ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „ALEXANDRU IOAN CUZA” DIN IAȘI
TOMUL LXIV, ȘTIINȚE JURIDICE, 2018, SUPLIMENT

CYBERWARFARE-UL – O FORMĂ ACTUALĂ DE CONFLICT

CYBERWARFARE – A CURRENT FORM OF CONFLICT

ADRIAN CRISTIAN MOISE[1]

Rezumat: Articolul prezintă şi analizează aspecte referitoare la fenomenul *cyberwarfare*-ului. *Cyberwarfare*-ul reprezintă un conflict bazat pe tehnologia informaţiei şi comunicaţiilor, ce implică efectuarea unor atacuri motivate politic asupra informaţiei şi a sistemelor informatice. Un atac referitor la *cyberwarfare* cuprinde încălcări ale legilor, politicilor sau ale altor reglementări de la nivel naţional şi internaţional, acest aspect contribuind de cele mai multe ori la încadrarea fenomenului de *cyberwarfare* în sfera de aplicare a criminalităţii informatice.
În acest articol se efectuează o analiză şi asupra principalelor instrumente şi norme juridice internaţionale care cuprind aspecte referitoare la dreptul internaţional al războiului, cât şi asupra unor tratate şi acorduri internaţionale care reglementează cooperarea internaţională şi investigarea criminalităţii informatice şi a atacurilor referitoare la *cyberwarfare*. De asemenea, se efectuează şi o prezentare referitoare la infractorii şi victimele fenomenului *cyberwarfare*-ului.
Cuvinte cheie: cyberwarfare, tehnologia informaţiei şi comunicaţiilor, criminalitate informatică, sistem informatic, informaţie

Abstract: The article presents and analyzes aspects related to the phenomenon of cyberwarfare. Cyberwarfare is a conflict based on information and communication technology that involves performing politically motivated attacks on information and information systems. An attack involving cyberwarfare includes violations of laws, policies, or other regulations at national and international level, this aspect contributing most often to framing the cyberwarfare phenomenon in the area of cybercrime.
This article also analyzes the main international legal instruments and norms that include international war law issues as well as international treaties and agreements governing international cooperation and investigation of cybercrime and

[1] Conferenţiar universitar doctor, Universitatea Spiru Haret din Bucureşti, Facultatea de Ştiinţe Juridice, Economice şi Administrative, Craiova, România; avocat, Baroul Dolj; email: adriancristian.moise@gmail.com.

cyberwarfare attacks. Also, there is a presentation about the offenders and victims of the cyberwarfare phenomenon.
Keywords: cyberwarfare, information and communication technology, cybercrime, information system, information

1. Introducere

În era tehnologiei informaţiei şi comunicaţiilor, cyberspaţiul şi informaţia au devenit concepte inseparabile. Practic, toată lumea utilizează zilnic cyberspaţiul în scopul de a obţine şi a transmite informaţii.

Ca în orice alt domeniu social, cyberspaţiul, care reprezintă o mare schimbare socială, a fost prezent la dezvoltarea teoriilor care definesc în mod diferit natura, semnificația și impactul acestui domeniu nou spațial. Există două direcţii de bază care descriu cyberspaţiul:[2] direcţia liberală care se referă la avantajele şi beneficiile cyberspaţiului şi direcţia realistă care descrie relaţia dintre cyberspaţiu şi puterea statului. Direcţia liberală recunoaşte caracterul democratic al cyberspaţiului, în timp ce utilizatorii acestuia sunt văzuţi ca observatori externi. De asemenea, direcţia liberală consideră că reţeaua Internet se dezvoltă printr-o cooperare internaţională intensă, în timp ce controlul acesteia este necesar pentru a supraveghea activităţile antisociale şi utilizarea în mod corespunzător a tehnologiei. Direcţia realistă consideră că cyberspaţiul este la fel ca orice alt spaţiu, acesta având semnificaţia a unui câmp de luptă şi a unei pieţe economice. În momentul în care, utilizarea cyberspaţiului a devenit o sursă de câştiguri noi, războiul în cyberspaţiu a devenit inevitabil.

Prin urmare, considerăm că cyberspaţiul nu reprezintă o sursă de forme noi de putere, ci reprezintă doar o zonă, în care puterea existentă se transferă din spaţiul real.

Reţeua Internet a creat un nou spaţiu, virtual, adică cyberspaţiul care coexistă cu spaţiul real. Cyberspaţiul prezintă mai multe caracteristici ce diferă de cele ale spaţiului real: capacitatea de a mobiliza utilizatorii; capacitatea de a furniza cantităţi mari de informaţii în orice moment; capacitatea de a elimina graniţele geografice şi distanţa dintre utilizatori. Se

[2] I. Bernik, *Cybercrime and cyberwarfare*, John Wiley and Sons, Inc., Hoboken, New Jersey, 2015, p. 52.

subliniază faptul că prin dezvoltarea Internetului s-a urmărit simplificarea comunicaţiei şi nu să se asigure siguranţa acesteia[3].

Pe lângă actele infracţionale tradiţionale (furtul, înşelăciunea, frauda, contrafacerea), care s-au transferat în cyberspaţiu, comportamentul deviant în cyberspaţiu include şi concurenţa agresivă şi lupta pentru puterea informaţiei.

Lupta cu sau pentru informaţii a luat o amploare considerabilă în ultimul timp, deoarece obţinerea informaţiilor conduce la dobândirea unui anumit grad de putere[4]. Astfel, din cauza creşterii exponenţiale de informaţii şi a cererii pentru acestea, lumea modernă se caracterizează printr-un anumit tip de putere, puterea informaţiei. Importanţa puterii informaţiei este mult mai evidentă în domeniul politicii, relaţiilor internaţionale şi în domeniul competiţiei inter-organizaţionale, unde luarea unor decizii responsabile social, ce sunt foarte importante pentru succesul acestor entităţi, necesită obţinerea unor informaţii corecte, în timp util, confidenţiale şi protejate. Prin urmare, în literatura de specialitate[5] s-a considerat că informaţia reprezintă puterea, iar nivelul de putere depinde de utilizarea informaţiilor. Dacă în trecut puterile militare, economice şi diplomatice reprezentau cele mai importante tipuri de putere, astăzi informaţia reprezintă cel mai important element pentru a obţine puterea în orice domeniu, aceasta fiind considerată de asemenea, un instrument de luare a deciziilor, de conducere a unor campanii agresive şi o forţă de multiplicare[6].

