Strategii de securitate cibernetică în era Internetului

Dan-Mircea SUCIU
Serviciul Român de Informații
rrsi@sri.ro

Abstract

Obviously, social networks, blogs, forums and the Internet in its whole bring a lot of benefits in the field of communication and technology. On the other hand, Information Age has a dark side, by providing the tools and opportunities necessary for presence and expanding of illegal groups; all technological means have to offer in the field of propaganda, recruitment, financing and so on. Taking into consideration the considerable risks associated to these activities it has become understandable that intelligence communities must elaborate proper strategies for more effective fight, de facto and de jure, against these threats. For that reason, intelligence and law enforcement agencies focus on simultaneously: prevention and countering of risks.

Keywords: intelligence communities, cyberspace, Information Age, social media, Internet, strategies.

1. Delimitări conceptuale. Strategii în societatea informațională

Revoluția informațională a schimbat fundamental societatea umană – transformare ce va continua şi în viitorul previzibil – oferind, totodată, oportunități nelimitate. Programele informatice performante şi rețelele de comunicații electronice sunt utilizate pe scară largă având aplicabilitate în cele mai diverse ramuri, de la medicină la industrie de vârf şi creație intelectuală.

În societatea globală actuală, implementarea şi perfecționarea unui cadru strategic unitar şi coerent care să reglementeze realitatea virtuală constituie o preocupare constantă a statelor cu democrații consolidate, dar şi a celor care tind către un asemenea statut.

A devenit un truism faptul că securitatea națională dobândeşte noi valențe, determinate de celeritatea modificărilor survenite în domeniile realității actuale. În acest context, România s-a înscris în direcția susținerii politicilor europene în domeniul *e-Government,* necesare pentru depăşirea decalajului digital existent între diverse state.

Conştientizând importanța acțiunilor coordonate, ca bază pentru o cooperare eficientă transnațională în menținerea securității şi combaterii criminalității, țara noastră a adoptat Strategia *„România digitală, e-strategia pentru o societate informațională”*.

Inițial, în *Programul de guvernare pentru perioada 2009-2012* a fost inclus un capitol distinct (capitolul 14**)** consacrat „Societății informaționale”, cu următoarele subdomenii: interoperabilitate; tehnologia informației; administrația publică minimală; e-România; crearea Punctului unic de contact; cybercrime; e-incluziune.

Astfel, era Internetului aduce, pe lângă o multitudine de schimbări preconizate, şi altele subtile, resimțite în activitatea de intelligence, deopotrivă în doctrină dar şi în operațiunile de culegere, analiză şi diseminare a informației relevante pentru securitatea națională. De aceea, se impune adaptarea rapidă a structurilor de analiză de intelligence la noile provocări prefigurate de extinderea riscurilor şi amenințărilor de tip informatic.

Mai mult, acest plan al *„e-realității”* determină transformări notabile manifestate la nivelul relațiilor dintre serviciile secrete şi instituțiile de aplicare a legii, pe de o parte, şi factorii de decizie la nivel politic şi militar, pe de altă parte[1].

Explozia dispozitivelor multimedia, care îmbină o varietatea de facilități în domeniul comunicării, şi apariția unor noi forme adaptate acestor gadget-uri (terminale telefonice multifuncționale, sisteme informatice în rețea wireless) ori modalitățile virtuale de interacțiune (de genul „Second life”) vor continua să confere noi valențe utilizatorului, ca beneficiar al informației destinate.

Diversificarea formelor de criminalitate informatică, cu implicații directe asupra componentelor de securitate (inter)națională, a determinat necesitatea cristalizării conceptului de *cyberintelligence,* cu toate mecanismele aferente dezvoltării unui domeniu de sine-stătător.

[1] The Information Warfare Site – resursă online de Studii în domeniul securității informaționale/Marea Britanie.

Din această perspectivă, serviciile de informații vor putea răspunde provocărilor prin[2]:

- configurarea de noi modalități care să asigure integrarea eficientă şi rapidă a schimbului intra-organizațional de date relevante;
- nunațarea formulelor de promovare a culturii de securitate, în funcție de profilul destinatarului.

Relevant în acest sens este faptul că Strategia de Securitate Cibernetică a fost inclusă pe ordinea de zi a Consiliului Suprem de Apărare a Țării (CSAT), desfăşurat în 5 februarie a.c..

