare sistem de control, fie el mic sau mare, devin ținte potențiale.

---

[7] Dancho Danchev, *Coordinated Russia vs Georgia Cyberattack in Progress*, Zero Day, Aug. 11, 2008, disponibil la https://www.zdnet.com/article/coordinated-russia-vs-georgia-cyber-attack-in-progress/, accesat la 26.08.2025.

[8] Thomas Reinhold, *Maßnahmen für den Cyberpeace*, 2018, disponibil la https://cyber-peace.org/cyberpeace-cyberwar/masnahmen-fur-den-cyberpeace/, accesat la 26.08.2025.

[9] Von Frank Jansen**,** *Cyberattacke auf Bundestagsabgeordnete: Russische Hacker schicken deutschen Politikern Phishing Mails.* Tagesspiegel, 14.07.2021, disponibil la https://www.tagesspiegel.de/politik/russische-hacker-schickendeutschen-politikern-phishing-mails-6858718.html, accesat la 26.08.2025.

[10] Termenul „Darknet” se referă, de obicei, la o porțiune a internetului care nu este indexată de motoarele de căutare tradiționale și care necesită software special pentru a fi accesată. Este adesea asociată cu intimitatea, anonimitatea și, uneori, cu activități ilegale, deși are și utilizări legitime, cum ar fi activismul politic în regimuri opresive sau pentru persoanele care sunt conștiente de protecția intimității.

Dacă infrastructura noastră critică (de exemplu, sistemele de transport, instalațiile de apă, spitalele și centralele electrice) ar fi oprite sau chiar folosite împotriva noastră, consecințele și mai ales efectele în lanț ar fi la fel de devastatoare ca într-un atac cu arme convenționale, atunci când lanțurile de aprovizionare sau sistemul de transport s-ar deteriora.

Cu toate acestea, unele guverne, din întreaga lume, se înarmează pentru un război cibernetic ofensiv, inclusiv Germania, care înființează o forță cibernetică militară dedicată, numită Kommando Cyber- und Informationsraum (CIR).

O discuție societală amplă despre legalitatea transformării dispozitivelor noastre în arme care pot fi folosite împotriva noastră în orice moment nu s-a materializat încă. Cu toate acestea, FIfF menționează mai multe motive pentru care armele cibernetice ar trebui scoase în afara legii, iar banii cheltuiți pentru menținerea vulnerabilității infrastructurii critice ar trebui folosiți în schimb pentru a acoperi lacunele de securitate.

Pot concluziona cu câteva considerații importante privind domeniul cibernetic:

1. ***Armele cibernetice*** **pot fi utilizate anonim.**

În rețelele virtuale globale precum internetul, este dificil să se identifice adevăratul făptaș, deoarece acesta folosește în mare parte mai multe dispozitive pentru a executa atacul, ceea ce face imposibilă revenirea la acțiune. În plus, atacurile sunt adesea comise într-un moment care sugerează o origine diferită. Și chiar dacă se pot găsi urme ale atacului, acestea nu dovedesc nimic, deoarece sunt digitale și, prin urmare, este imposibil de spus dacă au fost lăsate intenționat sau accidental deci nu se poate face cu claritate atribuirea atacurilor cibernetice.

2. Armele cibernetice **nu pot fi controlate.**

Programele malware sunt adesea programate să aibă o existență independentă. Nu pot fi luate în considerare dacă sunt folosite intenționat ca armă sau pur și simplu activate accidental. Armele de acest tip pot rămâne latente în sisteme ani de zile înainte de a provoca vreun rău. Ceea ce distinge armele cibernetice de armele convenționale, cum ar fi armele de calibru mic, este faptul că pot fi ușor furate, reproduse la infinit și răspândite pur și simplu prin copiere și lipire.

3. Armele cibernetice **sunt scumpe.**

Armata și serviciile secrete cheltuiesc sume uriașe de bani pentru analizarea sistemelor și cumpărarea de breșe de securitate. Întrucât doar lacunele deschise pot fi folosite ca arme, cumpărătorii de informații despre acestea sunt interesați să le mențină deschise cât mai mult timp posibil. Prin urmare, sume uriașe de bani sunt cheltuite la nivel global pentru a menține infrastructura critică nesigură și vulnerabilă în mod deliberat. Bineînțeles, aceste slăbiciuni pot fi (și sunt) descoperite și exploatate zilnic de către infractori și teroriști[11].

[11] FIfF - Director, 2017, *Cyberpeace statt Cyberwar!,* disponibil la https://-peasec.de/paper/2024/2024_ReinholdReuter_FromCyberWartoCyberPeace_ITforPeaSec.pdf, accesat la 26.08.2025.

3. INCIDENTE CIBERNETICE

În ultimii 16 ani s-au produs o serie de activități cibernetice dintre care prezint o listă cu cele mai relevante incidente cibernetice cu o probabilă influență de către unii actori statali sau nestatali.

Presupusul actor se bazează în mare parte pe informații publicate de agențiile de informații sau de aplicare a legii. Dovezile care stau la baza acestora au fost rareori dezvăluite și a trebuit să se ia în considerare faptul că astfel de acuzații pot avea și motivație politică. De asemenea, este important de menționat că distincția dintre activitățile de piraterie informatică ale unui stat și ale instituțiilor sale și grupurile nestatale care nu sunt direct conectate la un stat, dar se află sub controlul său indirect, este greu de făcut.

