

Dușan Baiski

Război pe Internet



Editura "Waldpress" din Timișoara, 2004
ISBN 973-8453-85-2

Coperta: Dușan Baiski

© Dușan Baiski
(www.dusanbaiski.eu)

Automanipulare sau, pur și simplu, manipulare

Crezi că vei fi îndeajuns de imparțial? – m-a întrebat la un moment dat un amic, aflând că am început să lucrez la o carte dedicată războiului electronic pe Internet din perioada agresiunii N.A.T.O. asupra Iugoslaviei din 1999. Voi încerca să fac tot posibilul, i-am răspuns. Acest lucru l-am și încercat: să nu mă las pradă vreunui resentiment vizavi de americani, „eroii” și artizanii războiului nedeclarat dus împotriva Iugoslaviei, contrar tuturor normelor juridice internaționale în vigoare la acea dată. Oare am reușit? Majoritatea veți spune că nu. Autorul este de naționalitate sârbă și nu poate fi imparțial. Desigur, această apreciere vă aparține. Parțial, aveți dreptate. Cum poate fi imparțial un individ care, în timpul bombardamentelor deseori „la nimereală” ale aviației N.A.T.O. ce atacă trenuri civile, convoaie umanitare și de refugiați, inclusiv albanezi, școli, spitale, case și blocuri de locuințe, îi scrie președintelui de atunci al României, Emil Constantinescu, o scrisoare deschisă publicată în săptămânalul național românesc „Formula AS” și în forumul de pe Internet al cotidianului „România liberă”, intrigat de faptul că un președinte al unei țări cu 23 de milioane de locuitori afirmă că bombardarea poporului sârb este „legitimă și necesară”? Cum poate fi imparțial un român de etnie sârbă care, atunci, a trimis la forumul de discuții „Timișoara” un mesaj în care scria că Timișoara a fost bombardată? Desigur, o glumă luată ca și glumă, însă de unii aproape crezută. Ce ușor e să manipulezi oamenii! Îndeosebi atunci când te folosești de o anumită conjunctură. Dar se pare că e mai ușor să le crezi unor S.U.A. și Marea Britanie speriate că un oarecare Saddam Husein dintr-un oarecare Irak aflat între Evul Mediu și mileniul III deține arme de distrugere în masă și, ca atare, este un pericol mondial, decât să crezi un cetățean român, fie el și de etnie sârbă, care încearcă să facă o radiografie a primului război electronic mondial. Lăsați însă deoparte orice resentimente față de sârbi. Chiar dacă, probabil unii dintre ei s-ar fi comportat conform imaginației unui individ precum Paul Goma. Nu judecați o întreagă națiune în funcție de faptele unor membri ai acesteia. Nu putem judeca românii după faptele lui Nicolae Ceaușescu. Nu putem judeca sârbii pentru faptele unui Slobodan Milošević. De fapt, ce știe străinătatea despre România? Dracula, Ceaușescu, Nadia Comăneci. Dar despre Iugoslavia restrânsă? Milošević, sârbi sângheroși, gropi comune, albanezi maltratați... Nimic altceva decât clișee abil construite și ulterior acceptate de minți credule, leneșe, manipulate de indiferent cine ar deține controlul mass-media. Deosebit de relevantă este poziția lui Tucidide din Atena (circa 455-395 î.d.H.) față de război (cităm din cartea „Război salvat” de Michael Kunczik, Editura InterGraf, 2002), membru al elitei Atenei și chiat comandant de oști în războiul din Peloponez, potrivit căruia războiul era un „dascăl brutal” care „reușește să facă să se desfășoare trăsăturile de caracter imanente omului, în special cele negative”. În „Istoria războiului peloponezian”, autorul amintit scrie: „Ceea ce s-a întâmplat însă în realitate în acel război, n-aș îndrăzni să povestesc după cele relatate de primul venit, nici măcar <<după părerea mea>>, ci eu am încercat să analizez cu toată minuțiozitatea posibilă atât cele trăite de mine, cât și știrile de la alții, căutând să deslușesc cât mai multe detalii. A fost o cercetare obositoare, deoarece martorii aceluiași eveniment nu mărturiseau aceleași lucruri, ci o făceau în conformitate cu simpatiile sau cu memoria lor.”