Puterea informaţiei se poate transmite foarte uşor, această caracteristică reprezentând cadrul pentru dezvoltarea personală, organizaţională, naţională şi internaţională. Puterea informaţiei este dorită de toată lumea datorită impactului pe care aceasta îl are asupra societăţii, dar cu toate acestea puterea informaţiei nu poate fi controlată, iar informaţia în societatea modernă nu poate fi monitorizată, controlată, reglementată şi limitată. În trecut, au fost puţine state care şi-au menţinut puterea lor asupra

[3] J. Eriksson, G. Glacomello, *The information revolution, security, and international relations: (IR) relevant theory?*, în International Political Science Review, vol. 27, no. 3/2006, pp. 221–244.

[4] M. Osborne, *Cyberattack, Cybercrime, Cyberwarfare*, CreateSpace Independent Publishing Platform, North Charleston, South Carolina, 2013, pp. 14-15.

[5] L. Armistead, *Information Operations: Warfare and the Hard Reality of Soft Power*, Brassey's Inc, Washington D.C., 2004, p. 15.

[6] W. Gragido, J. Pirc, *Cybercrime and Espionage. An Analysis of Subversive Multi-vector Threats*, Syngress Publishing Inc., Elsevier, Burlington, Massachusetts, 2011, p. 82.

popoarelor cu ajutorul informaţiilor pe care acestea le deţineau. În societatea modernă, dezvoltarea continuă a tehnologiei informaţiei şi comunicaţiilor a contribuit la sfârşitul monopolului puterii asupra informaţiei.

În societatea informaţională, puterea informaţiei se obţine, se menţine şi se controlează cu dificultate. Pentru a obţine poziţia dominantă asupra informaţiei sau superioritatea faţă de adversar există o luptă continuă între adversari în scopul obţinerii puterii informaţiei. Lupta dintre informaţie şi puterea informaţiei a generat un nou tip de conflict, numit *conflictul informaţiei*[7]. Domeniile în care conflictul informaţiei poate fi găsit se referă la informaţii şi la reţelele şi sistemele informatice, acest tip de conflict nefiind la fel de grav ca un conflict militar. *Conflictul informaţiei* reprezintă un conflict grav care nu cauzează în mod direct prejudicii fizice[8]. Efectele temporare produse de conflictul informaţiei sunt asemănătoare cu cele produse de un conflict militar şi sunt mai mari decât cele produse de un conflict economic.

Conflictul informaţiei este asemănător cu criminalitatea informatică şi diferit de războiul clasic, ceea ce determină elaborarea unei definiţii a noţiunii de *cyberwar* cu maximă atenţie.

2. Definiţia noţiunii de cyberwarfare

În prezent nu există o definiţie universal acceptată a noţiunii de *cyberwarfare*-război cibernetic- sau un consens cu privire la ceea ce ar trebui să cuprindă această noţiune, nu sunt stabilite clar mijloacele prin intermediul cărora cyberwarfare-ul se produce, cât şi motivele care determină producerea acestui fenomen[9]. În literatura de specialitate, pe lângă noţiunea de *cyberwarfare* mai este utilizată şi o altă denumire a acestei noţiuni, cum este *cyberwar*[10].

Cyberwarfare-ul „se referă la atacurile motivate politic săvârşite asupra tehnologiei informaţiei şi comunicaţiilor în scopul de accesa neautorizat sistemele şi reţelele informatice ale unei ţări, organizaţii sau grupuri cu intenţia de a comite acte de spionaj sau sabotaj[11]”. Războiul

[7] I. Bernik, *op.cit.*, p.55.
[8] *Ibidem*.
[9] D. Ventre, *Cyberwar and Information Warfare*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2011, pp. 247-249.
[10] L. J. Siegel, *Criminology. Theories, Patterns and Typologies*, ed. a 10-a, Cengage Learning, Belmont, California, 2010, pp. 479-481.
[11] I. Bernik, *op.cit.*, p. 54.

cibernetic poate fi înţeles ca o analogie la războaiele convenţionale, dar în schimb această analogie este controversată datorită preciziei şi motivaţiei politice a acesteia.

O altă definiţie a războiului cibernetic este următoarea: „*Cyberware-ul* reprezintă un conflict bazat pe Internet care implică efectuarea unor atacuri motivate politic asupra informaţiei şi a sistemelor informatice. Atacurile referitoare la războiul cibernetic pot dezactiva site-urile web şi reţelele oficiale, pot perturba sau dezactiva servicii esenţiale, pot fura sau modifica date clasificate şi paraliza sistemele financiare, printre multe alte posibilităţi”[12].

După opinia noastră, *cyberwarfare-ul* constă în utilizarea tehnologiei informaţiei şi comunicaţiilor în scopul de a perturba activităţile unui stat sau organizaţii, în special prin atacarea sistemelor informatice în scopuri militare sau strategice.

Cyberwarfare-ul utilizează un concept de război care poate fi definit drept o formă extremă de comunicare între două sau mai multe grupuri care încearcă să-și protejeze sau să-și mărească averea, interesele sau influența lor, prin acțiuni asupra: resurselor naturale, cum sunt petrolul şi zăcămintele de minerale; populaţiei, ce reprezintă elementul uman; mentalităţii, ce reprezintă elementul intelectual sau spiritual; teritoriului, ce reprezintă elementul geografic; informaţiilor, ce reprezintă elementul virtual.

