RĂZBOIUL CIBERNETIC – NOUL TEATRU DE RĂZBOI ȘI CLARIFICĂRILE LEGISLATIVE ALE ACESTUIA –

Dr. Marian-Valentin BÎNA
Misiunea de Sprijin a ONU în Libia
10.55535/GMR.2024.4.15

This study aims to highlight the growing strategic importance assumed by the field of cybernetics in the dynamics of international politics. Cyberspace, an artificial environment created par excellence by human activity, has become crucial for power in the 21st century. After land, water, air and outer space, cyberspace represents the fifth dimension of new conflicts. In order to overcome these obstacles, I have chosen to clarify, from a legislative point of view, the status of this new dimension of conflict management. For the most part, official documents found in open sources define cyberwarfare as the use of incisive techniques for intrusion or sabotage an actor's information and physical resources, actions carried out in the context of a conflict, through the use of technology and telecommunications networks, which aim to compromise the defence, functioning, as well as the economic and socio-political stability of the adversary.

Keywords: cyberspace; cyberwarfare; information technology; lines of code; Tallinn Manual;

INTRODUCERE

În era digitală modernă, fiecare domeniu de activitate conține complexe și inedite tehnologii, iar actualele acțiuni de luptă confirmă rolul marcant al inteligenței și tehnologiei militare în obținerea victoriei strategice, operative și tactice.

Având în vedere conflictele tradiționale – pe pământ, pe mare și în aer –, care implică teritorii fizice și resurse tangibile, s-a deschis, de fapt, un nou front: așa-numitul *război cibernetic*, care poate fi semnificat prin sintagma *teatru cibernetic al războiului* (Shultz, 2022). Diferența, cel mai important factor dintre acest spațiu de război și conflictele tradiționale, este natura sa substanțial imaterială. Armele folosite sunt linii de cod, iar câmpul de luptă este constituit dintr-un spațiu cibernetic infinit, care, din păcate, contribuie, pe de o parte, la o așa-zisă democratizare a informațiilor, iar pe de altă parte, le facilitează actorilor maligni posibilitatea de a influența publicul țintă, prin narațiunile și informațiile expuse.

EVOLUȚIA REGLEMENTĂRILOR APLICABILE SPAȚIULUI CIBERNETIC

În sistemul internațional, conceptele de *jus ad bellum* și *jus in bello* sunt cele care reglementează utilizarea potențială a forței într-un conflict. Aceste elaborări normative și doctrinare, printre altele, reprezintă limitarea comportamentului actorilor internaționali și impunerea restricțiilor, de exemplu cu privire la utilizarea anumitor arme, pentru a interzice atacurile împotriva unor ținte specifice sau împotriva populaţiei civile sau să pregătească disciplina care reglementează tratamentul care trebuie să fie rezervat prizonierilor de război pe lângă rolurile, drepturile și obligațiile combatantului. Astfel, prevederile *Convenției a III-a privitoare la tratamentul prizonierilor de război*, de la Geneva, adoptată în 1949, vizează protecția prizonierilor de război, drepturile și obligațiile acestora în lagărele de prizonieri de război (Portal legislativ).

Geneza acestor reglementări, cu siguranță, nu este recentă, iar de-a lungul secolelor, acesteau au evoluat și s-au adaptat la nevoile contextului practic, în cele din urmă, spațiului cibernetic. Una dintre primele încercări de a introduce o normă obligatorie în dreptul internațional, asupra acestor probleme, a avut loc odată cu stabilirea *Convenției privind criminalitatea cibernetică din 2001* (Consiliu Europei, 2001), promovată de către Consiliul Europei, care, deși a reprezentat un punct de pornire în domeniu, nu a abordat totuși problema reglementării așa-numitului

război cibernetic sau a tipurilor de atac cibernetic inserate în contextul unui război hibrid.

