ASPECTE JURIDICE ŞI TERMINOLOGICE PRIVIND RĂZBOIUL CIBERNETIC

LEGAL AND TERMINOLOGICAL ISSUES ON CYBER WAR

dr. Mihai-Ştefan DINU[1]

Rezumat: *Folosirea mijloacelor cibernetice în cadrul unor operaţii militare clasice a condus în ultimul deceniu la dezvoltarea unor tendinţe privind militarizarea spaţiului cibernetic, tendinţe dezvoltate pe fondul manifestării din ce în ce mai accentuate a atacurilor de tip cibernetic la adresa unor infrastructuri critice.*

Prezenta lucrare propune o radiografie a terminologiei specifice războiului cibernetic şi abordează aspecte mai puţin solide ale domeniului precum aplicabilitatea normelor legale în vigoare la nivel internaţional în cadrul spaţiului cibernetic.

Cuvinte-cheie: *spaţiu cibernetic, război cibernetic, drept internaţional, arme cibernetice, apărare cibernetică, drept aplicabil războiului cibernetic.*

Abstract*: In the last decade, use of cyber tools during military operations leads to the development of certain trends regarding the militarization of cyber space, theese trends developing on the background of increasing cyber attacks on some critical infrastructures.*

This paper proposes a brief analysis of specific terminology in the field of cyber warfare and approaches some less solid issues of the field such as aplicability of international legal norms in cyber space.

Keywords*: cyber space, cyber warfare, international law, cyber weapons, cyber defence, cyber law.*

1. Introducere

Avansul tehnologic în domeniul informaticii şi comunicaţiilor a condus la apariţia unei serii semnificative de transformări în majoritatea activităţilor umane. Aceste transformări, alăturate creşterii performanţei sistemelor informatice au dus la conştientizarea existenţei unui spaţiu nou, un spaţiu cu numeroase beneficii dar şi nebănuite ameninţări: spaţiul cibernetic (cyber space). Deşi, concret, existenţa spaţiului cibernetic poate fi atestată cu mai bine de patru

[1] Cercetător ştiinţific gr. II, în cadrul Facultăţii de Securitate şi Apărare a Universităţii Naţionale de Apărare „CAROL I”.

decenii în urmă, înţelegerea fundamentată ştiinţific a fenomenului poate fi considerat a se afla încă la începuturile sale. Urmare a caracteristicii ridicate de penetrabilitate a folosirii sistemelor informatice, astăzi există puţine aspecte ale vieţii în care spaţiul concreteţii fizice să nu se intersecteze cu cel cibernetic. Infrastructurile necesare susţinerii calităţii vieţii sunt astăzi, în cel de al doilea deceniu al secolului XXI, în cea mai mare măsură automatizate, susţinute de un sistem sau un complex de sisteme informatice: infrastructuri ale sistemului medical, sistemului financiar-bancar, infrastructuri de comunicaţii şi sisteme militare sunt doar câteva exemple evidente ale folosirii din plin a beneficiilor spaţiului cibernetic în activităţile cotidiene. Pe lângă aceste beneficii au existat în timp, şi o serie de vulnerabilităţi care, exploatate prin intermediul diverselor softuri informatice, au condus la deficienţe serioase privind funcţionarea acestor sisteme, efectele simţindu-se de la nivel individual la nivel organizaţional, cu influenţe majore asupra funcţionării unui stat, în special atunci când acestuia i-au putut fi exploatate vulnerabilităţi ale sistemelor informatice care asistau diverse procese de automatizare ale infrastructurilor de transport, bancare sau de comerţ.

De altfel, putem aprecia că toate aceste tipuri de infrastructuri se constituie în elemente majore ale spaţiului cibernetic, fapt sesizat şi de cercetători ai domeniului. Tocmai de aceea, am ales să exemplificăm în continuare, cu o hartă a elementelor spaţiului cibernetic (figura nr. 1).

