ASPECTE LEGALE ALE ACȚIUNII ÎN SPAȚIUL CIBERNETIC

LEGAL ASPECTS OF ACTION IN CYBERSPACE

Lt.col. drd. Virgil Florin TOȘA*

Articolul de față va aduce în atenție câteva aspecte referitoare la legislația internațională aplicabilă spațiului virtual și, îndeosebi, Manualului Tallin elaborat sub auspiciile NATO CCDCOE, și care reprezintă prima încercare de a lămuri unele aspecte referitoare la aplicabilitatea legilor conflictelor armate în domeniul conflictelor din spațiul cibernetic.

This paper aims is to offer some aspects on the international law applicable to cyber space and to the Tallinn Manual on the International Law Applicable to Cyber Warfare published by NATO CCDCOE, the first document regarding the law of armed conflict in cyber space

Cuvinte-cheie: Manualul Tallinn; spațiu cibernetic; război cibernetic.
***Keywords**: Tallinn Manual; cyber space; cyber warfare.*

Din ce în ce mai des primim confirmarea că domeniul cibernetic va deveni viitorul câmp de luptă, ceea ce implică pentru guvernele țărilor democratice un efort susținut pentru adoptarea unui set de măsuri active pentru a contracara amenințările militare sau a preveni atacurile potențiale pentru propria lor infrastructură națională.

Întrebarea care se poate pune este dacă statele care au fost supuse unor atacuri cibernetice importante ca efecte – iar în astfel de cazuri pot fi enumerate Estonia, Georgia – pot să răspundă cu o acțiune militară în conformitate cu dreptul internațional. Dar cazurile de infracționalitate cibernetică pot fi pedepsite în conformitate cu sistemul legislativ existent? Una dintre cele mai dificile chestiuni în situațiile prezentate anterior o reprezintă identificarea autorilor, pentru că este cunoscut faptul că, în spațiul cibernetic, un atac poate fi comandat de la distanță, iar execuția efectivă a acestuia să se efectueze de pe sisteme de calcul ale unor nevinovți, chiar fără ca aceştia să realizeze ce acțiuni efectuează mașinile lor de calcul, grupate în așa-numitele *botnet-uri*[1].

Dreptul la autoapărare în cazul unui atac armat este conferit statelor, în virtutea articolului 51 din Carta Națiunilor Unite[2]. Însă atacurile cibernetice nu pot fi incluse în categoria atacurilor armate, prin urmare similitudinea dintre cei doi termeni nu poate fi acceptată. Cu toate acestea, efectele pe care le pot produce atacurile cibernetice, ar putea fi uneori chiar mai mari decât cele produse de atacurile armate clasice. Referitor la această afirmație, o descriere cât se poate de simplă și concisă a fost făcută de către fostul secretar general NATO, Anders Fogh Rasmussen, menționată în cadrul vizitei sale în România din luna mai 2010, prin care explicitează foarte sugestiv de ce apărarea cibernetică este una dintre prioritățile fundamentale ale NATO: „Un atac cibernetic bine orchestrat vă poate stinge lumina în casa, în orașul vostru, în țara voastră. Poate închide controlul traficului aerian. Poate închide băncile. Pe scurt, un atac cibernetic poate înfrânge o țară fără ca vreun soldat să fi trebuit să-i treacă frontiera”[3].

Cazul Estoniei

Au trecut câțiva ani de la masivul atac electronic[4], care a paralizat temporar infrastructura națională Internet a Estoniei[5]. Din perspectiva NATO, acest atac constituie un moment istoric în evoluția Alianței, pentru că el reprezintă primul caz în care un stat membru solicită, în mod formal, asistență de urgență pentru apărarea sistemului său informatic.

Sunt voci care afirmă că un atac cibernetic ar putea avea efectele unei lovituri nucleare. Astfel,

***Școala de Aplicație pentru Forțele Aeriene „Aurel Vlaicu”, Boboc**
e-mail: *virgil.tosa@gmail.com*

Ene Ergma, purtătorul de cuvânt al Parlamentului Estonian, care are un doctorat în fizică nucleară, a făcut o comparație: „Când am privit o explozie nucleară şi explozia care s-a petrecut în țara noastră în luna mai (2008 n.a.), am văzut acelaşi lucru”. La fel ca radiația nucleară, un război cibernetic poate distruge un stat modern fără să curgă sânge.[6]

Întrucât atacul s-a derulat pe o perioadă de câteva săptămâni[7], miniştrii apărării țărilor NATO s-au reunit în grabă pentru a evalua consecințele strategice şi politice ale primului atac cibernetic masiv desfăşurat împotriva unui stat membru. În timpul acestei crize a devenit, în mod clar, evident pentru oficialii NATO că Alianța are nevoie atât de o doctrină coerentă a spațiului cibernetic, cât şi de o strategie comprehensivă de acțiune pentru mediul virtual.