Dacă ar fi să le credem psihologilor, atunci în fiecare clipă ori ne automanipulăm, ori suntem manipulați, ori amândouă la un loc. Din nefericire, nu sntem departe de adevăr. Așadar, este această carte credibilă? Ar fi absurd să susțin un asemenea lucru care, potrivit logicii, pare fals de la o poștă. Mă bazez însă pe memoria și cultura dumneavoastră generală. Ceea ce afirm eu în aceste pagini poate fi alăturat bucăților de mozaic din mințile dumneavoastră, legate de aceleași evenimente sau de evenimente similare. Rămâne în sarcina dumneavoastră să constituiți întregul. Iar concluzia vă aparține sută la sută.

e-razboi, un altfel de război

Cel de-al II-lea război mondial a fost un „război radio”. Războiul din Vietnam a fost un „război TV”, iar războiul din Kosovo a fost un „război Internet”.

Generalul german Walter Jerz, purtătorul de cuvânt al forțelor N.A.T.O. în Kosovo și Metohia (Iugoslavia), aprecia că atacul asupra Iugoslaviei a fost primul conflict militar din lume purtat și prin intermediul Internetului. La un simpozion al B.N.D. (Bundesnachrichtendienst, serviciul german de informații, cu 6 000 de angajați și cu un buget anual de 660 000 000 de mărci pe an până în 2001, a fost creat imediat după cel de-al doilea război mondial de către Gehlen, principalul coordonator al serviciilor secrete naziste Gestapo și Abwehr), același general a declarat că „falsificarea datelor este o armă a războiului psihologico-propagandistic”. Iar August Hanning, șeful B.N.D., a susținut că toate guvernele „antrenează cyber-soldați care să atace și să spioneze inamicul prin intermediul computerelor și să efectueze lovituri la distanță asupra punctelor cheie ale unei țări”. Pe de altă parte, generalul american Whesley Clark, fostul comandant al forțelor N.A.T.O. pentru Europa, a spus că „atacul asupra computerelor sârbești ar fi putut să întrerupă epurarea etnică și să micșoreze numărul celor afectați”. Numai că, după cum încă mai susțineau, la începutul lui 2001, specialiștii militari americani, asemenea atacuri nu erau avute în vedere în cadrul doctrinelor militare ale Statelor Unite ale Americii, iar problema în sine nu era încă rezolvată din punct de vedere legislativ. A existat însă în permanență teama că hackerii din Iugoslavia, dar și din alte țări, vor ataca rețeaua informatică a Pentagonului, așa cum s-a întâmplat, de exemplu, cu hackerii olandezi în timpul războiului din Golf din 1991 ori a intervenției în Somalia. Chiar dacă oficialii americani au susținut că site-urile sârbești nu au fost atacate în timpul agresiunii asupra Iugoslaviei în perioada martie-iunie 1999, indexul site-ului Ministerului Afacerilor Interne iugoslav a fost „pictat” cu zvastici. Hai să acceptăm că atacul a fost opera unor simpli hackeri și nicidecum o acțiune la comanda guvernului sau a armatei americane. Iată însă, potrivit publicației iugoslave „Vesti”, ce părere are dr. Slobodan R. Petrović, lucrător în cadrul poliției sârbe și autor al cărții „Criminalitatea digitală”, despre dezinteresul guvernului american pentru atacul împotriva sistemului informatic al Serbiei: „În timpul agresiunii N.A.T.O., americanii au plănuț să înceapă cyber-atacuri asupra Serbiei, dar acest lucru nu le-a ieșit la mână întrucât tehnologia informațională de la noi (prezentă în sistemul bancar, în poliție, armată...) nu se află într-un grad deosebit de interconectare, astfel că, din acest motiv, nu a fost interesantă pentru un asemenea gen de atacuri.”

Dar de hackeri nu au scăpat nici site-urile unor importante instituții americane. În 1999, aceștia au încercat de mai multe ori să pătrundă în baza de date a bazei aeriene din San Antonio, în care erau stocate date despre forțele americane din Bosnia și în care se găseau înregistrări și diverse documente despre atacurile aeriene asupra Irakului. Iată însă că specialiști din cadrul Centrului pentru studiul apărării din cadrul corporației „Rand” afirmă că „forțe mobile mici, înarmate cu date care ajung în fiecare secundă de la sateliți și de la detectoarele de pe teren, vor ataca rapid locurile din care se atacă sistemul informațional al țării lor, acolo unde nimeni nici nu se așteaptă.”