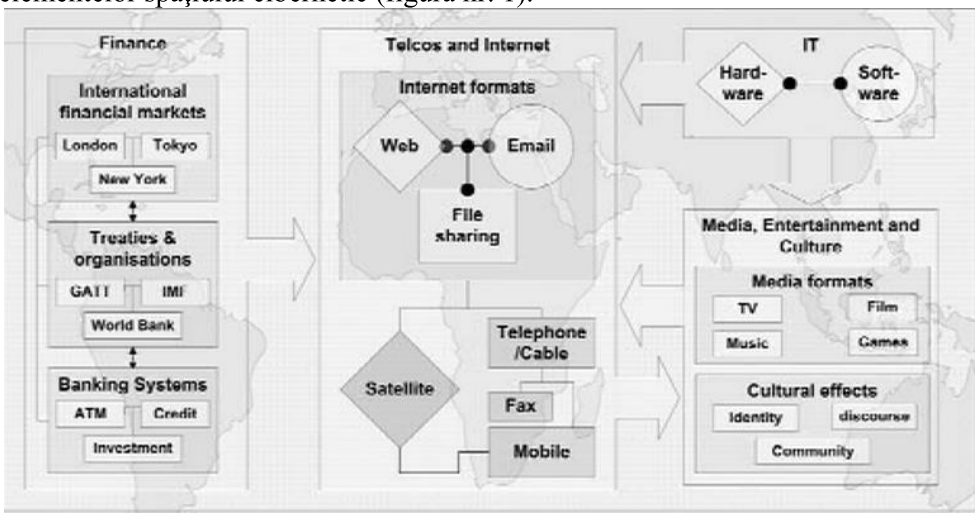


Figura nr. 1. Harta schematică propusă de Jason Whittaker,cu elemente ale spaţiului cibernetic.[2]

[2] Jason Whittaker, *The Cyberspace Handbook*, Routledge, London, 2003, p. 6.

2. Aspecte terminologice

În urma unei observaţii rapide se poate deduce că exploatarea vulnerabilităţilor sistemelor informatice asupra unuia dintre elementele figurate schematic în figura nr. 1 pot avea ca justificare o serie de situaţii precum:

- Experimentare (mentalitatea „să văd dacă pot")
- Obţinerea de foloase materiale (criminalitate cibernetică)
- Obţinerea de date şi informaţii (fie în scopul obţinerii unor foloase, fie în scop de spionaj)
- Limitarea sau distrugerea capacităţilor susţinute de infrastructuri critice (producere şi transport de energie, comunicaţii, finanţe-bănci etc.), ceea ce are ca efect limitarea capacităţilor de reacţie a unui stat în faţa unor ameninţări externe)

Fiecare dintre aceste situaţii este posibilă cu ajutorul softurilor informatice de tip *virus, worm, malware, troian* etc. Prin intermediul acestora utilizatorul lor poate:

- obţine acces la un sistem informatic, acces pe care îl poate exploata în scopul dorit: deturnare de fonduri, copiere sau ştergere de informaţii clasificate (la nivelul unor organizaţii civile şi militare)
- pe fondul lipsei de cultură de securitate a utilizatorilor sistemelor, să obţină date pe care le va folosi ulterior pentru a obţine accesul asupra unor conturi de mail sau chiar bancare.
- influenţa funcţionarea unor alte sisteme informatice angrenate în procesul de automatizare a unor infrastructuri critice (ale unor centrale atomice, electrice, sau de lansare a unor rachete), unele afectând direct funcţionarea unui stat, altele în mod indirect prin intermediul reacţiilor altor state care ar fi atacate de lansarea neautorizată a rachetelor menţionate anterior.

În acest context, putem creiona câteva aspecte cyber, după efectele acţiunilor de tip răuvoitor sau de tip atac, în sensul că putem vorbi de acţiuni de criminalitate cibernetică sau de atacuri cibernetice care pot fi considerate act de război. Pe acest fond literatura de specialitate a promovat concepte precum:

- cyber crime / infracţiuni cibernetice
- cyber war/ război cibernetic
- cyber warfare/ ducerea luptei cu mijloace cibernetice
- cyber conflict/ conflict cibernetic

Limitându-ne la tema studiului nostru vom aborda în continuare aspecte privind clarificarea terminologică a termenilor: cyber war, cyber warfare, cyber conflict, cyber weapons.

Atacurile cibernetice constituie un mod ieftin şi accesibil de lovire a capabilităţilor unui stat. În contextul dezvoltării rapide a sistemului cibernetic

global sistemul de interdependenţă este în continuă creştere simultan cu creşterea dependenţei de energie, transport, comunicaţii etc. Astfel, efectele unui atac cibernetic ar putea avea rezultate dezastruoase pentru întreaga activitate umană[3], conducând la criză economică, deficienţe în sistemele de comunicaţii[4], transporturi şi sănătate. Aceste atacuri se pot transforma, aşadar, facil în arme cibernetice. Dar ce se întâmplă atunci când atacurile cibernetice sunt iniţiate ca un act de război?