Fără îndoială, reglementările legislative făcute în acest sens se regăsesc în art. 2 paragraful 4 și art. 51 din Carta Națiunilor Unite (Statuto delle Nazioni Unite., 1945). Din combinarea dispozițiilor acestora reiese în mod clar că statele pot întreprinde un act de autoapărare atunci când vine vorba de folosirea forţei și când securitatatea națională sau integritatea teritorială sunt puse în pericol. Cu toate acestea, spațiul cibernetic ridică noi semne de întrebare, ca, de exemplu, în ceea ce privește existența și posibilitățile de extindere a suveranității unei țări în spațiul cibernetic. Răspunsul, deși nu este întocmai legal, ci de natură doctrinară exclusivă, poate fi găsit în *Manualul Tallinn*[1], întocmit de experți de top din lumea academică internațională, specialiști în drept internațional umanitar și drept militar. Manualul acționează, în esență, ca un cadru ce defineşte categoriile de drept internaţional aplicabile domeniului cibernetic (Manualul Tallin 2.0). În acest sens, manualul prescrie, în primul paragraf, că o țară are autoritatea de a exercita controlul asupra întregii infrastructuri și activități cibernetice de pe teritoriul său, cu consecința inevitabilă că, în cazul detectării unui atac de natură cibernetică, poate să îl califice drept atac armat, recunoscându-și expres posibilitatea de a se apăra (Ib.).

Pare oportun să ne concentrăm pe scurt asupra *Manualului de la Tallinn* care, după cum era anticipat, nu are efecte coercitive pentru state, doar primește un fel de efect coercitiv prin prisma noțiunilor de referință reglementate principal. Importanța reglementărilor în cauză se regăsește în reinterpretarea legislaţiei internaţionale existente, pe baza dualismului incontestabil dintre spațiul de luptă fizic (apă, aer, sol) și cel cibernetice. Deși infrastructura spațiului cibernetic există în cadrul statelor teritoriale prin corpuri fizice ce conțin date, fluxul acestora este doar parțial controlabil de către stat, care face, astfel, spațiul cibernetic imun la modalitățile tradiționale de reglementare a contextului de conflict și, mai presus de toate, deși este adevărat că este o nouă dimensiune, este la fel de adevărat faptul că nu poate fi considerat separat de cele trei dimensiuni tradiţionale menționate mai devreme.

Dacă *Manualul de la Tallinn* nu constituie o reglementare legislativă pentru state, acesta reprezintă un simplu ghid. Instrumentele care au putere legislativă sunt, în esență, reprezentate de tratatele internaționale și rezoluții ale Consiliului de Securitate al Națiunilor Unite. Pentru acestea din urmă, consider că este oportun să ne concentrăm asupra evoluției legislației NATO pe tema spațiului cibernetic.

[1] Manualul Tallinn a devenit o resursă influentă pentru consilierii juridici și experții politici care se ocupă de problemele cibernetice. În multe state, practica emergentă a statelor și luarea de poziții publice cu privire la dreptul internațional cibernetic de la publicarea manualului necesită o actualizare a ediției din 2017. (N.A.).

ABORDĂRI ALE NATO PRIVIND EVOLUȚIA SPAȚIULUI CIBERNETIC

Deşi Alianța Nord-Atlantică şi-a protejat întotdeauna sistemele de comunicaţii şi informatică, abia în 2002, la summitul de la Praga, *apărarea cibernetică* a fost inclusă pe agenda politică a Alianţei. În anul 2006, la summitul de la Riga, a fost reiterata protecția suplimentară a acestor sisteme informatice. În 2007, evenimentele binecunoscute din Estonia[2], ce au vizat o serie de atacuri cibernetice împotriva instituțiilor publice, a impus miniștrilor aliați ai apărării să convină asupra necesității urgente de intervenție în acest sens sector. Acest lucru a condus la aprobarea primei politici de apărare cibernetică a NATO, în ianuarie 2008. În același an, conflictul dintre Rusia și Georgia (Selene, 2018) a demonstrat că atacurile cibernetice pot deveni o componentă semnificativă a războiului convențional.

Abia în 2010, la Lisabona, NATO a dezvoltat un concept strategic în care recunoaște că atacurile cibernetice pot deveni atât de severe, încât amenință prosperitatea, securitatea și stabilitatea națională și euroatlantică. Din aprilie 2012, *apărarea cibernetică* a fost introdusă în întreg procesul de planificare a apărării NATO. În anii următori, războiul cibernetic a continuat să fie subiectul de planificare și consolidare pe masa NATO, ajungând spre aprobare în cadrul summitului din 2014, din Țara Galilor (Damiano, Scatto, 2021), unde noua politică de apărare cibernetică este recunoscută ca parte integrantă a sistemului de apărare, putându-se, astfel, recurge la folosirea forței în cazul autoapărării colective, conform reglementărilor din Carta Națiunilor Unite.

