DOI: 10.53477/1842-810X-21-15

EXTINDEREA ORDINII DE DREPT INTERNAȚIONAL UMANITAR ÎN SPAȚIUL INFORMAȚIONAL CU AJUTORUL DIPLOMAȚIEI DIGITALE

Dr. Daniel DUMITRU*
Cristina BODONI**

Amenințările hibride acoperă tot spectrul de știri false, război cibernetic/ informațional, acoperind periodic agenda multimedia în toate spațiile cunoscute de către om. Dacă pentru spațiile naturale ale Terrei avem norme și cutume respectate la nivel internațional, navigarea în spațiul digital nu conferă utilizatorului aceeași protecție dată de un cod de legi acceptat la nivel mondial, cu toate că avem un nou set de instrumente cu rol de scut împotriva pericolelor numit securitate cibernetică. Pentru ca această securitate cibernetică să fie acceptată de un număr cât mai mare de actori (ne)statali, avem nevoie norme internaționale, construite de profesioniști cu expertiză și gândire proactivă. Oamenii cu atribuții specifice pentru negocierea unor astfel de norme sunt diplomații, în cazul de față diplomații digitali. Care este rostul lor? Ce legătură este între război hibrid, diplomație digitală și drept umanitar? Sunt întrebări la care încercăm să răspundem prin intermediul acestei cercetări. În structura lucrării am utilizat concepte din normele DIU care se pot adapta operațiilor cibernetice și amenințărilor hibride. În cazul utilizării acțiunilor cibernetice agresive și a capacităților cibernetice, competența legii internaționale actuale este obiectivul articolului pentru apariția dreptului la autoapărare. Apoi, urmărim aspecte ale unor acțiuni militare care implică atacuri cibernetice, proiectate pe spectrul operației cibernetice, urmând ca aceste acțiuni cibernetice să fie examinate aplicând principii stabilite de legile existente.

**** Daniel DUMITRU este profesor universitar doctor, conducător de doctorat în domeniul Informații și Securitate Națională, Universitatea Națională de Apărare „Carol I", București. E-mail: daniel_dumitru64@yahoo.com.***
***** Cristina BODONI este doctorand în domeniul Informații și securitate națională, Universitatea Națională de Apărare „Carol I", București. E-mail: cristina_bodoni@yahoo.co.uk***

***Cuvinte-cheie**: amenințări hibride; atacuri cibernetice; drept internațional umanitar; operații militare; infracționalitate cibernetică; diplomație digitală.*

Argumentum

„Schimbarea este legea vieții.
Sunt sigur că cei care privesc doar spre trecut sau
prezent, vor rata viitorul.” John F. Kennedy

Inițiem acest demers cu citatul anterior întrucât el își menține valabilitatea, este mai actual ca oricând, deoarece atenționează oamenii legii cu privire la un viitor incert, în care indivizii au intrat într-un vortex al schimbării produsă de inovație tehnologică, pur și simplu amorală. Aici avem cu adevărat nevoie de noi norme sau de adaptarea celor vechi la noi cerințe. Astfel că implicarea oamenilor legii în reformularea codului legislativ național și internațional este permanentă, ei trebuie să fie conștienți de faptul că dreptul nu este un sistem de logică abstractă, este rezultatul unei negocieri între specialiști ai lumii juridice și jurisdicționale.

Aceasta este o rețea de aranjamente cu adânci rădăcini istorice și ramuri actuale, promovate în speranța că se vor utiliza practici vechi integrate proporțional în normele și cutumele actuale (inter)naționale ale securității, în special ale securității naționale[1]; indiferent de starea de fapt, pace sau război, dintre toate spațiile naturale și cel artificial − informațional, avem nevoie de o diplomație capabilă să utilizeze toate instrumentele posibile pentru a reuși să obțină norme internaționale utile pentru o cât mai mare parte a utilizatorilor de instrumente digitale[2]. Aceste norme au devenit necesare într-o lume în care numărul amenințărilor hibride a crescut exponențial, deoarece ele provoacă vulnerabilitate în sistemele de securitate și celor mai puternice state, riscul de escaladare crește proporțional, putând să se transforme oricând în război cibernetic. Acest sector de activitate a devenit unul dintre principalele amenințări de securitate cu care se confruntă toate tipurile de actori (ne)statali, în care nu avem încă acceptate mecanisme adecvate și legitimate în gestionarea noilor tipuri de război prin reguli transferabile în spațiul cibernetic.

În prezent avem o societate mondială anarhică, dar funcțională, care nu elimină conflictul, poate acționa în mod preventiv în scopul de a modifica forma conflictului,

[1] Adam C. Pritchard, Robert B. Thompson, *Securities Law and the New Deal Justices*, pdf, pp. 845-847, URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2552&context=articles, accesat la 03.06.2021.
[2] Shaun Riordan, *Cyberdiplomacy, Managing security and governance online*, Editura Policy Press, Cambridge, UK, 2019, p. 3.

punând mai mult accentul pe formele nonviolente de activitate coercitivă[3].

Obiectivul acestui studiu este de a prezenta diplomația digitală drept promotor pentru abordări inovative în dreptul războiului. În acest scop, extragem alineate ale articolelor relevante din cele Patru Convenții de la Geneva (Tratatele Umanitare) din 1949, Două Protocoale Adiționale din 1977 și Protocolul III din 2005, în procesele de adaptare la cerințele sistemului informațional globalizat.

Ipoteza de lucru pentru acest demers este un silogism care pleacă de la premisa că ororile războiului au condus la negocieri diplomatice pentru inițierea unor reguli internaționale care să poată intra în funcțiune în vremuri de război. În prezent, aceste convenții și protocoale sunt parte integrantă în Dreptul Internațional Umanitar (DIU). Dacă negocierile aparțin diplomaților, iar diplomația a intrat în era informațională, atunci diplomația digitală poate aduce în atenție negocierea diplomatică în planul DIU pentru a avea noi norme adaptate noilor cerințe ale spațiului informațional.

Această cercetare este empirică și exploratorie. Fiind enunțată prin intermediul unui silogism, ipoteza ne introduce în studiul transdisciplinar, construită pe principiul de cauzalitate cu ajutorul metodei inductive[4].