Considerăm că scopul final al unui război cinetic este de a acţiona asupra spaţiului din lumea reală. Dimensiunea cibernetică a războiului reprezintă doar un instrument suplimentar prin noi sisteme și instrumente pentru a acționa în lumea fizică.

Un atac referitor la cyberwarfare cuprinde încălcări ale legilor, politicilor sau ale altor reglementări de la nivel naţional şi internaţional, acest aspect contribuind de cele mai multe ori la încadrarea războiului cibernetic în sfera de aplicare a criminalităţii informatice[13].

Cyberwarfare-ul are ca scop obţinerea informaţiilor referitoare la aspecte economice, politice, culturale şi militare dintr-o altă ţară, având rol de ţintă, sau efectuarea unor operaţiuni ofensive sau defensive specifice în

[12] Conform definiţiei termenului de *cyberwarfare* de pe website-ul: http://searchsecurity.techtarget.com/definition/cyberwarfare, accesat 07.11.2018.

[13] L. J. Siegel, *op.cit.*, p. 480.

cyberspaţiu[14]. Referitor la primul scop, ţările îşi ating obiectivele cel mai frecvent prin intermediul spionajului[15]. Cu privire la al doilea scop, aceste operaţiuni se desfăşoară în cyberspaţiu prin intermediul unor activităţi asemănătoare cu cele militare. *Cyberwarfare-ul* nu afectează numai statele, ci şi organizaţiile private care doresc să acceseze neautorizat anumite informaţii referitoare la dezvoltarea acestora şi la politicile concurenţiale.

3. Caracteristicile cyberwarfare-ului

Cyberwarfare-ul reprezintă un fenomen nou care diferă printr-o serie de caracteristici de războiul tradițional, aceste diferențe ridicând probleme juridice, politice și practice pe care statele naționale vor trebui să le rezolve, atât individual, cât și colectiv. Cele mai importante caracteristici ale *cyberwarfare-ului* sunt următoarele:[16]

3.1. Costuri reduse

Instrumentele necesare pentru a desfăşura un cyberwarfare sunt disponibile pe reţeaua Internet, acestea având preţuri accesbile.

3.2. Dispariţia frontierelor geografice

În cadrul cyberwarfare-ului, investigatorii identifică cu dificultate atât locaţiile de unde sunt lansate atacurile cibernetice, cât şi persoanele care au săvârşit aceste fapte ilegale.

3.3. Manipularea percepţiei publice

Atacatorii din domeniul cyberwarfare-ului au capacitatea de a manipula cu uşurinţă percepţia publică prin producerea unor informaţii false sau prin modificarea unor fişiere multimedia.

3.4. Lipsa unor informaţii strategice

Metodele tradiţionale de colectare a informaţiilor de către organele de securitate naţională sunt depăşite, iar organele care au atribuţii în

[14] A. C. Moise, *Dimensiunea criminologică a criminalităţii din cyberspaţiu*, Ed. C.H. Beck, Bucureşti, 2015, p. 346.

[15] R. W. Taylor, T. J. Caeti, D. K. Loper, E. J. Fritsch, J. Liederbach, *Digital Crime and Digital Terrorism*, Pearson Prentice Hall, Upper Saddle River, New Jersey, 2006, p. 47.

[16] O. A. Bello, F. M. Aderbigbe, *Cyberwar- The new frontier of International Warfare*, în International Journal of Sustainable Development Research, 2015; 1(1), p. 4.

domeniul securităţii naţionale nu sunt pregătite pentru colectarea informaţiilor în legătură cu *cyberwarfare*-ul.

3.5. Dificultatea în avertizarea tactică şi în evaluarea atacului cibernetic

Caracterul anonim al cyberspaţiului îngreunează activitatea organelor de punere în aplicare a legii de identificare şi investigare a atacurilor săvârşite în cyberspaţiu.

3.6. Participarea în cadrul cyberwarfare-ului a unor organizaţii private

În cadrul *cyberwarfare*-ului pot fi implicate pe lângă statele naţionale şi organizaţii private.

3.7. Cyberwarfare-ul este un război atât ofensiv cât şi defensiv

Operaţiile *cyberwarfare*-ului ofensiv se încadrează în cadrul următoarelor acţiuni: distrugerea, perturbarea şi dezinformarea[17].

Operaţiile *cyberwarfare*-ului ofensiv care conduc la *distrugerea* sistemelor şi reţelelor infomatice se realizează mult mai rar.

Acţiunea de *perturbare* a sistemelor şi reţelelor informatice reprezintă cea mai întâlnită operaţie de cyberwarfare ofensiv. Acest tip de operaţiune poate fi exemplificat cel mai bine prin deteriorarea paginilor web, eliberarea de viruşi informatici, viermi şi alte software maliţioase care vizează distrugerea datelor critice din sistemele de procesare a informaţiilor.

Instrumentele utilizate de atacatorii cibernetici pentru a perturba activitatea sistemelor sau reţelelor informatice sunt disponibile pe Internet, orice persoană putând să le descarce şi apoi să le lanseze în atacul cibernetic. Rezultatul urmărit de cyberatacatori în cadrul acţiunii de perturbare constă în blocarea temporară a funcţionării sistemelor şi reţelelor informatice şi realizarea unor cheltuieli substanţiale pentru repararea sistemelor şi reţelelor informatice.

Acţiunea de *dezinformare* implică manipularea intenţionată a informaţiilor în scopul de a plasa adversarul într-o poziţie nefavorabilă în faţa opiniei publice. Prin urmare, obiectivul acestei acţiuni este crearea unui climat ostil faţă de poziţia politică a adversarului, astfel încât opinia publică să îl determine pe acesta să îşi schimbe poziţia politică. Acţiunea de

[17] T. O'Hara, *Cyber Warfare/Cyber Terrorism*, USAWC Strategy Research Project, Master of Strategic Studies Degree, U.S. Army War College, Carlisle Barracks, Carlisle, Pennsylvania, 17013-5050, 3 May 2004, pp. 8-9.

dezinformare diferă de celelalte două acţiuni ale cyberwarfare-ului ofensiv, prin faptul că acestea ţintesc nu numai pe adversar, ci şi pe cei care ar putea să ajute adversarul.