În cadrul summitului NATO din 2016, de la Varșovia, șefii de stat și de guvern aliați au recunoscut spațiul cibernetic ca domeniu operațional în care NATO trebuie să aibă capacitatea de a se apăra şi de a reacţiona (NATO, 2016).

Un alt moment crucial privind reglementarea legislativă a atacurilor cibernetice a avut loc în cadrul summitului NATO din 2021, de la Bruxelles, unde noua politică de apărare cibernetică a fost aprobată, ducând, astfel, la îndeplinirea sarcinilor de bază ale NATO, precum și a propriilor sale sarcini,generale de descurajare și apărare. S-a recunoscut, în mod expres, că impactul provocat de un atac vădit intenționat în spațiul cibernetic trebuie să fie considerat un atac armat din toate punctele de vedere. De fapt, tocmai cu această ocazie, cele 30 de state membre ale Alianței

[2] În 2007, Estonia a fost victima unui puternic atac cybernetic, care a afectat site-uri web guvernamentale, bănci și organizaţii informaționale. Atacatorul pare să fi fost Rusia, deși nu poate fi confirmat cu certitudine acest lucru. Primul atac cibernetic real care a avut loc în Estonia a condus la necesitatea extinderii domeniului de aplicare a articolului 5 din Pactul Atlantic, cu legitimarea consecventă de a putea recurge la mecanismul de autoapărare colectivă. În același context, a fost înființat Centrul de excelență pentru apărare cibernetică cooperativă (CCDCOE), unul dintre cele mai mari centre de excelență ale Alianței, situat chiar în Tallinn. Acest centru își propune să îmbunătățească modul de cooperare între statele membre din domeniul apărării cibernetice. (N.A.).

au confirmat că, în fața atacurilor cibernetice, poate fi invocat Articolul 5 din Tratat și a fost aprobată o nouă politică de apărare cibernetică pentru o nouă abordare a oricăror tipuri de amenințări cibernetice, chiar și a celor de nivel scăzut (Damiano, Scatto, ib.). La următorul summit al NATO, din 2023, de la Vilnius, statele membre au aprobat o nouă schemă de îmbunătățire a apărării cibernetice, privind apărarea și descurajarea globală a NATO. Conceptul va integra, în continuare, cele trei niveluri de apărare și anume:

- apărarea privind tehnologia informației;
- apărarea politică, militară și tehnică;
- apărarea privind cooperarea civil-militară, în timp de pace, criză și conflict, precum și angajamentul de colaborare cu sectorul privat.

ALTE CLARIFICĂRI CE REGLEMENTEAZĂ RĂZBOIUL CIBERNETIC

După cum am văzut, legile războiului sunt aplicate mai degrabă în context fizic, acest lucru nefiind la fel de eficient în domeniul cibernetic, ridicând, astfel, probleme privind dificultatea identificării atacatorului și a eficienței cu care este caracterizat acest tip de atac.

Clasificarea atacatorilor este doar una dintre numeroasele probleme din acest domeniu. În anul 2000, McConnell International a elaborat un raport foarte interesant care examinează infracțiunile și atacurile produse în spațiul cibernetic și pedepsele aferente. Analizând starea actuală a legilor din 52 de state, au constatat că doar o mică parte dintre ele și-au schimbat legislația pentru a aborda, astfel, diferitele atacuri cibernetice, dar principala problemă a fost reprezentată de spațiul cibernetic transnațional, deoarece pot exista probleme majore atunci când un atac cibernetic criminal implică mai multe națiuni (Cyber Crime Treaty, 2024; Soafer, Goodman, 2001, pp. 1-34).

Pentru a determina dacă este sau nu necesară intervenția militară, este necesară identificarea corectă a agresorului, deoarece, în funcție de cine este atacatorul, de unde provine atacul și ce este atacat, vor fi aplicate reguli diferite. În societatea actuală, în spațiul cibernetic, criminalii devin din ce în ce mai experți în utilizarea tehnologiei informatice. Instrumentele de hacking, cu tutoriale video despre cum să fie folosite, sunt disponibile gratuit. Așa-numitul *„script kiddies”*[3] sau persoanele cu puține cunoștințe tehnice pot găsi deja codul scris pentru a realiza acțiunile dorite.

[3] Un script kiddie, prin definiție, este o persoană fără expertiză tehnică, ce utilizează instrumente sau scripturi automate preexistente, pentru a lansa atacuri asupra sistemelor sau rețelelor de calculatoare, https://www.sangfor.com/glossary/cybersecurity/what-are-script-kiddies. (N.A.).