În 2008, la Summitul NATO de la Bucureşti, a fost introdusă în discuție şi ideea de apărare a spațiului cibernetic în NATO. În acest cadru, oficialii NATO şi experții din domeniul cibernetic au reanalizat experiența estoniană. Ca urmare, capitolul 47 din Declarația comună a liderilor statelor membre NATO precizează: „NATO rămâne angajată în eforturile de întărire a apărării sistemelor informatice cheie ale Alianței împotriva atacurilor cibernetice. Recent am adoptat o politică NATO în domeniul apărării împotriva atacurilor cibernetice şi dezvoltăm structurile şi autoritățile necesare implementării acesteia. Politica noastră în domeniul apărării împotriva atacurilor cibernetice evidențiază necesitatea pentru NATO şi națiunile membre de a proteja sistemele informatice cheie, în acord cu responsabilitățile lor specifice; schimbul de experiență; şi asigurarea unei capabilități de sprijin pentru națiunile aliate, la cerere, de respingere a unui atac cibernetic. Aşteptăm cu interes continuarea dezvoltării capabilităților NATO de apărare împotriva atacurilor cibernetice şi întărirea legăturilor dintre NATO şi autoritățile naționale”[8].

Câmpul de luptă digital

În timp ce eforturile NATO de apărare cibernetică vor fi îndreptate spre protejarea infrastructurii informatice civile, împotriva actorilor statali sau nonstatali care susțin astfel de atacuri, NATO trebuie să-şi dubleze eforturile pentru a-şi securiza propriile sisteme împotriva atacurilor cibernetice.

Câmpul de luptă al secolului XXI abundă de echipamente din domeniul tehnologiei informației, făcându-l cu atât mai vulnerabil la atacuri cibernetice. Sunt puțini adversari care au demonstrat reale abilități în întreruperi grave ale funcționării sistemelor de comandă-control ale NATO, prin intermediul acțiunilor cibernetice ofensive, ceea ce poate presupune că viitoarele strategii ofensive pot face apel într-o mai mare măsură la utilizarea instrumentelor cibernetice în câmpul de luptă digital.

Pentru a anticipa şi a se apăra împotriva amenințărilor viitoare, Agenția NATO pentru Comunicații şi Informații[9] – NCIA –, cu sediul la Bruxelles, precum şi centrele vitale naționale de comandă-control, vor trebui să se mențină la curent cu ultimele noutăți în domeniul tehnologiei informației.

Echipa de experți ai NATO, condusă de către fostul secretar de stat american Madeleine Albright, care a elaborat Noul concept strategic al NATO, a avertizat că următorul atac vizând o țară NATO ar putea „foarte bine să se producă pe un cablu de fibră optică”[10].

Raportul grupului Albright releva că un atac informatic asupra unei infrastructuri vitale a unui stat membru ar echivala cu un atac armat şi justifică retorsiunea. „Un atac pe scară largă vizând sisteme de control şi comandă ale NATO sau rețelele electrice ar putea duce la măsuri de apărare colectivă, în baza articolului 5”, au subliniat experții.

ÎnciudaaşteptărilorpotrivitcăroraalianţaNATO va avea în vedere folosirea forței militare împotriva inamicilor care lansează atacuri cibernetice vizând statele membre[11], aşteptări survenite după atacuri repetate provenind din Rusia, asupra unor țări ale Alianței şi în urma avertismentelor serviciilor de informații privind amenințarea din ce în ce mai mare din partea Chinei, în Declarația Summitului NATO din Țara Galilor, din 2014, se apreciază că atacurilor cibernetice, pot „atinge un nivel care să amenințe prosperitatea, securitatea şi stabilitatea națională şi euroatlantică. Impactul acestora poate fi la fel de dăunător pentru societățile moderne ca şi un atac convențional”[12]. De aceea NATO consideră că apărarea cibernetică este parte a sarcinii de bază a alianței privind apărarea colectivă. În cadrul acestui summit însă, s-a decis că nu orice atac cibernetic împotriva unei țări membre a Alianței va

fi tratat în virtutea articolului 5 al Cartei NATO, ci va fi analizat de către Consiliul Nord-Atlantic „de la caz la caz”.

