ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA” DIN IAŞI
TOMUL LXV/SUPLIMENT, ŞTIINŢE JURIDICE, 2019

Atacurile cibernetice şi legitima apărare în dreptul internaţional

International Law on Cyber Attacks and Self-Defence

Carmen Moldovan[1]

Rezumat:
Legitima apărare a statelor este de natură cutumiară şi constituie unul dintre drepturile esenţiale pe care le poate exercita un stat, în temeiul dispoziţiilor articolului 51 din Carta Naţiunilor Unite. Condiţiile de exercitare a legitimei apărări nu fac obiectul studiului prezentului articol, în care analiza se va concentra pe analiza argumentelor care pot veni în sprijinul includerii atacurilor informatice în categoria noţiunii „atac armat” ce justifică recurgerea la legitima apărare de către statul victimă.

Cuvinte-cheie: spaţiu cibernetic; răspundere; *ius ad bellum; ius in bello;* imputabilitate.

Abstract:
State's legitimate self-defence is considered Customary International Law and one of the essential rights a State can exercise, under the provisions of Article 51 of the Charter of the United Nations. The aim of this paper is to examine the conditions for exercising the legitimate self-defence instead the analysis will focus on arguments that support the idea of including cyber attacks in the „armed attack” notion, that justifies the recourse to force by the victim State.

Keywords: Cyberspace; responsibility; *ius ad bellum*; *ius in bello;* imputability.

Aspecte introductive

Dezvoltarea internetului şi a tehnologiilor de comunicare are un efect pervaziv asupra tuturor aspectelor vieţii, deci şi asupra regulilor dreptului internaţional. Procesul de schimbare, început de cel puţin douăzeci de ani, va continua, astfel că este necesară clarificarea modalităţii în care regulile existente pot fi adaptate noilor situaţii sau este necesară adoptarea unor norme noi. Statele şi dreptul internaţional nu au putut să ţină pasul cu ritmul extrem de dinamic al dezvoltării tehnologiei, mai adaptabile fiind marile companii private (desemnate în general sub denumirea *Bigtech*) care au adoptat propriile reglementări în privinţa folosirii Internetului, astfel că se constată o schimbare a paradigmei, de la controlul statal în stabilirea regulilor aplicabile unui domeniu către controlul exercitat de entităţile private.

[1] Lector univ. dr., Universitatea „Alexandru Ioan Cuza” din Iaşi, Facultatea de Drept, carmen.moldovan@hotmail.com.

Adaptarea reglementărilor existente sau adoptarea unora noi care să corespundă spaţiului cibernetic va constitui, cu siguranţă, o provocare, până în prezent neexistând *opinio iuris* în cadrul statelor cu privire la semnificaţia conduitei responsabile a statelor în spaţiul cibernetic, caracterizat ca un spaţiu paralel celui fizic al existenţei noastre (care este rezultat al evoluţiei în mii de ani), dezvoltat relativ recent ca o creaţie unică a omului, care îl menţine şi dezvoltă, continuând să ia amploare[2].

Existenţa unui vid de reglementare în privinţa spaţiului cibernetic (cyberspace)

Dreptul internaţional nu defineşte spaţiul cibernetic şi nici diversele activităţi sau operaţiuni pe care statele sau entităţi private ori simpli particulari le pot desfăşura aici. La nivel universal nu există niciun instrument juridic cu efect obligatoriu care să reglementeze aceste aspecte, la nivel regional fiind adoptate o serie de reglementări.

Una dintre acestea este *Convenţia cu privire la criminalitatea informatică de la Budapesta*[3], intrată în vigoare şi la care sunt parte şi Statele Unite ale Americii şi alte state din afara Consiliului Europei[4]. Însă Convenţia are un domeniu de aplicare destul de restrâns, deoarece priveşte activitatea indivizilor pe internet ce constituie elemente ale infracţiunilor informatice, pornografiei infantile, nefiind un instrument exhaustiv de reglementare, care să fie util pentru tema abordată de prezenta lucrare.

Tot la nivel regional, Organizaţia pentru Cooperarea Statelor în Domeniul Securităţii Internaţionale Informatice[5] a definit noţiunea „război informatic" (*information war*) „confruntarea între două sau mai multe state în spaţiul

---

[2] N. Melzer, *Cyberwarfare and International Law*, UNIDIR Ressources, 2011, https://www. files.ethz.ch/isn/134218/pdf-1-92-9045-011-L-en.pdf (accesat la 10 ianuarie 2020).