Acţiunea de dezinformare reprezintă este cea mai puţin invazivă acţiune a celor trei tipuri de operaţii ale *cyberwarfare*-ului ofensiv, deoarece aceasta nu depinde de interacţiunea cu sistemul informatic al adversarului. Subliniem faptul că un dezavantaj major al acestui tip de acţiune este acela că executarea cyberatacului trebuie să fie gestionată în detaliu, iar deconspirarea sursei de dezinformare poate avea ca rezultat o reacţie puternic ostilă împotriva făptuitorului şi o consolidare a sprijinului pentru adversar.

Cyberwarfare-ul defensiv este conceput să funcţioneze în întreagă gamă de operaţiuni militare şi nonmilitare în scopul de a îndeplini obiectivele securităţii naţionale. Menţinerea libertăţii de utilizare a sistemelor şi reţelelor informatice reprezintă un obiectiv principal al domeniului securităţii naţionale.

Scopul principal al *cyberwarfare*-ului defensiv este asigurarea protecţiei necesare a infrastructurii critice.

Cyberwarfare-ul defensiv are patru obiective cheie pe care doreşte să le îndeplinească[18]. Primul obiectiv al *cyberwarfare*-ului defensiv se referă la stabilirea unui mediu cibernetic de protecţie, care să menţină libertatea de utilizare a sistemelor şi reţelelor informatice. Al doilea obiectiv al *cyberwarfare*-ului defensiv se referă la detectarea cyberatacurilor. Al treilea obiectiv al *cyberwarfare*-ului defensiv se referă la repararea rapidă şi eficientă a sistemelor şi reţelelor informatice. Al patrulea obiectiv al *cyberwarfare*-ului defensiv constă în răspunsul la atacul cibernetic lansat, ce se referă la identificarea locaţiei de unde a fost lansat cyberatacul, cât şi la identificarea atacatorului, permiţând ulterior efectuarea unor operaţiuni ale *cyberwarfare*-ului ofensiv în scopul de a reprima cyberatacul.

Operaţiile *cyberwarfare*-ului defensiv sunt grupate în cinci categorii, concepute pentru a asigura confidenţialitatea, integritatea, disponibilitatea, non-repudierea şi autentificarea datelor informatice. *Confidenţialitatea* datelor informatice se referă la acţiunile care vizează ca informaţiile cuprinse în sistemele informatice să nu fie dezvăluite persoanelor neautorizate. *Integritatea* datelor informatice se referă la

[18] T. O'Hara, *op.cit.*, p. 11.

acţiunile care trebuie să asigure consistenţa informaţiilor prin prevenirea creării, modificării sau distrugerii neautorizate a datelor informatice. *Disponibilitatea* datelor informatice se referă la acţiunile ce trebuie să asigure faptul că utilizatorilor legitimi nu li se va refuza în mod nejustificat accesul la resurse, ce include date şi alte resurse de comunicaţii. *Non-repudierea* se referă la acţiunile destinate să asigure că o persoană care a luat parte la o comunicare în mediul online, nu va putea susţine ulterior că această comunicare nu a avut loc. *Autentificarea* datelor informatice se referă la acţiunile care au ca scop asigurarea identităţii participanţilor la o tranzacţie în mediul electronic.

În final, evidenţiem faptul că operaţiile cibernetice ofensive şi defensive reprezintă puncte esenţiale în cadrul cyberwarfare-ului, fiind deosebit de utile pentru a sprijini domeniul securităţii naţionale. În vremuri de pace, operaţiile cibernetice ofensive şi defensive conlucrează cu alte elemente din domeniul puterii naţionale în scopul de a preveni apariţia crizelor şi a conflictelor.

4. Tipuri de cyberwarfare

La fel ca în cazul infractorilor din domeniul criminalităţii informatice, statele naţionale profită de avantajele utilizării noilor tehnologii în scopul de a-şi susţine interesele de politică externă, de a desfăşura activităţi de propagandă pentru a influenţa mentalitatea poporului, cât şi în vederea atingerii scopurilor lor militare.

Cele mai des întâlnite tipuri de cyberwarfare sunt următoarele:[19] spionajul, activităţile de propagandă, operaţiunile de informare şi cyberwarfare-ul în activităţile militare.

4.1. Spionajul

Spionajul reprezintă o formă de a obţine informaţii, ce implică pătrunderea în anumite zone în care se păstrează informaţii cu caracter confidenţial. Această activitate este desfăşurată de spioni în numele şi în scopurile serviciilor de informaţii externe şi ţărilor lor.

Utilizând activităţile de spionaj, statele naţionale încearcă să furnizeze date şi informaţii pentru domeniul securităţii naţionale, precum şi pentru nevoile economiei private. Astfel, ţările îşi ajută companiile şi

[19] I. Bernik, *op.cit.*, pp. 68-77.

organizaţiile prin oferirea acestora a unor informaţii economice importante din punct de vedere strategic. Un exemplu de sistem cibernetic de spionaj des utilizat în *cyberwarfare* este sistemul de spionaj *Echelon*[20], ce este utilizat în special pentru a aduna date militare şi politice, dar, avantajul puterii, obţinut în domeniul militar şi politic este incomplet, dacă nu există şi o dominaţie economică. Aceste sisteme de spionaj sunt utilizate de organele din domeniul securităţii naţionale în cadrul etapei de obţinere de informaţii.

Dacă activităţile de obţinere de informaţii se comit în sfera economică, atunci aceste activităţi se încadrează în sfera spionajului industrial. Ţinta spionajului industrial îl reprezintă datele atât în format material cât şi în format electronic. Spionajul industrial se desfăşoară pe mai multe niveluri, implicând ţări, organizaţii internaţionale şi persoane fizice. Metodele de spionaj industrial utilizează în special noile evoluţii în tehnologia informaţiei şi comunicaţiilor.