Tabelul 1[12] Lista incidentelor cibernetice relevante cu actori probabil statali sau influențați de stat

Anul	Presupusul actor	Descrierea incidentului cibernetic
2007	Rusia	Atacul cibernetic asupra site-urilor web ale guvernului și ale altor instituții, bănci și ministere din Estonia, care a împiedicat accesul la acestea, este adesea considerat primul atac cibernetic semnificativ condus de stat. Rusia a negat orice implicare oficială, iar atacul a fost atribuit unei organizații patriotice de tineret rusești.
2008	Rusia	Atacurile cibernetice împotriva site-urilor web din Georgia și Osetia de Sud în timpul conflictului militar cu Rusia au împiedicat funcționarea platformelor de informații publice și a serviciilor media. Aceste incidente sunt adesea considerate a fi primele încercări de utilizare a capacităților cibernetice ca mijloc în conflictele militare.
2010	SUA / Israel	Programul malware Stuxnet a fost folosit pentru a sabota în mod silențios programul nuclear iranian. Timpul său de dezvoltare și implementare, probabil lung, care a implicat informații specifice despre sistemele industriale vizate, a reprezentat o „revelație” internațională asupra modului în care statele utilizează atacurile cibernetice în scopuri de politică externă.
2012	Iran	Un malware numit Shamoon/Wiper a fost folosit împotriva companiilor petroliere industriale din Arabia Saudită. Malware-ul fusese dezvoltat în mod explicit pentru a se răspândi rapid în rețelele infectate și a face computerele vizate inutile prin ștergerea fișierelor relevante ale sistemului de operare. Acesta a afectat până la 30.000 de sisteme IT.
2012	SUA / Israel	Programul malware Flame a fost utilizat în Orientul Mijlociu în scopuri de spionaj și informații, în special în Iran, Israel, Palestina, Liban și Arabia Saudită. A fost considerat a fi cea mai versatilă dezvoltare de malware de până

[12] Christian Reuter (editor), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace (Technology, Peace and Security I Technologie, Frieden und Sicherheit),* Publisher: Springer Vieweg; Second Edition 2024, Year: 2024, pp. 145-147.

		acum, cu o vastă varietate de module pentru a infecta diferite sisteme IT și a efectua multiple sarcini asupra acestora. Prin urmare, Flame este văzut ca primul „framework multifuncțional pentru atacuri cibernetice” dezvoltat de stat.
2013	China	Un raport al companiei de securitate IT Mandiant, cu sediul în SUA, a analizat mai multe atacuri cibernetice pe termen lung și a dezvăluit existența unei forțe cibernetice militare în China, pe baza analizelor criminalistice IT. Unitatea „PLA 61.389” fusese acuzată de atacuri de spionaj cu arme cibernetice personalizate.
2014	Israel	Campania de malware Duqu 2.0 a fost utilizată în scopuri de spionaj, cu mecanisme de camuflare deosebit de versatile. Este probabil o dezvoltare și o extindere ulterioară a versiunilor anterioare care au fost detectate în 2011.
2014	Palestine	XtremeRAT a fost o campanie de malware de tip spear-phishing în contextul conflictelor din Orientul Mijlociu, pe care un grup de activiști palestinieni a folosit-o pentru spionaj și furt de date.
2015	SUA	Grupul Equation este numele unei campanii de malware cu o infrastructură și o bază tehnologică extrem de complexe. Campania a fost activă timp de mai mulți ani, primele indicii fiind din 1996. Instrumentele sale extrem de dezvoltate și framework-urile de malware au fost dezvoltate și extinse de-a lungul anilor și au asemănări cu incidente precum Stuxnet și Flame.
2015	Rusia	În contextul conflictului din Ucraina de Vest, Rusia a fost acuzată de atacuri împotriva companiilor energetice ucrainene, care au oprit furnizarea de energie electrică pentru aproximativ 700.000 de locuitori timp de câteva ore. Programele malware BlackEnergy și Killdisk au fost folosite pentru a obține acces și a închide sistemele IT.
2016	Rusia	În pregătirile pentru alegerile prezidențiale din SUA din 2016, au fost efectuate atacuri cibernetice împotriva Comitetului Național Democrat, care au dus la o gravă încălcare a securității datelor. Ulterior, unele dintre documente au fost divulgate. Atacul cibernetic este considerat o interferență severă și de lungă durată în procesul electoral democratic din SUA. Până la sfârșitul anului 2018, anchetele au fost încă în desfășurare.
2016	SUA/ Marea Britanie	Israelul a dezvăluit că serviciile de informații americane și britanice au interceptat în mod secret fluxuri video în timp real de la drone militare și avioane de vânătoare israeliene. Eforturile lor de supraveghere s-au concentrat pe monitorizarea activităților militare din Gaza, anticiparea oricăror potențiale acțiuni israeliene împotriva Iranului și urmărirea exportului global de tehnologie israeliană pentru drone.
2017	Iran	Un malware care viza anumite sisteme de control industrial (SCADA) a fost implementat împotriva companiilor petrochimice saudite. Acesta fusese special conceput pentru a declanșa daune fizice și distrugerea acestor instalații, deși acest lucru nu s-a întâmplat niciodată din cauza unor erori de programare.
2017	Coreea de Nord	După dezvăluirea exploit-ului fatal zero-day EternalBlue, care fusese furat de la NSA și afectase sistemele Microsoft Windows, a fost implementat un malware numit WannaCry care a folosit această realizare remarcabilă. Acesta s-a răspândit masiv în întreaga lume și i-a obligat pe utilizatorii afectați să ceară răscumpărare prin criptarea hard disk-urilor lor.