În cadrul doctrinelor militare, războiul informațional și componentele sale (deci și hacking-ul) ocupă deja un loc important. Paul Vasile, șeful Direcției Planificare Strategică și Controlul Armamentului din Statul Major General, scria în anul 2000 (deci nu cu mult după agresiunea N.A.T.O. asupra Iugoslaviei) în „Cotidianul” (vezi www.cotidianul.ro): „Putem accepta, cel puțin pentru această etapă, că în sens strict militar războiul informațional, la modul cel mai general, reprezintă totalitatea operațiilor informaționale, desfășurate la nivel tactic, operativ și strategic, pe timp de pace, criză, escaladare a crizei și totalitatea operațiilor informaționale, desfășurate la nivel tactic, conflictual, în scopul realizării unor obiective sau influențării unor anumite ținte.”

Războiul informațional integrează forme de manifestare distincte: războiul de comandă și control (forma strict militară), războiul bazat pe informații (intelligence), războiul psihologic, războiul electrosonic, războiul hackerilor (s.n.), războiul informațiilor economice, războiul în spațiul realității virtuale.”

După 11 septembrie 2001, când au fost atacate New-York-ul și Washington-ul, situația pare a se fi schimbat radical, atacurile asupra turnurilor gemene ale lui World Trade Center și asupra Pentagonului fiind mai degrabă ocazia și nicidecum cauza luării unei serii de măsuri. Doar timpul va demonstra că ele vor fi eficiente ori nu în lupta împotriva terorismului, însă cu siguranță vor afecta într-un fel sau altul libertatea și intimitatea nu doar ale cetățenilor celei mai așa-zis democratice țări din lume, ci ale tuturor oamenilor de pe această planetă.

Primul atac al hackerilor legat de atacul terorist asupra WTC și a Pentagonului a fost realizat asupra unui mare număr de servere pe care se găseau găzduite site-uri și pagini web personale înregistrate la „NetNames”, o organizație pentru înregistrarea de domenii Internet. Potrivit site-ului croat <http://active-security.org>, un oarecare „Fluffi Bunni” îl susținea pe Osama bin Laden. Iar accesările realizate prin „NetNames” erau redirecționate înspre o pagină de web unde se afla un pamflet la adresa intoleranței religioase a Occidentului și a Americii imperialiste, semnat de așa-numitul „Fluffi Bunni”. Despre același subiect va relata și o știre apărută la 18 septembrie 2001 pe site-ul românesc cu adresa <http://stiri.rol.ro> care, la rândul său, cita o informație BBC preluată de la agenția românească de presă „Mediafax”: „Unul dintre cele mai importante atacuri s-a produs la sfârșitul săptămânii, când un hacker autointitulat Fluffi Bunni a intrat în serverul companiei NetNames, ai cărei vizitatori erau automat îndrumați către o pagină cu mesajul «Dacă vrei să vezi Internet din nou, dați-mi-l pe bin Laden, plus cinci milioane de dolari»”.

Site-ul croat amintit mai înainte se referă (data: 16 septembrie 2002, deci la cinci zile după atacul asupra WTC și Pentagon) la un apel al hackerilor croați din gruparea „Chaos Computer Club”. Adunați la aniversarea împlinirii a douăzeci de ani de la înființarea grupei, aceștia, în loc să stea la taifas, au lansat un apel către hackeri din alte grupări și/sau țări de a se abține de la orice atac asupra rețelelor sau site-urilor grupărilor orientate spre Islam, indiferent cât de afectați ar fi după atacurile asupra WTC și Pentagon. „Îi rugăm pe oameni să-și aducă aminte că Internetul este un sistem de comunicare”, a spus Andy Mueller-Maguhn, membru al grupării amintite.

Nu aceeași atitudine a avut-o însă creatorul virusului „Votați în legătură cu războiul”, mascat într-un program care promova o anchetă referitoare la faptul dacă trebuie sau nu ca S.U.A. să se implice în război după atacul de la 11 septembrie 2001. Se presupunea că virusul cu pricina a fost totuși creat de un hacker care nu are nici un fel de legătură cu teroriștii sinucigași care au atacat New York-ul și Washington-ul.

