RĂZBOIUL CIBERNETIC ȘI TERORISMUL CIBERNETIC – TRĂSĂTURI ȘI RĂSPUNSURI LA ACESTE AMENINȚĂRI –

Colonel (r.) dr. Romică CERNAT

În ultimii ani, spațiul cibernetic a obținut o importanță strategică ascendentă, astfel că statele au început să-l trateze ca pe un domeniu similar celui terestru, maritim și aerian, care trebuie să fie securizat pentru a-și proteja interesele lor naționale. Atacurile cibernetice sunt, acum, un element comun al conflictelor internaționale, atât separat, cât și în contextul unor operații militare mai ample. Atacurile în spațiul virtual s-au amplificat și diversificat în ceea ce privește actorii și metodele. Deoarece statele au devenit mult mai dependente de tehnologia informației și componentele rețelei critice de infrastructură, apar multe întrebări cu privire la faptul dacă un stat este organizat în mod corespunzător pentru a-și apăra mijloacele sale digitale strategice. Spațiul cibernetic integrează funcționarea infrastructurilor critice, precum instituțiile guvernamentale, de securitate națională și comerțul. Întrucât spațiul virtual transcende granițele geografice, o mare parte a acestuia este în afara controlului și influenței unui stat.

Cuvinte-cheie: război cibernetic, sistem informatic, program nuclear, terorism cibernetic, virus informatic.

CONSIDERAȚII PRELIMINARE

Conceptul de *„atac cibernetic"* este relativ recent și se referă la o gamă largă de activități desfășurate prin utilizarea tehnologiei informației și a comunicațiilor (TIC). Utilizarea atacurilor de Interdicție a Serviciului de Distribuție a Datelor (ISDD) a devenit o metodă larg răspândită pentru a îndeplini obiective politice, prin întreruperea serviciilor on-line. În acest tip de atacuri, un server este copleșit de traficul de internet, astfel încât accesul la anumite site-uri este degradat sau interzis. Apariția virusului informatic Stuxnet, în iunie 2010, pe care unii îl consideră primul atac cibernetic, a arătat că atacurile cibernetice ar putea avea un efect distructiv și de durată. Creat pentru a sabota programul nuclear al Iranului, sistemul distructiv de programe pentru calculatoare Stuxnet a atacat sistemele de control industriale computerizate, cu care operează centrifugele nucleare ce produc uraniu îmbogățit, și avea ca finalitate autodistrugerea fizică a instalațiilor. Evenimente internaționale recente au ridicat semne de întrebare cu privire la situația în care un atac cibernetic ar putea fi considerat un act de război și ce fel de opțiuni de răspuns au la dispoziție statele victimă.

Apariția virusului informatic Stuxnet, în iunie 2010, pe care unii îl consideră primul atac cibernetic, a arătat că atacurile cibernetice ar putea avea un efect distructiv și de durată. Creat pentru a sabota programul nuclear al Iranului, Stuxnet a atacat sistemele de control industriale computerizate, cu care operează centrifugele nucleare ce produc uraniu îmbogățit, și avea ca finalitate autodistrugerea fizică a instalațiilor.

Având în vedere cele prezentate, consider că este imperios ca fiecare stat să dispună măsurile și mecanismele necesare la nivel național și de participare la nivel european și internațional, în domeniul asigurării securității rețelelor și sistemelor informatice, în vederea asigurării unui nivel comun ridicat de securitate și a stimulării cooperării în domeniu[1].

Atacurile cibernetice asupra Sony Entertainment ilustrează dificultățile în clasificarea atacurilor și elaborarea unei politici de răspuns. Pe 24 noiembrie 2014, corporația Sony a fost obiectul unui atac cibernetic care a dezactivat sistemele sale TIC, a distrus datele și stațiile de lucru și a accesat e-mailuri interne și alte date. Biroul Federal de Investigații (FBI) al Statelor Unite ale Americii și directorul Serviciului de Informații Naționale (SIN) au atribuit atacurile informatice guvernului

[1] *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, în *Monitorul Oficial*, Partea I nr. 21 din 9 ianuarie 2019, p. 1.

nord-coreean. Coreea de Nord a negat implicarea sa în atac, dar a lăudat un grup de hacktiviști, numit *„Gardienii Păcii”*, pentru că au făcut o *„faptă justă”*. În timpul unei conferințe de presă, pe 19 decembrie 2014, președintele Obama a promis să *„răspundă proporțional”* la presupusa agresiune cibernetică a Coreii de Nord, *„într-un loc, timp și mod ales de noi”*[2]. Președintele Obama a categorisit incidentul ca un act de *„cyber-vandalism”*, în timp ce alți analiști l-au catalogat ca un act de război cibernetic.

Odată cu natura globalizată a internetului, autorii pot lansa atacuri cibernetice de oriunde în lume și pot direcționa atacurile prin servere ce aparțin unor terțe țări. O analiză profundă a principalelor atacuri cibernetice asupra agențiilor guvernamentale, companiilor din sectorul de apărare și de înaltă tehnologie sau a infracțiunilor economice cu pierderi de mai mult de un milion de dolari evidențiază amploarea acestui fenomen.

Acest incident ilustrează dificultățile în ceea ce privește clasificarea atacurilor cibernetice, actorii implicați, motivațiile lor, precum și problemele de suveranitate referitoare la site-ul pe care actorii au fost localizați fizic. Odată cu natura globalizată a internetului, autorii pot lansa atacuri cibernetice de oriunde în lume și pot direcționa atacurile prin servere ce aparțin unor terțe țări. O analiză profundă a principalelor atacuri cibernetice asupra agențiilor guvernamentale, companiilor din sectorul de apărare și de înaltă tehnologie sau a infracțiunilor economice cu pierderi de mai mult de un milion de dolari evidențiază amploarea acestui fenomen[3]. A fost atacul cibernetic asupra Sony, o corporație privată cu sediul în Japonia, un atac asupra SUA? Mai mult, ar putea fi considerat un act de terorism, o utilizare a forței sau o infracțiune informatică? În categorisirea atacurilor asupra Sony ca un act de *„vandalism cibernetic”*, care, de obicei, include compromiterea site-urilor web și este, în genere, domeniul actorilor motivați politic cunoscuți sub numele de *„hacktiviști”*, președintele Obama a avut rezerve despre ce tip de răspuns ar putea fi considerat *„proporțional”* și împotriva cui. O altă întrebare potențială asociată ar putea fi circumstanțele în care SUA ar angaja trupe pentru a răspunde la un atac cibernetic. În relație logică este și întrebarea dacă SUA și alte state puternice au o strategie eficientă de descurajare în vigoare? Directorul Serviciului Național de Informații al SUA, James Clapper, a afirmat despre actorii războiului cibernetic că, *„dacă ei obțin*

[2] Barack Obama, *„Remarks by the President in Year-End Press Conference”*, 12 decembrie 2014, în *The White House Office of the Press Secretary*, disponibil la https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference, accesat la 20.12.2019.