Aceste atacuri pot varia de la cele simple, de vandalism, la operațiuni bine gândite împotriva infrastructurii critice. În aceste context, identificarea sursei unui atac cibernetic necesită identificarea locației fizice a sistemului atacator, de exemplu, urmărirea atacului și atribuirea acestuia unei anumite adrese IP, identificarea sistemului sau a sistemelor utilizate, identificarea persoanelor responsabile de atacul produs și, eventual, identificarea organizației care îl sponsorizează. În cazuri rare, toate aceste elemente pot fi concentrate într-un singur subiect.

Datorită necesității de a integra informații din partea comercială și cea guvernamentală, agențiile de informații și militare complică, astfel, identificarea și pot duce la o întârziere semnificativă a investigației vizavi de atacul produs. Într-un mediu în care atacurile pot avea loc în mai puțin de o secundă și, mai ales, la un cost zero, atunci când ai deja echipament electronic adecvat, plasarea de astfel de atacuri facilitează răspândirea și creșterea exponenţială a numărului de subiecţi care pot recurge la asemenea măsuri (Strouble, Carroll, 2008).

CONCLUZII: PROVOCĂRI ȘI PERSPECTIVE

În prezent, încă nu există un set de reglementări complete, astfel apărând o serie de probleme de aplicare pentru legislația internațională, în primul rând, identificarea momentului în care unui stat îi este permis să recurgă la autoapărare și, deci, la eventuala folosire a forței, dacă ar fi victimă a unui atac cibernetic.

Actualele reglementări legislative referitoare la războiul cibernetic lipsesc în situația nefastă de a surmonta o criză care, chiar și mâine, din păcate, ar putea duce la evenimente dramatice. Absența unor standarde predeterminate pentru evaluarea și reacția la atacurile cibernetice, care sunt adoptate în mod valabil de către statele membre ale Uniunii Europene sau de către țările membre ale NATO, ar putea constitui elementul fundamental al unei posibile înfrângeri în spațiul cibernetic. Trebuie să sperăm că, poate, cât mai curând posibil, guvernele occidentale, NATO, precum și alte entități comerciale pot avea resurse și criterii omogene și oportune de realizare a unor standarde defensive uniforme, adecvate și suficiente pentru a contracara orice atac de natură cibernetică.

După cum istoria ne-a învățat să adoptăm decizii care, într-un fel, limitează suveranitatea națională, acestea pot fi dificil de implementat, mai ales pentru că orice formă de integrare duce, inevitabil, la o erodare a suveranității statului. Ar trebui, cu toate acestea, ca spațiul cibernetic să poată fi gestionat mult mai eficient dacă este partajat cu alte state sau membri ai unor organizaţii internaţionale.

Poate că am putea merge până acolo încât să spunem că integrarea națională, mai degrabă decât o posibilitate, ar trebui considerată o cerință inevitabilă

și obligatorie privind validitatea defensivă, tocmai pentru că atacurile cibernetice ar putea produce efecte dăunătoare, comparabile cu atacurile fizice, cu consecințe larg răspândite. Este necesar și indispensabil ca eventualele conduite să fie identificate și codificate fără întârziere de către state și actorii internaționali, implementând-se la nivelul spațiului cibernetic și reinterpretându-le în baza legislaţiei în vigoare.

Prin urmare, acum este clar că spațiul cibernetic reprezintă deschiderea unui nou front, ce trebuie luat în condiderare. În ciuda faptului că NATO a declarat posibilitatea aplicării Articolului 5, în eventualitate producerii unui atac cibernetic împotriva vreunui membru al Alianței, această situație necesită o evaluare precisă și concisă, realizată prin metode relevante, lipsite de ambiguități. Lipsa unor standarde predeterminate pentru evaluarea atacurile cibernetice ar putea pune probleme țărilor membre ale NATO, care au metode interne diferite pentru a le contracara. Pentru a depăși această ambiguitate, ar fi de dorit ca NATO să adopte standarde uniforme pentru a evalua atacurile cibernetice individuale și pentru a determina dacă acestea au atins un nivelul de crescut de severitate care ar face din el un atac armat.

Potrivit celor prezentate în cadrul acestui articol, putem afirma că legile războiului sunt aplicate mai degrabă în context fizic, acest lucru nefiind la fel de eficient în domeniul cibernetic, ridicând, ca atare, probleme privind dificultatea identificării atacatorului și eficiența cu care este caracterizat acest tip de atac.