Senatul american a aprobat lărgirea domeniilor în care este acceptată utilizarea sistemului secret pentru supravegherea poștei electronice dezvoltat de către F.B.I. (Federal Bureau of Investigation) sub numele de „Carnivore” (denumire pe care nici nu mai e necesar să o traducem în limba română; ulterior, acest nume a fost schimbat, proiectul denumindu-se DCS1000), astfel încât să fie cuprinse și cercetările legate de terorism și criminalitate prin Internet. Se consideră însă că principala măsură, respectiv Legea privind lupta împotriva terorismului 2001 (Combating Terrorism Act of 2001) va permite serviciilor secrete americane să lărgască modalitățile de control al Internetului și-i va da Executivului american posibilitatea să „folosească mai bine cuceririle importante ale științei și tehnologiei” în lupta împotriva terorismului. Din nefericire, nu există încă o definiție unanim acceptată a acestei noțiuni.

Potrivit unei informații apărute pe www.active-security.org în septembrie 2000, compania de software „Network ICE”, în încercarea de a satisface puterea, respectiv regulamentele privind supravegherea poștei electronice, a anunțat dezvoltarea unui program de „e-mail sniffing” care, după câte se pare, va fi folosit ca alternativă pentru controversatul „Carnivore” al F.B.I.-ului. Deocamdată această companie a anunțat codul sursă al programului „Altivore” și a publicat un program demo pe paginile sale web.

O altă „minune a științei și tehnicii mondiale” este, fără îndoială, așa-numitul sistem de spionaj global „Echelon”, creat de unul din serviciile secrete americane (N.S.A. – National Security Agency, ale cărei baze au fost puse în 1952 de președintele american de atunci, Harry Truman, și de care Guvernul S.U.A. nu a aflat decât în 1957), la care cooperează membrii grupului UKUSA și anume: Government Communications Head Quarters (G.C.H.Q.) din Marea Britanie, Communications Security Establishment (C.S.E.) din Canada, Defense Security Directorate

(D.S.D.) din Australia și General Communications Security Bureau (G.C.S.B.) din Noua Zeelandă. Este lesne de observat că e vorba de țări în care limba oficială (sau una dintre cele două limbi oficiale, în cazul Canadei) este cea engleză. În mod cert, este o fisură ce, în timp, poate deveni o adevărată falie între membrii Alianței Nord Atlantice. Unul dintre cei care au studiat temeinic acest sistem este și croatul Kruno Peradenić care, la un seminar derulat la Zagreb, descria „Echelon” ca fiind un sistem ce are capacitatea de a colecta și analiza informațiile transmise din orice colț al lumii prin intermediul telefonului, telefaxului, e-mail-ului ori telexului. Într-un cuvânt, concluzionează același Kruno Peradenić, „Echelon este o rușinoasă încălcare a constituției și o amenințare a intimității cetățenilor nevinovați din întreaga lume. Dacă agențiile guvernamentale pot încălca, cu de la sine putere, cele mai elementare drepturi ale omului fără prea multă înțelegere, atunci s-ar putea ajunge la suspiciune generalizată și la ruperea alianțelor între țările importante pentru supravegherea păcii în lume.” Evident, nu e decât părerea unui muritor care nu contează în calculele celor care au născocit sistemul. Numai că muritorul cu pricina are dreptate. Cu toate că „Echelon” este produsul războiului rece, creat pentru a împiedica răspândirea comunismului, el se dovedește util nu doar pentru spionarea cetățenilor din aria țărilor UKUSA, inclusiv a politicienilor și a organizațiilor neguvernamentale, ci și în spionajul tehnologic și comercial. Un asemenea colos (doar la stația Menwith Hill, aproape de Yorkshire?ul de Nord, Anglia, existau la un moment dat 25 de receive, 1 400 de salariați ai NSA și 350 de funcționari pe teren) nu putea să fie desființat deodată cu prăbușirea sistemului comunist în Europa.