4.2. Operaţiunile de informare

Obiectivul general al operaţiunilor de informare este dominarea cyberspaţiului prin prevenirea, distrugerea şi schimbarea ameninţărilor inamicului, prin sistemele de supraveghere şi control şi prin sistemele de infrastructură critică. Operaţiunile de informare au de obicei, ca ţintă un grup de persoane pe care un stat naţional doreşte să-l supună sau să-l slăbească. Prin urmare, activităţile desfăşurate de acel stat în cadrul operaţiunilor de informare trebuie să împiedice acel grup de persoane să desfăşoare o anumită activitate sau să se abţină de la efectuarea ei.

Operaţiunile de informare utilizează în spaţiul virtual tipuri de înşelăciuni, acţiuni asupra stării psihologice a oamenilor şi asupra mentalităţii acestora, generând un impact semnificativ asupra opiniei publice şi asupra societăţii în ansamblul ei.

Cele mai frecvent săvârşite operaţiuni de informare sunt următoarele: atacurile asupra sistemelor şi reţelelor informatice, publicitatea negativă în mass-media, *spam*-ul şi ameninţările cu perturbarea infrastructurii critice de informaţii.

4.3. Activităţile de propagandă

[20] Sistemul Echelon se referă la o reţea globală de sisteme informatice care cercetează în mod automat prin mesajele interceptate, cuvinte cheie, adrese de fax şi adrese de e-mail, ce sunt ulterior selectate automat într-o staţie.

Activităţile de propagandă în domeniul cyberwarfare-ului vizează influenţarea comportamentului uman dintr-o anumită ţară, prin intermediul mass-mediei şi a politicii.

4.4. Cyberwarfare-ul în activităţile militare

Cyberwarfare-ul prezintă o dimensiune dublă. Pe de o parte, conflictul se desfăşoară în scopul de a controla cyberspaţiul. Pe de altă parte, chiar dacă războiul cibernetic reprezintă o formă nouă de conflict, atunci strategiile şi tacticile pe care acesta le implică, aparţin unui război cu obiective convenţionale. *Cyberwarfare*-ul reprezintă un tip de război, ce utilizează intensificatori de forţă pentru războiul cinetic. Eficienţa războiului cibernetic se referă la eliminarea noţiunii de asimetrie[21].

Actorii care conduc operaţiunile militare diferă: armate, servicii de informaţii, hackeri, teroriști etc. Aceşti actori sunt implicaţi în lupte declarate şi asimetrice, unele fiind legitime, altele nu, aceştia putând adopta strategii de atac frontal sau de disimulare. Dar în cyberspaţiu, aceste calităţi nu mai sunt de actualitate. Toţi combatanţii din cyberspaţiu se află în acelaşi spaţiu, utilizează aceleaşi tehnici, instrumente şi mijloace. În cyberspaţiu ţintele sunt vizibile pentru toţi atacatorii[22].

Cyberspaţiul permite desfăşurarea conflictelor între state, între state şi actori neguvernamentali şi între actori neguvernamentali. În cyberspaţiu nu contează dacă autorul atacului este mic sau mare, slab sau puternic sau dacă reprezintă o ţară, ţinta fiind lovită tot timpul în acelaşi mod. Prin urmare, evidenţiem faptul că problema asimetriei nu mai este de actualitate.

5. Infractorii şi victimele în cadrul cyberwarfare-ului

Orice persoană fizică care are cunoştinţe avansate în domeniul tehnologiei informaţiei şi comunicaţiilor poate deveni un infractor în cyberspaţiu.

---

[21] Războiul asimetric reprezintă un termen care explică lupta dintre beligeranții a căror putere militară, strategii sau tactici diferă semnificativ. De asemenea, acest termen poate descrie un conflict în care resursele de luptă diferă semnificativ între beligeranți. Astfel, fiecare parte folosește forțele sale și slăbiciunile adversarului pentru a învinge.

[22] D. Ventre, *Cyberwar and Information Warfare, op.cit.*, p. 226.

În timpul războiului cibernetic, infractorii pot deveni şi victime în acelaşi timp. Victima unui cyberwarfare poate fi orice ţară, organizaţie, sau chiar persoană fizică[23].

Infractorii din domeniul cyberwarfare-ului utilizează tehnologia informaţiei şi comunicaţiilor în scopul de a distruge sau de a perturba grav infrastructura critică de informaţii de importanţă vitală pentru societate: reţelele informatice guvernamentale, reţelele de telecomunicaţii, sistemele de navigaţie pentru transportul maritim şi aerian, sistemele de control al apei, sistemele energetice, sistemele financiare, sau alte funcţii de importanţă vitală pentru societate.

6. Combaterea cyberwarfare-ului

La nivel internaţional nu s-a elaborat încă o legislaţie care să incrimineze în mod expres războiul cibernetic, există doar nişte instrumente şi norme juridice internaţionale care cuprind doar aspecte referitoare la dreptul internaţional al războiului, cum sunt Convenţia de la Geneva, Protocolul adiţional la Convenţiile de la Geneva din 12 august 1949 privind protecţia victimelor conflictelor armate internaţionale, Carta Naţiunilor Unite, Convenţia Consiliului Europei privind criminalitatea informatică, legislaţia internaţională privind drepturile omului, şi anumite tratate şi acorduri internaţionale, cum ar fi de exemplu, Organizaţia Tratatului Atlanticului de Nord – NATO –, care reglementează cooperarea internaţională şi investigarea criminalităţii informatice şi a atacurilor referitoare la războiul cibernetic[24].