2018	Rusia	În primăvara anului 2018, a fost publicat un atac de hacking împotriva sistemelor și rețelelor IT guvernamentale germane. Atacul fusese activ, dar ascuns timp de mai bine de un an și fusese efectuat cu mare atenție - fără replicare automată sau infectarea sistemelor IT. Scopul său principal fusese probabil spionajul.
2018	Iran	Departamentele de Justiție și Trezorerie ale SUA au pus sub acuzare Iranul, susținând furtul de proprietate intelectuală de la peste 300 de universități, pe lângă agenții guvernamentale și firme de servicii financiare.
2019	Coreea de Nord	În februarie 2019, Biroul 121 din Coreea de Nord a atacat Banca din Valletta, Malta, încercând să fure 14,5 milioane de dolari prin atacuri de tip phishing.
2019	China	Corporația aerospațială europeană Airbus a dezvăluit că a fost victima unor atacuri cibernetice chineze care au dus la furtul de date de identificare personale și IT aparținând mai multor membri ai personalului său european.
2020	Iran	În timpul pandemiei de COVID-19, hackerii susținuți de guvernul iranian au depus eforturi pentru a infiltra conturile personalului care lucrează pentru Organizația Mondială a Sănătății (OMS)
2020	China	Autoritățile americane au susținut că hackerii asociați cu guvernul chinez au încercat să fure cercetări americane legate de un vaccin împotriva coronavirusului.
2021	Coreea de Nord	Hackerii guvernului nord-coreean s-au angajat într-o campanie complexă de inginerie socială împotriva cercetătorilor în securitate cibernetică, utilizând conturi false de Twitter (redenumite X) și un blog fals pentru a atrage țintele să viziteze site-uri web infectate sau să deschidă atașamente de e-mail compromise. Aceștia și-au abordat țintele sub pretextul colaborării la un proiect de cercetare, campania concentrându-se pe persoane asociate cu Centrul pentru Studii Strategice și Internaționale (CSIS) din Washington, D.C. 2023
2021	China	Norvegia a indicat China ca fiind sursa unui atac cibernetic asupra sistemului său de e-mail parlamentar în martie 2021.
2022	Iran	Hackerii susținuți de guvernul iranian s-au infiltrat în Consiliul de Protecție a Sistemelor Merit din SUA, exploatând vulnerabilitatea log4shell încă din februarie 2022. În urma brеșei, acești hackeri au instalat software de minare a criptomonedelor și au implementat programe malware pentru a obține date sensibile.
2023	China	Autoritățile din SUA și Japonia au emis avertismente, afirmând că hackeri sponsorizați de statul chinez au introdus software de manipulare în routere pentru a viza agenții guvernamentale, industrii și companii din ambele națiuni. Acești hackeri folosesc implanturi de firmware pentru a menține o prezență secretă și a naviga în rețelele țintelor lor. China a negat aceste acuzații.
2023	Rusia	Rusia intensifică atacurile cibernetice împotriva agențiilor ucrainene de aplicare a legii, în special a unităților care colectează și analizează dovezi ale crimelor de război rusești, potrivit oficialilor ucraineni. Atacurile cibernetice rusești au vizat în primul rând infrastructura ucraineană pentru cea mai mare parte a războiului

4. MILITARIZAREA SPAȚIULUI CIBERNETIC

De la descoperirea Stuxnet, termenul de război cibernetic – derivat din război ca conflict militar între state și termenul de spațiu cibernetic – a fost inventat în legătură cu incidente de acest tip. Cu toate acestea, acesta neglijează o distincție vitală care trebuie luată în considerare atunci când se gestionează și se interpretează astfel de evenimente: dacă inițiatorii unui atac cibernetic nu au fost ordonați direct de un guvern, atacul în cauză este o infracțiune „normală", care ține de urmărirea penală națională și internațională și de cooperarea polițienească.

Aceste acorduri multilaterale există deja, cum ar fi Convenția de la Budapesta privind criminalitatea cibernetică emisă în 2001 (Consiliul Europei, 2001). Numai odată ce un guvern este presupusul atacator, interpretarea incidentului privește nivelul politic și devine relevantă în dreptul internațional. Aici, trebuie făcută o distincție critică cu privire la o reacție adecvată: Avem de-a face cu un spionaj al serviciilor de informații, care vizează în principal confidențialitatea unui sistem (ar trebui analizat domeniul *„Spionaj cibernetic și apărare cibernetică"),* cu un sabotaj, cu scopul de a distruge un sistem sau cu activități militare direcționate către obiective strategice clare? În acest scop, trebuie să analizăm daunele deja provocate. În funcție de intenția atacatorului și de malware-ul aplicat, gama poate merge de la un simplu furt la oprirea temporară a unui serviciu IT până la daune specifice sistemelor IT și subordonate[13].

Întrebările privind războiul cibernetic depășesc aspectul pur tehnic al întreținerii sistemelor IT sau al atacurilor asupra acestor sisteme. Pe lângă aspectele de apărare și ofensivă și instrumentele necesare, doctrinele politice de securitate și strategice militare ale statelor joacă un rol semnificativ. Acestea determină în ce măsură un stat identifică spațiul cibernetic ca domeniu militar și cum îl tratează conform măsurilor luate de alte state.

De câțiva ani, cel târziu de la descoperirea Stuxnet, guvernele au perceput din ce în ce mai mult spațiul cibernetic ca pe un domeniu militar. Conform unui studiu realizat de Institutul Națiunilor Unite pentru Cercetarea Dezarmării (UNIDIR)[14], cel puțin 47 de state au operat programe cibernetice militare în 2013, dintre care zece națiuni aveau o intenție nominal ofensivă - o situație care probabil se va fi schimbat de atunci. Constatăm că, în 2012, Barack Obama, fiind președintele SUA la acea vreme, și-a instruit liderii militari și ai serviciilor secrete să creeze o listă cu cele mai critice ținte militare potențiale din spațiul cibernetic și să dezvolte soluții pentru perturbarea acestor ținte până la distrugerea lor[15].

---

[13] Gary D. Brown and Owen W. Tullos, *On the Spectrum of Cyberspace Operations,* Small Wars – Journal, Dec 11, 2012; SSRN, disponibil la https://ssrn.com/abstract-=2400536 or.http:// dx.doi.org/ 10.2139/ssrn.2400536, accesat la 27.08.2025.

[14] **UNIDIR** - United Nations Institute for Disarmament Research.

[15] Pentru detalii suplimentare, se poate consulta articolul original de la The Guardian: *Obama orders US to draw up overseas target list for cyber-attacks*, disponibil la https://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas, accesat la 27.08.2025.

Președintele Barack Obama a emis în octombrie 2012 o directivă de politică prezidențială denumită sub acronimul PPD-20 (Presidential Policy Directive 20). Documentul, intitulat complet "U.S. Cyber Operations Policy", a fost clasificat, dar unele informații au fost făcute publice în 2013 prin dezvăluirile lui Edward Snowden[16]. Această directivă a fost emisă în contextul în care SUA se confruntau cu amenințări cibernetice tot mai sofisticate, inclusiv atacuri atribuite unor actori statali precum China.

PPD-20 a subliniat importanța integrării operațiunilor cibernetice în strategia națională de securitate, alături de opțiunile diplomatice și militare tradiționale. Cu toate acestea, autorizațiile acordate pentru atacuri cibernetice ofensive fără consimțământul altor state au ridicat întrebări legate de legalitatea și etica unor astfel de acțiuni.