S-a tot pomenit în mass-media de puterea extraordinară a unor sateliți de a realiza fotografii de deosebită acuratețe a oricărui punct de pe glob. Scepticii afirmă însă că nu ar fi decât o gogoriță născocită de serviciile secrete. În realitate, ar fi necesare resurse financiare uriașe (chiar și pentru o superputere militară cum sunt S.U.A.) pentru performanța de a se putea urmări și fotografia, fiindcă de fotografiat vorbeam, orice punct de pe Pământ. Și oricând. Dacă urmărim aceeași logică, tot cei sceptici ar putea afirma că și „Echelon” este o gogoriță. În clipa de față, sistemul „Echelon” se folosește de serviciile unor sateliți cum sunt cei trei „Orion/Vortex”, produși de compania „TRW”, care au fiecare o rază de acțiune de până la 22 300 de mile și sunt folosiți pentru urmărirea telecomunicațiilor. Sau cei doi „Trumpet”, realizați de „Boeing”, care au o rază de acțiune cuprinsă între 200 și 22 300 de mile și sunt folosiți pentru supravegherea telefoanelor mobile. După cum vă este cunoscut, companiile de telecomunicații folosesc ele însele serviciile de retransmisie ale unor sateliți, alții decât cei pomeniți. Aceștia însă se află sub controlul celor din sistemul „Echelon”. Hacking de stat? Da. Citând cotidianul rusesc „Komsomolskaia Pravda”, publicația „Cuget liber” (www.cugetliber.ro) spune că agentul F.B.I. Michael Schuler i-a invitat în Statele Unite, în 2000, pe Vasili Gorșkov și pe Aleksei Ivanov, care l-au ajutat, în necunoștință de cauză, să obțină acces la rețelele serviciilor ruse de securitate. Cunoscuți drept hackeri, cei doi i-au prezentat lui Schuler metodele lor de lucru, ceea ce a permis F.B.I. să obțină parolele de acces pentru serverele din Rusia. După care au fost arestați fiind acuzați de comiterea unor delict informatice împotriva unor bănci americane.

Ei bine, ar comenta aceiași sceptici. Dar cum află americanii ce vorbește un român, de exemplu? „Echelon” se folosește de dicționare speciale, care conțin diferite cuvinte-cheie. Din moment ce un român pronunță la telefonul său mobil cuvântul „America”, nu este exclus ca din acel moment să-i fie înregistrată vocea, iar apoi să-i fie stocată. Iar dacă acest român recidivează, e posibil să intre binișor în atenția specialiștilor de la „Echelon”. Programele de calculator de care dispun le permit să caute și să găsească amprenta unei voci, iar pe urmă să analizeze în detaliu orice convorbire. În plus, nu mai e nici o problemă să afle cui aparține acea voce. În cazul abonamentelor, companiile telefonice din România solicitau la un moment dat nu doar datele personale ale viitorului abonat, ci și extrase de carte funciară pentru imobilele deținute de aceștia. Faptul că, odată, pe vremea lui Ceaușescu, serviciul secret român cunoscut sub denumirea de Securitate citea scrisorile pe care le considera suspecte, încălcând deci un drept constituțional, inviolabilitatea corespondenței, pare acum o banală glumă. Cine poate crede că așa-zii „băieți buni” ne apără de așa-zii „băieți răi” când clientelismul local, regional sau național a ajuns să fie multinațional, iar interesele unui grup de indivizi care doresc să conducă întreaga lume dictează de unde și până unde este democrație, de unde și până unde este legal și de unde începe ilegalul? Dar să nu filosofăm. Cert este că într-o lume care se dorește a fi tot mai sigură, devenim tot mai nesiguri. Și tot mai lipsiți de intimitate din rațiuni pe care le dictează același grup de

indivizi. Rațiuni care, evident, le servesc numai lor.