Articolul conține trei secțiuni. În prima, *Diplomație digitală și diplomația cibernetică, amenințări hibride și război informațional,* avem definite conceptele principale aferente diplomației și securității în era informațională. În cea de-a doua secțiune, *Actualizarea războiului tradițional și extinderea lui în spațiul cibernetic*, includem terminologia pentru războiul cibernetic și ale unor incidente cibernetice, prin exemple factuale ale unor situații limită cu care statele se pot confrunta și care au produs reinterpretarea securității statelor. În cea de-a treia secțiune, *Acțiuni ostile cibernetice și riposte politico-diplomatice, limite pentru război și drept umanitar internațional,* corelăm factorii și conceptele descrișii cu aspecte relevante ale DIU adaptat războiului în era informațională.

1. Diplomație digitală și diplomație cibernetică, amenințări hibride și război informațional

Diplomația a fost definită gradual, în funcție de contextul vremurilor, mediului și de către oamenii care au influențat politicile externe ale statelor, apoi în cadrul organizațiilor internaționale. Una dintre definițiile valabile după aproape două secole este cea a baronului Ferdinand de Cussy, din 1846, când definește diplomația

[3] A.J.R. Groom, André Barrinha and William C. Olson, *International Relations Then and Now Origins and Trends in Interpretation,* Second Edition, Routledge, Taylor & Francis Group, New York, USA, 2019, p. 117.

[4] Marcel T. Djuvara, *Metoda inductivă și rolul ei în științele explicative*, Editura Noua Tipografie Profesională Dimitrie C. Ionescu, București, 1910, p. 6.

ca fiind „totalitatea cunoștințelor și principiilor care sunt necesare pentru a conduce bine afacerile publice între state”[5]. În 1975, Mircea Malița considera diplomația un nucleu profesional în jurul căruia gravitează patru elemente distincte[6]: „istoria, relațiile internaționale, teoria situațiilor conflictuale și dreptul internațional”. În secolul al XXI-lea, Corneliu Bjola și Markus Kornprobst consideră că diplomația este alcătuită din patru componente: „comunicare instituționalizată, dublă recunoaștere, concentrare pe furnizarea de bunuri publice și capacitate productivă (adică luarea deciziilor, relații și norme globale)”[7]. Aceasta și-a însușit oficial instrumentele consacrate ale erei informaționale, fapt care a determinat conectarea unor termeni tehnici din domeniul tehnologiilor, informațiilor și comunicațiilor cu diplomația. După multe încercări de a alătura diplomația cu spațiul informațional, de a o impune pe platforme independente, rețele de socializare și motoare de căutare de pe internet, precum și un tip specific de activitate întreprinsă la un moment dat, *digital* și *cibernetic* sunt cele două adjective care au rămas reprezentative pentru diplomația practicată în anii ’20 ai acestui secol. Deseori, le avem explicate ca fiind sinonime[8]. Alteori, găsim în articole, manuale sau documente oficiale „prefixe diferite, aceeași semnificație: cibernetic, digital, net, online, virtual, e-”[9] alăturate diplomației.

În documente oficiale recente ale Uniunii Europene diplomația cibernetică apare mai des decât diplomația digitală. În „Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy”, publicat în februarie 2021, Annegret Bendiek și Matthias C. Kettemann nu amintesc deloc diplomația digitală. Ei poziționează diplomația cibernetică pe aceeași linie cu politica externă digitală, ca formă de stil, pentru a nu repeta termenii. Totodată, autorii evidențiază rolul diplomației și propun un mandat extins pentru Serviciul European de Acțiune Externă (echivalentul unui Minister de Externe la nivelul Uniunii Europene), în construirea unui cod normativ prin negocieri pentru spațiul cibernetic și informațional și pentru care trebuie să fie împuternicit pentru această sarcină a diplomației cibernetice[10]. Pentru Barrinha

[5] Ferdinand de Cussy, *Dictionnaire ou manuele-lexique du diplomate et du consul*, Tipographie de F. A. Brockhaus, Leipzig, 1846, p. 256.

[6] Mircea Malița, *Diplomația. Școli și Instituții*, Editura Didactică și Pedagogică, ediția a II-a, București, 1975, p. 44.

[7] Corneliu Bjola, Markus Kornprobst, *Understanding International Diplomacy Theory, Practice and Ethics*, Second Edition, Routledge, Abington, Oxon, UK, 2018, p. 238.

[8] André Barrinha, Thomas Renard, „Cyber-diplomacy: the making of an international society in the digital age”, *Revue Global Affairs*, nr. 3:4-5, pp. 353-364, 2017, URL: https://doi.org/10.1080/23340460.2017.1414924, accesat la 25.10.2021.

[9] Jovan Kurbalija, *An introduction to internet governance*, Published by DiploFoundation, Geneva, Switzerland, 2016, p. 14.

[10] Annegret Bendiek, Matthias C. Ketteman, *A revising the EU Cybersecurity Strategy: A call for EU Cyber Diplomacy*, SWP Comment, nr. 16, 16.02.2021, p. 3, URL: https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf, accesat la 21.10.2021.

și Renard diplomația cibernetică reprezintă o „practică internațională emergentă care încearcă să construiască o societate cibernetică internațională, punând în legătură interesele naționale ale statelor cu dinamica societății mondiale – tărâmul predominant în care a evoluat spațiul cibernetic în ultimele patru decenii”[11]. De remarcat este că nici aici, termenul de diplomație digitală nu apare niciodată. Ilan Manor susține că diplomația digitală reprezintă „digitalizarea diplomației publice”[12], iar Corneliu Bjola îi atribuie rolul principal în „utilizarea rețelelor sociale în scopuri diplomatice”[13]. Pentru Brian Hocking și Jan Melissen, diplomația digitală este adesea echivalată cu diplomația publică, dar include și:

- schimbarea agendelor de politică externă;
- agendele cibernetice pentru probleme și scenarii de negociere;
- managementul cunoașterii în problema gestionării eficiente a datelor;
- prestarea serviciilor consulare digitalizate și gestionarea crizelor[14].

Din definițiile de mai sus desprindem o idee comună, aceea că practica diplomatică în secolul al XXI-lea indică faptul că diplomația a intrat în era informațională, ea se află în proces accelerat de hibridizare în „mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta”[15].

Astfel că, pentru a gestiona amenințările și riscurile de a instrumentaliza amenințările hibride și războiul cibernetic avem la dispoziție mijloace coercitive și noncoercitive (din domeniile diplomației, securității și apărării) pentru a alege între multiple abordări și înțelesuri pe măsura acestora, în condițiile în care nici noile definiții ale amenințărilor hibride nu sunt puține.