[3] *„Significant Cyber Incidents Since 2006”*, în *Center for Strategic & International Studies*, disponibil la https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa, accesat la 7 ianuarie 2020.

recunoaștere la nivel mondial, la un cost redus și nu vor suferi nicio consecință, ei vor acționa în același mod, din nou, și vor continua să o facă iarăși, până când vom acționa împotriva lor"[4].

POZIȚIA STATELOR ȘI ORGANISMELOR INTERNAȚIONALE PRIVIND RĂZBOIUL CIBERNETIC

Infrastructura critică a statelor a fost, pentru mult timp, supusă amenințărilor fizice, iar acum este din ce în ce mai expusă riscului de atacuri în spațiul virtual[5]. Războiul cibernetic este, de obicei, conceptualizat ca acțiune stat-contra-stat, echivalent cu un atac armat sau folosirea forței în spațiul virtual, care poate declanșa un răspuns militar, cu o utilizare proporțională a forței. Infractorii, teroriștii și spionii, în activitatea lor, se bazează foarte mult pe tehnologiile cu suport cibernetic pentru a îndeplini obiectivele organizaționale. Teroriștii cibernetici sunt indivizi sponsorizați de actori statali și nestatali, care se angajează în atacuri informatice pentru a-și îndeplini obiectivele. Organizațiile teroriste transnaționale, insurgenții și jihadiștii au folosit internetul ca instrument pentru planificarea atacurilor, radicalizare și recrutare, ca o metodă de popularizare a propagandei, ca mijloc de comunicare, precum și pentru scopuri perturbatorii.

Teroriștii cibernetici sunt indivizi sponsorizați de actori statali și nestatali, care se angajează în atacuri informatice pentru a-și îndeplini obiectivele. Organizațiile teroriste transnaționale, insurgenții și jihadiștii au folosit internetul ca instrument pentru planificarea atacurilor, radicalizare și recrutare, ca o metodă de popularizare a propagandei, ca mijloc de comunicare, precum și pentru scopuri perturbatorii.

Nu există încă niște criterii clare pentru a stabili dacă un atac cibernetic este o infracțiune, un act de hacktivism, terorism sau utilizarea forței de către un stat, echivalentă cu un atac armat. De asemenea, nu au fost încă elaborate instrumente legale internaționale, cu caracter obligatoriu, care să reglementeze în mod explicit relațiile inter-statale în spațiul virtual.

În septembrie 2012, Departamentul de Stat al SUA a luat o poziție publică cu privire la faptul dacă atacurile cibernetice ar putea fi interpretate ca utilizare a forței în conformitate cu prevederile articolului 2, alineatul 4, din Carta ONU și ale Dreptului Internațional cutumiar. Potrivit consilierului de stat pe probleme juridice în funcție, Harold Koh, *„activitățile cibernetice care au ca rezultat nemijlocit*

[4] Chris Strohm, *„FBI Provides More Proof of North Korea Link to Sony Hack"*, 7 ianuarie 2015, în *Bloomberg*, disponibil la https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony, accesat la 20 decembrie 2019.

[5] The White House, *National Strategy for Counterterrorism of the United States of America*, octombrie 2018, p. 19, disponibil la https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf, accesat la 20 decembrie 2019.

moartea, vătămarea persoanelor sau distrugeri semnificative vor fi tratate, cel mai probabil, ca utilizare a forței"[6]. Exemplele oferite în comentariile lui Koh au inclus declanșarea distrugerii unei uzine nucleare, deschiderea unui baraj și provocarea de pagube prin inundații sau de accidente aviatice prin interferarea în controlul traficului aerian. Concentrându-se mai degrabă pe efectele obținute decât pe mijloacele cu care acestea sunt realizate, această definiție a războiului cibernetic se integrează cu ușurință în cadrul juridic internațional existent. În cazul în care un actor folosește un mijloc cibernetic pentru a produce efecte cinetice, care ar putea justifica utilizarea forței militare în alte circumstanțe, atunci întrebuințarea acestei arme cibernetice poate fi asimilată utilizării forței.

Unul dintre obiectivele de apărare ale SISC este de a lucra la nivel internațional „pentru a încuraja un comportament responsabil și să se opună celor care ar încerca să perturbe rețelele și sistemele, făcându-i să renunțe și să descurajeze actorii rău intenționați, rezervându-și dreptul de a-și apăra bunurile naționale".

Koh a explicat că atacurile cibernetice asupra rețelelor informatice pe timpul unui conflict armat în curs de desfășurare vor fi guvernate de aceleași principii de proporționalitate care se aplică altor acțiuni în temeiul legii conflictelor armate. Aceste principii includ represalii ca răspuns la un atac cibernetic, cu o utilizare proporțională a forței militare. În plus, *„activitățile specifice rețelei de calculatoare, care se ridică la nivelul unui atac armat sau al unei amenințări iminente"*, pot declanșa dreptul unui stat la autoapărare, în conformitate cu prevederile articolului 51 din Carta ONU. Koh citează, în remarcile sale, Strategia Internațională pentru Spațiul Cibernetic 2011 (SISC), care prevede că, *„atunci când se justifică, Statele Unite vor răspunde la actele ostile din spațiul cibernetic așa cum ar răspunde la orice altă amenințare la adresa țării noastre"*[7]. Unul dintre obiectivele de apărare ale SISC este de a lucra la nivel internațional *„pentru a încuraja un comportament responsabil și să se opună celor care ar încerca să perturbe rețelele și sistemele, făcându-i să renunțe și să descurajeze actorii rău intenționați, rezervându-și dreptul de a-și apăra bunurile naționale"*[8]. Creșterea gradului de conștientizare a amenințării mediului

6 Harold Hongju Koh, *„International Law in Cyberspace"*, în *U.S. Department of State*, *Archived content*, 18 septembrie 2012, disponibil la https://2009-2017.state.gov/s/l/releases/remarks/197924.htm, accesat la 20 decembrie 2019.