Sub titlul „Puterea și slăbiciunea spionajului electronic”, cotidianul sârbesc „Dnevnik” din 6 februarie 2002 aducea la cunoștința cititorilor săi faptul că croații au putut să înregistreze convorbirile telefonice ale lui Slobodan Milošević din Karađorđevo, întrucât au una dintre cele mai moderne tehnici de urmărire electronică, rămasă de la fosta J.N.A. (Jugoslovenska Narodna Armija - Armata Populară Iugoslavă). Știrea era preluată de la publicația „Globus” din Zagreb, care a publicat stenograma unor convorbiri telefonice ale lui Slobodan Milošević din Karađorđevo cu membri ai familiei sale, cu colaboratori apropiați, prieteni și oameni de stat. În perioada 1996-1998, au fost înregistrate aproximativ 700 de asemenea convorbiri, acțiunea fiind condusă de Serviciul Secret Croat. Mulți au pus însă la îndoială autenticitatea materialului, dar și posibilitatea unei asemenea operațiuni. Specialiștii au ajuns totuși la concluzia că a fost posibil din cel puțin două motive. Întâi și întâi pentru faptul că Croația este, cu siguranță, dacă nu singura, atunci printre puținele state care, pe lângă Statele Unite ale Americii, dispune de o așa-zisă comunitate informativă și o „construcție umbrelă pentru comunitatea informativă”. În ajunul ruperii sale de Iugoslavia, în 1990, Croația a primit din partea Germaniei cea mai modernă tehnică de urmărire și ascultare a traficului telefonic. În fostul centru de pregătire a apărării teritoriale de la Rakitje, lângă Zagreb, au fost instalate aparaturi pentru ascultarea simultană a 50 000 de convorbiri telefonice.

J.N.A. a avut în cadrul supersecretei sale baze militare de la Velika Buna, care se găsește între Zagreb și Sisak, o unitate specială pentru urmărirea comunicațiilor radiotelefonice din întreaga Europă de Sud-Est. Acest centru, mai spune aceeași publicație sârbă, a fost dotat cu cea mai modernă tehnică „Johnson-Watkinson” pentru urmărirea și înregistrarea comunicațiilor electronice din regiune. Chiar la începutul războiului, acest centru a fost predat autorităților de la Zagreb de către însuși comandantul său. Așa a ajuns Croația în posesia tehnicii fostei J.N.A. Mai târziu, Croația a cumpărat o tehnică mai modernă.

Persoane bine informate susțin că serviciul croat pentru urmărire electronică a instalat sisteme de urmărire a comunicațiilor electronice pe cote înalte, în apropierea graniței cu fosta Republică Federală Iugoslavia. Unul dintre centre a funcționat pe muntele Papuk, în Slavonia de Vest, altul - pe poligonul de la Đakova, în timp ce serviciul central a funcționat în cazarma fostei J.N.A. din Zagreb.

Posibilitățile serviciului de informații „Komint” (cunoscut și sub numele de „Sigint”) în noul veac, scrie „Dnevnik” (www.dnevnik.co.yu), au fost cu mult îmbunătățite din punct de vedere tehnic, însă problema de bază în ascultarea cu succes o constituie și pe mai departe posibilitățile fizice de accesare a legăturilor și a bazelor de date apărute, întrucât sunt tot mai actuale și măsurile pentru detectarea încercărilor de accesare și utilizare neautorizate. De asemenea, e tot mai grea acțiunea de spargere a cifrurilor pentru întreținerea legăturilor, fiindcă în permanenta actualizare a criptografiei se investesc tot mai mulți bani, iar mijloacele de apărare sunt tot mai greu de spart. În permanență se perfecționează și tehnica de ascultare. Serviciul american electronic N.S.A. folosește în principal doi furnizori pentru obținerea de aparatură sofisticată pentru strângerea tainică de informații secrete, de mesaje și date care circulă prin sistemele informatice; este vorba de AST și IDEAS. Cele două companii oferă noi tipuri de recordere, demultiplexoare, scannere și procesoare pentru calculatoare, care sunt construite pentru ascultare și elaborarea de date pe tipurile europene de aparaturi de telecomunicații cu legături multicanal și microunde, ale căror semnale transportă informații cu o viteză de 160 Mbps. Pentru urmărirea semnalelor optice se utilizează un aparat AST „model 257E”.

Sistemul „Komint”, des înlocuit cu denumirea „Sigint” și care se referă la serviciul informativ al legăturilor, adeseori înseamnă și o clasă de sateliți de telecomunicații, ce se folosesc pentru ascultarea legăturilor internaționale prin radio, telefon, fax și e-mail. Rolul „Komint”-ului este în permanentă creștere. Activitatea lui a fost cel mai bine scoasă în evidență în timpul „războiului rece”, când au fost înființate serviciile statelor occidentale pentru ascultarea rețelelor de telecomunicații ale statelor din Pactul de la Varșovia. De la sfârșitul anilor '90 din secolul al XX-lea, aceste sisteme au început să fie folosite pentru spionarea legăturilor economice.