Consecințele acestei directive prezidențiale au devenit evidente în ceea ce privește oportunitățile de spionaj și manipulare cibernetică dezvăluite în 2013, pe care Agenția Națională de Securitate (NSA)[17] le dezvolta în SUA. Aceasta a fost distribuită parțial ca agenți digitali camuflați în produse comerciale. În mod tradițional, NSA este subordonată liderului comandamentului cibernetic al SUA, adică forțelor cibernetice ofensive ale forțelor armate americane, care au, prin urmare, acces direct la tehnologiile NSA.

În Comunicatul Summitului de la Varșovia din 2016, NATO a integrat apărarea în spațiul cibernetic în apărarea colectivă, conform articolului 5 din Tratatul Atlanticului de Nord. Prin urmare, evaluează și atacurile cibernetice și aspectul agresiunii militare.

Forțele CNO[18] sunt alocate unității organizaționale a comandamentului strategic de recunoaștere. Sarcina acestei unități este accesul ofensiv la sistemele IT străine.

În context militar sau de securitate cibernetică, CNO se referă la ansamblul activităților desfășurate în rețele informatice, împărțite în trei mari categorii:

1.CNA (Computer Network Attack) – atacuri asupra sistemelor informatice pentru a perturba, degrada, distruge sau manipula date și funcționarea sistemelor țintă;

2.CND (Computer Network Defense) – apărare activă sau pasivă a rețelelor proprii împotriva atacurilor sau intruziunilor;

3. CNE (Computer Network Exploitation) – exploatarea sistemelor străine pentru colectarea de informații, adesea fără a altera sistemele vizate.

Așadar, în contextul enunțului de mai înainte, forțele CNO alocate comandamentului strategic de recunoaștere se ocupă în principal de accesul ofensiv la sisteme IT străine, ceea ce corespunde componentei CNE

[16] Edward Snowden nu a publicat o „lucrare” în sens academic, dar informațiile la care ne-am referit provin din documentele clasificate ale guvernului SUA pe care el le-a dezvăluit în 2013, în special prin intermediul jurnaliștilor Glenn Greenwald, Laura Poitras și publicații ca *The Guardian* și *The Washington Post*.

[17] NSA - National Security Agency.

[18] CNO - **Computer Network Operations** (Operațiuni în Rețele de Calculatoare).

(Computer Network Exploitation), dar ar putea include și CNA, în funcție de misiune.

Un exemplu edificator este Germania. Cu toate acestea, acestea se antrenează în prezent în rețele de antrenament închise și nu au fost încă utilizate, conform anunțurilor oficiale (Comitetul de Apărare al Parlamentului Federal German, 2016). La sfârșitul anului 2017, Ministerul Federal al Apărării a integrat oficial unitățile organizaționale ale Forțelor Armate Federale care se ocupă de IT și spațiul cibernetic într-o unitate organizațională separată.

„Spațiul cibernetic și informațional” este format din 16.000 de angajați și are un nivel organizațional comun cu ramurile serviciului militar al Armatei, Marinei, Forțelor Aeriene și Serviciului Medical conform informațiilor Ministerului Federal al Apărării din Germania.

Ministerul Apărării al Germaniei a anunțat în aprilie 2016 planurile de înființare a unei noi ramuri militare, denumită „*Cyber și Informațională”* (Cyber- und Informationsraum - CIR), pentru a consolida apărarea cibernetică a Bundeswehr-ului. Această structură a fost activată la 1 aprilie 2017 și a fost echivalată cu celelalte ramuri tradiționale ale armatei. Inițial, CIR a fost format din 13.500 de posturi, provenind din alte ramuri ale armatei, și a fost condusă de un inspector cu rang de general-locotenent. Planurile de dezvoltare vizau atingerea unui efectiv de 16.000 de persoane până în 2021. În 2022, efectivul a ajuns la aproximativ 15.000 de militari și civili[19].

În plus, unitatea CNO a fost transformată într-un Centru pentru Operațiuni de Rețea și extinsă cu 20 de posturi. Datorită informațiilor necesare privind țintele relevante din spațiul cibernetic, se presupune că aceasta cooperează mai strâns cu serviciul federal de informații.

Orientările strategice ale Cărții Albe arată că aceste măsuri de restructurare sunt legate de posibilități îmbunătățite de apărare, precum și de o orientare strategică ofensivă impusă a Forțelor Armate Federale în spațiul cibernetic: *„Capacitatea acțiunii comune a Forțelor Armate Federale în toate dimensiunile este criteriul superior de referință”* și *„o superioritate a impactului trebuie atinsă la toate nivelurile de intensitate”*.

Pentru a atinge acest obiectiv, Ministerul Federal al Apărării, în cooperare cu Ministerul Federal de Interne, Construcțiilor și Patriei, a fondat o nouă agenție pentru inovații în securitatea IT, care ar trebui să ia exemplu din Agenția pentru Proiecte de Cercetare Avansată în Apărare din SUA (DARPA)[20].

Sarcina acestei agenții este de a iniția, promova și finanța proiecte de cercetare și inovare în domeniul securității cibernetice, în special *„soluțiile de securitate IT de mâine”* conform Ministerului Federal al Apărării din

[19] en.wikipedia.org, Defense News, Deutsche Welle.
[20] **DARPA** - Defense Advanced Research Projects Agency.

Germania, 2016. Pentru perioada 2019-2022, agenția ar fi putut cheltui un total de aproximativ 200 de milioane de euro[21].

Militarizarea crescândă a spațiului cibernetic prezintă mai multe provocări în domeniile dreptului internațional și politicii de securitate pentru societatea internațională și statele individuale, la care se va face referire în abordările următoare.

Războiul rus împotriva Ucrainei, care a început în februarie 2022, a arătat pentru prima dată un conflict militar deschis, care a fost însoțit și de activități puternice în spațiul cibernetic[22]. Pe lângă aceasta, așa cum s-a arătat în Tabelul 1 de mai înainte, au existat destul de multe incidente rău intenționate - cu obiective și magnitudini diferite. Acest lucru sugerează posibilele domenii de aplicare și consecințe ale viitorului război cibernetic și, prin urmare, relevanța (crescătoare) a subiectului.