Aşa cum afirma Daniel Ventre conceptul de război cibernetic (cyber war) poate produce multe confuzii[5]. Acelaşi autor sublinia faptul că folosirea termenului de război cibernetic este condiţionată de tendinţele politice. Dacă atacurile cibernetice au loc în timpul unei perioade intense din punct de vedere politic sau pe timpul desfăşurării unui conflict armat, atunci există motive suficiente ca astfel de atacuri să fie numite război cibernetic[6].

În ciuda acestei clarificări, într-o lucrare anterioară, Ventre afirma faptul că războiul cibernetic trebuie considerat drept dimensiunea tehnică a războiului informaţional. Apelarea la capabilităţi cibernetice de către un stat în scopul desfăşurării unor operaţii cibernetice agresive pentru a lovi obiective militare, o infrastructură statală sau indirect dimensiunea societală a unui stat ţintă, poate fi percepută drept desfăşurare a unui război convenţional în care cel puţin o componentă se bazează pe sisteme informatice sau activează pe câmpul digital de luptă[7]. În acest caz modul de ducere a războiului ar fi de natură cibernetică, această situaţie justificând folosirea termenului de *cyber warfare.*

În acest context, acţiunile militare din spaţiul cibernetic s-ar încadra în tipul de operaţii numite operaţii în spaţiul cibernetic. Astfel, operaţiile în spaţiul cibernetic reprezintă acţiunea de angajare a capabilităţilor specifice spaţiului cibernetic (forţe cibernetice, de exemplu), atunci când scopul principal este acela de a realiza obiective militare în/prin spaţiul cibernetic[8]. Forţele cibernetice reprezintă o capabilitate nouă, considerată critică printre capabilităţile militare,

---

[3] Dănuţ Turcu, *Main Information Security Activities Of An Intelligence Service,* in Buletin of "CAROL I" National Defence University, No. 1/2014, Bucuresti, 2014, p.51.

[4] Sorin Topor, *Aproach About Joint Cyber And Electronic Warfare And Futures Of The Military Operations*, in the 10th International Scientific Conference "Strategies XXI": Strategic Changes In Security And International Relations, vol. 3, "CAROL I" National Defence University Publishing House, Bucharest, 2014 , pp. 72-76.

[5] *Ibidem*, p.120.

[6] *Ibidem.*

[7] Eric Filiol, *Aspects opérationnels d'une cyberattaque: renseignement, planification et conduit*, in Cyberguerre et Guerre de l'Information. Stratégies, Règles, Enjeux, Hermès Lavoisier, Paris, France, 2010, *apud* Daniel Ventre, *Cyber Conflict: Competing National Perspective,* ISTE Ltd, London, 2012, p. 121.

[8] ***, *FM 3-38, Cyber Electromagnetic activities*, Department of the army, feb. 2014, Washington DC, p. 1-3.

antrenate să desfăşoare misiuni în spaţiul cibernetic. La bază acestea sunt echipe mici, formate din specialişti super calificaţi[9].

Termenul de forţe cibernetice nu a fost definit în mod oficial, deci rămâne un subiect deschis dezbaterii, însă apelând la metoda comparativă aceste forţe pot fi comparate cu cele de operaţii speciale: în aceste echipe factorul uman este mai important decât echipamentul, calitatea este mai importantă decât cantitatea, armele acestei categorii de forţe, fiind de natură specifică acţiunilor în spaţiul cibernetic.

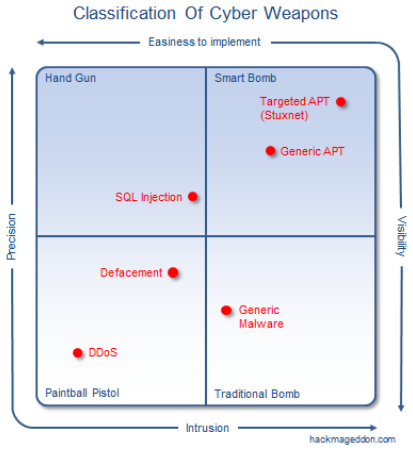
Aşadar, armele cibernetice constau, în cea mai mare parte din elemente software, combinate uneori cu elemente hardware. Astfel, armele cibernetice pot fi clasificate în trei categorii, după cum urmează:

•*arme ofensive neechivoce*, de tipul malware: *viruşi, viermi, troiani, bombe logice* şi *acţiuni de tip denial of service;*

•*arme cu uz dual* de tipul *monitorizare reţea, scanare de vulnerabilităţi, testarea penetrabilităţii, criptare, camuflarea de conţinut şi camuflarea comunicaţiilor;*

•*arme defensive neechivoce*, de tipul *firewall* sau *disaster recovery systems.*

O altă clasificare a armelor cibernetice este propusă de Stefano Mele[10] într-un studiu realizat în anul 2012, de către Institutul Italian de Studii Strategice (figura nr. 2).