[3] *Convenţia cu privire la criminalitatea informatică* (*Convention sur la cybercriminalité*, STCE no. 185), adoptată în cadrul Consiliului Europei la Budapesta la 23 noiembrie 2001, intrată în vigoare la 1 iulie 2004. România a semnat Convenţia la 23 noiembrie 2001, a ratificat-o la 12 mai 2004 prin Legea nr. 64/2004, publicată în M. Of. al României, partea I nr. 343 din 20 aprilie 2004. Convenţia are forţă juridică obligatorie pentru România de la 1 septembrie 2004.

[4] Informaţii detaliate cu privire la statele părţi la Convenţie sunt disponibile la adresa: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=sGiE7jat (accesată la 20 octombrie 2019).

[5] Shanghai Cooperation Organization on Cooperation in the Field of International Security/Organizaţia de cooperare din Shanghai (SCO) este o organizaţie internaţională compusă din opt state membre (Republica India, Republica Kazahstan, Republica Populară Chineză, Republica Kârgâz, Republica Islamică Pakistan, Federaţia Rusă, Republica Tadjikistan şi Republica Uzbekistan), care a fost înfiinţată în 2001 prin Declaraţia privind înfiinţarea SCO (Shanghai, 15 iunie 2001) în scopul cooperării politice, militare şi economice, https://ccdcoe.org/organisations/sco/ (accesată la 10 ianuarie 2020).

informatic în scopul deteriorării sistemelor informatice, a proceselor sau resurselor, structurilor critice sau a altor structuri, subminării sistemului politic, economic sau social, spălarea psihologică în masă pentru destabilizarea societăţii şi a statului precum şi pentru a forţa statul să ia decizii în interesul unei alte părţi".

Aceeaşi situaţie de vid este întâlnită şi în cazul noţiunilor „terorism cibernetic" sau „război cibernetic" (*cyberwarfare*), astfel că, din perspectiva dreptului internaţional, analiza acestor situaţii are ca punct de pornire *ius ad bellum*[6], precum şi dispoziţiile Cartei Naţiunilor Unite, care în articolul 2 par. 4 prevede interdicţia ca statele să recurgă la folosirea forţei sau la ameninţarea cu folosirea forţei[7], iar în articolul 51 prevede posibilitatea recurgerii la legitima apărare[8].

În ceea ce priveşte conţinutul dispoziţiilor menţionate, trebuie identificată folosirea unor termeni diferiţi: articolul 2 par. 4 se referă la interdicţia folosirii forţei, în timp ce articolul 51 prevede posibilitatea recurgerii la legitimă apărare în cazul comiterii unui atac armat[9].

La nivel internaţional au existat divergenţe în privinţa posibilităţii aplicării aceloraşi reguli ca în cazul conflictelor armate, în cazul atacurilor cibernetice şi a apărut întrebarea dacă este necesară adoptarea unui cadru normativ special în acest sens, însă opinia majoritară este că, din perspectiva articolului 51 din Carta Naţiunilor Unite, cel puţin unele atacuri cibernetice pot atinge nivelul de gravitate al atacurilor armate.

De asemenea, în cazul calificării atacului cibernetic ca atac armat, trebuie avută în vedere aplicarea *ius in bello*, după începerea ostilităţilor, care influenţează legalitatea folosirii forţei şi presupun respectarea principiilor discriminării între obiectivele militare şi aşezările civile (în sensul că atacurile trebuie limitate la obiectivele militare, iar aşezările civile nu ar trebui să

---

6 M. Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 B.C. Int'l & Comp. L. Rev. 439 (2009), http://lawdigitalcommons.bc.edu/iclr/vol32/iss2/16 (accesată la 20octombrie 2019).

7 Articolul 2 paragraful 4 din Carta Națiunilor Unite prevede: „Toți Membrii Organizației se vor abține, în relațiile lor internaționale, de a recurge la amenințarea cu forța sau la folosirea ei fie împotriva integrității teritoriale ori independenței politice a vreunui stat, fie în orice alt mod incompatibil cu scopurile Națiunilor Unite".