5. DREPTUL INTERNAȚIONAL ÎN SPAȚIUL CIBERNETIC

În ceea ce privește regulile stabilite de operare internațională, se pune întrebarea cum pot fi acestea aplicate în spațiul cibernetic. Dificultatea lămuririi acestui subiect devine deja evidentă odată cu discuțiile privind o definiție comună a spațiului cibernetic: în timp ce standardele tehnice ghidează înțelegerea SUA și a Europei de Vest și acoperă numărul de sisteme IT și infrastructura de rețea a acestora, astfel încât securitatea se referă în primul rând la integritatea acestor sisteme, alte țări precum Rusia sau China consideră informațiile, care sunt salvate, transmise și publicate în acestea, ca parte a spațiului cibernetic. Drept urmare, securitatea, în special la nivel național, depășește integritatea sistemelor tehnice și devine o problemă de control și acces la aceste informații - un punct de vedere dificil de reconciliat cu principiile drepturilor omului[23].

---

[21] Prin comparație, bugetul DARPA din 2018 a fost de 3,17 miliarde de dolari. Deși este necesar să menționăm că DARPA are o gamă mult mai largă de cercetări. Vezi https://www.darpa.mil/about-us/buget.

[22] Thomas Reinhold and Christian Reuter, *Zur Debatte über die Einhegung eines Cyberwars: Analyse militärischer Cyberaktivitäten im Krieg Russlands gegen die Ukraine*, Zeitschrift für Friedens- und Konfliktforschung, 2023, 12 (1), pp. 135–149, disponibil la https://doi.org/10.1007/s42597-023-00094-y, accesat la 27.08.2025.

[23] Fragmentul citat provine din *„Rezoluția 66/24 a Adunării Generale a Organizației Națiunilor Unite”*, adoptată la 3 noiembrie 2011, intitulată *„Promovarea și protecția drepturilor omului în contextul securității naționale”*. (A/RES/66/24). Această rezoluție subliniază importanța echilibrului între măsurile de securitate națională și respectarea drepturilor fundamentale ale omului. Rezoluția abordează preocupările legate de utilizarea excesivă a măsurilor de securitate care pot afecta drepturile civile și politice ale indivizilor, inclusiv dreptul la viață privată, libertatea de exprimare și dreptul la un proces echitabil. De asemenea, subliniază necesitatea ca statele să adopte măsuri de securitate care să fie proporționale, necesare și conforme cu obligațiile internaționale în domeniul drepturilor omului. În contextul tehnologic actual, această rezoluție este relevantă pentru discuțiile privind protecția datelor personale, supravegherea digitală și accesul autorităților la informațiile private ale cetățenilor. Ea pune în evidență tensiunea între necesitatea de a asigura securitatea națională și protejarea drepturilor fundamentale ale individului. Pentru a consulta textul integral al rezoluției, se poate accesa site-ul oficial al Națiunilor Unite.

5.1. Manualul Tallinn

Experții convocați de Centrul de Excelență pentru Apărare Cibernetică Cooperativă al NATO (CCDCOE- **C**ooperative **C**yber **D**efense **C**entre **o**f **E**xcellence) au încercat pentru prima dată să rezolve această problemă în 2013 cu așa-numitul *Manual Tallinn*, un manual care include 95 de linii directoare pentru națiuni în cazul unui război cibernetic. Chiar dacă nu este obligatoriu, acesta evidențiază caracteristicile specifice ale spațiului cibernetic în care se aplică dreptul internațional (NATO CCDCOE, 2013) și indică modul în care dreptul internațional poate fi interpretat pentru conflictele militare din acest nou domeniu. În 2017, CCDCOE a publicat o a doua versiune a manualului, intitulată *„Manualul Tallinn 2.0 privind dreptul internațional aplicabil operațiunilor cibernetice”* (NATO CCDCOE, 2017), care continuă această evaluare, în special a comportamentului statelor, precum și a regulilor și normelor în timp de pace.

5.2. Natura virtuală a spațiului cibernetic

Provocarea centrală constă în **virtualitatea spațiului cibernetic**, care subminează abordările și reglementările bazate pe frontiere teritoriale sau pe localizarea mijloacelor militare. La fel de problematice sunt imaterialitatea programelor malware, precum și posibilitatea nelimitată de a le reproduce. În plus, datorită structurii spațiului cibernetic și principiilor de transmitere a datelor, este ușor să acționezi în secret sau să ascunzi originea reală a unui atac utilizând servere proxy sau alte sisteme IT străine piratate și exploatate, ceea ce duce la problema atribuirii. În plus, sistemele IT sunt adesea extrem de interconectate și controlează direct sau indirect procesele așa-numitelor infrastructuri critice, cum ar fi alimentarea cu energie electrică sau apă, comunicațiile sau traficul.

Prin urmare, deteriorarea sistemului IT al unei națiuni poate avea consecințe potențial incalculabile, cu impacturi grave asupra unor ținte neintenționate inițial. Deoarece accesul ascuns la sistemele IT în scopul spionajului sau evaluării situației militare este adesea legat de aplicarea de programe malware și manipularea funcțiilor sistemului IT, pragul pentru astfel de amenințări este superficial.

În ceea ce privește conceptele centrale ale dreptului internațional, aceste caracteristici ale spațiului cibernetic ridică o serie de probleme. De exemplu, aceasta se referă la acordul internațional privind nonviolența și dreptul la autoapărare conform articolului 2, paragraful 4, și articolului 51 din *Carta ONU*, precum și la principiile de adecvare și proporționalitate a reacțiilor militare: Ce înseamnă „utilizarea forței” în spațiul cibernetic? Când sunt considerate „arme” programele malware și diverse instrumente și metode de atac cibernetic? Când vorbim despre un „atac armat”?

Abordările anterioare de aplicare a acestor concepte în spațiul cibernetic se referă de obicei la consecințele armelor clasice, cinetice, pentru a evalua incidente cibernetice specifice și posibile reacții legitimate de dreptul internațional. Astfel, Manualul Tallinn definește atacurile armate în spațiul cibernetic ca fiind *„activități cibernetice care duc în mod proxim la*

deces, vătămări corporale sau distrugeri semnificative" (NATO CCDCOE, 2013).