7 *„International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World"*, mai 2011, în *U.S Departament of State*, p. 14, disponibil la https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, accesat la 20 decembrie 2019.

8 *Ibidem*, p. 12.

în spațiul virtual a condus la două procese internaționale majore, orientate spre dezvoltarea unui consens expertizat internațional în rândul autorităților cibernetice internaționale.

Reglementări NATO pentru spațiul cibernetic. La un an după atacul privind ISDD în 2007, din Estonia, NATO a înființat Centrul de Excelență și Cooperare în Domeniul Apărării Cibernetice (CECDAC) în Tallinn, Estonia. CECDAC găzduiește grupuri de lucru și cursuri de drept și etică în spațiul virtual, precum și exerciții de apărare împotriva atacurilor cibernetice. În 2009, Centrul a convocat un grup internațional de experți independenți pentru a elabora un manual care să fie aprobat printr-un act normativ și să reglementeze modul de acțiune în cazul unui război cibernetic. Manualul Tallinn, după cum este cunoscut, a fost publicat în 2013[9]. Acesta stabilește 95 de *„norme severe scrise”*, care reglementează consecințele conflictului cibernetic în raport cu suveranitatea și responsabilitatea statului, legea conflictelor armate, dreptul umanitar și legea neutralității. Manualul Tallinn este un text academic și, deși oferă justificări rezonabile pentru aplicarea dreptului internațional, nu este obligatoriu, iar autorii evidențiază faptul că nu vorbesc în numele NATO sau al CECDAC.

Manualul Tallinn stabilește 95 de „norme severe scrise”, care reglementează consecințele conflictului cibernetic în raport cu suveranitatea și responsabilitatea statului, legea conflictelor armate, dreptul umanitar și legea neutralității.

Se poate spune că NATO, în prezent, nu are o poziție clară privind modul de aplicare a prevederilor articolelor 4 și 5 din Tratatul NATO în spațiul cibernetic și nu definește atacurile informatice ca o acțiune militară explicită. Manualul Tallinn echivalează utilizarea forței cu acele operații cibernetice ale căror *„efecte ... sunt asimilate cu cele care ar rezulta dintr-o acțiune care se califică drept un atac armat cinetic”*[10]. În cazul în care un atac este considerat a fi orchestrat de o organizație cibernetică infracțională, fie motivată politic sau financiar, atunci poate fi responsabilitatea statului atacat pentru a selecta un răspuns adecvat jurisdicției sale. Cu toate acestea, caracterul transnațional al majorității organizațiilor infracționale în spațiul cibernetic poate complica deciziile privind competența.

Manualul Tallinn este un text academic și, deși oferă justificări rezonabile pentru aplicarea dreptului internațional, nu este obligatoriu, iar autorii evidențiază faptul că nu vorbesc în numele NATO sau al CECDAC.

Dreptul conflictelor armate privind războiul cibernetic. Represaliile ca răspuns la atacuri armate sunt permise în dreptul internațional

[9] *„Tallinn Manual on the International Law Applicable to Cyber Warfare”*, în *The NATO Cooperative Cyber Defence Centre of Excellence*, p. 5, disponibil la http://csef.ru/media/articles/3990/3990.pdf, accesat la 6 ianuarie 2020.

[10] *Ibidem*, p. 54.

atunci când un stat beligerant încalcă, în timp de pace, dreptul internațional sau legea conflictelor armate în timp de război. Cu toate acestea, termenul de *„atac armat”* nu are o definiție prevăzută de un act normativ și este încă deschis la interpretare, completare și modificare în ceea ce privește atacurile cibernetice. Așa-numita *„Lege a Războiului”*, de asemenea, cunoscută ca *Legea Conflictului Armat*, concretizată în Convențiile de la Geneva, Haga și Carta ONU, poate, în anumite circumstanțe, să se aplice și atacurilor cibernetice, dar nu s-au consemnat încercări din partea statelor de a o aplica sau existența unor acorduri specifice cu privire la aplicabilitatea sa, relevanța sa, în aceste condiții, rămânând neclară. Aplicarea devine complicată, de asemenea, și din cauza dificultăților în atribuire, de utilizarea potențială a computerelor de la distanță, precum și de posibilele daune produse unor terțe părți rezultate din contraatacurile cibernetice, care ar putea fi dificil de controlat sau restricționate. În plus, rămân problemele legate de granițele teritoriale și ceea ce reprezintă un atac armat în spațiul cibernetic. Aplicarea legii ar părea mai clară în situațiile în care un atac cibernetic provoacă daune fizice, cum ar fi întreruperea unei rețele electrice. După cum am menționat, Manualul Tallinn abordează mai multe dintre aceste întrebări[11]. În lipsa unei definiții juridice pentru ceea ce constituie un *„atac armat”* în spațiul cibernetic, profesorul Michael Schmitt a propus următoarele criterii de analiză în conformitate cu dreptul internațional: severitatea, urgența, cauzalitatea, invazivitatea, cuantificarea, legitimitatea prezumtivă și responsabilitatea[12].

În lipsa unei definiții juridice pentru ceea ce constituie un „atac armat” în spațiul cibernetic, profesorul Michael Schmitt a propus următoarele criterii de analiză în conformitate cu dreptul internațional: severitatea, urgența, cauzalitatea, invazivitatea, cuantificarea, legitimitatea prezumtivă și responsabilitatea.

Principiile de bază cuprinse în Convenția de la Haga privind întrebuințarea forțelor armate sunt cele referitoare la necesitate militară, proporționalitate, umanitarism și echitate. Dacă armata unui stat desfășoară operații cibernetice în conformitate cu aceste principii, se poate spune că este angajată într-un război cibernetic.

Poziția Consiliului Europei privind infracționalitatea informatică. În acest context, Convenția Consiliului Europei privind infracționalitatea informatică este primul tratat internațional care încearcă să armonizeze

[11] Oona A. Hathaway, *„The Law of Cyber-Attack”,* în *California Law Review*, vol. 100, nr. 4, 2012, pp. 6-23, disponibil la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932, accesat la 6 ianuarie 2020.