8 Articolul 51 din Carta Națiunilor Unite prevede: „Nicio dispoziție din prezenta Cartă nu va aduce atingere dreptului inerent de autoapărare individuală sau colectivă în cazul în care se produce un atac armat împotriva unui Membru al Națiunilor Unite, până când Consiliul de Securitate va fi luat măsurile necesare pentru menținerea păcii și securității internaționale. Măsurile luate de Membri în exercitarea acestui drept de autoapărare vor fi aduse imediat la cunoștința Consiliului de Securitate și nu vor afecta în nici un fel puterea și îndatorirea Consiliului de Securitate, în temeiul prezentei Carte, de a întreprinde oricând acțiunile pe care le va socoti necesare pentru menținerea sau restabilirea păcii și securității internaționale".

9 C.M. Petras, *The Use of Force in Response to Cyber-Attack on Commercial Space Sustems-Reexamining Self-Defense in Outer Space in Light of the Convergence of U.S. Military and Commercial Space Activities*, Journal of Air Law and Commerce, Volume 67, Issue 4, 2002, p. 67.

constituie obiect al atacurilor) şi a principiului proporţionalităţii (în sensul că se va folosi doar forţa necesară pentru a răspunde atacului)[10].

Având în vedere lipsa unei terminologii clare în acest domeniu în care se folosesc termeni ca *cyber attacks, cyber operations, cyberwar, cyberwarfare, cyber ostilities, cyber conflict, information war*[11], în textul prezentei lucrări vor fi folosite ca noţiuni echivalente cea de „atacuri cibernetice" şi cea de „atacuri informatice".

Aplicarea regulilor generale ale dreptului internaţional în spaţiul cibernetic pentru acoperirea vidului de reglementare

În ciuda divergenţelor cu privire la aplicarea regulilor dreptului internaţional clasic referitoare la conflictele armate[12], situaţia actuală este parţial clarificată, urmare a lucrărilor grupurilor speciale de lucru instituite de Adunarea Generală a Naţiunilor Unite – *Open-ended Working Group (OEWG)*[13] şi *Group of Governmental Experts (GGE)*[14], care au reţinut aplicarea regulilor şi principiilor dreptului internaţional public în spaţiul digital (*cyberspace*)[15], însă nu este clarificat cum anume urmează ca acestea să fie puse în aplicare sau cum trebuie să fie adaptate, având în vedere diferenţele dintre spaţiul fizic şi spaţiul digital sau virtual.

---

10 E.F. Mejia, *Act and Actor Attribution in Cyberspace. A Proposed Analytic Framework*, în Strategic Studies Quarterly, 2014, p. 115.

11 N. Melzer, *op. cit.*, p. 22.

12 M.E. O` Connell, *Cyber Security without Cyber War*, Journal of Conflict and Security Law, Volume 17, 2012, p. 190-191; M. Hoisington, *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, Boston College International and Comparative Law Review, Volume 32, Issue 2, 2009, p. 448.

13 Prin Rezoluția 73/27 din 5 decembrie 2018, Adunarea Generală a Națiunilor Unite a stabilit *Open-Ended Working Group (OEWG*), la care sunt invitate să participe toate statele. OEWG a avut prima sa întâlnire în 2019 și va prezenta raportul său Adunării Generale în 2020. Textul rezoluției este disponibil la adresa: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27 (accesată la 10 ianuarie 2020).

14 Prin Rezoluția 73/266 din 2003 a Adunării Generale a ONU, Secretarului General i s-a solicitat să înființeze un grup de experți guvernamentali care să analizeze conduita statelor în spațiul cibernetic în contextul securității internaționale. Acest grup de experți a fost înființat în anul 2004 – Group of Governmental Experts (GGE). Membrii GGE în 2019-2021 sunt: Australia, Brazilia, China, Estonia, Franța, Germania, India, Indonezia, Japonia, Iordania, Kazahstan, Mauritius, Mexic, Maroc, Țările de Jos, Norvegia, România, Federația Rusă, Singapore, Africa de Sud, Regatul Unit al Marii Britanii, Statele Unite ale Americii și Uruguay. O prezentare comparativă a activităților desfășurate de OEWG și GGE este disponibilă la adresa: https://dig.watch/processes/un-gge (accesată la 10 ianuarie 2020).

15 Rezoluția Adunării Generale a ONU nr. 73/27 din 5 decembrie 2018 face referire la rapoarte ale celor două instituții în care se menționează aplicarea regulilor dreptului internațional în spațiul cibernetic, disponibilă la adresa: https://undocs.org/A/RES/73/27 (accesată la 10 ianuarie 2020).