Avem la dispoziție un număr impresionant de definiții care implică termeni generici ai securității, protecției și siguranței, în special, pentru cele referitoare la amenințările la adresa securității în situații care derivă din comportamentele actorilor (ne)statali și individuali, iar pentru a nu complica cadrul nostru conceptual, pentru securitate națională am ales următoarea definiție de lucru: în sensul ei larg, securitatea la nivel național reprezintă o stare de normalitate a unui stat, „o țară în care fiecare cetățean trăiește într-un mediu sigur și are încredere că instituțiile, pe care el le susține, îl apără și îl protejează”[16]. Această definiție introduce amenințările

[11] André Barrinha, Thomas Renard, *op. cit.* p. 353.

[12] Ilan Manor, *The Digitalization of Public Diplomacy*, Palgrave Macmillan Publishers, Basingstoke, UK, 2019, passim.

[13] Corneliu Bjola, Markus Holmes, *Digital Diplomacy: Theory and Practice*, Routledge New Diplomacy Studies, Abington, UK, 2015, p. 4.

[14] Brian Hocking, Jan Melissen, *Diplomacy in the Digital Age,* Clingendael Report, Netherlands Institute of International Relations Clingendael, Clingendael, Netherlands, 2015, pp. 3-4.

[15] ***, *Strategia de securitate cibernetică a României,* p. 4, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf, accesat la 20.10.2021.

[16] ***, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. „Împreună, pentru o*

hibride, deoarece ele „înglobează amestecul de activități coercitive și subversive, de metode convenționale și neconvenționale (de exemplu, diplomatice, militare, economice, tehnologice) care pot fi utilizate într-un mod coordonat de actorii statali sau nestatali pentru a realiza obiective specifice, fără a se depăși limita pragului de stare de război declarată oficial”[17]. Astfel, avem o trimitere la atac și conflict armat. Atacul armat este unul „săvârşit de o persoană cu o armă de foc sau cu obiecte, dispozitive, substanţe sau animale care pot pune în pericol viaţa, sănătatea ori integritatea corporală a persoanelor”[18]. În cazul nostru, războiul extins în spațiul cibernetic, „o extensie a suprafeței de atac a unei națiuni”[19]. Pentru a înțelege mai bine sensul practic, polemologic, al acestui nou domeniu, avem următoarea definiție: „războiul cibernetic reprezintă operații militare efectuate pe rețele informaționale într-un conflict declarat între dușmani de stat sau de națiune, cu acțiuni strecurate în viața fiecărui individ prin intermediul fiecărui instrument cu acces la internet, de la telefonul mobil la frigiderul inteligent”[20]; iar Henrotin a definit războiul informațional ca fiind un set de acțiuni și atacuri conduse pe teren informațional, care au ca rezultat distrugerea sau punerea în incapacitate a infrastructurii inamice, unde automatizarea colectării de informații a devenit fragmentată datorită multitudinii de senzori folosiți și în automatizarea represaliilor, în special prin utilizarea de mine „inteligente” capabile să stabilească dacă ar trebui să fie detonate în apropierea unui anumit vehicul[21]. Toate aceste definiții ne introduc în lumea real-virtuală a războiului cibernetic, cel care avea să transforme toate celelalte domenii care sunt direct sau indirect asimilate războiului, al polemologiei.

2. Actualizarea războiului tradițional și extinderea acestuia în spațiul cibernetic

În scop practic, pentru a putea evidenția diferite situații desfășurate în spațiul informațional, avem nevoie de câteva elemente distinctive care să facă diferența

România sigură și prosperă într-o lume marcată de noi provocări”, Monitorul Oficial, Partea I, nr. 574, din 1 iulie 2020, p. 5.

[17] ***, *Comunicare Comună către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor din 5 decembrie 2018, Plan de acțiune împotriva dezinformării*, pdf, p. 2, URL: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52018JC0036&from=RO, accesat la 04.06.2021.

[18] ***, *Legea nr. 192 din 25 octombrie 2019 pentru modificarea şi completarea unor acte normative din domeniul ordinii şi siguranţei publice*, publicată în Monitorul Oficial, nr. 868, din 28 octombrie 2019, p. 14.

[19] Jacob G. Oakley, *Waging Cyber War. Technical Challenges and Operational Constraints*, Apress Publications, New York, USA, 2019, p. 8.

[20] *Ibidem,* p. 20.

[21] Joseph Henrotin, *The Art of war in the network age. Back to the future*, John Wiley & Sons, Inc. Publications, New Jersey, USA, 2016, p. 51.

între operațiile ostile din spațiul cibernetic care susțin operațiile militare din teatrele de operații și amenințările hibride.

În acest sens, există atacurile cibernetice din statele ex-sovietice care, prin modul lor de acțiune, au creat precedente în domeniul securității (inter)naționale. Ca prim exemplu, atacurile cibernetice asupra Estoniei din 2007 au inclus atacuri de tip botnet executate de computerele zombie. Timp de trei săptămâni, hackerii au vizat infrastructura digitală a țării, indiferent de nivelul utilizatorilor, publici sau privați. Atacurile distribuite de refuz de serviciu (DDOS)[22] au produs prăbușirea serviciilor de toate tipurile, începând cu serviciile bancare online, multimedia sau de servicii de e-guvernare, puse în practică cu ajutorul unor instrumente digitale construite pe baza unor algoritmi, care, la rândul lor, au fost transformate în platforme care includeau inteligența artificială. Problemele au apărut în timpul unei dispute politice dintre statul rus și Estonia, pe tema mutării monumentului *Soldatului de bronz*, eveniment planificat în 26 aprilie; demonstrațiile pro-ruse s-au accentuat la nivel local, s-au primit atenționări și de la Kremlin și începând cu ziua următoare, timp de trei săptămâni, țara s-a blocat efectiv[23]. Apoi, după Estonia, a urmat un val de atacuri cibernetice similare în alte state ex-sovietice. Acestea au integrat și sincronizat activitatea cibernetică cu acțiuni clasice de apărare a sistemelor automatizate și au inclus măsuri inedite, algoritmi în spațiul virtual, în spațiul fizic − drone sau alte tipuri de tehnică militară cu sisteme autonome fără pilot, precum și a altor capabilități cibernetice; nu au făcut excepție nici presiunea economică sau diplomatică[24]. Rezultatul a fost de creștere a efectelor strategice în Lituania (iunie 2008) și Kârgâzstan (ianuarie 2009)[25]; războiul ruso-georgian de cinci zile cu coordonare integratoare, începute cu atacuri cibernetice lansate de Rusia pe 29 iulie 2008[26] și intensificate prin operații militare la 8 august 2008.