Articolul 5 este piatra de temelie a Tratatului Nord-Atlantic, din 1949, potrivit căreia un „atac armat” asupra unei sau a mai multor țări membre ale Alianței „va fi considerat un atac asupra tuturor”. Această clauză a fost invocată după atacurile din 11 septembrie 2001, de către SUA, pentru a justifica îndepărtarea regimului taliban din Afganistan.

De ce totuşi este dificil a răspunde la atacurile cibernetice conform Articolului 5 al Tratatului de la Washington ?

Este dificil de identificat dacă un atac informatic este lansat de către o țară, de o grupare teroristă sau doar de către un grup de tineri hackeri. Infrastructura informațională actuală prezintă câteva facilități care reprezintă avantaje deosebite pentru potențialii atacatori informatici în sensul că sursa atacului cibernetic este dificil de identificat. Astfel, există tehnici de ascundere a adresei IP reale (IP spoofing). De asemenea, există situri care oferă utilizatorilor adrese anonime. Atacatorii pot să-şi transmită atacul prin intermediul multiplelor noduri de rețea fapt ce îngreunează urmărirea activității acestora.

Manualul Tallinn

Alianța Nord-Atlantică a înființat, la 28 octombrie 2008, la Tallin, în Estonia, Centrul NATO de Excelență pentru Cooperarea în Domeniul Apărării Cibernetice (NATO CCDCOE). Locul înființării acestui centru de excelență este desigur legat de atacul la care a fost supusă Estonia în 2007, dar şi de propunerea făcută de această țară, imediat după aderarea la NATO, în 2004[13].

Acest centru de excelență a publicat, după o cercetare de trei ani, „Manualul Tallin asupra legislației internaționale aplicabilă războiului cibernetic”.

Manualul Tallinn a fost elaborat de către un grup de experți independenți, care au identificat în legislația internațională acele referințe aplicabile războiului cibernetic şi au creat un set de 95 de reguli care vor putea guverna acest tip de conflicte. Autorii afirmă că acest produs nu este un document obligatoriu, care nu crează obligațiile unui document juridic, ci el exprimă punctele de vedere ale experților jurişti care au participat la elaborarea sa[14]. Aşadar, manualul nu reprezintă un izvor de drept în sens formal. Cu toate acestea, aşa cum este cazul „Manualului de la San Remo asupra dreptului internațional aplicabil în conflictele armate pe mare”, el poate fi adoptat în practica statelor în viitor.

Aşa cum autorii înşişi au observat, nu există încă niciun tratat care să se ocupă în mod special cu legislația aplicabilă războiului cibernetic.

Manualul cuprinde două părți:

- o parte referitoare la regulile de drept internațional ce guvernează admisibilitatea recurgerii la forță între state – *jus ad belum*.
- cea de-a doua parte, care se ocupă efectiv de regulile ce trebuie respectate pe timpul războiului cibernetic – *jus in bello*.

În cea de-a doua parte a manualului sunt concentrate o sumă de reguli generale de drept internațional umanitar, aplicabile acestui tip de război, cuprinzând conducerea ostilităților, protecție persoanelor, ocupația şi neutralitatea.

Cele 95 de reguli ale manualului definesc responsabilitatea statului în operațiile cibernetice în raport cu dreptul internațional, aplicarea principiului interzicerea utilizării forței, circumstanțele în care poate fi invocat dreptul la autoapărare, comportamentul părților în timpul ostilităților cibernetice etc. Acesta afirmă, printre altele, că „există un conflict armat internațional ori de câte ori există ostilități, care pot include sau fi limitate la operațiuni cibernetice care apar între două state sau mai mult” şi că „operațiunile cibernetice de sine stătătoare pot avea potențialul de a declanşa un conflict armat internațional”.

Aceste norme rămân deschise pentru interpretare, în funcție de evoluția tehnologiei şi a capabilităților cibernetice precum şi la critici. Unii experți s-au concentrat pe provocarea atribuirii (de exemplu, atribuirea statelor responsabilitatea pentru un atac cibernetic, organizat de către un grup nonstatal); posibilitatea de a invoca dreptul la autoapărare.

Potrivit manualului, contramăsurile proporționale împotriva atacurilor online efectuate de un stat sunt permise. Astfel de măsuri nu implică, însă, folosirea forței, cu excepția cazului în care atacul cibernetic inițial a condus la moartea unor persoane sau la deteriorarea gravă a unor proprietăți.