De asemenea, continuă să rămână incert care este nivelul de gravitate al unui atac cibernetic, pentru a putea fi considerat atac armat sau forţă, în sensul articolului 2 par. 4 din Carta Naţiunilor Unite, mai ales luând în considerare că, pentru a fi considerat ilicit din perspectiva dreptului internaţional, un act nu trebuie să constituie forţă sau atac armat, ci să fie rezultatul unei încălcări a unei obligaţii internaţionale[16].

Regulile dreptului internaţional cu privire la autorizarea folosirii forţei

Autorizarea folosirii forţei de către membrii Naţiunilor Unite este atributul Consiliului de Securitate. Textul articolului 51 din Cartă nu consacră în mod expres posibilitatea exercitării legitimei apărări preventive sau anticipate, însă este susţinută puternic de state precum Regatul Unit al Marii Britanii şi Statele Unite ale Americii. Această doctrină a fost afirmată în secolul al XIX-lea, în incidentul *Caroline*[17] şi permite folosirea forţei anticipat sau preventiv de către un stat dacă atacul este iminent.

În practică, acest concept a fost folosit în mai multe situaţii pentru a justifica folosirea forţei de către Statele Unite ale Americii: activităţile militare şi paramilitare în Honduras în anii 1980, acţiunile de bombardare din 1986 în Libia, operaţiunile din Irak, începând din anul 2003[18]. Validarea folosirii forţei armate de către Consiliul de Securitate poate constitui un argument important în susţinerea doctrinei dreptului la apărare preventivă sau anticipată, însă Curtea Internaţională de Justiţie nu a recunoscut existenţa unui astfel de drept[19].

Totodată, nici Consiliul de Securitate nu a recunoscut în toate situaţiile caracterul legitim al folosirii forţei în mod preventiv, un bine cunoscut exemplu în acest sens fiind atacurile realizate de către Israel asupra unui reactor nuclear iranian, în anul 1981, motivat de neprobarea iminenţei, condiţie specifică a legitimei apărări anticipate[20], formulare ce înseamnă că nu a respins posibilitatea exercitării acesteia. De asemenea, trebuie subliniat că regulile referitoare la folosirea forţei se aplică atât entităţilor statale, cât şi celor nestatale.

---

16 N. Melzer, *op. cit.*

17 M.C. Waxman, *The Caroline Affair in the Evolving International Law of Self-Defense, Review of Craig Forcese, Destroying the Caroline: The Frontier Raid thatReshaped the Right to War* (Irwin Law, 2018), disponibil la adresa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3240618 (accesată la 20 octombrie 2019).

18 C. Moldovan, *Drept internațional public. Principii și instituții fundamentale*, ediția a II-a, Editura Universul Juridic, București, 2019, p. 111-114.

19 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States), Merits, Judgement, 27 June 1986, parag. 194-197. Textul integral al hotărârii este disponibil la adresa*: www.icj-cij.org (*accesată la 10 ianaurie 2020).

20 *Resolution 487 (1981), 9 June 1981*, https://unispal.un.org/unispal.nsf/ d744b47860e5c97e85256c40005d01d6/6c57312cc8bd93ca852560df00653995 (accesată la 10 ianuarie 2020).

Abordări ale noţiunii „atac cibernetic”

Odată cu evoluţia mijloacelor de comunicare, a Internetului şi a tehnologiei, în general, comiterea de atacuri şi reacţia de răspuns la acestea nu mai au loc în cadrul stabilit de Carta Naţiunilor Unite în 1945[21], astfel că este necesară interpretarea regulilor stabilite în contextul şi în conformitate cu evoluţia instituţiilor şi a relaţiilor interstatale.

Comiterea atacurilor cibernetice sau informatice (nu este încă stabilită o terminologie uniformă sau unitară cu privire la termenii cei mai adecvaţi) reprezintă o realitate a prezentului. Regatul Unit al Marii Britanii a suferit 800 de atacuri / oră în cursul anului 2019[22], şi nu este singurul exemplu în acest sens. Pe de altă parte, încă din 2011, Statele Unite ale Americii au adoptat *International Strategy for Cyberspace*[23], care prevede dreptul la exercitarea legitimei apărări, în temeiul articolului 51 din Carta Naţiunilor Unite, prin folosirea oricăror mijloace necesare şi adecvate, pentru apărarea statului, a aliaţilor şi partenerilor Statelor Unite, a intereselor acestora, cu evitarea folosirii forţei armate în situaţiile în care va fi posibil.