Toate acestea aveau să pară simple exerciții în comparație cu războiul ruso-ucrainean pornit în anul 2014, în urma căruia Federația Rusă avea anexeze Peninsula Crimeea. Acest tip de conflict armat a creat un precedent în care s-a dovedit că tratatele, convențiile și protocoalele internaționale referitoare la DIU sunt depășite, că războiul hibrid încorporează moduri diferite de război conduse prin strategii, tactici și mijloace convenționale, integrând formațiuni neregulate, acte teroriste și infracționale, inclusiv violență și constrângere, fără a face diferența între civili și combatanți.

[22] Scott Augenbaum, *The Secret to Cybersecurity. A Simple Plan to Protect Your Family and Business from Cybercrime*, Forefront Books, New York, USA, 2019, kindle e-book, p. 34.
[23] Damien McGuinness, *How a cyber attack transformed Estonia*, 27.04.2017, URL: www.bbc.com/news/3965541, accesat la 03.06.2020.
[24] David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age,* Crown Publishing Group, a division of Penguin Random House LLC, New York, USA, 2018, pp. xv-xvi.
[25] *Ibidem.*
[26] *Ibidem.*

Rusia este primul stat recunoscut la nivel internațional care a recurs în mod direct la utilizarea războiului hibrid, răspândirea conflictului în Ucraina de Est nu a făcut decât să dovedească faptul că Rusia dispunea de toate mijloacele necesare pentru a pune în aplicare arta acestuia, putea acoperi întreg lanțul de la cauză la efect în teatrul de operații de război sau conflict cu resurse materiale minime, fără arme fizice și fără pierderi de vieți omenești, în special pentru partea atacatoare[27]. „Războiul hibrid este o oglindă a lumii în care trăim, o reflectare a societății care o duce; prin urmare, o societate hibridă se va angaja în război hibrid”[28].

3. Acțiuni ostile cibernetice și riposte politico-diplomatice, limite pentru război și drept umanitar internațional

În sistemul internațional contemporan, principala normă care reglementează utilizarea forței în dreptul internațional este Carta Organizației Națiunilor Unite (ONU). Baza sa legală este menționată în articolul 2, alin. 4 al Cartei ONU, după cum urmează: „Toți membrii se abțin să recurgă la amenințarea sau utilizarea forței în relațiile lor internaționale, fie împotriva integrității teritoriale sau a independenței politice a oricărui alt stat, fie în orice mod incompatibil cu obiectivele Organizației Națiunilor Unite”[29].

De asemenea, Carta ONU prevede autoapărarea legitimă a statului și cea colectivă în articolul 51: „Nimic din această Cartă nu va afecta dreptul inerent de autoapărare individuală sau colectivă în cazul unui atac armat împotriva unui membru al Organizației Națiunilor Unite, până când Consiliul de Securitate va fi luat măsurile necesare pentru menținerea păcii și securității internaționale. Măsurile luate de către Membri în exercitarea acestui drept de autoapărare sunt notificate imediat Consiliului de Securitate și nu afectează în niciun fel puterea și îndatorirea Consiliului de Securitate, în temeiul prezentei Carte, de a lua întreprinde oricând acțiunile pe care le consideră necesare pentru a menține sau restaura pacea și securitatea internațională”[30].

Principala problemă pentru tema noastră, care derivă din acest articol al Cartei, este aceea că normele internaționale existente sunt evazive, nu se pot aplica în mod eficient în spațiul informațional. Declarațiile de război, comunicatele și luările de poziție diplomatice sunt puse la grea încercare în condițiile în care părțile implicate în războiul hibrid nu mai sunt doar statele, subiect primar al dreptului internațional public.

[27] Brin Najžer, *The Hybrid Age: International Security in the Era of Hybrid Warfare*, I.B. Tauris Bloomsbury Publishing, London, 2020, p. 27.
[28] *Ibidem*.
[29] ***, *Carta Națiunilor Unite** din 26 iunie 1945, Monitorul Oficial, 26 iunie 1945, pdf, p. 2, URL: http://www.anr.gov.ro/docs/legislatie/internationala/Carta_Organizatiei_Natiunilor_ Unite_ONU_.pdf, accesat la 03.06.2020.
[30] *Ibidem*, p. 10.

Nu avem criterii legale care pot fi aplicabile acțiunilor hibride și celor ostile din spațiul cibernetic, atunci când ele sunt desfășurate de stat în mod direct sau prin proxy și dacă aceste acțiuni pot fi catalogate ca fiind conflict armat între stat și adversarul său. Hibridizarea războiului a demonstrat în 2014, că noile instrumente militare pot evita normele internaționale semnate prin cele 40 de convenții și protocoale internaționale referitoare la DIU, dreptul de a purta război, *jus ad bello* sau regulile de respectat din timpul războiului, *jus in bello*.

Jus ad bellum reprezintă un aspect generic în analiza legală a operațiilor cibernetice care pot fi efectuate de forțele armate. Activitățile desfășurate în spațiul cibernetic permit statului să efectueze operații cu rezultate letale sau dăunătoare pe lângă cele care nu folosesc forța dar ele pot provoca moartea, vătămarea corporală sau pagube materiale. Luate separat sau în ansamblu, aceste tipuri de acțiuni pot fi considerate atacuri armate sau utilizarea forței, în conformitate cu dreptul internațional deoarece statele și Organizațiile Interguvernamentale (OIG-urile) relevante au inclus în cadrul legislativ infracționalitatea din spațiul cibernetic. Aceasta evidențiază un spectru larg de moduri de încălcare a legilor. Printre ele găsim tot felul de atacuri la persoane, operatori și instituții private sau publice. Unele dintre infracțiuni sunt universal acceptate, altele sunt interpretate la nivel național. Pentru infracțiunile cibernetice transfrontaliere universal definite găsim:

- criminalitate de tip nou, provocată online (furturile de identitate, date financiare sau de plată cu cardul; furt și vânzare de date corporative, șantajul etc.) pe rețele de socializare, e-mail și internet;
- criminalitate convențională, dar reinterpretată, precum escrocheriile, ingineriile sociale, traficul ilegal de toate tipurile, spălarea banilor, hărțuirea cibernetică, instigarea la ură etc[31].