[12] Katharina Ziolkowski, *„Ius ad bellum in Cyberspace – Some Thoughts on the ‹Schmitt-Criteria› for Use of Force”*, în *Legal&Policy Branch NATO CCD COE*, pp. 1-7, disponibil la https://ccdcoe.org/uploads/2012/01/5_3_ZiolkowskiIusAdBellumInCyberspace.pdf, accesat la 6 ianuarie 2020.

legile din fiecare țară, cu privire la ceea ce constituie activitatea infracțională în domeniul cibernetic. Acest tratat de aplicare a legii, de asemenea, cunoscut sub numele de *„Convenția de la Budapesta”*, impune semnatarilor să adopte legi penale împotriva diferitelor tipuri de activități specifice în spațiul virtual, pentru a permite instituțiilor de aplicare a legii să investigheze astfel de activități și să coopereze cu agenții similare ale altor state semnatare[13]. Deși este larg recunoscut ca cel mai de substanță acord internațional privind securitatea cibernetică, unii observatori îl consideră totuși un eșec[14]. Unii criticii avertizează că prevederile Convenției sunt limitate pe partea de implementare și nu există legislație corespondentă în toate țările, astfel că infractorii, în acest domeniu, pot opera nestingheriți. În plus, până în septembrie 2019, doar 64 de state au ratificat-o.

Rezoluțiile Adunării Generale a ONU referitoare la spațiul cibernetic. O serie de rezoluții ale Adunării Generale a ONU referitoare la securitatea informatică au fost adoptate în ultimii 19 ani. O rezoluție a solicitat redactarea unui raport elaborat de un grup internațional de experți guvernamentali din 15 state, inclusiv SUA. Scopul declarat al acestui proces a fost de a construi o *„cooperare pentru un mediu al TIC, pașnic, sigur, eficient și deschis”*, prin realizarea unui acord asupra *„normelor, regulilor și principiilor de comportament responsabil al statelor”* și identificarea măsurilor de consolidare a încrederii și a capacităților, inclusiv pentru schimbul de informații. Spre deosebire de activitatea desfășurată la Tallinn sub auspiciile NATO, acest proces, condus de SUA, a inclus atât China, cât și Rusia. Raportul rezultat în 2010, denumit uneori ca Raportul Grupului de Experți Guvernamentali, a recomandat o serie de măsuri pentru a *„reduce riscul de interpretări eronate care rezultă din întreruperile TIC”*, dar nu a inclus niciun acord cu caracter obligatoriu[15].

O serie de rezoluții ale Adunării Generale a ONU referitoare la securitatea informatică au fost adoptate în ultimii 19 ani. Una dintre rezoluții a solicitat redactarea unui raport elaborat de un grup internațional de experți guvernamentali din 15 state, inclusiv SUA, cu scopul de a construi o „cooperare pentru un mediu al TIC, pașnic, sigur, eficient și deschis”, prin realizarea unui acord asupra „normelor, regulilor și principiilor de comportament responsabil al statelor” și identificarea măsurilor de consolidare a încrederii și a capacităților, inclusiv pentru schimbul de informații.

[13] *„Convention on Cybercrime”*, Budapesta, 23.XI.2001, în *Council of Europe, European Treaty Series No. 185*, pp. 7-13, disponibil la https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680081561, accesat la 6 ianuarie 2020.

[14] Jack Goldsmith, *„Cybersecurity Treaties: A Skeptical View”*, 2 iunie 2011, în *Future Challenges in National Security and Law, edited by Peter Berko witz*, pp. 1-11, disponibil la http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf., accesat la 6 ianuarie 2020.

[15] United Nations Secretary General, *„Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”*, 30 iulie 2010, *United Nations General Assembly*, pp. 7-8, disponibil la https://www.un.org/ga/search/view_doc.asp?symbol=A/65/201, accesat la 6 ianuarie 2020.

Cu toate acestea, unii analiști consideră că raportul reprezintă un progres în depășirea diferențelor dintre SUA și Rusia cu privire la diferite aspecte ale securității cibernetice. În decembrie 2001, Adunarea Generală a adoptat Rezoluția 56/183, care a aprobat Summitul Mondial privind Societatea Informațională, pentru a discuta oportunitățile și provocările societății informaționale. Acest Summit a fost convocat pentru prima dată la Geneva, în 2003, apoi în Tunis, în 2005, și, ulterior, la Geneva, în mai 2013. Delegați din 175 de țări au participat la primul Summit, unde au adoptat o Declarație de Principii – o foaie de parcurs pentru realizarea unei societăți informaționale deschise. Summitul de la Geneva a lăsat alte probleme, mai controversate, nerezolvate, inclusiv problema administrării și a finanțării internetului. La ambele reuniuni la nivel înalt, propunerile ca SUA să renunțe la controlul Corporației Internet pentru Alocarea Numelor și Numerelor au fost respinse. Un tratat internațional care să interzică războiul cibernetic și utilizarea informațiilor ca armă a fost propus în cadrul ONU de către delegațiile Rusei și Germaniei.

În decembrie 2001, Adunarea Generală a adoptat Rezoluția 56/183, care a aprobat Summitul Mondial privind Societatea Informațională, pentru a discuta oportunitățile și provocările societății informaționale. Acest Summit a fost convocat pentru prima dată la Geneva, în 2003, apoi în Tunis, în 2005, și, ulterior, la Geneva, în mai 2013. Delegați din 175 de țări au participat la primul Summit, unde au adoptat o Declarație de Principii – o foaie de parcurs pentru realizarea unei societăți informaționale deschise.

Alte acorduri internaționale privind războiul cibernetic. Unele organisme de drept internațional, în special cele asociate cu aviația și marina, pot aplica normele de securitate cibernetică, de exemplu, prin interzicerea perturbării controlului traficului aerian sau a altui comportament care ar putea pune în pericol siguranța aeronautică[16]. Planuri bilaterale, tratate reciproce de asistență juridică între țări pot fi aplicabile pentru investigații infracționale în domeniul securității cibernetice și al urmăririi penale.