Operaţiunile cibernetice, actele de spionaj informatic sau recunoaşterea pregătirii pentru un conflict ulterior nu reprezintă, potrivit reglementărilor actuale, acte interzise şi nici atacuri armate[24], astfel că este necesară distincţia între actele care sunt infracţionale şi actele ce pot fi calificate drept război cibernetic (*cyberwarfare*), ce produc efecte similare atacurilor armate[25]. De asemenea, este necesară stabilirea caracterului ostil al operaţiunilor informatice şi, în funcţie de acesta, urmează identificarea reacţiilor de răspuns permise de regulile dreptului internaţional.

Cu titlu de exemplu, Franţa, prin mai multe reglementări (*Livre blanc sur la defence et la sécurité nationale*, din 2013, *International Cyber Strategy* din 2017, *Strategic Review of Cyberdefense* din 2018), a reglementat un sistem naţional de

---

21 Carta Națiunilor Unite a fost semnată la San Francisco la 26 iunie 1945, la încheierea Conferinței Națiunilor Unite pentru Organizația Internațională și a intrat în vigoare la 24 octombrie 1945.

22 Conform informațiilor disponibile la adresa: https://www.infosecurity-magazine.com/news/uk-councils-800-cyberattacks-per/ (accesată la 20 octombrie 2019).

23 *International Strategy on Cyberspace: Prosperity, Securiy and Openness in a Networked World*, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accesat la 10 ianuarie 2020); D. P. Fidler, *International Law and the Future of Cyberspace: The Obama Administration's International Strategy for Cyberspace,* ASIL Insight, Issue 15, Volume 15, 2011, https://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration%E2%80%99s, accesat la 10 ianuarie 2020.

24 T.D. Gill, P.A. Ducheine, *Anticipatory Self-Defense in the Cyber Context,* în International Law Studies, Volume 89, 2013, p. 440.

25 M. Roscioni, *World Wide Warfare-Jus ad bellum and the Use of Cyber Force*, Max Planck Yearbook of United Nations Law, Volume 14, 2010, p. 115, https://www.mpil.de/files/pdf3/mpunyb_03_roscini_141.pdf (accesată la 10 ianuarie 2020); M. Hoisington, *op. cit.*, p. 446.

calificare a unui incident informatic (*cyber security incident*) în funcţie de valoarea sau interesul legitim prejudiciat, iar acest sistem are efecte extrateritoriale nu doar dacă se petrece pe teritoriul francez, ci şi dacă atacurile privesc sisteme de computere franceze aflate în afara teritoriului statului francez.[26] Abordarea franceză este centrată pe ideea de suveranitate şi pune accentul pe acţiunea în sine de penetrare a sistemului informatic, nu pe consecinţe.

Includerea atacurilor informatice în categoria atacurilor „armate", potrivit regulilor dreptului internaţional public, prezintă atât un interes teoretic, cât şi practic, mai ales dacă am avea, ipotetic, ca punct de plecare un scenariu în care la un moment dat s-ar constata nefuncţionarea globală a serviciilor cu care în general persoanele sunt obişnuite (de la accesul la Internet la informaţiile bancare, control al traficului, elemente de infrastructură), toate aceste efecte fiind produse de un atac cibernetic. Prejudiciile produse ar fi, fără îndoială, deosebit de grave şi ar putea semnifica disfuncţionalitatea societăţii în ansamblul ei. Efectele ar putea fi comparate cu cele ale unui atac armat sau chiar nuclear.

Unul dintre aspectele care trebuie lămurite este dacă atacul trebuie să producă prejudicii fizice şi victime pentru a fi considerat un atac armat sau se poate admite că prejudicii nemateriale produse în afara unui conflict armat de tip clasic pot fi considerate folosire a forţei sau un act de război, mai ales pornind de la ideea că atacurile cibernetice pot avea ca obiectiv producerea de daune directe sau indirecte şi, de asemenea, pot fi şi mijloc de presiune pentru anumite state. Astfel, ar putea fi incluse în categoria atacurilor cibernetice asimilate atacurilor armate atacuri asupra centralelor nucleare, distrugerea unui dig din apropierea unei aşezări locuite şi lăsarea fără protecţie a populaţiei, deturnarea avioanelor şi intervenirea în controlul traficului aerian.