Celor două tipuri de infracționalitate li se adaugă cele aferente protejării securității naționale, unde definițiile pot fi similare, dar ele sunt interpretate prin prisma națiunii, drepturilor și obligațiilor cetățenilor acestuia. Mai specific, eroii unei țări pot fi inamici sau trădători în altul, indiferent de spațiul în care ei își desfășoară acțiunile. Printre aceste acțiuni, la nivel legislativ național, avem prevăzute în *Codul Penal al României*, în capitolul *Infracţiuni contra securităţii naţionale* (art. 394-412)[32]: înalta trădare, trădarea prin transmitere de informaţii secrete de stat și ajutarea inamicului; acțiunile împotriva ordinii constituționale și acțiunile ostile contra statului, spionajul, atentatele, în special, al celui care pune în pericol securitatea națională; diversiunea, comunicarea informațiilor false, propaganda, complicitatea, tăinuirea unor informații referitoare la posibilă trădare

[31] David B. Skillicorn, *Cyberspace, Data Analytics, and Policing,* CRC Press, Boca Raton, Taylor & Francis Group, LLC, Boca Raton, Florida, 2021, pp. 15-16.

[32] *** *Codul Penal al României*, Monitorul Oficial al României, partea 1, nr. 575, 25 iunie 2004, pp. 876-879.

sau act ostil, organizarea unor rețele de spionaj etc. Activitatea de spionaj face obiectul codificării în sistemul internațional în Regulamentele de la Haga (1899 și 1907), A Patra Convenție de la Geneva (1949) și în Actul Adițional I (1977) al Convențiilor de la Geneva.

În cazul nostru, spionajul cibernetic poate produce efecte proporționale cu scopurile și țintele acestor tipuri de acțiuni. Ele pot afecta state, organizații și indivizi relevanți, de la simple spargeri de parolă a unor adrese de e-mail aparținând unor persoane publice, până la daunele materiale în viața reală sau pierderea efectivă a vieții[33]. „Infracționalitatea din spațiul cibernetic"[34] a început să fie tratată serios la nivel regional prin măsuri ferme. Una dintre acestea, la nivelul Uniunii Europene, este „Decizia (PESC) 2020/1127 Consiliului din 30 iulie 2020 privind măsuri restrictive împotriva atacurilor cibernetice care amenință Uniunea sau statele sale membre".

Extrapolând această idee, avem acțiuni care se pot extinde din mediul real în mediul virtual, provocând reacții rapide politico-diplomatice, militare, de apărare sau de atac. Unele pot include toate posibilitățile de reacție existente într-un stat. Această reacție reprezintă dreptul de autoapărare în spațiul cibernetic al entităților statale împotriva imixtiunilor. Tipurile de atac s-au diversificat, mercenarii au intrat în spațiul informațional, fiind cunoscuți drept hackeri și diferențiindu-se, metaforic, prin mai multe culori, după ce, inițial, ei erau încadrați în trei categorii: white hats; grey hats; black hats (pălării albe, gri sau negre), aceste coduri de culoare exprimând progresiv gradul de legalitate a activităților în spațiul cibernetic, de la legal (alb) până la ilegal (negru). În DIU, mercenariatul este prevăzut în Protocolul din 1977, la art. 47, astfel: „mercenarii sunt persoane special recrutate în țară sau în străinătate pentru a lupta într-un conflict armat; ele iau parte direct la ostilități în vederea obținerii unui avantaj personal şi care este efectiv promis de către o parte la conflict sau în numele ei, o remunerare superioară aceleia promise sau plătite contingentelor armatelor regulate, având un grad şi o funcție similară în forțele armate ale acestei părți; și nu sunt membri ai forțelor militare ale unei părți din conflict" [35].

Aflăm în mod recurent din mass-media că diferiți membri ai corpurilor diplomatic, consular sau administrativ, din cadrul unor ambasade sunt învinuiți de spionaj[36], considerăm oportun să explicăm termenul generic de *spion*, acesta fiind

[33] Scott Augenbaum, *op.cit*., p. 35

[34] **** Convenția privind criminalitatea informatică din 23.11.2001 *) (Convenția de la Budapesta - 2001)*, Monitorul Oficial, Partea I, nr. 343 din 20 aprilie 2004, p. 1.

[35] **** Protocolul adițional I la convențiile de la Geneva 1949, adoptat la Geneva în 1977, cu privire la protecția victimelor de război în conflictele armate internaționale,* URL: https://lege5.ro/Gratuit/he3daojy/protocolul-nr-1-1977-aditional-la-conventiile-de-la-geneva-din-12-august-1949-privind-protectia-victimelor-conflictelor-armate-internationale, accesat la 03.06.2021.

[36] N.A.: Unul dintre exemplele recente se referă la un flagrant organizat în luna martie a.c., în care au fost implicați un ofițer de marină italian în timp ce înmâna documente secrete atașatului militar

asimilat cu activitatea de intelligence din mediul informațional, cel al spionajului cibernetic. Statutul lor tradițional a fost detaliat în Convențiile de la Haga. Acesta este explicat în art. 27-29 din Convențiile II (1899) și IV (1907), în art. 29, 30 și 31 din Convenția VI (1907), pornind de la modul de identificare a unei persoane ca fiind spion: „Spionul este o persoană care obține pe ascuns sau sub pretexte mincinoase, adună ori încearcă să adune informații în zone de operații ale unui stat beligerant cu intenția de a le comunica părții adverse”[37]. Clandestinitatea, pretextul fals, intenția de a comunica informațiile acumulate părții inamice se regăsesc în acțiunile lor desfășurate la limita (i)legalității.

Spionii, mercenarii, diversioniștii și sabotorii sunt la un clic distanță, amenințările și conflictele armate (hibride) actuale intră sub spectrul furtului, dezinformării, falselor informări sau accesului neautorizat la sistemele de rețea ale unui alt stat. Atunci, astfel de acțiuni pot fi protejate conform protocoalelor de la Haga. Cu toate acestea, mercenariatul și operațiile de spionaj cibernetic depășesc prevederile actelor juridice și/sau cutumelor din dreptul internațional, deoarece implică interferențe ale unor actori statali sau nestatali în sistemele altui stat și încalcă principiul neintervenției din art. 2, alin. (7) din Carta ONU. Acesta interzice statelor să intervină în afacerile interne ale altor state, statele victime pot protesta împotriva acestor acțiuni raportându-le Consiliului de Securitate al ONU, dar în mod real, lucrurile nu se întâmplă așa. Leon Panetta, fost secretar al Departamentului de Apărare al SUA, declara la un moment dat că: „Am văzut de prima mână cum vehiculele moderne, cum ar fi platformele de la distanță și sistemele cibernetice au schimbat modul în care se desfășoară războaiele. Acestea oferă soldaților noștri capacitatea de a se confrunta cu inamicul și de a schimba cursul războiului, chiar dacă sunt departe. În partea dreaptă a spectrului spațiului cibernetic există utilizarea forței sau atacul armat în operațiunile cibernetice. Oficialii Pentagonului afirmă în mod expres că atacurile cibernetice împotriva SUA vor fi privite ca o acțiune de război”[38].