TERORISMUL CIBERNETIC – CARACTERISTICI DEFINITORII

Ca și în cazul războiului cibernetic, în majoritatea legislațiilor naționale sau în legislația internațională nu există un consens privind o definiție a ceea ce constituie *terorismul cibernetic*. Unele definiții, abordând actele de terorism ce transcend frontierele, fac trimitere la activități și prejudicii definite în legislația privind fraudele și abuzurile în rețelele și sistemele informatice. Un aspect important al acestor documente juridice face referire la *„pedeapsa pentru o infracțiune”*, care atrage după sine amenzi sau închisoare și sugerează că partea

[16] Oona A. Hathaway, *op. cit.*, pp. 11, 28, 31-32.

agresoare săvârșește un act infracțional mai degrabă decât un act de terorism, în timp ce alții susțin că este un act de război, dacă sunt săvârșite de către un actor statal

De exemplu, Statele Unite ale Americii consideră că este ilegal pentru o entitate să *„acceseze cu bună știință un calculator fără autorizare sau să depășească nivelul de acces autorizat și, prin intermediul unor astfel de comportamente, să se obțină informații, pentru care s-a considerat de către Guvern, printr-un act normativ, că necesită protecție împotriva divulgării neautorizate, din motive de securitate națională sau relații externe, sau sunt restricționate din alte rațiuni, cu motive să se creadă că astfel de informații, obținute în modul acesta, pot fi utilizate pentru a prejudicia SUA sau pot fi folosite în avantajul oricărui stat străin”*[17]. Potrivit FBI, internetul și utilizarea mediei sociale, în special, sunt printre principalii *„factorii care au contribuit la evoluția peisajului amenințării terorismului”*, de la atacurile teroriste din 11 septembrie 2001[18].

Statele Unite ale Americii consideră că este ilegal pentru o entitate să „acceseze cu bună știință un calculator fără autorizare sau să depășească nivelul de acces autorizat și, prin intermediul unor astfel de comportamente, să se obțină informații, pentru care s-a considerat de către Guvern, printr-un act normativ, că necesită protecție împotriva divulgării neautorizate, din motive de securitate națională sau relații externe, sau sunt restricționate din alte rațiuni”.

Unele analize juridice definesc terorismul cibernetic ca *„utilizarea premeditată de activități perturbatoare sau amenințarea cu acestea, împotriva calculatoarelor sau rețelelor, cu intenția de a cauza un prejudiciu sau a realiza alte obiective sociale, ideologice, religioase, politice sau similare sau pentru a intimida orice persoană în scopul promovării unor astfel de obiective”*[19]. Cu toate acestea, astfel de acțiuni au, de asemenea, statut infracțional și, în general, se referă la persoane sau organizații mai degrabă decât la actorii statali. Unele definiții ale terorismului cibernetic se concentrează pe distincția dintre acțiunea distructivă și cea perturbatoare, terorismul generând o teamă comparabilă cu cea a atacului fizic și nu este doar un dezastru costisitor. Deși blocarea distribuită a unui serviciu în sine nu produce acest tip de frică sau de distrugere, problema este potențialul pentru efectele de ordinul al doilea sau al treilea[20]. De exemplu, dacă serviciile de telecomunicații și de urgență au fost complet inoperabile

[17] H. Marshall Jarrett, *„Prosecuting Computer Crimes”*, în *Office of Legal Education Executive Office for United States Attorneys*, pp. 12-13, disponibil la https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ccmanual.pdf, accesat la 6 ianuarie 2020.

[18] FBI, *„Terrorism”*, în *What We Investigate*, disponibil la https://www.fbi.gov/investigate/terrorism, accesat la 6 ianuarie 2020.

[19] Barry C. Collin, *„Cyberterrorism”*, în *Institute for Security and Intelligence, 11th Annual International Symposium on Criminal Justice Issues*, p. 1, disponibil la https://www.nato.int/structur/library/bibref/cyberterrorism.pdf , accesat la 6 ianuarie 2020.

[20] DDoS – Distributed Denial of Service.

într-o perioadă de criză, efectele unui astfel de atac asupra infrastructurii ar putea fi catastrofale. Cu toate acestea, într-o astfel de situație, sistemul de servicii de urgență în sine nu este cel mai probabil o țintă, ci, mai degrabă, rezultatul unor daune colaterale la o rețea de telecomunicații vulnerabilă**.** De la atacul din 2007 în Estonia, NATO a stabilit autoritățile cu responsabilități în domeniul apărării cibernetice, cu obiective de dezvoltare a strategiei în acest domeniu și de centralizare a capacităților de apărare în rândul membrilor. O politică privind apărarea cibernetică și un plan de acțiune asociat au fost adoptate în 2011, iar pentru a facilita efortul de centralizare, a fost înființată, în 2012, Agenția Comunicațiilor și Societății Informaționale NATO[21].

În literatura de specialitate, în scop analitic și statistic, există diferite definiții pentru sintagma „terorism cibernetic", la fel cum există mai multe definiții pentru termenul „terorism".

Caracteristicile terorismului cibernetic. În literatura de specialitate, în scop analitic și statistic, există diferite definiții pentru sintagma *„terorism cibernetic"*, la fel cum există mai multe definiții pentru termenul *„terorism"*. Terorismul a fost definit ca fiind violența premeditată, motivată politic, comisă împotriva țintelor necombatante, de subgrupuri naționale sau agenți clandestini, de obicei în scopul de a influența o anumită colectivitate. Dorothy Denning, expert în securitate, definește terorismul cibernetic ca fiind *„... operațiile motivate politic, de pătrundere neautorizată în rețele de date și informații secrete, menite să provoace prejudicii grave, cum ar fi pierderea de vieți omenești sau pagube economice cu consecințe grave"*[22]. Agenția Federală de Managementul Urgențelor a SUA definește terorismul cibernetic ca *„atacurile ilegale și amenințările de atac împotriva computerelor, rețelelor, precum și informațiilor stocate pe acestea, atunci când sunt săvârșite pentru a intimida sau a constrânge un guvern sau populația unui stat, în scopul promovării unor obiective politice sau sociale"*[23].

Terorismul a fost definit ca fiind violența premeditată, motivată politic, comisă împotriva țintelor necombatante, de subgrupuri naționale sau agenți clandestini, de obicei în scopul de a influența o anumită colectivitate.

Alți analiști evidențiază faptul că un atac fizic care distruge centrele computerizate pentru infrastructurile critice, cum ar fi internetul, telecomunicațiile sau rețelele de energie electrică, chiar fără a atinge

---

[21] Olivier Kempf, *„NATO and Cyberdefense"*, în *NDC Research Paper*, article nr. III.6, mai 2013, p. 3, disponibil la https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf, accesat la 7 ianuarie 2020.