Pentru a verifica dacă atacurile cibernetice pot fi calificate drept atacuri armate, în doctrina de specialitate au fost propuse o serie de criterii: gravitatea atacului (în sensul că a cauzat prejudicii materiale sau distrugeri ale proprietăţilor într-un grad mai mare decât orice altă formă de constrângere); nemijlocirea producerii atacului; legătura de cauzalitate între atacuri şi efectele negative cauzate; caracterul invaziv al acestora (sunt comise în scopul de a cauza rău); posibilitatea cuantificării efectelor; prezumţia că atacul este nelegitim[27].

Din elementele scenariului sumbru prezentat anterior rezultă că producerea de atacuri cibernetice este foarte eficientă, rapidă şi nu la fel de costisitoare ca un „atac clasic", cu folosirea forţelor armate. De asemenea, identificarea sursei, a persoanelor responsabile şi stabilirea unei eventuale imputabilităţi către un anumit stat poate fi un proces dificil. Atacuri informatice

---

[26] P. Roguski, *France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations Part. I*, http://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accesată la 15 octombrie 2019).

[27] M.N. Schmitt, *Computer Network Attacks and the Use of Force in International Law: Thoughts on a Normative Framework*, Columbia Journal of Transnational Law, Volume 37, 1999, p. 915.

de o asemenea anvergură ar putea fi comise de particulari, organizaţii teroriste, cu sau fără sprijinul statelor.

Problemele date de vidul de reglementare ar putea fi rezolvate de Organizaţia Naţiunilor Unite, entitate ce are ca scop crearea de standarde de comportament pentru state în cadrul internaţional, dar şi sarcina de a interveni în acest domeniu şi de a insista în adoptarea unor instrumente juridice care să reglementeze conduita statelor şi a entităţilor non-statale.

Rolul organismelor special înfiinţate în cadrul Adunării Generale a Naţiunilor Unite, cu atribuţii complementare, *Open-ended Working Group* (OEWG) la iniţiativa Federaţiei Ruse şi a Republicii Chineze şi *Group of Governmental Experts* (*GGE*), este identificarea şi clarificarea obligaţiilor pe care statele trebuie să le respecte pentru a avea un comportament responsabil în spaţiul cibernetic (spaţiul virtual).

Până în prezent, o concluzie este certă (exprimată de către state[28] în expunerea poziţiilor lor, în cadrul OEWG): în spaţiul virtual sunt aplicabile regulile dreptului internaţional, fără a se preciza, însă, în ce măsură, care este conţinutul adaptat al acestor reguli specificului spaţiului virtual şi cum ar trebui să fie interpretate. De asemenea, Raportul 2014-2015 al GGE include o secţiune separată cu privire la norme, reguli şi principii pentru conduita responsabilă a statelor în spaţiul cibernetic şi pune accentul pe aplicarea suveranităţii statelor şi a regulilor şi principiilor dreptului internaţional conduitei statelor în activităţile derulate în legătură cu mijloacele şi tehnologiile de comunicare [29].

Dificultăţi în privinţa exercitării legitimei apărări în spaţiul cibernetic

Posibilitatea recurgerii la forţă armată, în conformitate cu regulile dreptului internaţional actual, este redusă şi se referă la exercitarea legitimei apărări. În accepţiunea sa clasică, exercitarea legitimei apărări este posibilă în condiţiile comiterii unui atac, conform dispoziţiilor articolului 51 din Carta Naţiunilor Unite.

O interpretare extensivă a noţiunii „atac" determină concluzia aplicabilităţii dreptului la legitima apărare în cazul comiterii de atacuri cibernetice. Însă, în această privinţă, în ciuda aspectelor reţinute de cele două organisme ale Adunării Generale, nu există o abordare sau un punct de vedere general sau uniform acceptat de către state.

În cazul în care în discuţie este posibilitatea exercitării unei legitime apărări preventive sau anticipate, aspectul cel mai dificil de probat este caracterul

[28] Australia, Canada, China, Iran, Marea Britanie.

[29] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 (accesat la 20 octombrie 2019).

iminent al atacului, urmat de natura actelor care pot fi folosite ca răspuns, urmat de respectarea condiţiei proporţionalităţii reacţiei statului victimă[30].

În cazul în care în discuţie este posibilitatea exercitării legitimei apărări în forma sa clasică, prevăzută de articolul 51 din Carta Naţiunilor Unite, problema rămasă neclară este în ce poate consta reacţia de răspuns a statului atacat, având în vedere că, în privinţa justificării folosirii legitimei apărări, aceasta depinde de natura actului ostil, nu de calitatea autorului.