Legile războiului sau *jus ad bellum* condiţionează strict dreptul de a utiliza forţa şi cuprinde toate standardele legale care reglementează legalitatea utilizării forţei de către guvernele statelor naţionale[25]. *Jus ad bellum* impune următoarele principii fundamentale: dreptul de a utiliza forţa, existenţa unei autorităţi obiective, legal constituite, iar utilizarea forţei trebuie să fie aplicată ca ultimă soluţie. De asemenea, legile războiului recunosc dreptul la apărare.

---

[23] A. C. Moise, *op.cit.*, p. 347.

[24] C. A. Theohary, J. W. Rollins, *Cyberwarfare and Cyberterrorism: In Brief*, Congressional Research Service, CRS Report, Prepared for Members and Committees of Congress, 27 March 2015, pp. 4-8; D. Ventre, *Information Warfare*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009, pp. 279-286.

[25] D. Ventre, *Information Warfare*, *op.cit.*, pp. 280-281.

Legile din timpul războiului sau *jus in bello* reglementează cadrul legal cu privire la ceea ce este acceptat sau nu este acceptat în timpul ostilităţilor[26]. Legile referitoare la război alcătuiesc dreptul internaţional al războiului: *jus ad bellum* este cuprins în Carta Naţiunilor Unite, iar *jus in bello* este prevăzut în Convenţia de la Geneva.

Reglementarea juridică a cyberspaţiului şi a activităţilor din cadrul acestuia, precum şi activităţile legate de identificarea şi investigarea cyberatacurilor reprezintă cele importante elemente pentru o protecţie eficientă împotriva acţiunilor ilegale săvârşite de infractorii din domeniul *cyberwarfare*-ului.

Termenul de *cyberwarfare* a fost grupat în cinci forme, care variază de la cele mai uşoare până la cele mai grave forme:[27] vandalismul pe web; campaniile de dezinformare; colectarea de date cu caracter secret; perturbarea sistemelor şi reţelelor informatice; atacurile săvârşite împotriva infrastructurii critice naţionale. Definiţiile *cyberwarfare*-ului utilizează mai degrabă termenul de război într-un sens descriptiv şi retoric, şi nu într-un sens juridic.

Cu toate acestea, remarcăm faptul că noţiunea de *cyberwarfare* cuprinde acţiuni care ar putea să nu se potrivească cu conceptul juridic al războiului, putând genera de cele mai multe ori confuzie. Utilizarea acestor expresii sau termeni referitori la noţiunea de *cyberwarfare*, care au o întindere mult mai cuprinzătoare decât un termen sau o definiţie juridică corespunzătoare, poate avea consecinţe semnificative pentru aplicarea legii, protecţia persoanelor şi a proprietăţii şi pentru executarea operaţiunilor.

În plus, în ciuda utilizării frecvente la nivel internaţional a termenilor de *cyberwarfare* şi cyberwar, pentru a defini noţiunea de război cibernetic, nu ştim dacă aceştia sunt cei mai potriviţi şi justificaţi cu privire la dreptul internaţional al războiului.

În literatura de specialitate s-a subliniat faptul că există mai multe principii, pe baza cărora se susţine ideea că reglementarea juridică a *cyberwarfare*-ului este mai adecvată din perspectiva războiului clasic. Totodată, se remarcă faptul, că orice modificare sau deviere de la aceste

[26] *Idem*, p. 281.

[27] L. R. Blank, *Cyber War/Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace*, Emory University School of Law, Legal Studies Research Paper Series, Research Paper No. 14-286, p. 5.

principii semnifică o încălcare a dreptului internaţional al războiului, indiferent dacă acestea apar în spaţiul real sau cyberspaţiu.

Principiile internaţionale care intră sub incidenţa dreptului internaţional al războiului, incluzând şi domeniul cyberwarfare-ului, sunt următoarele:[28]

a. Principiul discriminării, ce se referă la utilizarea legitimă a tacticilor şi a armelor militare, făcându-de deosebirea între ţintele militare şi cele civile. Majoritatea atacurilor din domeniul *cyberwarfare*-ului încalcă principiul discriminării, deoarece acestea au ca ţinte şi obiective civile.

b. Principiul proporţionalităţii se referă la utilizarea armelor şi tacticilor militare în mod proporţional cu ţintele militare, multe războaie cibernetice neavând o ţintă militară bine definită.

c. Principiul legalităţii constă în faptul că utilizarea forţei militare nu trebuie să fie în contradicţie cu normele dreptului internaţional şi cu acordurile internaţionale. Multe războaie cibernetice nu încalcă legile războiului, ci pot încălca diferite norme referitoare la dreptul internaţional, cum ar fi de exemplu, în domeniul comunicaţiilor electronice.

d. Principiul necesităţii se referă la utilizarea forţei şi tacticilor militare în mod necesar pentru a se atinge scopul urmărit. Întrucât atacurile din domeniul *cyberwarfare*-ului nu au un obiectiv bine definit, acestea nu pot fi necesare.

e. Principiul umanităţii se referă la faptul că utilizarea forţei militare nu trebuie să provoace suferinţe inutile victimelor. Orice armă care provoacă urmări în afara locului şi timpului unei zone de război este ilegală. Întrucât, *cyberwarfare*-ul nu vizează o anumită zonă de război, sentimentul de frică se poate răspândi foarte uşor în multe arii.

f. Principiul neutralităţii constă în faptul că utilizarea forţei militare nu trebuie să provoace prejudicii persoanelor din ţările, ce sunt declarate în mod oficial a fi neutre. *Cyberwarfare*-ul poate afecta infrastructura critică din ţările declarate în mod oficial a fi neutre.

Subliniem faptul, că *cyberwarfare*-ul încalcă majoritatea principiilor de bază ale dreptului internaţional al războiului. De asemenea, constatăm că este imposibil să clasificăm războiul cibernetic într-un război în adevăratul sens al cuvântului, ci mai mult ca o crimă specifică și cu un impact mai larg din punct de vedere social. Deşi efectele *cyberwarfare*-ului

[28] I. Bernik, *op.cit.*, pp. 98-99.

nu sunt imediate, acestea pot fi la fel de periculoase şi dăunătoare ca cele ale războiului clasic.