[22] Dorothy Denning, *„Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy",* în *Nautilus Institute,* conference on *„The Internet and International Systems"*, p. 3, disponibil la https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf , accesat la 6 ianuarie 2020.

[23] Sarah Gordon, *„Cyberterrorism?"*, în *Symantec white paper*, iulie 2002, p. 4, disponibil la https://www.symantec. com/avcenter/reference/cyberterrorism.pdf , accesat la 7 ianuarie 2020.

vreodată o tastatură, de asemenea, poate contribui la sau să fie etichetat ca terorism cibernetic[24]. Proporția din infracționalitatea informatică ce poate fi atribuită în mod direct sau indirect teroriștilor este dificil de determinat. Cu toate acestea, există legături între grupurile teroriste și infractori, care permit rețelelor teroriste să se extindă la nivel internațional, prin valorificarea resurselor informatice, activități de spălare a banilor sau prin rutele de tranzit operate de infractori[25].

Unii experți estimează că atacuri cibernetice avansate sau structurate, împotriva mai multor sisteme și rețele, inclusiv supravegherea țintelor și testarea unor noi instrumente sofisticate de *pătrunderi neautorizate*, ar putea necesita o perioadă de pregătire de la doi la patru ani, în timp ce un atac cibernetic complex coordonat, care să provoace perturbări în masă împotriva sistemelor integrate, eterogene poate necesita șase la zece ani de pregătire[26].

Circumstanțe de analiză privind terorismul cibernetic. Distincțiile dintre infracțiune, terorism și război tind să se estompeze atunci când se încearcă să se descrie un atac asupra unei rețele de calculatoare (ARC), în moduri comparative din alte domenii ale vieții sociale. De exemplu, în cazul în care un stat ar sponsoriza în secret actori nestatali care inițiază un ARC pentru a sprijini activitățile teroriste sau pentru a crea perturbări economice, distincția dintre infracționalitatea informatică și războiul cibernetic devine mai puțin clară, deoarece este dificil de spus de unde provine un atac cibernetic, având în vedere că un atacator poate direcționa suspiciune către o terță parte, inocentă.

Proporția din infracționalitatea informatică ce poate fi atribuită în mod direct sau indirect teroriștilor este dificil de determinat. Cu toate acestea, există legături între grupurile teroriste și infractori, care permit rețelelor teroriste să se extindă la nivel internațional, prin valorificarea resurselor informatice, activități de spălare a banilor sau prin rutele de tranzit operate de infractori.

[24] Edward V. Linden, *„Focus on terrorism”*, în *Nova Science Publishers, Inc*, vol. 9, p. 6, disponibil la https://books.google.ro/books?id=wl-Ds42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+200,+p.6&source=bl&ots=dRkvffLk4i&sig=ACfU3U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4 sKHSzXB8wQ6AEw AH oECAoQAQ#v =onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism%E2%80%9D%2C%20Computerworld%2C%20August%2011%2C%202003%2C%20p.6&f=false, accesat la 7 ianuarie 2020.

[25] Rollie Lal, *„Terrorists and organized crime join forces”*, în *The New York Times*, 24 mai 2005, p. 1, disponibil la https://www.nytimes.com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html, accesat la 7 ianuarie 2020.

[26] Clay Wilson, *„Computer Attack and Cyberterrorism”*, în *Naval History and Heritage Command*, p. 17, disponibil la https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html, accesat la 7 ianuarie 2020.

De asemenea, interacțiunile dintre teroriști și infractorii care folosesc TIC pot estompa, uneori, distincția dintre infracționalitatea informatică și terorismul cibernetic.

Totodată, pot fi cazuri în care persoane fizice furnizează expertiză în calculatoare unui infractor sau terorist și pot să nu conștientizeze intențiile persoanei care a solicitat sprijinul. În acest context, rămâne, în continuare, dificilă identificarea surselor responsabile pentru cele mai multe atacuri perturbatoare, dar din ce în ce mai sofisticate, care compromit internetul. Având în vedere dificultatea de a determina autorul intruziunii sau al atacurilor cibernetice, unii autori susțin că, spre deosebire de răspunderea specifică actelor infracționale tradiționale, accentul ar trebui să fie pus mai degrabă pe faptă decât pe făptuitor, iar pragul pentru declanșarea de acțiuni defensive sau ofensive ar trebui să fie coborât. Internetul a fost folosit ca principal instrument de recrutare pentru insurgenți în Irak[27]. Insurgenții au creat multe site-uri în limba arabă, care au avut responsabilitatea de a conține planuri codificate pentru noi atacuri. Unele dintre acestea oferă sfaturi cu privire la modul de a construi și a întrebuința arme și cum să se treacă prin punctele de control la frontieră[28]. Alte articole de știri relatează despre o generație mai tânără de teroriști și extremiști, cum au fost cei din spatele atentatelor cu bombă din iulie 2005, din Londra, care au învățat noi abilități tehnice pentru a-i ajuta să evite detectarea, potrivit prevederilor legii aplicate TIC[29].

Pot fi cazuri în care persoane fizice furnizează expertiză în calculatoare unui infractor sau terorist și pot să nu conștientizeze intențiile persoanei care a solicitat sprijinul. În acest context, rămâne, în continuare, dificilă identificarea surselor responsabile pentru cele mai multe atacuri perturbatoare, dar din ce în ce mai sofisticate, care compromit internetul.

Când este considerat atacul cibernetic terorism cibernetic? Unii analiști sunt de părere că sintagma de *„terorism cibernetic"* este inadecvată, deoarece un atac cibernetic la scară largă poate produce, pur și simplu, dezordine, suferință, nu teroare, așa cum ar produce o bombă sau o altă armă chimică, biologică, radiologică sau nucleară. Cu toate acestea, alți analiști cred că efectele unui atac la scară largă asupra rețelelor de calculatoare ar fi imprevizibile și ar putea produce

---

[27] Jonathan Curiel, *„Iraq's tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet"*, în *San Francisco Chronicle*, 10 iulie 2005, pp. 1-3, disponibil la https://www.sfgate.com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php, accesat la 7 ianuarie 2020.

[28] *Ibidem*, p. 1.