Acțiunile extinse în spațiul cibernetic afectează direct normele internaționale care prevăd dreptul la viață, recunoscute la nivel mondial prin acceptarea punctelor enunțate în Declarația Universală a Drepturilor Omului din 1948 și în conformitate cu articolul 51 din Carta ONU, pătrund în domeniul Convențiilor de la Geneva și în Protocoalele lor adiționale. În Protocolul Adițional I găsim norme care se pot adapta spațiului

rus. Sursa: *Italian officer 'caught selling secrets to Russia', 31 March 2021*, URL: https://www.bbc.com/news/world-europe-56588506?fbclid=IwAR3R2Whyuzk8rQaskWaBvUxd Jv5r MIgj_B xQF2t419G5cGUATNw3jdbAjto, accesat la 21.10.2021.

[37] James Brown Scott, *The Hague conventions and declarations of 1899 and 1907, accompanied by tables of signatures, ratifications and adhesions of the various powers, and texts of reservations,* New York Oxford University Press American Branch, Toronto, Canada, 1915, p. 118.

[38] Jennifer, Wang, *The White House and Pentagon Deem Cyber-Attacks, An Act of War,* URL: http://www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-actof-war/, accesat la 03.06.2021.

informațional, întrucât aici avem conflictele armate naționale fără specificații tehnice. În acest areal, acțiunile din spațiul cibernetic pot fi integrate în acest protocol prin gama largă de daune fizice sau deces, ori de vătămare a mediului, doar că noul mediu implică și mediul online, unde impactul operațiilor cibernetice poate avea rezultate similare cu cele ale efectelor produse în urma acțiunilor militare tradiționale.

În ghidul *Tallinn Manual on the International Law Applicable to Cyber Warfare* este descrisă situația similară pentru *jus ad bellum* pentru spațiul cibernetic, de unde derivă faptul că infrastructurile cibernetice din propriile țări fac parte din infrastructura națională și că orice atac asupra ei este ilegală[39], indiferent de nivelul atins de acest atac. Însă, nu toate atacurile cibernetice pot fi catalogate drept un atac armat care să poată activa structurile de apărare legitimă. Însă, efectele unui atac armat cibernetic pot fi echivalente cu cele care ar rezulta dintr-o acțiune care se califică drept un atac armat tradițional[40]; așadar, atacurile armate cibernetice au bază în atacuri cibernetice, de la simple incursiuni în sisteme informaționale private/individuale până la acțiuni cibernetice unice pentru atingerea obiectivelor de securitate națională față de alte state, fapt care acordă statelor dreptul de autoapărare, cu condiția ca acestea să respecte DIU, implicit, cele patru Convenții de la Geneva semnate în august 1949 și două protocoale suplimentare semnate în 1977. Avantajul oferit de către Convențiile de la Geneva și Protocoalele Adiționale este acela că, după semnarea, ratificarea și aderarea la aceste norme, Convențiile au fost acceptate la nivel universal. De exemplu, Protocolul Adițional I a fost acceptat de către 200 de state[41] (ONU are 193 de state membre). Devenind documente legale fundamentale, Convențiile de la Geneva și Protocoalele lor Adiționale guvernează conflictele armate între state, dezvoltând astfel principiile DIU al conflictelor armate. DIU reprezintă „ansamblul normelor de drept internațional, de sorginte cutumiară sau convențională, destinate în scopul reglementării în mod special a problemelor survenite în situații de conflict armat internațional și fără caracter internațional"[42], cu două ramuri de bază: a) Dreptul conflictelor armate (dreptul războiului propriu-zis) și b) Dreptul internațional umanitar (dreptul umanitar propriu-zis)[43].

Protocoalele Adiționale din 1977 la Convențiile de la Geneva au fost impuse de impactul inovațiilor în tehnologiile armelor și schimbările în modul de a purta războaiele, reprezentând o adaptare a convențiilor și a precedentului protocol la inovații tehnologice și modificări în dreptul războiului secolului al XX-lea. Al doilea

[39] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, Cambridge, 2017, p. 15.
[40] *Ibidem,* p. 54.
[41] ***, *Geneva Conventions of 1949 and Additional Protocols, and their Commentaries, By State*, URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountry.xsp, accesat la 27.10.2021.
[42] Anatolie Bulgac, Sergiu Sîrbu, *Drept Internațional Umanitar (Ghid),* Centrul Editorial-Poligrafic Medicina, Chișinău, 2019, p.8.
[43] Anatolie Bulgac, Sergiu Sîrbu, *op. cit.,* pp. 8-9.

Protocol Adițional este primul document internațional în care sunt descrise, fără a fi numite direct, situațiile în care se pot regăsi civili angrenați în conflicte (inter) naționale și structuri de luptă asimetrică, în care se specifică aria de aplicabilitate, apoi avem specificate în mod clar, în articolul 4, și actele de terorism[44].

Atacul armat are multe valențe. Conform art. 49 din Protocolul Adițional I, „prin expresia atacuri se înţeleg actele de violenţă împotriva adversarului, fie că aceste acte sunt ofensive sau defensive”[45]. Acestea implică acțiuni violente întreprinse la nivel de individ, de grup sau nivel (inter)național pentru obținerea unor obiective specifice. Atacul are două forme tradiționale în domeniul polemologiei, atacul armat internațional și cel la nivel național, specific în războaiele civile. Lor li s-au adăugat actorii nestatali, precum organizațiile internaționale sau altfel de actori individuali sau organizați în diverse entități cu putere și influență în arena internațională.

În cazul conflictului armat internațional dintre două sau mai multe state se aplică Convențiile de la Geneva, în conflictul armat în spațiul național dintre un stat și un grup armat organizat avem posibilitatea de a urmări în ce măsură se respectă părțile și dacă ele respectă civilii și bunurile; avem cel de-al treilea articol comun al Convenției de la Geneva[46]. Indiferent de modul în care este caracterizat conflictul armat, metodele de conflict trebuie să respecte legea conflictelor armate[47].