[9] Porche, Isaac R. III, Bruce J. Held, Jerry M. Sollinger, Timothy M. Bonds, Ian P. Cook, Bradley Wilson, R. Wayne Dudding, and Christopher Paul, *The Army's Role in Cyberspace*, unpublished RAND research, 2008.

[10] Stefano Mele, *Cyberweapons: Aspetti giuridici e strategici,* Instituto Italiano di Studi Strategici Niccolo Machiaveli, Roma, 2012, pp. III-XV

Figura nr. 2. Clasificare a armelor cibernetice propusă de Stefano Mele[11]

3. Context actual. Relaţionări cu viziunile NATO şi UE

NATO şi-a formulat misiunile în spaţiul cibernetic (protejarea reţelelor, îmbunătăţirea capabilităţilor statelor membre, cooperarea cu state partenere, cu UE şi industria) în anul 1999, după ce a suferit primul atac major în timpul Operation Allied Force.

Astăzi, NATO îşi bazează activitatea în domeniul cyber pe două documente: Cyber Defence Policy (CDP) şi Planul de Acţiune (iunie 2011). Potrivit CDP, NATO:

- integrează aspectele privind apărarea cibernetică în structurile NATO şi în procesul de planificare în scopul de a îndeplini sarcinile de bază privind apărarea colectivă şi managementul crizelor.
- îşi concentrează efortul în direcţia prevenirii, rezilienţei, şi apărării structurilor cyber NATO şi aliate.
- recomandă dezvoltarea cerinţelor minime pentru apărarea cyber la nivel naţional a structurilor critice pentru misiunile NATO.
- colaborează cu partenerii, organizaţiile internaţionale, sectorul privat, instituţii de învăţământ superior şi mediul academic.

Structurile care implementează aceste măsuri sunt cuprinse în schema de mai jos (figura nr. 3):

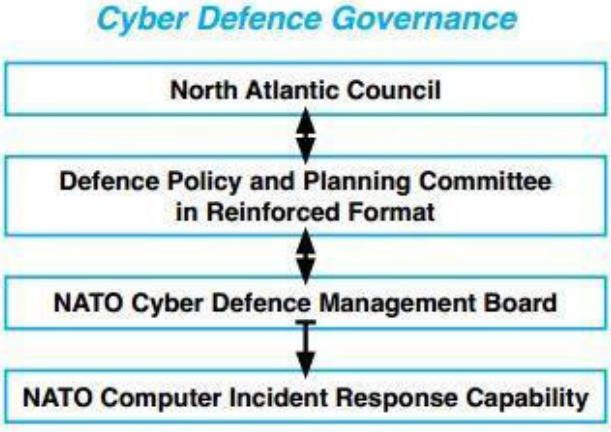


Figura nr. 3. Structura de răspuns NATO în cazul atacurilor cibernetice[12]

[11] *Ibidem*

[12] Pierluigi Paganini, *NATO has constitued Cyber Response Teams, securityaffairs.co/wordpress/-20705/cyberwarfare-2/nato-atack-response-teams.html*

De asemenea, la nivelul UE există practici diferite privind apărarea cibernetică, în special la nivelul strategiilor naţionale, în 2013 Consiliul European făcând apel pentru proiectarea unui cadru UE privind Politica de Apărare Cibernetică.

4. Norme juridice aplicabile războiului cibernetic

Luând în considerare modul de manifestare a atacurilor cibernetice în coroborare cu tendinţele actuale manifestate la nivelul statelor de a implementa strategii de securitate cibernetică şi de a dezvolta structuri şi capabilităţi militare care să poată desfă şura operaţii în spaţiul cibernetic, apare aspectul reglementării juridice a desfăşurării acestor operaţii, care la nivel general sunt percepute drept acţiuni de război cibernetic.