Strategia, aprobată de CSAT, vizează implementarea unor măsuri de securitate care să determine creşterea nivelului de protecție a infrastructurilor cibernetice, în concordanță cu noile concepte şi politici din domeniul apărării cibernetice elaborate şi adoptate la nivelul NATO şi al Uniunii Europene.

În context[3], ministrul pentru Societatea Informațională, Dan Nica, a atenționat asupra „țintelor" atacurile cibernetice care *„se îndreaptă de la o zonă economică explicită, gen atacuri asupra site-urilor băncilor, către o zonă economică şi politică.* Cu acelaşi prilej, Dan Nica a subliniat necesitatea *„adoptării măsurilor existente la partenerii noştri din Marea Britanie, SUA, Germania şi Franța".*

Stricto senso, activitatea de *cyberintelligence* presupune furnizarea către beneficiari a diverselor tipuri de produse informaționale care să contribuie la fundamentarea unor decizii de natură să asigure securitatea cyberspațiului şi decelarea amenințărilor subsumate acestui domeniu.

În conformitate cu atribuțiile sale legale privind identificarea activităților derulate de entități cibernetice ostile ce urmăresc obținerea accesului la rețele informatice de interes național şi culegerea de informații confidențiale, Serviciului Român de Informații (SRI) informează cu promptitudine instituțiile vizate. Potrivit legii, în exercitarea acestor competențe, SRI are calitatea de autoritate națională în domeniul *cyberintelligence.*

Viziunea strategică 2011-2015 „SRI în era informațională" anticipează în mod profesionist provocările cu care ne vom confrunta în acest interval temporar.

[2] "Intelligence in the Internet Era", A. Denis Clift, 2003.
[3] www.romania-atualitati.ro, accesat la data de 06.02.2013.

Ilustrativ este că, celebrul atac cibernetic „Red October", realizat prin utilizarea unui „troian", a constituit, începând cu anul 2011, obiectul investigațiilor derulate de SRI, care a întreprins, în cooperare cu alte instituții responsabile interne (STS, SIE, CERT-RO) şi externe, măsuri de contracarare pentru restabilirea funcționării normale a rețelelor respective[4].

- Centrul Național de Răspuns la Incidente de Securitate Informatică (CERT-RO) a fost înființat la jumătatea anului 2011, în subordonarea Ministerului Comunicațiilor şi Societății Informationale, şi a devenit operațional la finele anului 2011, având ca atribuții principale prevenirea, analiza, identificarea şi reacția la incidentele cibernetice.

La sfârşitul lunii februarie a.c., compania de securitate informatică „Kaspersky Lab" a anunțat depistarea unui atac cibernetic de proporții, prin utilizarea unui program malware, (MiniDuke), care a vizat instituții guvernamentale din mai multe țări europene, printre care şi România. Impactul incidentului recent a fost estimat de SRI ca fiind mai mare decât cel al operațiunii „Octombrie Roşu" (care a vizat, în special, resursele României din Marea Neagră), prin profilul entităților compromise, al complexității tehnologice şi al resurselor utilizate.[5] Reprezentanții SRI au precizat că atacul ar putea fi realizat de o entitate statală, motiv pentru care, prin echipele specializate de reacție la atacuri cibernetice, Serviciul întreprinde măsuri active pentru identificarea tuturor entităților afectate, limitarea consecințelor şi stoparea atacului.

În Viziunea 2015, intitulată *O organizație globală şi integrată de Intelligence,* Statele Unite ale Americii au înscris printre obiectivele Comunității de Informații *„dezvoltarea capacității integrate pentru a contracara provocările în creştere din cyber-spațiu"*.

- În septembrie 2012, mai multe bănci americane importante au fost victimele unuia dintre cele mai mari atacuri cibernetice din istorie. Site-urile „Bank of America", „Wells Fargo", „US Bank" şi „PNV Bank" s-au confruntat cu dificultăți de funcționare, iar accesul clienților a fost restricționat temporar, afectând în mod evident activitățile băncilor. Având în vedere complexitatea atacului, experții au indicat că acesta ar fi fost sprijinit de guvernul iranian, ca răspuns la *„sancțiunile economice dure impuse de SUA şi aliații lor europeni"* instituțiilor financiare din Iran[6].