Cyberwarfare-ul a modificat conceptele tradiţionale de securitate şi suveranitate naţională, deoarece acesta funcționează într-un mediu complet nou, care nu a fost anticipat din punct de vedere legislativ.

Un alt aspect important se referă la domeniul de definire a competențelor organelor de punere în aplicare a legiii în cyberspațiu. Dreptul internațional conferă fiecărui stat național dreptul la libertate pe teritoriul acestuia. Acest principiu consacră fiecărei țări dreptul la autonomie, siguranță și suveranitate pe teritoriul său național. Astfel, nici unei țări nu-i este permis să-și folosească forțele armate pentru a invada teritoriul unei alte țări pe mare, aer sau pământ. Principiul suveranității unui stat în cybespațiu nu este clar. În cadrul Capitolului I al art. 2 alin. 4 din Carta Națiunilor Unite, se prevede că „toate statele membre care se angajează în relații internaționale trebuie să se abțină de la amenințarea sau utilizarea forței împotriva integrității teritoriale sau a independenței politice a vreunui stat, fie în alt mod incompatibil cu scopurile Organizaţiei Naţiunilor Unite”. Deși, autoritățile de punere în aplicare a legii protejează fizic teritoriul unei țări, problema referitoare la reglementarea protecției cyberspațiului nu este încă clarificată.

O altă problemă legată de reglementarea cyberwarfare-ului, se referă la detectarea și identificarea cazurilor individuale de criminalitate informatică ca fiind un caz politic, ideologic sau comercial al unei lupte planificate cu atenție pentru informare. Convenția Consiliului Europei privind criminalitatea informatică reprezintă singurul instrument juridic obligatoriu de la nivel internațional care se referă la criminalitatea în legătură cu sistemele informatice și de comunicare. Convenția nu face nici o distincție între erori, accesul ilegal într-un sistem informatic și declararea unui război de către un anumit stat. Este dificil să se demonstreze motivul și scopul atacului unui anumit stat datorită tehnicilor și naturii intruziunilor, acest aspect privând țările de posibilitatea de a răspunde în mod activ la atacurile cibernetice ale unui alt stat, deoarece acestea nu pot stabili cu precizie că într-un anumit caz se confruntă cu perturbarea unui sistem informatic.

Un alt aspect al reglementării juridice necorespunzătoare a *cyberwarfare*-ului se referă atât la etapa de colectare a probelor digitale, cât şi la desfăşurarea întregului proces de investigare criminalistică a

cyberwarfare-ului la nivel naţional şi internaţional. În ciuda faptului că legislaţia penală şi procesual-penală defineşte importanţa probelor digitale, în practică organele de punere în aplicare a legii se confruntă încă cu înţelegerea proceselor de investigare criminalistică a infracţiunilor săvârşite în cyberspaţiu, ceea ce măreşte gradul de îndoială cu privire la autenticitatea probelor digitale colectate şi la posibilităţile de contestare a acestor probe pe parcursul desfăşurării procedurilor judiciare. Datorită caracterului transfrontalier al *cyberwarfare*-ului, organele de aplicare a legii depind de cooperarea judiciară dintre toate statele naţionale implicate în *cyberwarfare*. În prezent, Convenţia Consiliului Europei privind criminalitatea informatică identifică necesitatea unei cooperări judiciare reciproce în baza cererilor de asistenţă judiciară sau a tratatelor bilaterale şi a acordurilor de asistenţă reciprocă. Cu toate acestea, această Convenţie încă nu a fost semnată şi ratificată de multe state naţionale, şi ca urmare a acestui aspect, infractorii din domeniul *cyberwarfare*-ului acţionează şi lansează atacuri cibernetice mai ales din aceste ţări[29].

Evidenţiem faptul că legislaţia actuală în domeniul protecţiei datelor cu caracter personal împiedică organele de punere în aplicare a legii să examineze traficul de Internet la punctele de intrare din ţara lor. Astfel, reglementările juridice actuale de la nivel internaţional şi naţional în domeniul cooperării judiciare şi protecţiei datelor cu caracter personal, împietează de cele mai multe ori buna desfăşurare a procesului de investigare criminalistică a *cyberwarfare*-ului.

Referitor la Carta Naţiunilor Unite, subliniem faptul că acest instrument juridic de la nivel internaţional oferă fiecărui stat membru dreptul la autoapărare, care se aplică inclusiv în cazul cyberatacurilor. Cu toate acestea, posibilitatea unui contraatac se aplică numai în situaţia, în care un atac se află în desfăşurare. De exemplu, un atac lansat împotriva unui sistem informatic este înţeles în mod asemănător cu activitatea de spionaj. Prin urmare, nu este permisă utilizarea forţei de către un stat naţional în scopul de a recurge la represalii.

Carta Naţiunilor Unite prevede trei excepţii de la interzicerea utilizării forţei, dintre care numai a treia situaţie este relevantă pentru sensul de „atac armat” din cadrul art. 51 al Capitolului VII din acest instrument juridic. În primul rând, un stat poate folosi forța cu consimțământul statului

[29] C. A. Theohary, J. W. Rollins, *op.cit.*, p. 7.

teritorial, cum ar fi atunci, când un stat care se luptă cu un grup armat, solicită asistență din partea unuia sau mai multor state. În al doilea rând, un stat poate folosi forța ca parte a unei operațiuni multinaționale, autorizată de Consiliul de Securitate în temeiul Capitolului VII, astfel cum se prevede la art. 42: „În cazul, în care Consiliul de Securitate va socoti că măsurile prevăzute în Articolul 41 nu ar fi adecvate ori că s-au dovedit a nu fi adecvate, el poate întreprinde, cu forţe aeriene, navale sau terestre, orice acţiune pe care o consideră necesară pentru menţinerea sau restabilirea păcii şi securităţii internaţionale. Această acţiune poate cuprinde demonstraţii, măsuri de blocadă şi alte operaţiuni executate de forţe aeriene, maritime sau terestre ale Membrilor Naţiunilor Unite".