[29] Michael Evans și Daniel McGrory, *„Terrorists Trained in Western Methods Will Leave Few Clues"*, în *London Times*, 12 iulie 2005, pp. 1-3, disponibil la https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q, accesat la 7 ianuarie 2020.

suficientă perturbare economică, frică și decese în rândul civililor, pentru a se califica drept un act de terorism[30]. Așadar, se pot evidenția cel puțin două puncte de vedere pentru a defini termenul de terorism cibernetic, și anume:

1. *bazat pe efecte*: terorismul cibernetic există atunci când atacurile informatice duc la efecte care sunt suficient de perturbatoare pentru a genera o teamă comparabilă cu cea a unui act tradițional de terorism, chiar dacă sunt săvârșite de către infractori;
2. *bazat pe intenție*: terorismul cibernetic există atunci când atacurile informatice ilegale sau motivate politic sunt săvârșite pentru a intimida sau a constrânge un guvern sau anumite personalități pentru a promova un obiectiv politic sau pentru a provoca prejudicii sau pagube economice grave.

Se pot evidenția cel puțin două puncte de vedere pentru a defini termenul de terorism cibernetic, și anume: unul bazat pe efecte și unul bazat pe intenție.

Eficiența legislației curente. Au instituțiile cu rol în domeniul securității autoritatea de care au nevoie pentru a lupta în mod eficient și a câștiga războiul în spațiul virtual? Anumiți analiști au susținut că, pentru a-și îndeplini misiunea de apărare, instituțiilor cu atribuții în domeniul apărării ar trebui să li se acorde o autoritate sporită asupra protecției infrastructurilor critice din sectorul privat. Cu toate acestea, proprietarii de afaceri, în special în sectorul IT, susțin că acest lucru ar reprezenta o *„militarizare a spațiului cibernetic”*, care ar crea neîncredere în rândul consumatorilor și al acționarilor și ar putea limita potențialul de inovare, ceea ce ar duce la scăderea profitului.

Așa cum s-a evidențiat, comunitatea internațională trebuie să elimine doza de ambiguitate cu privire la ceea ce constituie un *„atac armat”* în spațiul cibernetic și care sunt pragurile pentru ca un atac cibernetic să fie considerat un act de război, un incident de importanță națională sau ambele. Fără o linie de delimitare clară și consecințe specifice conturate cu claritate, strategiile de descurajare pot fi incomplete. Pe de altă parte, o lipsă de limitări explicite și consecințe ar putea constitui o formă de ambiguitate strategică, ceea ce ar genera instituțiilor cu atribuții în domeniul apărării manevrabilitate operațională.

[30] Serge Krasavin, *„What is Cyber-terrorism?”*, în *Computer Crime Research Center,* p. 1, disponibil la http://www. crime-research.org/analytics/Krasavin/, accesat la 7 ianuarie 2020.

CONCLUZII

Astăzi, în mod evident, spațiul cibernetic a devenit o altă dimensiune cu potențial atât de cooperare, cât și de conflict. Îngrijorarea în ceea ce privește potențialul de daune generat de terorismul cibernetic a crescut, deoarece un volum tot mai mare al activității economice se desfășoară on-line.

Majoritatea instituțiilor din domeniul apărării, ordinii publice și securității naționale sunt susținute parțial de servicii și produse de înaltă tehnologie civile, cel mai adesea sub formă de sisteme de comunicații și software de calculator. Un procent ridicat de mesaje militare *„curge”* prin canale de comunicare comerciale, iar această situație creează o vulnerabilitate pe timpul unui conflict sau al unei situații de criză. În conflictele viitoare, care implică războiul cibernetic între state, distincția dintre țintele militare și civile ale unui stat s-ar putea estompa și sistemele informatice civile pot fi văzute tot mai mult ca ținte viabile, vulnerabile la atac de către adversari. Tehnologia rețelelor și sistemelor informatice, de asemenea, a estompat granițele dintre războiul cibernetic, infracționalitatea informatică și terorismul cibernetic. Reprezentanți ai guvernelor și companiilor civile afirmă că, acum, infracționalitatea informatică și disponibilitatea pentru închirierea serviciilor aferente în vederea unui atac cibernetic, de către organizațiile infracționale, sunt o amenințare în creștere la adresa securității naționale a statelor, precum și pentru economia acestora.

Majoritatea instituțiilor din domeniul apărării, ordinii publice și securității naționale sunt susținute parțial de servicii și produse de înaltă tehnologie civile, cel mai adesea sub formă de sisteme de comunicații și software de calculator.

Instrumente noi și sofisticate de infracționalitate informatică ar putea opera pentru a permite unui actor statal sau grup terorist să rămână neidentificat în timp ce conduce atacuri informatice prin intermediul internetului. Putem concluziona că incidente de terorism convențional din trecut au fost deja asociate cu infracționalitatea informatică și că vulnerabilitățile calculatoarelor pot face sistemele de infrastructură critice guvernamentale și civile să pară atractive ca ținte pentru un atac cibernetic. Sunt indici care sugerează posibile legături între infractori cibernetici și grupurile teroriste care doresc să prejudicieze economia unui stat sau interesele de securitate națională ale acestuia.

Este clar faptul că grupările teroriste folosesc calculatoare și internetul pentru obiective suplimentare, asociate cu propagarea terorismului. Acest lucru poate fi văzut în modul în care extremiștii

creează și utilizează numeroase site-uri pe internet pentru activități de recrutare și de strângere de fonduri, precum și în scopuri de instruire a Jihadului. Mai mulți infractori care au fost recent condamnați pentru infracțiuni cibernetice au folosit abilitățile lor tehnice pentru a obține informații de pe cardurile de credit furate, în scopul de a finanța alte activități teroriste convenționale.

Statele întâmpină dificultăți legate de stabilirea strategiei pentru selectarea și aplicarea unui răspuns adecvat militar sau juridic, după un astfel de atac cibernetic.

Etichetarea unui *„atac cibernetic”* ca *„infracționalitate informatică”* sau *„terorism cibernetic”* este problematică din cauza dificultății în stabilirea cu certitudine a identității, intenției sau motivațiilor politice ale atacatorului.

Statele întâmpină dificultăți legate de stabilirea strategiei pentru selectarea și aplicarea unui răspuns adecvat militar sau juridic, după un astfel de atac cibernetic.