[4] Site-ul Serviciului Român de Informații, www.sri.ro
[5] www.ziare.com, accesat la data de 04.03.2013.
[6] money.cnn.com, accesat la data de 04.03.2013.

În contextul în care publicațiile „The New York Times" şi „The Wall Street Journal" au anunțat (31.01.2013) că sistemele lor informatice au fost accesate de hackeri din China, experți în securitatea cibernetică au susținut că *„administrația americană ia în considerare măsuri diplomatice şi comerciale mai dure"*.

Bunăoară, au fost acordate prerogative extinse preşedintelui Barack Obama care poate ordona un atac preventiv dacă SUA detectează *„dovezi credibile privind iminența unui atac digital major din străinătate"*. Decizia face parte dintr-o serie de măsuri recente, în contextul în care Administrația SUA intenționează să adopte primele reglementări naționale asupra modului în care armata americană poate răspunde unui atac cibernetic. Noile politici vor reglementa, de asemenea, cadrul normativ în care agențiile de informații pot analiza rețelele de computere pentru a identifica indiciile unor potențiale atacuri asupra SUA şi, maniera în care, cu acordul preşedintelui, pot ataca adversarii cu un cod destructiv, chiar dacă nu a fost declarat război[7].

La rândul său, Federația Rusă, recunoscând pericolul confruntării informaționale globale, accentuat de perfecționarea continuă a formelor de activitate ilegală în domeniul ciberneticii, îşi propune armonizarea infrastructurii informaționale naționale cu rețelele şi sistemele informaționale globale.

În acelaşi scop, Grupul pentru operațiuni cibernetice al Ministerului britanic al Apărării („Defence Cyber Operations Group" – DCOG), unitate responsabilă de dezvoltarea şi desfăşurarea armelor cibernetice pentru Armata Marii Britanii, va deveni operațional în 2015, potrivit Comisiei speciale pentru Apărare din cadrul Camerei Comunelor.

Potrivit Strategiei pentru Securitate Cibernetică a Ministerului britanic al Apărării, DCOG include „Unitatea mixtă pentru Operațiuni Cibernetice a Centrului Guvernamental de Comunicații", a cărei misiune este „de a dezvolta noi tactici, tehnici şi planuri pentru a pune în aplicare acțiunile Armatei, precum consolidarea securității, prin operațiuni în spațiul cibernetic".[8]

Pe de altă parte, Comisia UE propune noi reglementări în domeniul cibernetic, solicitând ca motoarele de căutare, furnizorii de energie, băncile şi alte companii să raporteze autorităților guvernamentale *„orice întrerupere a funcționării sistemelor"*. Propunerea urmează să fie analizată în Parlamentul

[7] global.nytimes.com, accesat la data de 04.02.2013.
[8] www.intelligenceonline.com, accesat la data de 12.02.2013.

European de către liderii celor 27 de guverne din statele UE. Se preconizează că după modificările şi completările aferente, în aproximativ 2 ani, propunerea se va materializa într-un document juridic cu caracter obligatoriu pentru statele comunitare.

„Sistemele informaționale pot fi afectate de incidente de securitate, precum greşeli umane, evenimente naturale, erori tehnice sau atacuri malițioase. Aceste incidente devin din ce în ce mai mari, mai frecvente şi mai complexe”, susține Comisia UE. Potrivit documentului, riscul ca UE să fie tot mai expusă unor asemenea atacuri este din ce în ce mai mare, având în vedere că statele comunitare au reglementări diferite în domeniul cibernetic şi că deseori *„ezită să facă schimb de informații cu țările vecine de teamă că propriile sisteme ar deveni vulnerabile"*[9].

Statele europene acționează însă cu rapiditate în direcția extinderii unităților de securitate cibernetică. Astfel, Centrul European împotriva Criminalității Cibernetice (EC3) de la Haga şi-a început activitatea la începutul acestui an şi promovează cooperarea cu firme din sectorul IT şi al securității.

Un centru similar al Interpol este în curs de înființare şi îşi va începe activitatea în septembrie 2014, în Singapore.[10]

În acelaşi sens, recent, premierul Italiei Mario Monti a semnat decretul pentru constituirea structurii echivalente a Computer Emergency Response Team (CERT), organism destinat apărării spațiului cibernetic italian public şi privat, ca parte importantă a unui Plan de Securitate Cibernetică. Acesta conturează cadrul pentru colaborarea italiană cu echipele CERT din fiecare țară europeană care a aderat la această inițiativă.