5.3 Caracteristicile aplicării programelor malware

O astfel de abordare, însă, este insuficientă, deoarece nu ia în considerare suficient faptul că amploarea, momentul și forma daunelor provocate de atacurile cibernetice nu sunt comparabile cu armele convenționale în multe privințe:

• În primul rând, este posibil ca programele malware să se răspândească necontrolat dincolo de rețelele IT și să afecteze sisteme externe care nu au fost ținta atacului și care aparțin, eventual, unei națiuni neimplicate. De exemplu, versiuni inactive ale Stuxnet au fost descoperite pe zeci de mii de sisteme din întreaga lume[24]. Aplicarea programelor malware care operează în secret pe o perioadă mai lungă de timp sau utilizează metode indirecte de manipulare a subsistemelor și, prin urmare, nu provoacă daune direct vizibile și atribuibile, este la fel de problematică.

• În plus, tendința actuală către tehnologiile cloud complică și mai mult localizarea geografică a sistemelor IT, deoarece datele electronice sunt procesate și stocate nu pe un singur computer, ci posibil pe diverse astfel de sisteme care sunt adesea distribuite la nivel global.

Legată de aceasta este așa-numita problemă a atribuirii („Atribuirea atacurilor cibernetice"): Dreptul la autoapărare al fiecărei națiuni implică faptul că originea unui atac la care națiunea este obligată să reacționeze prompt trebuie să fie clară. În spațiul cibernetic, însă, așa cum s-a menționat mai sus, este o practică obișnuită efectuarea de atacuri din sisteme externe deturnate special în acest scop pentru a acoperi sursa. În consecință, urmărirea acestor atacuri prin mai multe etape nu poate fi efectuată într-un mod prompt și fiabil din punct de vedere criminalistic.

Limitarea particulară a utilizării militare permise a programelor malware se dovedește a fi la fel de dificilă. De obicei, instrumentele, metodele și software-ul IT utilizate de infractori, experți în securitate IT și forțe militare pentru a accesa sistemele IT sunt abia distincte. Cu toate acestea, în funcție de intenție, utilizarea lor are rezultate foarte diferite: De exemplu, dezvăluirea, analiza și remedierea punctelor slabe (expert în securitate IT), furtul datelor cardului de credit (infractori) sau perturbarea sau distrugerea unui sistem militar, cum ar fi un program de monitorizare a aerului (militar). Pe lângă instrumente, identificabilitatea agenților statali sau militari, termenul de combatanți în spațiul cibernetic și distincția lor de civili sunt greu de realizat cu tehnologiile actuale. Cu toate acestea, astfel de etichete sunt esențiale pentru a gestiona agenții în situații de criză și de război.

Grupuri de experți dezbat aceste chestiuni în cadrul Organizației Națiunilor Unite și al Organizației pentru Securitate și Cooperare în Europa

[24] Chien, E., Falliere, N. and Murchu, L.O. (2011). W32, *Stuxnet Dossier*; disponibil la https://symantec-enterprise-blogs.security.com/threat-intelligence/stuxnet-dossier-espionage, accesat la 28.08.2025.

(OSCE). Cu toate acestea, nu putem încă vedea abordări specifice pentru reglementări internaționale obligatorii în spațiul cibernetic, în special în ceea ce privește „dreptul la război" (jus ad bellum) și „legile războiului" (jus in bello).

6. CAMPANIA „CYBER PEACE"

În campania lui pentru pacea cibernetică „Cyberpeace", Forumul Informaticienilor pentru Pace și Responsabilitate Socială (Forum of Computer Scientists for Peace and Societal Responsibility, 2014), folosește un simbol interesant - vezi Fig.1. Forumul solicită încetarea tuturor operațiunilor militare pe internet prin creșterea gradului de conștientizare cu privire la astfel de pericole pentru, printre altele, confidențialitatea individuală și drepturile omului.

Potrivit Forumului, cea mai mare amenințare constă în defecte (neraportate) și lacune din interiorul sistemelor IT utilizate pentru atacuri cibernetice. Deoarece astfel de atacuri pot fi cu greu controlate, ele ar putea afecta părțile civile și infrastructurile critice care furnizează energie, apă, comunicații și sănătate, precum și alte sisteme IT cu posibile lacune de securitate. În special atacurile cibernetice guvernamentale, care pot folosi cele mai multe resurse și influență, pot slăbi aceste sisteme și pot amenința funcționarea societății și chiar viața umană.

Forumul cere ca toate armele cibernetice să fie abolite prin crearea unor acorduri internaționale obligatorii privind controlul armelor, dezarmarea și renunțarea la dezvoltarea și utilizarea armelor cibernetice pentru acțiuni ofensive la nivel guvernamental. În același timp, internetul ar trebui să funcționeze ca o resursă civilă și pașnică, fără a fi folosit abuziv pentru spionarea civililor. Legat de aceasta, conceptul de suspiciune generală ar trebui abandonat și înlocuit cu obținerea de dovezi de încredere.

Pragul pentru activitățile militare este mai scăzut la nivel cibernetic, deoarece nu creează impresia unui război real, ceea ce face necesară desființarea tuturor armelor cibernetice. Aceasta implică extinderea acordurilor existente, cum ar fi Convenția de la Geneva, la spațiul cibernetic.

În special când este vorba de infrastructuri critice care garantează furnizarea de bunuri și servicii existențiale, a căror eșec poate amenința vieți omenești, perturbarea lor din exterior ar trebui tratată ca o crimă de război. Toți operatorii de infrastructuri critice ar trebui să fie obligați să își asigure și să protejeze sistemele de atacuri în mod independent și transparent și, dacă este posibil, să le detașeze de internet pentru a preveni accesul infractorilor. În același timp, guvernele ar trebui să instituie o inițiativă obligatorie la nivel internațional în spațiul cibernetic pentru a proteja internetul ca infrastructură critică și pentru a sprijini cercetarea și dezvoltarea strategiilor de pace.