Sugestiile pentru creșterea motivației privind securitatea spațiului cibernetic pot include solicitarea ca toate programele achiziționate pentru agențiile naționale să fie certificate în cadrul unui program de testare, cu anumite criterii comune, și să reprezinte o cerință obligatorie pentru achiziționarea de software, cu toate că analiștii din domeniu subliniază faptul că procesul de certificare software este de lungă durată și poate interfera cu inovația și competitivitatea pe piața de software la nivel mondial.

În final, am putea sugera ca agențiile care operează sistemele naționale de securitate să achiziționeze produse software dintr-o listă de produse evaluate și testate în laborator, într-un program derulat de instituțiile cu atribuții în domeniul securității.

BIBLIOGRAFIE:

1. ***, *„Convention on Cybercrime”*, în *Council of Europe, European Treaty,* disponibil la https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId= 0900001680 081561.
2. ***, FBI, *„Terrorism”*, în *What We Investigate*, disponibil la https://www.fbi.gov/investigate/terrorism
3. ***, *„International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World”*, în *U.S Departament of State*, disponibil la https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/ international_ strategy_for_cyberspace.pdf.
4. ***, *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice*, în *Monitorul Oficial*, partea I nr. 21 din 09 ianuarie 2019.

5. *** *„National Strategy for Counterterrorism of The United States of America”*, în *The White House*, disponibil la https://www.whitehouse.gov/wp-content/uploads/2018/10/NSCT.pdf.
6. ***, *„Significant Cyber Incidents Since 2006”*, în *Center for Strategic & International Studies*, disponibil la https://csis-prod.s3.amazonaws.com/s3fs-public/200108_Significant_Cyber_Events_List.pdf?aj4_VlDq2hSan2U8O5mS29Iurq3 G1QKa.
7. ***, *„Tallinn Manual on the International Law Applicable to Cyber Warfare”*, în *The NATO Cooperative Cyber Defence Centre of Excellence*, disponibil la http://csef.ru/media/articles/3990/ 3990.pdf.
8. ***, United Nations Secretary General, *„Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security”*, *United Nations General Assembly*, disponibil la https://www.un.org/ga/search/ view_ doc.asp?symbol=A/65/201.
9. Barry C. Collin, *„Cyberterrorism”*, în *Institute for Security and Intelligence*, *11th Annual International Symposium on Criminal Justice Issues*, disponibil la https://www.nato.int/structur/library/bibref/cyberterrorism.pdf.
10. Jonathan Curiel, *„Iraq’s tech-savvy insurgents are finding supporters and luring suicide-bomber recruits over the Internet”*, în *San Francisco Chronicle*, disponibil la https://www.sfgate.com/news/article/TERROR-COM-Iraq-s-tech-savvy-insurgents-are-2623261.php.
11. Dorothy Denning, *„Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for Influencing Foreign Policy”*, în *Nautilus Institute,* conference on *„The Internet and International Systems”,* disponibil la https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf .
12. Michael Evans și Daniel Mcgrory, *„Terrorists Trained in Western Methods Will Leave Few Clues”*, în *London Times*, disponibil la https://www.thetimes.co.uk/article/terrorists-trained-in-western-methods-will-leave-few-clues-3tgqxdp7q0q.
13. Jack Goldsmith, *„Cybersecurity Treaties: A Skeptical View”*, în *Future Challenges in National Security and Law”,* disponibil la http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf.
14. Sarah Gordon, *„Cyberterrorism?”*, în *Symantec white paper*, disponibil la https://www.symantec.com/avcenter/reference/cyberterrorism.pdf.
15. Oona A. Hathaway, *„The Law of Cyber-Attack”,* în *California Law Review,* disponibil la https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2134932.
16. Jarrett H. Marshall, *„Prosecuting Computer Crimes”*, în *Office of Legal Education Executive Office for United States Attorneys,* disponibil la

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ ccmanual. pdf .
17. Olivier Kempf, *„NATO and Cyberdefense”*, în *NDC Research Paper*, disponibil la https://www.chaire-cyber.fr/IMG/pdf/nato_and_cyberdefense_olivier_kempf_05.2013.pdf.
18. Harold Hongju Koh, *„International Law in Cyberspace”*, în *U.S. Department of State*, *Archived content*, disponibil la https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.
19. Serge Krasavin, *„What is Cyber-terrorism?”*, în *Computer Crime Research Center,* disponibil la http://www.crime-research.org/analytics/Krasavin/.
20. Rollie Lal, *„Terrorists and organized crime join forces”*, în *The New York Times*, disponibil la https://www.nytimes. com/2005/05/24/opinion/terrorists-and-organized-crime-join-forces.html.
21. Edward V. Linden, *„Focus on terrorism”*, în *Nova Science Publishers, Inc*, disponibil la https://books.google.ro/books?id=wlDs42YMDIC&pg=PA30&lpg=PA30&dq=Dan+Verton,+%E2%80%9CA+Definition+of+Cyber-terrorism%E2%80%9D,+Computerworld,+August+11,+2003, +p.6&source=bl&ots=dRkvffLk4i&sig=ACfU3U3wC6ltTKQ2aQM6vL-EkQ2bVKetYg&hl=ro&sa=X&ved=2ahUKEwjBoJaJsYbnAhVil4sKHSzXB8wQ6AEwAHoECAoQAQ#v=onepage&q=Dan%20Verton%2C%20%E2%80%9CA%20Definition%20of%20Cyber-terrorism%E2%80%9D%2C%20Computerworld%2C%20August%2011%2C%20 2003%2C%20p.6&f=false.
22. Barak Obama, *„Remarks by the President in Year-End Press Conference”*, în *The White House Office of the Press Secretary*, disponibil la https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference.
23. Chris Strohm, *„FBI Provides More Proof of North Korea Link to Sony Hack”*, în *Bloomberg*, disponibil la https://www.bloomberg.com/news/articles/2015-01-07/clapper-warns-of-more-potential-north-korean-hacks-after-sony.
24. Clay Wilson, *„Computer Attack and Cyberterrorism”*, în *Naval History and Heritage Command*, disponibil la https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html.
25. Katharina Ziolkowski, *„Ius ad bellum in Cyberspace – Some Thoughts on the ‹Schmitt-Criteria› for Use of Force”*, în *Legal & Policy Branch NATO CCD COE*, disponibil la https://ccdcoe.org/uploads/2012/01/5_3_Ziolkowski_IusAdBellumInCyberspace.pdf.