Securitatea cibernetică constituie una din prioritățile agendei de lucru şi a Oficiului Federal pentru Apărarea Constituției din Germania (BfV)[11], dar şi a Direcției Centrale de Informații Interne (DCRI) din Franța, care îşi propun să suplimenteze numărul experților în „Jihadul cibernetic”[12].

După doi ani de pregătire, Forțele Israeliene de Apărare (IDF) au dat în folosință propriul Centru de Control pentru Apărare Cibernetică. Decizia a fost adoptată în condițiile în care, importante surse militare implicate în apărarea cibernetică, au semnalat o creştere semnificativă a capabilităților şi surselor atacurilor comise asupra infrastructurii digitale a IDF, ce variază de la hackeri amatori la actori statali.

[9] www.wsj.com, accesat la data de 05.02.2013.
[10] www.tagesspiegel.de, accesat la data de 20.02.2013.
[11] www.faz.net, accesat la data de 31.01.2013.
[12] www.lemonde.fr, accesat la data de 31.01.2013.

Centrul de Control va permite armatei israeliene să monitorizeze toate tentativele de atacuri virtuale, fiind în permanent contact cu sistemul guvernamental pentru apărare cibernetică, denumit „TEHILA" (acronimul ebraic pentru „Infrastructura Guvernului în Era Internet").

De asemenea, Centrul menține legătura cu Autoritatea Securității Informațiilor din cadrul Agenției Israeliene de Securitate (Shin Bet), responsabilă cu protejarea împotriva atacurilor cibernetice asupra infrastructurii energetice naționale, a piețelor financiare, rețelelor de comunicații şi sectorului transporturi[13].

2. Particularități şi scopuri în folosirea Internetului

Conceptul de „revoluție online" a fost asociat crizelor sociale din statele arabe, dar sintagme precum „revoluția Twitter ori SMS" au fost utilizate anterior în descrierea mişcărilor de protest din Moldova sau Iran (2009) ori în cazul răsturnării de la putere a preşedintelui filipinez Joseph Estrada (2001).

În situția mişcărilor de protest, rețelele de socializare sunt mult mai utilizate decât mijloacele de comunicare tradiționale. Numai rețeaua Facebook are peste 800 de milioane de utilizatori la nivel mondial (din care 350 de milioane acceseează platforma prin intermediul dispozitivelor mobile), 9,3 milioane fiind în Egipt, 4,5 milioane în Arabia Saudită, 4,1 milioane în Maroc, 850.000 în teritorile Palestiniene şi aproximativ 400.000 în Libia.

Alegerea Internetului ca instrument de acțiune este determinată de mai multe argumente, printre care:

- *(cvasi) anonimitatea comunicării şi facilitatea accesului;*
- *lacunele legislative care permit manifestarea anumitor comportamente aflate la limita legii;*
- *lipsa cenzurii sau a vreunui control guvernamental;*
- *audiență enormă în toate regiunile geografice;*
- *flux rapid al informației şi eficiență în transmiterea de mesaje multimedia (text, grafică, fotografii, video);*
- *costuri mici pentru dezvoltare şi menținere a unei prezențe WEB;*
- *audiența crescută şi înmulțirea rapidă a numărului de utilizatori situați în zone geografice îndepărtate.*

[13] www.jpost.com, accesat la data de 13.02.2013.

În doctrina de specialitate, s-au cristalizat teorii care apreciază necesitatea extinderii conceptului de spațiu cibernetic şi la alte sisteme cum ar fi:

- *Surveillance Control and Data Acquisition* (SCADA*)* pentru operarea rețelelor care controlează funcționarea unor componente ale infrastructurii critice aparținând unui stat (transport apă, energie, transporturi auto, aeriene, feroviare etc.). Preluarea controlului acestor sisteme este prezentată momentan în scenarii de film, dar există şi un pericol real, fapt susținut de cazul unui individ din Queensland (Australia), care folosind Internetul, o legătură wireless şi un produs software clandestin (practic, furat) a preluat controlul asupra sistemului de supravegere al colectării deşeurilor dintr-un rezervor de ape uzate şi a reuşit deversarea într-un râu şi apele de coastă a cca. 1 milion m^3 ape poluate. Individul a reuşit să intre în sistemul de securitate software din a 45 a încercare[14];
- *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* (C4ISR), sisteme militare de comunicații şi informatice.