Utilizarea armelor convenționale ca reacție la un atac cibernetic contrazice în egală măsură politica pașnică a Forumului. Din cauza problemei atribuirii, sursa unui atac cibernetic nu poate fi identificată. Prin

urmare, armele convenționale ar putea provoca o escaladare militară fără un set solid de dovezi.

Cu toate acestea, națiunile sunt îndemnate să urmeze o strategie defensivă pentru a-și proteja sistemele IT împotriva atacurilor cibernetice și, prin urmare, să li se permită să utilizeze instrumente (de hackeri) pentru apărare și expunerea lacunelor de securitate existente.

Figura1. Logo-ul campaniei Cyberpeace[25].

Astfel de lacune de securitate, odată identificate, ar trebui raportate oficial, în special pentru sistemele IT publice și corporative, și închise înainte de a putea fi exploatate, în loc să fie lăsate deschise pentru serviciile de informații sau forțele armate. În consecință, conștientizarea publicului și încrederea în strategiile cibernetice defensive vor crește. În plus, pentru a preveni apariția unor astfel de deficiențe, securitatea ar trebui să fie un aspect central pentru arhitectura computerelor, sistemelor de operare, infrastructurilor și rețelelor. Sistemele educaționale ar trebui să promoveze educația în jurul competențelor IT și al importanței acestora pentru societate pentru a crește numărul de experți calificați, a îmbunătăți securitatea și calitatea sistemelor IT și a revigora discuțiile pe teme etice și politice legate de tehnologie.

Transparența și democrația sunt alte aspecte centrale ale campaniei. Prin promovarea oficială a dezvoltării independente și transparente, a examinării și a analizei de risc a software-ului, breșele de securitate pot fi identificate și prevenite în mod deschis, crescând securitatea, în special pentru infrastructurile critice.

În plus, în loc să fie domeniul serviciilor secrete și al companiilor de consultanță militară, strategiile și atacurile de securitate cibernetică ar trebui confirmate oficial și discutate deschis pentru a fi incluse în procesul decizional democratic. Întrucât libertatea de exprimare și de întrunire sunt

[25] Christian Reuter (editor), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace (Technology, Peace and Security I Technologie, Frieden und Sicherheit),* Publisher: Springer Vieweg; Second Edition 2024, Year: 2024, p. 161.

drepturi fundamentale ale omului, ele ar trebui respectate în mod egal în spațiul cibernetic și nu ar trebui să justifice urmărirea penală sau activitățile militare. Pentru a contribui în continuare la protejarea drepturilor omului, ar trebui înființate centre de securitate cibernetică independente și reglementate democratic pentru a preveni atacurile cibernetice și a stabili pacea cibernetică.

Ca instrument esențial pentru formarea opiniei publice, discuțiile despre spațiul cibernetic în mass-media și politică ar trebui să urmeze termeni definiți și să nu fie folosite pentru a induce în eroare și a alimenta conflictele. Prin urmare, Forumul oferă și definiții pentru o mai bună înțelegere a termenilor legați de spațiul cibernetic.

7. RĂZBOIUL CIBERNETIC ȘI PACEA CIBERNETICĂ – MĂSURI LA NIVELUL ROMÂNIEI

Războiul cibernetic se referă la utilizarea atacurilor informatice coordonate pentru a perturba, deteriora sau distruge infrastructuri informatice și rețele esențiale, în scopuri militare, politice sau economice. România, ca stat membru al Uniunii Europene și NATO, este conștientă de riscurile tot mai mari din spațiul cibernetic și a adoptat o serie de măsuri pentru a-și proteja securitatea națională și a promova pacea cibernetică.

7.1. Cadrul legislativ și instituțional

România a dezvoltat un cadru legislativ și instituțional pentru a preveni și gestiona amenințările cibernetice:

- Legea securității cibernetice (în proces de actualizare): reglementează protejarea rețelelor și sistemelor informatice de interes național;

- CERT-RO (Centrul Național de Răspuns la Incidente de Securitate Cibernetică): monitorizează, analizează și reacționează la incidentele cibernetice;

- Directoratul Național de Securitate Cibernetică (DNSC): creat în 2021, are rolul de coordonare strategică și operativă în domeniul securității cibernetice;

- SRI – Centrul Național Cyberint: responsabil pentru combaterea amenințărilor cibernetice la adresa securității naționale.

7.2. Colaborarea internațională

- România participă activ în inițiativele NATO privind apărarea cibernetică, inclusiv în exerciții precum **Locked Shields** și **Cyber Coalition**.

- Contribuie la dezvoltarea politicilor de **diplomație cibernetică** în cadrul UE și susține **Codul de conduită responsabilă în spațiul cibernetic** promovat de ONU.

7.3. Capacități de apărare cibernetică

-Armata României dezvoltă componente dedicate războiului cibernetic, inclusiv în cadrul **Comandamentului Apărării Cibernetice**.

- Înființarea unui **centru de excelență în securitate cibernetică** la București, numit **Centrul European de Competențe în domeniul Securității Cibernetice** (EU Cyber Centre), oferă României un rol cheie în dezvoltarea politicilor europene de apărare cibernetică.

7.4. Educație și conștientizare

- Inițiative precum **CyberSmart**, parteneriate între universități, DNSC și sectorul privat promovează alfabetizarea cibernetică.

- Dezvoltarea de programe educaționale în securitate cibernetică în licee și universități tehnice (ex: Politehnica București, Universitatea Babeș-Bolyai).

7.5. Parteneriate public-private

- Colaborarea dintre autorități și companii private din IT&C este esențială pentru detectarea rapidă a amenințărilor și schimbul de informații.

- Inițiative precum **Cyberintelligence4Gov** sau **Forumurile DNSC** ajută la coagularea unui front comun împotriva amenințărilor cibernetice.

7.6. Concluzie

România este activ implicată în combaterea războiului cibernetic și în promovarea păcii cibernetice, prin politici interne solide, colaborări internaționale și investiții în educație și tehnologie. Continuarea acestor eforturi este esențială pentru protejarea intereselor naționale și menținerea stabilității în regiune.