Cel mai puternic sistem „Komint” îl posedă S.U.A., acesta fiind cunoscut sub numele de USSS și este alcătuit din unități militare N.S.A. pentru susținere electronică, părți din C.I.A. pentru război electronic și alte organizații. Acest sistem colaborează cu servicii de ascultare electronică ale altor state, printre care mai cunoscută este colaborarea în cadrul alianței U.K./U.S.A. (cinci state).

Totodată, se face schimb bilateral de informații între S.U.A. și alte servicii naționale de ascultare electronică. În lume, pe lângă U.K./U.S.A. există servicii de ascultare electronică în alte 30 de țări. Un serviciu militar „Komint” în afara S.U.A. și U.K./S.U.A. este organizația rusă F.A.P.S.I., care numără 54 000 de oameni. Un asemenea serviciu are și China. Multe state din Orientul Mijlociu și din Asia, așa cum sunt Pakistanul și India, au fiecare câte un sistem „Komint” foarte dezvoltat. De când a fost construit sistemul U.K./S.U.A. („Echelon”), pentru ascultare se utilizează 120 de sateliți, din care 40 sunt angajați în ascultarea legăturilor comerciale, 30 pentru controlul spațiului cosmic din jurul Terrei și pentru ascultarea legăturilor militare, în vreme ce pentru urmărirea spațiului fostei U.R.S.S. sunt utilizați 50 de sateliți.

Pomeneam mai sus de faptul că, datorită componenței grupului care concluează la sistemul „Echelon”, în N.A.T.O. există o fisură. Iată însă că a apărut și o a doua. Autor este același: S.U.A. Americanii au semnat în 2000 actele de înființare ale T.P.I., însă nici administrația Clinton, nici ulterior cea a lui Bush nu s-au oboșit să solicite Senatului ratificarea acordului. Ba, mai mult, și de aici cea de-a doua fisură, administrația Bush a anunțat Organizația Națiunilor Unite că S.U.A. își rezervă dreptul de a ignora orice dispoziții ale T.P.I. – Tribunalul Penal Internațional, prima instanță abilitată să judece persoanele suspecte de crime de război, genocid sau crime împotriva umanității. Așadar, dacă unii dintre cei 200 000 de militari americani aflați în 2002 în afara teritoriului S.U.A. ar fi săvârșit fapte de genul celor enumerate mai sus ei nu ar fi putut fi judecați de T.P.I. La insistențele, presiunile și, ceea ce nu este deloc exclus, șantajul americanilor, câteva state, printre care Israelul și România s-au grăbit să semneze cu S.U.A. acorduri de neextrădare a militarilor americani. Gestul României a iritat puternic membrele N.A.T.O. din Europa. Dacă Marea Britanie, aliatul tradițional al S.U.A., și Italia vor ceda presiunilor americane, nu este exclus să fie urmate și de celelalte membre ale N.A.T.O. și atunci actuala fisură va dispărea. Însă T.P.I. ori va fi desființat, ori va deveni ridicol. Și va demonstra încă o dată că a fost înființat formal, doar pentru a-i aduce pe sârbii cei indisciplinați în rând cu lumea. Cu lumea supusă, evident.

De altfel, se cunoaște foarte bine faptul că, în ton cu rolul pe care și l-a impus, și anume al celui de jandarm mondial, S.U.A. nu dau pentru prima dată dovadă de aroganță. Prin abandonarea Tratatului de la Kyoto, privitor la măsurile pentru diminuarea efectului de seră, americanii, cu cel mai mare procent în poluarea mediului înconjurător, au reușit să irite nu doar obișnuiții săi inamici, ci și aliații din cadrul N.A.T.O.. Iar la reuniunea din 2002, de la Johannesburg (Africa de Sud), unde s-a pus din nou problema mediului înconjurător și unde au participat numeroși șefi de state și de guverne, Colin Powell, reprezentantul S.U.A., a fost huiduit copios de către chiar concetățeni de-ai lui. Și de această dată S.U.A. și-au etalat aroganța de mare putere și de și mai mare poluator al atmosferei. Astfel că devine de-a dreptul ridicolă mirarea americanilor în fața atitudinii ostile la adresa lor, atitudine ce riscă să devină planetară.