Nu este de neglijat faptul ca unele state, cum ar fi China[15], şi-au declarat intenția de a-şi structura propriile capabilități de război informațional, defensive şi ofensive.

Conform unui articol[16] publicat pe site-ul institutului „The Middle East Media Research Institute" (MEMRI) există şase grupuri semnificative care desfăşoară aşa-zisul jihad electronic: Hackboy, Ansar Al-Jihad Lil-Jihad Al-Electroni, Munazamat Fursan Al-Jihad Al-Electroni, Majmu'at Al-Jihad Al-Electroni, Majma' Al-Haker Al-Muslim şi Inhiyar Al-Dolar.

Spre deosebire de grupurile obişnuite de hackeri, grupurile de mujahedini virtuali sunt subordonate unei ideologii şi strategii comune, în curs de clarificare. În ianuarie 2007, „mujahedinii internauți" au fost invitați la semnarea unui Pact special, care prevedea *„unificarea eforturilor sub conducerea grupului denumit Muhajirun Brigades"*. Un extras din declarația unui jihadist postată pe o pagină web, aparținând acestui grup, ilustrează adevăratele intenții şi posibilități de moment ale acestora: *„Am examinat cele mai multe din manualele hackerilor, dar nu am găsit articole despre cum să se indisponibilizeze rețelele dispuse peste tot în lume. Nu am citit despre cum se pot ataca rețelele din întreaga lume, adică cel mai important țel al unui hacker şi al cuiva angajat în jihadul electronic. Nu vorbesc despre atacurile site-urilor web, ci despre toate rețelele din lume,*

[14] DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism*, 2005.
[15] Military Power of the People's Republic of China, Report to Congress, 2007.
[16] Special Dispatch Series - No. 1702, MEMRI/ 2007.

inclusiv cele militare care controlează radare, rachete sau comunicații ...Dacă toate acestea vor fi indisponibilizate pentru doar o zi, aceasta va aduce colapsul Vestului, dar pe noi ne va afecta foarte puțin".

Se consideră că primul atac terorist cibernetic s-a petrecut în 1998, când „tigrii tamili" au suprasolicitat ambasadele srilankeze timp de două săptămâni, cu cca. 800 mesaje email/zi. Mesajul conținea textul: *"Suntem tigrii negri din Internet şi facem acest lucru pentru a vă întrerupe comunicația".*

Prezența teroriștilor sau a simpatizanților acestora în Internet se materializează în:

- sute de site-uri web înființate şi întreținute de grupări (inclusiv ale simpatizanților);
- menținerea unor numeroase forumuri de discuții;
- monitorizarea site-urilor de interes pentru colectarea de informații;
- conferințe on-line, folosind serviciul chat, prin care liderii spirituali propagă ideologia religioasă sau politică a grupării);
- comunicarea prin email;
- efectuarea de tranzacții financiare prin mijloace de plată electronică;
- transmiterea codificată a unor mesaje mesaje criptate prin tehnici steganografice;
- lansarea unor atacuri cibernetice sau răspândirea de viruşi sau coduri malițioase care să afecteze calculatoarele unor instituții publice sau private.

Analizând modul în care sunt folosite serviciile Internetului, putem conchide că grupările teroriste utilizează aceste mijloace în scopuri *operative, informative* şi pentru *instruire*. Folosirea Internetului în scop operativ, pentru coordonarea unor acțiuni, este exemplificată prin acțiunea desfăşurată, în data de 25.09.2005, de un membru al forumului de discuții „Muntada al- SafNet" care, pentru a declanşa un atac concertat (de tip Distributed Denial of Service – DDOS) împotriva a două web site-uri aparținând unor grupuri autodeclarate în favoarea dialogului creştin-musulman, a postat următorul anunț:

„Cea mai mare campanie pentru distrugerea site-urilor web ale cruciaților: Ne trebuie mujahedini! Momentul declanşării atacului este joi la ora 19:00 GMT. Atacul va dura o oră. Avem 50 mujahedini, deci suntem gata pentru campanie".[17]

În Internet, terorismul a găsit un mijloc extraordinar, logistic şi operațional, de a-şi promova interesele, fiind preferat acest mod de utilizare.

[17] BRYNJAR Lia, *Al-Qaeda online: Understanding Jihadist Internet Infrastructure*, Janes Intelligence Review, ianuarie 2006.