CONCLUZII

Răspunsul la întrebarea inițială depinde în mod esențial de conceptele care stau la baza războiului cibernetic și păcii cibernetice. Acestea sunt deschise discuțiilor, deoarece disputele privind definițiile termenilor cruciali, cum ar fi armele cibernetice sau spațiul cibernetic, sunt nerezolvate. În consecință, în vremuri de militarizare crescândă a spațiului cibernetic, aplicarea dreptului internațional la acesta este încă o provocare.

În același timp, tot mai mulți activiști încearcă să încadreze pacea cibernetică. Printre aceștia se numără Forumul Informaticienilor pentru Pace și Responsabilitate Socială, care pledează pentru dezarmarea internațională, capacitățile militare cibernetice pur defensive și formalizarea tot mai mare a organizației și a dreptului internațional în spațiul cibernetic.

Pentru a recapitula, provocările centrale pe care le prezintă armele cibernetice sunt:

• Militarizarea spațiului cibernetic;

• Solicitată de militarizarea sa, aplicarea dreptului internațional în spațiul cibernetic;

• Dificultățile rezultate din caracteristicile spațiului cibernetic și malware (care duc la probleme de atribuire și, prin urmare, probleme de diferențiere a criminalității cibernetice de atacurile cibernetice), precum și din lipsa normelor și definițiilor internaționale;

• Controlul armelor în spațiul cibernetic este complicat de problemele menționate mai sus. Utilitatea ofensivă a capacităților cibernetice defensive și caracterul cu dublă utilizare al sistemelor IT civile împiedică și mai mult eforturile depuse.

Măsurile pentru depășirea acestor probleme și pentru realizarea păcii cibernetice includ:

• Abordări cooperative și declarative, adică promovarea interacțiunii și a schimbului de informații, pe de o parte, și angajamentele unilaterale privind controlul armelor, pe de altă parte;

• **Abordări informaționale**, adică creșterea cooperării atunci când vine vorba de colectarea de informații;

• **Abordări tehnice**, adică creșterea securității cibernetice prin mijloace tehnice, în special prin intensificarea cercetărilor.

Sau, mai sintetic spus ***măsurile pentru realizarea păcii cibernetice ar fi:***

• **Permiterea doar a politicilor cibernetice pur defensive**. Accentul ar trebui să se pună pe protejarea sistemelor IT; toate celelalte capacități ar trebui să fie dezarmate;

• **Ilegalizarea răspunsurilor convenționale la atacurile cibernetice**. Deoarece sursa unui atac cibernetic nu poate fi identificată, armele convenționale nu ar trebui folosite ca răspuns;

• **Extinderea Convenției de la Geneva la spațiul cibernetic** pentru a face statele responsabile din punct de vedere juridic pentru acțiunile lor în spațiul cibernetic.

BIBLIOGRAFIE

BRIGHT A., *Estonia Accuses Russia of „Cyber Attack“*, Christian Science Monitor, May 17, 2007, disponibil la https://www.csmonitor.-com/2007/0517/p99s01-duts.html;

BROWN G.D., TULLOS O., *On the Spectrum of Cyberspace Operations*, Small Wars – Journal, Dec 11, 2012; SSRN, disponibil la https://-ssrn.com/abstract=2400536 sau http://dx.doi.org/ 10.2139/ssrn.-2400536;

CHIEN, E., FALLIERE, N., MURCHU L.O, disponibil la https://symantec-enterprise-blogs.security.com/threatintelligence/stuxnet-dossier-espionage.

DANCHEV D., *Coordinated Russia vs Georgia Cyberattack in Progress, Zero Day*, Aug. 11, 2008, disponibil la https://www.zdnet.com/-article/coordinated-russia-vs-georgia-cyber-attack-in-progress/.

FULGHUM D., *Why Syria's Air Defenses Failed to Detect Israelis, Aviation Week & Space Technology*, October 5, 2007, disponibil la https://cyber-peace.org/wp-content/uploads/2016/11/IMRA-Friday-

October-5-2007-Why-Syrias-Air-Defenses-Failed-to-Detect-Israelis.pdf;

JANSEN VF., *Cyberattacke auf Bundestagsabgeordnete: Russische Hacker schicken deutschen Politikern Phishing Mails*, Tagesspiegel, 14.07.2021, disponibil la https://www.tagesspiegel.de/-politik/russische-hacker-schickendeutschen-politikern-phishing-mails-6858718.html;

NAKASHIMA E., WARRICK J., *Stuxnet was work of U.S. and Israeli experts, officials say*, The Washington Post, June 2, 2012, disponibil la https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/ gJQAlnEy6U_story.html;

REINHOLD T., *Maßnahmen für den Cyberpeace*, 2018, disponibil la https:-//cyber-peace.org/cyberpeace-cyberwar/masnahmen-fur-den-cyberpeace/;

REINHOLD T., REUTER C., Zur Debatte über die Einhegung eines Cyberwars: Analyse mil-itärischer Cyberaktivitäten im Krieg Russlands gegen die Ukraine, Zeitschrift für Friedens- und Konfliktforschung, 2023, 12 (1), pp. 135–149, disponibil la https://doi.org/10.1007/s42597-023-00094-y;

REUTER C. (editor), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace (Technology, Peace and Security I Technologie, Frieden und Sicherheit)*, Publisher: Springer Vieweg; Second Edition 2024, Year: 2024;

SANGER D., *Syria War Stirs New U.S. Debate on Cyberattacks*, New York Times, 2014 disponibil la https://www.nytimes.com/-2014/02/25/world/middleeast/obama-worried-about-effects-of-waging-cyberwar-in-syria.html;

FIfF - Director, 2017Cyberpeace statt Cyberwar!, disponibil la https://-peasec.de/paper/2024/2024_ReinholdReuter_FromCyberWartoCyberPeace_ITforPeaSec.pdf;

The Guardian, Obama orders US to draw up overseas target list for cyber-attacks, disponibil la https://www.theguardian.com/world/-2013/jun/07/obama-china-targets-cyber-overseas.

en.wikipedia.org, Defense News, Deutsche Welle;

https://www.darpa.mil/about-us/buget;

„Rezoluția 66/24 a Adunării Generale a Organizației Națiunilor Unite", adoptată la 3 noiembrie 2011, intitulată „Promovarea și protecția drepturilor omului în contextul securității naționale", (A/RES/66/24).