Din aceste motive, apare ca necesară clarificarea şi definirea noţiunii „atac cibernetic sau informatic", pentru a fi asigurată continuitatea reacţiilor comunităţii internaţionale. O astfel de definire sau clarificare ar face posibilă identificarea acţiunilor pe care le pot întreprinde statele şi, de asemenea, stabilirea unui sistem echitabil de sancţionare a celor care au încălcat securitatea cibernetică. Însă discuţia este diferită în cazul în care atacul informatic este iminent, deoarece ar putea fi considerată justificată legitima apărare preventivă sau anticipată[31].

Unul dintre cele mai sensibile aspecte care are legătură cu atragerea răspunderii pentru atacuri este verificarea condiţiei imputabilităţii. Ca reguli generale, aceasta poate fi directă, în situaţiile în care statul este responsabil pentru actele şi omisiunile indivizilor care exercită autoritatea de stat, sau indirectă, atunci când nu îndeplineşte obligaţia de *due dilligence* în prevenirea unor astfel de acte[32].

Conţinutul actual al paradigmei *ius ad bellum* nu oferă răspunsuri şi nici remediile acceptabile în ceea ce priveşte reacţia faţă de atacurile cibernetice, iar tehnologia nu permite sau face dificilă atribuirea către o anumită entitate sau identificarea intenţiei autorului[33].

Cel mai dificil proces este de prezentare a unor dovezi clare şi convingătoare şi respectarea standardului stabilit în domeniul dreptului penal în stabilirea vinovăţiei dincolo de orice îndoială rezonabilă, ceea ce echivalează cu cerinţa imputabilităţii conduitei ilicite[34].

Poziţia NATO în privinţa calificării atacurilor cibernetice ca atacuri armate

Relevanţă deosebită pentru discuţiile în această materie prezintă *Tallinn Manual on the International Law applicable to cyberwarfare*, adoptat în cadrul NATO în 2013 şi completat în anul 2017, ca rezultat al activităţii de cercetare a unui grup de experţi desemnaţi de *NATO – Cooperative Cyber Defence Center for*

---

30 H.B. Robertson, *Self-Defense against Computer Network Attack under International Law*, în International Law Studies, Volume 76, 2002, p. 138-139; C.M. Petras, *op. cit.*, p. 66.

31 Ryan J. Hayward, *Evaluating the „imminence" of a cyber attack for purposes of anticipatory self-defense*, Columbia Law Review, Volume 117. No. 2, https://columbialawreview.org/content/evaluating-the-imminence-of-a-cyber-attack-for-purposes-of-anticipatory-self-defense/ (accesată la 20 octombrie 2019).

32 E.F. Mejia, *op. cit.*, p. 118.

33 M. Hoisington, *op. cit.*, p. 452.

34 E.F. Mejia, *op. cit.*, pp. 122-123.

Excellence[35]. Înfiinţarea Centrului de excelenţă şi redactarea manualului au reprezentat reacţia NATO la atacurile cibernetice ale Rusiei asupra Estoniei, în anul 2007.

Potrivit concluziilor din acest document internaţional, unele operaţiuni cibernetice pot fi suficient de grave astfel încât să poată fi clasificate drept atacuri armate din perspectiva articolului 51 din Carta Naţiunilor Unite[36]. În viziunea experţilor care au întocmit *Tallinn Manual*, nu sunt incluse în actele armate acţiunile de colectare a datelor privind informaţii secrete (*cyber intelligence gathering*) sau furtul acestora şi nici operaţiunile cibernetice care implică o întrerupere temporară sau periodică a unor servicii informatice neesenţiale.

Opinia unanimă a experţilor, în sensul includerii în categoria atacurilor armate a celor cibernetice, este că „orice folosire a forţei care răneşte sau ucide persoane ori deteriorează sau distruge proprietăţi" îndeplineşte cerinţele unui atac armat[37], ceea ce corespunde şi criteriilor atacurilor clasice[38], fără a fi în discuţie un anumit număr de victime sau un anumit grad de deteriorare a bunurilor.

Într-o altă abordare, neacceptată în unanimitate de către membrii grupului de experţi, este pus în aplicare un prag inferior al unei operaţiuni cibernetice, pentru a fi inclusă în categoria atacurilor armate, în sensul următor: chiar dacă o operaţiune cibernetică nu produce în mod imediat distrugeri ale bunurilor sau vătămări corporale, amploarea şi consecinţele ei negative ar putea determina calificarea ei ca atac armat [39].