De exemplu, în data de 27.01.2013, pe contul Facebook „Taib Al-Kalam Min Ulama Ahl Al-Islam" (în traducere, „Vorbe din partea teologilor neamului Islamic"), configurat în limba arabă, a fost postat un mesaj, semnat cu pseudonimul „Islami Al-Jinsiya" („musulman de naționalitate"), conținând referiri la viitoarele atacuri Al - Qaeda, despre care se afirmă că ar urma să aibă loc în SUA, Franța, Danemarca şi alte state din Europa. Postarea respectivă avea titul „Harta Al-Qaeda şi a viitoarelor sale atacuri".

În cadrul mesajului era adresată întrebarea: *„Unde va ataca Al-Qaeda în viitor? ...Următoarele atacuri ale Al-Qaeda vor fi lansate, cu voia lui Dumnezeu, în inima tărâmului necredinței, SUA, şi în Franța, Danemarca, alte state din Europa, în țările care au susținut şi continuă să susțină statul francez, precum şi în alte locații care vor fi precizate de Al-Qaeda cu alte ocazii. (...) Atacurile vor fi puternice, grave, alarmante, cutremurătoare, şocante şi terifiante"*.

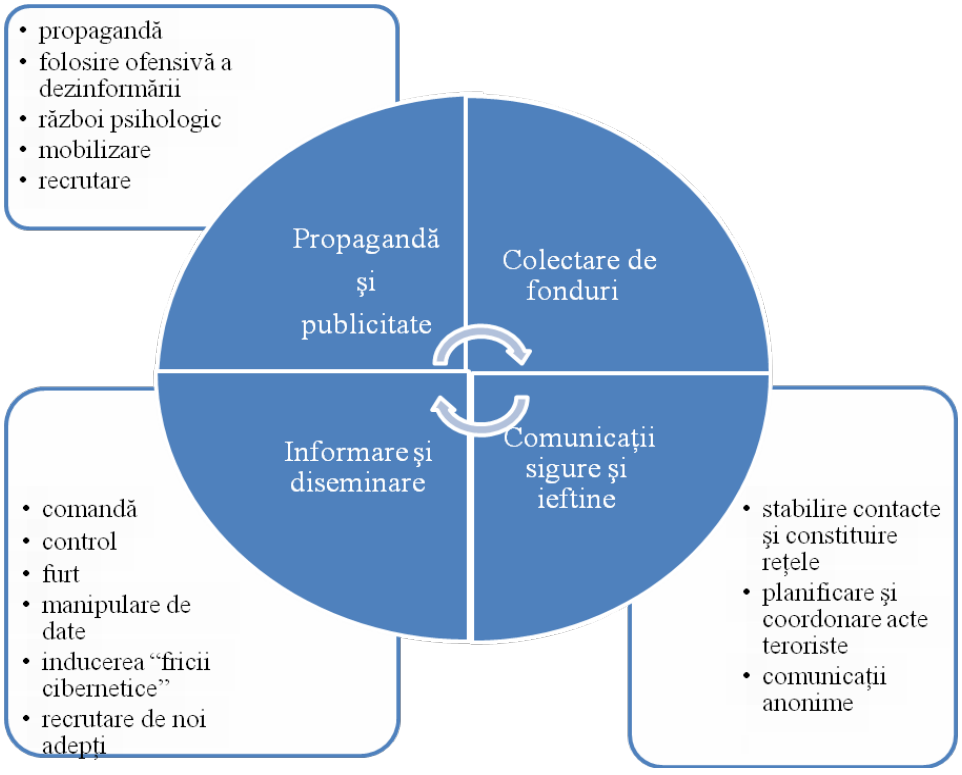

Figura 1 – *Scopurile utilizării Internetului de către organizațiile teroriste*

Statele a căror societate este dependentă în mare măsură de tehnologiile avansate conştientizează pericolul declanşării unor atacuri cibernetice (nu neapărat teroriste) şi au iniţiat măsuri concrete pentru contracararea şi anihilarea unor forme de atac cibernetic, axate pe: crearea unui cadru legislativ adecvat care să permită structurilor responsabile să coopereze şi să acţioneze eficient; investiţii masive în măsuri de securitate; înfiinţarea unor centre de intervenţie în caz de urgenţă, aşa-numitele *Computer Emergency Response Teams* (CERT). În paralel, se acţionează pentru dezvoltarea unor studii de cercetare pentru identificarea unor forme de ripostă şi contracarare adecvate, precum şi pentru dezvoltarea unui cadru educaţional de securitate la nivelul populaţiei şi al angajaţilor din sectorul guvernamental, respectiv privat.