Manualul susține că, în conformitate cu Convențiile de la Geneva, atacurile cibernetice

îndreptate asupra unor anumite elemente de infrastructură civilă cheie, se plasează în afara legii. Astfel, regula 80 din manual prevede următoarele: „În scopul evitării pierderilor ulterioare grave în rândul populației civile, o grijă deosebită trebuie să fie acordată în timpul atacurilor cibernetice unor ansambluri şi instalații care conțin forțe periculoase, cum ar fi barajele, digurile şi centralelor nucleare, precum şi instalațiilor situate în vecinătatea acestora[15]. Spitalele şi unitățile medicale sunt, de asemenea, protejate, în condițiile în care acestea sunt plasate sub auspiciile normelor care reglementează războaiele tradiționale.

Concluzii

Acest manual a stabilit, pentru prima dată, un set de reguli de drept internațional aplicabile operațiilor cibernetice şi desigur a oferit comentarii ample pe marginea acestor reguli. Aceste comentarii au drept scop să exprime atât opiniile majoritare ale grupului de experți dar şi pe cele minoritare. Această abordare este utilă şi deschide calea acordurilor internaționale în domeniul războiului cibernetic aşa cum este cazul, spre exemplu, a Convențiilor de la Geneva asupra dreptului internațional umanitar. Un impediment major pe viitor în adoptarea unor astfel de tratate internaționale, pornind de la acest manual, îl reprezintă faptul că unii actori importanți în spectrul operațiilor cibernetice, care au dovedit capabilități importante în acest domeniu – Rusia şi China – nu au fost reprezentați în cadrul grupului de experți, autori ai manualului.

Această lipsă de diversitate în rândul grupului de experți aduce în discuție întrebarea: Cât de cuprinzătoare sunt opiniile cuprinse în Manualul Tallinn?

Lucrarea a beneficiat de suport financiar prin proiectul cu titlul „Studii doctorale şi postdoctorale Orizont 2020: promovarea interesului național prin excelență, competitivitate şi responsabilitate în cercetarea științifică fundamentală şi aplicată românească”, număr de identificare contract POSDRU/159/1.5/S/140106. Proiectul este cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013. Investeşte în Oameni!

NOTE:

1 http://us.norton.com/botnet/, accesat la 8.02.2015.
2 *Carta ONU*, http://www.un.org/en/documents/charter/, accesat la 08.02.2015.
3 http://www.money.ro/versiune-pdf/rasmussen-un-atac-cibernetic-poate-invinge-o-tara-fara-a-fi-nevoie-de-vreun-soldat.html, accesat la 11.12.2012
4 Atacul a fost identificat ca fiind de tipul Denial of Service.
5 Atacul a survenit la scurt timp după ce autoritățile estoniene au mutat statuia foarte controversată a Soldatului Armatei Roşii din centrul capitalei într-un cimitir militar situat la marginea oraşului, în timpul primăverii din 2007.
6 Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack, WIRED*, Aug. 22, 2007, pe http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html, accesat la 1.02.2015.
7 Aprilie - mai 2007.
8 *Declarația Summitului NATO* de la Bucureşti din 2008, http://www.summitbucharest.ro, accesat la 8.10.2009.
9 http://www.nato.int/cps/en/natolive/topics_69332.htm, accesat la 8.02.2015.
10 *NATO 2020: Assured security; Dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO*, NATO Public Diplomacy Division, Brussels, 2010, p. 45.
11 David E. Sanger, *NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack*, The New York Times, 31.08.2014.
12 *Declarația Summitului din Țara Galilor adoptată de şefii de stat şi de guvern participanți la reuniunea Consiliului Nord-Atlantic din Țara Galilor*, 4-5 septembrie 2014 pe http://www.presidency.ro/?_ RID=det&tb=date&id=15216&_PRID=, accesat la 10.12.2014.
13 http://ccdcoe.org/history.html, accesat la 8.02.2015.
14 *Tallinn Manual*, 2013, p. 11.
15 *Idem,* p. 223.

BIBLIOGRAFIE

Carta ONU.
Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge, 2013.
Declarația Summitului din Țara Galilor adoptată de şefii de stat şi de guvern participanți la reuniunea Consiliului Nord-Atlantic din Țara Galilor, 4-5 septembrie 2014.
NATO 2020: Assured security; Dynamic engagement. Analysis and recommendations of the group of experts on a new strategic concept for NATO, NATO Public Diplomacy Division, Brussels, 2010.