Manualul de la Tallinn nu răspunde tuturor aspectelor legate de calificarea atacurilor cibernetice şi legalitatea reacţiilor din partea statului victimă şi nici asupra întrebării dacă mecanismul de securitate colectivă şi apărare al NATO, prevăzut în articolele 4 şi 5 din Tratatul Nord-Atlantic[40], este declanşat de activităţile cibernetice[41].

---

35 M.N. Schmitt (ed.), *Tallinn Manual on International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013, disponibil şi la adresa: http://csef.ru/media/articles/3990/3990.pdf, accesată la 10 ianuarie 2020. Informaţii suplimentare pot fi consultate la adresa: https://ccdcoe.org/research/tallinn-manual/ (accesată la 10 ianuarie 2020).

36 *Idem.*

37 *Idem*, p. 54-55

38 Ryan J. Hayward, *Evaluating the „imminence" of a cyber attack for purposes of anticipatory self-defense,* Columbia Law Review, Volume 117. No. 2, https://columbialawreview.org/content/evaluating-the-imminence-of-a-cyber-attack-for-purposes-of-anticipatory-self-defense/ (accesată la 20 octombrie 2019).

39 M.N. Schmitt (ed.), *op. cit.*, p. 56-57.

40 Tratatul Nord-Atlantic a fost adoptat la Washington la 4 aprilie 1949. Articolul 4 din Tratatul Nord-Atlantic prevede: „Părţile se vor consulta ori de câte ori, în opinia vreuneia dintre ele, este ameninţată integritatea teritorială, independenţa politică sau securitatea oricăreia dintre părţi". Articolul 5 din Tratatul Nord-Atlantic prevede: „Părţile convin că un atac armat împotriva uneia sau mai multora dintre ele, în Europa sau în America de Nord, va fi considerat un atac împotriva tuturor părţilor şi, în

Concluzii

Ca regulă generală, folosirea forţei implică şi respectarea regulilor dreptului internaţional umanitar. În situaţia includerii atacurilor cibernetice în sfera atacurilor „armate" care justifică folosirea legitimei apărări, apare şi rămâne în continuare actuală întrebarea în funcţie de ce criterii sau elemente poate fi pusă în discuţie aplicarea concretă a acestor reguli, deoarece este imposibilă distincţia, în spaţiul virtual, între obiectivele civile şi cele militare.

Lucrările recente ale organismelor special înfiinţate de către Adunarea Generală a Naţiunilor Unite reprezintă încercări de clarificare a cadrului normativ aplicabil statelor în spaţiul cibernetic în definirea comportamentului responsabil, însă foarte multe aspecte legate de activitatea statelor şi a altor entităţi în acest spaţiu rămâne în continuare „într-o zonă gri" a regulilor dreptului internaţional, dominată de reglementările actorilor privaţi şi de interesele statelor de a nu stabili un cadru normativ clar.

Stabilirea controlului efectiv al statului, ca cerinţă pentru stabilirea imputabilităţii şi antrenarea răspunderii internaţionale a statelor, este de asemenea dificilă, iar furnizarea de ajutor financiar sau de echipamente pentru sprijinirea unui atac cibernetic ori chiar oferirea unui spaţiu (*safe haven base*) pentru persoanele implicate în comiterea atacurilor s-ar putea dovedi insuficiente pentru stabilirea controlului efectiv al statului.

consecinţă, sunt de acord că, dacă are loc un asemenea atac armat, fiecare dintre ele, în exercitarea dreptului la autoapărare individuală sau colectivă, recunoscut prin art. 51 din Carta Organizației Națiunilor Unite, va sprijini partea sau părțile atacate, prin realizarea imediată, individual și împreună cu celelalte părți, a oricărei acțiuni pe care o consideră necesară, inclusiv folosirea forței armate, în vederea restabilirii și menținerii securității în spațiul Atlanticului de Nord. Orice astfel de atac armat și toate măsurile adoptate ca urmare a acestuia vor fi imediat aduse la cunoștință Consiliului de Securitate. Aceste măsuri vor înceta după adoptarea de către Consiliul de Securitate a măsurilor necesare pentru restabilirea și menținerea păcii și securității internaționale".

41 U. Häußler, *Cyber Security and Defence From the Perspective of Articles 4 and 5 of the NATO Treaty*, https://ccdcoe.org/uploads/2010/01/6.Haussler_CDfromArticles4and5Perspective-1.pdf (accesată la 10 ianuarie 2020).