Din punct de vedere organizatoric, anumite capabilităţi de acţiune în spaţiul cibernetic se pot materializa prin înfiinţarea unor structuri de monitorizare şi analiză a spaţiului cibernetic, urmate de organisme de răspuns şi reacţie în cazuri de urgenţă (de tip CERT). Complementar, dezvoltarea politicilor de securitate coerentă, concomitent cu crearea unui cadru legislativ optim şi educarea personalului – inclusiv prin desfăşurarea periodică de exerciţii de simulare a unor atacuri cibernetice – ar contribui la formarea unei culturi de securitate în acest domeniu.

3. Consideraţii finale

Evoluţiile tehnologice din ultimele decenii au generat o puternică dependenţă a societăţii de mijloacele de comunicaţii electronice, aspect conştientizat pe scară largă, de la oamenii obişnuiţi, la lideri politici şi societăţi multinaţionale. Astăzi vorbim în mod frecvent despre realitate virtuală, spaţiu cibernetic - *cyberspace* -, chiar dacă nu toată lumea are o percepţie reală asupra naturii acestuia. Foarte multă lume asociază acest spaţiu cu Internetul, fapt care este în mare măsură întemeiat, deoarece oferă un mediu de întâlnire pentru culturile lumii sau pentru indivizi aflaţi la poli geografici opuşi. Internetul a devenit astfel un integrator de culturi, un mediu de derulare a afacerilor, de satisfacere a nevoilor consumatorilor sau ale guvernanţilor, oferind posibilităţi de comunicare nemaiîntâlnite în urmă cu câteva decenii şi oportunităţi pentru geneza unei *agore* în care oamenii promovează ideologii şi se raliază acestora.

În acest context, am putea aprecia că se dezvoltă o societate a Internetului, cu propriile reguli, cu legislaţie şi morală specifică, cu avantajele şi, din păcate, corelativ, şi cu dezavantajele sale. Aşa cum orice societate are componente care acţionează pozitiv, conform valorilor definite

şi cristalizate de-a lungul istoriei, în aceeaşi măsură asistăm la o recrudescență, în spațiul cibernetic, a activității unor grupuri care acționează în scopuri antisociale, deseori infracționale.

În această zonă întunecată, identificăm o gamă variată de „autori" de la grupuri de hackeri asociați criminalității gulerelor albe („white collar crimes"), membrii ai crimei organizate, escroci, hoți, persoane cu debilități psihice, mergând până la terorişti.

O abordare organizatorică şi tehnică, cu accent pe *strategic foresight* (previziune strategică) are şanse reale de succes dacă măsurile şi metodele de contracarare sunt aplicate perseverent şi profesionist.

Acordarea resurselor financiare şi umane necesare, în scopul cercetării tehnico-ştiințifice a fenomenului, precum şi o cooperare eficientă între sectorul public şi cel privat, prin capitalizarea resurselor umane, ştiințifice, financiare şi de *intelligence*, sunt necesare în vederea formării unei strategii comune de apărare, care să rezulte din voința exprimată a statelor, ale căror interese comune de combatere a cybercriminalității depăşesc interesele individuale.

Bibliografie

1. A. Denis Clift, *Intelligence in the Internet Era*, 2003.
2. Brynjar Lia, *Al-Qaeda online: Understanding Jihadist Internet Infrastructure*, Janes Intelligence Review, ianuarie 2006.
3. DCSINT Handbook 1.02, *Cyber Operations and Cyber Terrorism*, 2005.
4. *Military Power of the People's Republic of China*, Report to Congress, 2007.
5. Special Dispatch Series - No. 1702, MEMRI, 2007.

Surse Internet

1. www.intelligenceonline.com
2. *The Information Warfare Site* – resursă online de Studii în domeniul securității informaționale/Marea Britanie
3. www.ziare.com
4. money.cnn.com
5. www.faz.net
6. global.nytimes.com
7. www.lemonde.fr
8. www.tagesspiegel.de
9. www.jpost.com
10. www.wsj.com