Acțiunile cibernetice sunt utilizate ca instrumente versatile în conflictele armate, prin intermediul cărora atacurile pot atinge nivelul atacurilor armate în cadrul *jus in bello*, care pot provoca întreruperea legăturilor între forţele armatei terestre, maritime, aeriene și ale telecomunicațiilor cu comandamentele aferente și între ele; de a reduce la minimum încrederea în guvern și în stat, în general; de a teroriza populația civilă și pentru a veni în ajutorul campaniilor militare tradiționale. Astfel de situații au provocat statele să ia decizii importante. Ele au început să își înființeze divizii cibernetice. De exemplu, Atacurile Teroriste de la 11 septembrie 2001 din SUA au produs multe schimbări, printre acestea regăsim crearea primei divizii cibernetice din cadrul Biroului Federal de Investigații (FBI[48]).

DIU oferă posibilitatea armonizării legilor referitoare la actualele probleme puse de acțiunile ostile din spațiul cibernetic pentru că majoritatea statelor lumii sunt semnatare ale Convențiilor și Regulamentelor de la Haga, Convențiilor de la Geneva și Protocoalelor lor Adiționale. Acțiunile din spațiul virtual sunt transfrontaliere, întreprinse la nivel global proporțional cu nivelul de acceptare al DIU din toate spațiile naturale. Astfel că cele trei principii ale DIU pot fi extinse,

[44] *** *Protocolul nr. 2/1977 adițional, op. cit*., pp. 24-25.
[45] *** *Protocolul nr. 1/1977 adițional, op. cit.,* p. 24.
[46] Anatolie Bulgac, Sergiu Sîrbu, *op.cit.,* pp. 8-12.
[47] *Ibidem.*
[48] Nancy E. Marion, Jason Twede, *An Encyclopedia of Digital Crime*, ABC-CLIO, LLC Publishers, Santa Barbara, California, USA, 2020, p. XXIII.

pentru că: avem nevoie de *proporționalitate* în alegerea mijloacelor, metodelor și efectivelor în război; *de a se face discriminare* între civili și combatanți, între structuri_civile și militare, în scopul *evitării* suferinței oamenilor și distrugerilor materiale[49]. Aceste principii sunt asumate prin umanitate, imparțialitate, neutralitate, independență, voluntariat, unitate și universalitate[50], cu atât mai mult cu cât, în era informațională avem nevoie de un sistem care să ateste legitimitate libertăților în spațiul cibernetice, parafrazându-l pe John Stuart Mill: unde se termină libertatea unui stat pe internet, acolo începe libertatea celuilalt.

Concluzii

Pe parcursul acestei lucrări am făcut delimitarea definițiilor de lucru aferente diplomației, războiului, spațiului cibernetic și DIU. Am evidențiat concepte teoretice prin exemple reale din spațiile naturale și virtual în scopul sublinierii nevoii de corelare a DIU cu atacurile și acțiunile ostile conduse în spațiul informațional, ca drept al războiului valabil în toate spațiile cunoscute de către om.

Am dezvoltat idei prin intermediul cărora observăm la final că diplomația pusă în practică cu mijloace informaționale a intrat în atenția opiniei publice cu ajutorul diplomației publice, atunci când sunt utilizate formule consacrate ale comunicării pe rețele de socializare de pe internet. Acest aspect este deseori integrat unor concepte similare, precum diplomația digitală și diplomația cibernetică, dar indiferent de termenul preferat, scopul complex al diplomației (negociere, reprezentare, infirmare, construire, menținere și consolidare a legăturilor între state) rămâne neschimbat, menținându-și valabilitatea în orice spațiu cunoscut. Diplomația are misiunea fundamentală de a găsi soluții pașnice pentru relațiile bi- sau multilaterale, prin tratate și convenții. Ele pot include adaptări ale unor variante existente sau ale unora inedite, cauzate de popularizarea noilor tehnologii și redimensionarea abordării războiului, de la războiul clasic la cel din spațiul cibernetic.

Implementarea unor sisteme inovative în specificul mediului diplomatic nu este ceva excepțional. Nici ideea folosirii unor instrumente de lucru tehnologizate nu este nouă. Faptul cu adevărat inedit este acceptarea în spirală a setului de transformări succesive în mediul instituțional și interministerial al afacerilor externe din toate statele lumii; au început să aducă simultan noi tehnici de lucru. Complexitatea și volatilitatea din mediul informațional sunt puse în congruență cu pachetele de norme internaționale cu greu acceptate de actorii internaționali pe parcursul secolului al XX-lea și ale unor cutume diplomatice vechi de sute de ani și cu mii de ani de conflicte armate. În aceste condiții, războiul a devenit informațional și/sau cibernetic. În spațiul aferent, părțile implicate nu mai sunt doar actori statali, privați

[49] *Ibidem*, p. 59.
[50] *Ibidem,* pp. 15-16.

sau individuali. Aici se impune includerea unor noi amendamente în DIU, care să fie acceptate de către toate părțile interesate, actori statali sau nestatali, privați sau individuali; să includă legiferarea unor practici militare alcătuite în tandem: oameni și roboți, tehnică automatizată și echipamente militare informaționalizate.

Analiza războiului cibernetic transpusă prin prisma DIU, a celor Patru Convenții de la Geneva și ale celor Două Protocoale Adiționale ale acestor Convenții conduce la concluzia că regulile care stau la baza organizării operațiilor militare sunt adaptabile conflictului cibernetic. Pentru acest areal, precum și de a negocia noi acte normative internaționale, avem nevoie de oameni specializați. Însă, reducând aceste aspecte la termeni generici, regăsim aceste cerințe în atribuțiile diplomaților, aceștia trebuind doar să își adapteze competențele la cerințele erei informaționale.

Așadar, obiectivul și ipoteza acestui studiu se confirmă. Diplomația digitală poate fi un promotor pentru abordări inovative în dreptul războiului. Negocierile aparțin diplomaților, așa cum declarațiile de război și pace aparțin tot diplomației. Când diplomația a pășit în era informațională, și-a extins și atribuțiile în mod proporțional, implicit și pentru negocierile referitoare la extinderea DIU pentru situațiile produse în spațiul cibernetic. Astfel că, trebuie să avem în vedere faptul că puterea de distrugere materială și umană se află la un clic distanță. Această stare de fapt devine o cerință pentru a ajusta rapid convențiile aferente DIU actual la posibilele paradigme strategice privind pregătirea și desfășurarea operațiilor militare sau ostile ale unor indivizi sau state, aflați cu toții în spatele unui monitor al unui computer.

BIBLIOGRAFIE:

1. ***, *Carta Națiunilor Unite ,* publicată în Monitorul Oficial din 26 iunie 1945.

2. ***, *Codul Penal al României,* publicat în Monitorul Oficial al României, partea 1, nr. 575, 25 iunie 2004.