BIBLIOGRAFIE:

1. Brown, G., Poellet, K. *The Customary International Law of Cyberspace.* În *Strategic Studies Quarterly*, http://www.jstor.org/stable/26267265, accesat la 2 august 2024.
2. *Carta Națiunilor Unite* (1945), https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf., accesat la 12 iunie 2024.
3. *Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021*, Brussels Summit, https://www.nato.int/cps/en/natohq/news_185000.htm, Press Release (2021) 086, publicat pe 14 iunie 2021, actualizat pe 1 iulie 2022, accesat la 22 august 2024.
4. *Council of Europe* (2001). *Convention on Cybercrime*, https://www.coe.int/it/web/portal/home (STE nr. 185), https://rm.coe.int/1680081561, accesat la 27 mai 2024.
5. *Council of Europe action against Cybercrime*, https://www.coe.int/it/web/portal/coe-action-against-cybercrime#:~:text=La%20Convenzione%20sulla%20criminalit%C3%A0%20informatica%20(2001)%20%C3%A8%20l'unico,tra%20i%20suoi%20Stati%20parti, accesat la 22 iunie 2024.
6. *Cyber Crime Treaty*. Global Information Assurance Certification Paper, https://www.giac.org/paper/gsec/839/cybercrime-treaty/101761, accesat la 22 iunie 2024.
7. *Cyber defence*. *NATO*, https://www.nato.int/cps/en/natohq/topics_78170.htm, accesat la 2 august 2024.

8. Damiano, L., Scatto, E. *Nato, la nuova "Cyber Defence Policy": ecco le priorità dell'Alleanza nella difesa dello spazio cibernetico*, https://www.agendadigitale.eu/sicurezza/nato-la-nuova-cyber-defence-policy-ecco-le-priorita-dellalleanza-nella-difesa-dello-spazio-cibernetico/, accesat la 12 iunie 2024.
9. *Manualul Tallinn* 2.0. CyberLaws, https://www.cyberlaws.it/2019/manuale-tallinn/, accesat la 22 august 2024.
10. NATO (2016). *Cyber defence,* https://www.nato.int/cps/en/natohq/topics_78170.htm., accesat la 22 august 2024.
11. Pool, P. (2013). *War of the Cyber World: The Law of Cyber warfare. The International Lawyer*, sursa: http://www.jstor.org/stable/43923953, accesat la 22 august 2024.
12. Portal legislativ, https://legislatie.just.ro/Public/DetaliiDocument/255597, accesat la 12 august 2024.
13. Sironi de Gregorio, F. (2019). *Il Manuale di Tallinn 2.0*., CyberLaws, https://www.cyberlaws.it/2019/manuale-tallinn/, accesat la 12 iulie 2024.
14. Shultz, N. (2022), https://www.fordhamilj.org/iljonline/cyber-warfare-the-newest-theater-of-war, accesat la 22 iulie 2024.
15. Soafer, A., Goodman, S. (2021). *Cyber crime and Security The Transnational Dimension. In The Transnational Dimension of Cyber Crime and Terrorism*, vol. Hoover Institution's National Security Forum Series, pp. 1-34, California: Hoover Institution Press, https://www.hoover.org/sites/default/files/uploads/documents/0817999825_1.pdf, accesat la 22 august 2024.
16. *Statuto delle Nazioni Unite* (1945), https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf; Organizzazione delle Nazioni Unite, https://www.miur.gov.it/documents/20182/4394634/1.%20Statuto-onu.pdf, accesat la 27 mai 2024.
17. Strouble, D., Carroll, M. (2008). *Law and Cyber War*, SAIS 2008 Proceedings, http://aisel.aisnet.org/sais2008/37, accesat la 12 iulie 2024.
18. *The North Atlantic Treaty* (4 aprilie 1949. Washington D.C., https://www.nato.int/cps/en/natohq/official_texts_17120.htm, accesat la 22 iunie 2024.
19. Verri, S. (8 august 2018). *La guerra dimenticata: sintesi e analisi del conflitto russo-georgiano 10 anni dopo.* Euronews, https://it.euronews.com/2018/08/08/la-guerra-dimenticata-sintesi-eanalisi-del-conflitto-russo-georgiano-10-anni-dopo, accesat la 12 iulie 2024.
20. https://www.sangfor.com/glossary/cybersecurity/what-are-script-kiddies, accesat la 22 august 2024.