În al treilea rând, un stat național poate folosi forța în conformitate cu dreptul inerent de autoapărare individual sau colectivă, prevăzut la art. 51[30] din Capitolul VII al Cartei Națiunilor Unite ca răspuns la un atac armat. Astfel, art. 51 recunoaște dreptul la autoapărare individuală sau colectivă în cazul unui atac armat asupra unui membru al ONU până când Consiliul de Securitate decide asupra măsurilor necesare pentru asigurarea păcii și securității internaționale. Cu toate acestea, dreptul la autoapărare este limitat de răspunsul la un atac armat, iar acțiunea în temeiul acestei restricții este mai restrânsă decât conceptul de „utilizare a forței", care este interzis de art. 2 alin. 4, Capitolul I din Carta Naţiunilor Unite. Considerăm că aceasta înseamnă că o țară poate deveni victima „utilizării forței", ce nu este considerată drept un atac armat și, prin urmare, nu are dreptul la autoapărare.

În cazul unui cyberatac asupra rețelei Internet, o țară ce are rolul de victimă, poate răspunde în procesul de autoapărare, prin luarea unor măsuri rezonabile, proporționale și necesare în scopul a-și proteja propria siguranță, numai în cazul, în care atacul ar atinge nivelul al unui conflict armat, ceea ce înseamnă că trebuie să producă aceleași consecințe. În cazul, în care un cyberatac nu se desfășoară în paralel sau înainte de atacul militar cinetic,

[30] Art.51 din Capitolul VII al Cartei Naţiunilor Unite prevede: „Nici o dispoziţie din prezenta Cartă nu va aduce atingere dreptului inerent de autoapărare individuală sau colectivă în cazul în care se produce un atac armat împotriva unui Membru al Naţiunilor Unite, până când Consiliul de Securitate va fi luat măsurile necesare pentru menţinerea păcii şi securităţii internaţionale. Măsurile luate de Membri în exercitarea acestui drept de autoapărare vor fi aduse imediat la cunoştinta Consiliului de Securitate şi nu vor afecta în nici un fel puterea şi îndatorirea Consiliului de Securitate, în temeiul prezentei Carte, de a întreprinde oricând acţiunile pe care le va socoti necesare pentru menţinerea sau restabilirea păcii şi securităţii internaţionale".

atunci considerăm că prevederile art. 2 alin. 4 din Carta Naţiunilor Unite pot fi luate în considerare, numai în situaţia, în care scopul unor astfel de atacuri cibernetice este de a provoca daune fizice și distrugerea infrastructurii critice.

Referitor la Organizaţia Tratatului Atlanticului de Nord -NATO-, aceasta a constatat cât de utilă este cooperarea şi asistenţa reciprocă internaţională în cazul lansării unor atacuri cibernetice, numai în timpul războiului cibernetic dintre Rusia şi Estonia din anul 2007. Atacul cibernetic lansat de Rusia împotriva sistemelor informatice guvernamentale ale Estoniei a intrat în domeniul de aplicare a prevederilor art. 5 din Tratatul NATO, care prevăd că un atac săvârşit împotriva unui stat membru al NATO, obligă alianța să exercite dreptul la autoapărare individuală sau colectivă, recunoscut prin art. 51 din Carta Naţiunilor Unite.

NATO a făcut un pas înainte pentru prima dată pentru consolidarea luptei împotriva *cyberwarfare*-ului, prin intermediul Declaraţiei Summitului NATO de la Bucureşti din luna aprilie a anului 2008, care prevede în art. 47, că NATO se angajează să protejeze infrastructura critică de informaţii împotriva cyberatacurilor şi să combată aceste cyberatacuri.

În cadrul NATO, un rol important în domeniul securităţii cibernetice îl are organismul Cooperative Cyber Defence Centre of Excellence – CCDCOE –, ce are sediul în oraşul Tallinn din Estonia. CCDCOE reprezintă o organizaţie responsabilă cu pregătirea statelor membre NATO, dirijarea exerciţiilor de atac şi sprijinirea NATO în cazul unui atac cibernetic internaţional[31]. Poate adera la această organizaţie oricare dintre statele membre NATO, în timp ce proiectele de cooperare sunt coordonate împreună cu statele partenere NATO, mediul academic şi sectorul privat. Totuşi, am observat nu toate statele membre NATO s-au alăturat organizaţiei CCDCOE, multe dintre aceste state optând pentru utilizarea propriilor reţele militare de apărare împotriva atacurilor cibernetice[32].

7. Concluzii

Cyberwarfare-ul este un conflict între mai multe state naţionale, dar ar putea implica şi actori neguvernamentali. În cadrul *cyberwarfare*-ului

[31] K. Geers, *North Atlantic Treaty Organization. Cooperative Cyber Defence Centre of Excellence*, Strategic Cyber Security, CCD COE Publication, Tallinn, 2011, p. 25.

[32] A. C. Moise, *op.cit.*, pp. 382-383.

este dificil de a direcţiona forţa atacului, iar ţinta cyberatacului poate fi militară, industrială sau civilă. Armele utilizate în *cyberwarfare* se referă atât la componenta hardware, cât şi la componenta software.

Referitor la atribuirea cyberatacului, trebuie să subliniem faptul că infractorii din *cyberwarfare* sunt greu de identificat. Victoria şi înfrângerea sunt departe de a fi recunoscute în cyberspaţiu, deoarece aceste concepte au o semnificaţie redusă într-un spaţiu, în care actorii politici, ideologi, religioşi, economici şi militari se luptă pentru diferite motive.

Aceşti actori utilizează propriul cod de conduită în cadrul războiului, conducând la o stare discordantă şi haotică a conflictului, întrucât nu există în prezent o reglementare juridică corespunzătoare a fenomenului *cyberwarfare*-ului, un cod de etică, norme şi valori.