3. ***, *Comunicare Comună către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor din 5 decembrie 2018, Plan de acțiune împotriva dezinformării*, pdf, p. 2, URL: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52018JC0036&from=RO

4. ***, *Convenția (de la Geneva privitoare la Protecția persoanelor civile în timp de război din 12 august 1949 (IV)*, URL: https://crucearosie.ro/assets/Uploads/Conventia-de-la-Geneva-IV.pdf

5. ***, *Geneva Conventions of 1949 and Additional Protocols, and their Commentaries, By State*, URL: https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountry.xsp

6. ***, *Strategia de securitate cibernetică a României*, URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf

7. ***, *Convenția privind criminalitatea informatică din 23.11.2001*) (Convenția de la Budapesta - 2001)*, publicată în Monitorul Oficial, Partea I, nr. 343, 20.04.2004.

8. ***, *Legea nr. 192 din 25 octombrie 2019 pentru modificarea şi completarea unor acte normative din domeniul ordinii şi siguranţei publice*, publicată în Monitorul Oficial, nr. 868, din 28.10.2019.

9. ***, *Strategia Națională de Apărare a Țării pentru perioada 2020-2024. „Împreună, pentru o Românie sigură şi prosperă într-o lume marcată de noi provocări"*, Monitorul Oficial, Partea I, nr. 574, din 01.07.2020,

10. ***, *Protocolul adiţional I la convenţiile de la Geneva 1949, adoptat la Geneva în 1977, cu privire la protecţia victimelor de război în conflictele armate internaţionale*, URL: https://lege5.ro/Gratuit/he3daojy/protocolul-nr-1-1977-aditional-la-conventiile-de-la-geneva-din-12-august-1949-privind-protectia-victimelor-conflictelor-armate-internationale

11. ***, *Protocolul nr. 2/1977 adiţional la convenţiile de la Geneva din 12 august 1949 privind protecţia victimelor conflictelor armate fără caracter internaţional*)*, URL: https://lege5.ro/gratuit/he3daojz/protocolul-nr-2-1977-aditional-la-conventiile-de-la-geneva-din-12-august-1949-privind-protectia-victimelor-conflictelor-armate-fara-caracter-international

12. AUGENBAUM, Scott, *The Secret to Cybersecurity. A Simple Plan to Protect Your Family and Business from Cybercrime*, Forefront Books, New York, USA, 2019.

13. BARRINHA., André; RENARD, Thomas, "Cyber-diplomacy: the making of an international society in the digital age", *Revue Global Affairs*, no. 3:4-5, 2017, URL: https://doi.org/10.1080/23340460.2017.1414924

14. BJOLA, Corneliu; HOLMES, Markus, *Digital Diplomacy: Theory and Practice*, Routledge New Diplomacy Studies, Abington, UK, 2015,

15. BJOLA, Corneliu; KORNPROBST, Markus, *Understanding International Diplomacy Theory, Practice and Ethics*, Second Edition, Routledge, Abington, Oxon, UK, 2018,

16. BENDIEK, Annegret; KETTERMAN, Matthias C., *A revising the EU Cybersecurity Strategy: A call for EU Cyber Diplomacy*, SWP Comment, nr. 16, 16.02.2021, URL: https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf

17. BULGAC, Anatolie; SÎRBU, Sergiu, *Drept Internaţional Umanitar (Ghid),* Centrul Editorial-Poligrafic Medicina, Chișinău, 2019.

18. DE CUSSY; Ferdinand, *Dictionnaire ou manuele-lexique du diplomate et du consul,* Tipographie de F.A. Brockhaus, Leipzig, 1846,

19. DJUVARA, Marcel T., *Metoda inductivă și rolul ei în științele explicative,* Editura Noua Tipografie Profesională Dimitrie C. Ionescu, București, 1910.

20. GROOM, A.J.R.; BARINHA; André; OLSON, William; Olson, *International Relations Then and Now Origins and Trends in Interpretation*, Second Edition, Routledge, Taylor & Francis Group, New York, USA, 2019,

21. HENROTIN, Joseph, *The Art of war in the network age. Back to the future,* John Wiley & Sons Inc. Publications, New Jersey, USA, 2016.

22. HOCKING, Brian; MELISSEN, Jan, *Diplomacy in the Digital Age,* Clingendael Report, Netherlands Institute of International Relations Clingendael, Clingendael, Netherlands, 2015.

23. KURBALIJA, Jovan, *An introduction to internet governance*, Published by DiploFoundation, Geneva, Switzerland, 2016.

24. MCGUINESS, Damien, „How a cyber attack transformed Estonia", 27.04.2017, URL: www.bbc.com/news/3965541

25. MALIȚA, Mircea, *Diplomația. Școli și Instituții*, Editura Didactică și Pedagogică, ediția a II-a, București, 1975.

26. MANOR, Ilan, *The Digitalization of Public Diplomacy*, Palgrave Macmillan Publishers, Basingstoke, UK, 2019.

27. MARION, Nancy E.; TWEDE, Jason, *An Encyclopedia of Digital Crime*, ABC-CLIO, LLC Publishers, Santa Barbara, California, USA, 2020.

28. NAJZER, Brin, *The Hybrid Age: International Security in the Era of Hybrid Warfare,* I.B. Tauris Bloomsbury Publishing, London, 2020.

29. OAKLEY; Jacob G., *Waging Cyber War. Technical Challenges and Operational Constraints,* Apress Publications, New York, USA, 2019

30. PRITCHARD, Adam C., THOMSON, Robert B; *Securities Law and the New Deal Justices*, pdf, URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article= 2552&context=articles

31. RIORDAN, Shaun, *Cyberdiplomacy, Managing security and governance online,* Editura Policy Press, Cambridge, UK, 2019.

32. SANGER, David E., *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Crown Publishing Group, a division of Penguin Random House LLC, New York, USA, 2018.

33. SKILLICORN, David B., *Cyberspace, Data Analytics, and Policing,* CRC Press, Boca Raton, Taylor & Francis Group, LLC, Boca Raton, Florida, 2021.

34. SCHMITT, Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* Cambridge University Press, Cambridge, 2017.

35. SCOTT, James Brown, *The Hague conventions and declarations of 1899 and 1907, accompanied by tables of signatures, ratifications and adhesions of the various powers, and texts of reservations,* New York Oxford University Press American Branch, Toronto, Canada,1915, p. 118.

36. WANG, Jennifer, *The White House and Pentagon Deem Cyber-Attacks, An Act of War*, *Forbes*, URL: http://www.forbes.com/sites/reuvencohen/2012/06/05/the-white-house-and-pentagon-deem-cyber-attacks-an-actof-war/