Dacă la nivelul războiului de tip clasic normele juridice internaţionale sunt clare, aplicabile şi produc efecte, în cazul războiului de tip cibernetic aspectele de ordin juridic sunt încă la nivelul incipient, fără o unitate comparabilă cu normele de drept internaţional umanitar.

Similar practicilor de apărare cibernetică la nivelul UE, şi în cazul normelor juridice aplicabile conflictelor ciber, reglementările sunt caracterizate în general de instanţe naţionale, cele mai multe aparţinând ramurii de drept penal, din moment ce până de curând atacurile de tip cibernetic erau considerate numai din punct de vedere al infracţiunilor ce pot fi săvârşite, şi mai puţin al efectelor produse, unele dintre acestea comparabile cu efectele rezultate din acţiuni militare specifice războiului tradiţional.

Una dintre puţinele încercări de adaptare a dreptului războiului la specificul spaţiului cibernetic a fost realizată la nivelul Alianţei Atlanticului de Nord, prin intermediul *NATO Cooperatice Cyber Defence Centre of Excellence*[13] de la Tallinn, Estonia. Această iniţiativă a fost finalizată prin editarea. *Manualului de la Talan în domeniul dreptului internaţional aplicabil războiului de tip cibernetic,* cunoscut sub numele de Manualul de la Tallinn[14].

Manualul reprezintă un prim efort de codificare la nivel internaţional a normelor aplicabile în domeniul cibernetic, însă perspectivele de implementare sunt încă incerte, având în vedere caracterul special al spaţiului cibernetic, spaţiu care nu poate fi limitat de frontiere, nu poate fi afectat de principii privind suveranitatea sau jurisdicţia în aspecte care ţin de ducerea războaielor în acest spaţiu.

[13] https://ccdcoe.org
[14] https://ccdcoe.org/tallin-manual.html

Concluzii

Având în vedere cele expuse anterior suntem de părere că:

•România ar trebui să îşi dezvolte capabilităţile de tip cyber warfare cel puţin la nivel minim, aşa cum este recomandat prin Politica de Apărare Cyber a NATO (Cyber Defence Policy);

•prin similitudine cu forţele speciale se pot dezvolta echipe de forţe cibernetice;

•unul dintre cele mai importante elemente ale capabilităţii de cyber warfare este dezvoltarea şi diseminarea unei culturi de securitate şi apărare în domeniul cyber, dezvoltare care este realizabilă prin cooperare cu mediul academic militar, proiectarea de cursuri postuniversitare, programe de master şi de licenţă care să cuprindă discipline destinate dezvoltării culturii de apărare cyber.

Eforturile naţionale trebuie însă, susţinute de iniţiativele la nivel internaţional în scopul dezvoltării unor norme legislative la nivel internaţional care să poată face parte din ramura de drept internaţional în domeniul dreptului războiului.

BIBLIOGRAFIE

*** *FM 3-38, Cyber Electromagnetic activities*, Department of the army, feb. 2014, Washington DC;

cyberwarfare-2/nato-atack-response-teams.html

https://ccdcoe.org

https://ccdcoe.org/tallin-manual.html

MELE Stefano, *Cyberweapons: Aspetti giuridici e strategici,* Instituto Italiano di Studi Strategici Niccolo Machiaveli, Roma, 2012;

PAGANINI Pierluigi, *NATO has constitued Cyber Response Teams, securityaffairs.co/wordpress/20705/;*

PORCHE Isaac R. III, HELD J. Bruce, SOLLINGER M. Jerry, BONDS M. Timothy, COOK P. Ian, WILSON Bradley, DUDDING R. Wayne, and PAUL Christopher, *The Army's Role in Cyberspace*, unpublished RAND research, 2008;

TOPOR Sorin, *Aproach About Joint Cyber And Electronic Warfare And Futures Of The Military Operations*, in the 10th International Scientific

Conference "Strategies XXI": Strategic Changes In Security And International Relations, vol. 3, "CAROL I" National Defence University Publishing House, Bucharest, 2014;

TURCU Dănuţ, *Main Information Security Activities Of An Intelligence Service,* in Buletin of "CAROL I" National Defence University, No. 1/2014, Bucuresti, 2014;

VENTRE Daniel, *Cyber Conflict: Competing National Perspective,* ISTE Ltd, London, 2012;

WHITTAKER Jason, *The Cyberspace Handbook*, Routledge, London, 2003.