Nu trebuie nicidecum uitat rolul pe care l-a jucat C.I.A. în crearea Internetului. Inițiatorii acestui sistem planetar de telecomunicații au avut se pare o imaginație mai puternică decât înșiși autorii de science fiction, cu Isaac Asimov în frunte. Iată, au spus cei de la C.I.A., noi facem publice datele pe care le deținem despre fiecare țară în parte. Altfel spus, doar că nu au invitat pe față lumea să procedeze la fel. Nu cu mult timp în urmă, abia ce a trecut ceva mai mult de un deceniu, un întreg sistem, cel comunist, controla strict orice mijloc mass-media, de la o banală fițuică de cartier până la radioul și televiziunea națională, nu care cumva să scape vreo informație care să ajute pactul nord-atlantic în activitatea sa de spionaj. Astăzi, C.I.A. poate fi mândră de copilul său, Internetul. Cu costuri minime se poate spiona o planetă întreagă, se poate citi starea de spirit a oricărei regiuni de pe glob, se pot copia informații cu duiumul. Dar, mai mult, se poate influența un popor întreg, începând cu cel american, bineînțeles. De aici putem deja vorbi despre concepția conflictelor de mică intensitate, despre războiul psihologico-propagandistic etc.

În 2002 și tot sub pretextul luptei împotriva terorismului, Parlamentul european adoptă și el o lege care obligă nu doar operatorii de Internet, ci și pe cei de telefonie fixă și mobilă să stocheze informații detaliate despre convorbirile fiecărui abonat. De acum înainte, se vor arhiva numerele de telefon apelate, durata fiecărei convorbiri și conținutul acesteia, secunda, minutul, ora și ziua când s-a efectuat aceasta, precum și traseul fiecărui cetățean care are un telefon celular pe care nu trebuie neapărat să-l folosească, ci doar să-l poarte în buzunar. Acest ultim lucru e posibil întrucât telefoanele mobile comunică în permanență cu stațiile de bază. Ratificată de parlamentele celor cincisprezece țări membre ale U.E., legea adoptată la Bruxelles este obligatorie pentru statele candidate la aderare, deci și pentru România. „Cu aprobarea

Occidentului – spune Bogdan Chireac în editorialul „Adevărului” din 4 iunie 2002, cei care vor conduce serviciile secrete din România vor deține o putere pe care securitatea lui Ceaușescu nu a visat-o vreodată. Dacă lucrurile vor scăpa aici de sub controlul legii, România, integrată în N.A.T.O. și U.E., riscă să ajungă mai puțin liberă decât România lui Ceaușescu...”. Iată că „Echelon” se extinde mai repede decât au crezut creatorii săi.

Nu e un secret faptul că S.U.A., Japonia și China dispun deja de supercalculatoare. Compania americană I.B.M. („International Business Mashines) a făcut cunoscută versiunea comercială a celui mai puternic calculator din lume, care poate să prelucreze 12,3 bilioane de date pe secundă. Acesta folosește microprocesoare pe bază de cupru în locul celor siliconice și un program (software) pentru servicii comerciale și de rezolvare a problemelor de inginerie de genul celor pentru design-ul avioanelor, denumit RS/6000 SP.

În China, a fost dat în folosință un computer care poate efectua 384 de miliarde de calcule pe secundă. Denumit „Puterea invincibilă”, acesta este inclus printre cele 48 de supercalculatoare existente în lume care sunt folosite în domeniul afacerilor. Cotidianul chinez „Zenmin Zibao” scria că în prima jumătate a anului 2000 a fost realizată prima mobilizare on-line pentru apărarea țării în domeniul apărării antiaeriene. Prin acest act, puterea de la Beijing dovedește că-și dă seama de importanța tehnologiei informatice. Cheia victoriei în războiul strategic informațional al secolului al XXI-lea stă în suveranitatea propriei rețele informaționale, susțin conducătorii militari chinezi. Controlul rețelei informatice naționale chineze de către o putere, alta decât cea chineză, ar pune în primejdie interesele vitale naționale și ar însemna agresarea civilizației chineze, se afirmă într-un studiu al staff-ului armatei chineze.

Și, totuși, de ce s-a derulat în 1999 primul e-război mondial? Pe de-o parte pentru că cetățeni de etnie sârbă au existat în mai toate statele lumii și firește că au fost de partea conaționaliilor lor agresați de forțele N.A.T.O. Pe de altă parte, pentru că nu au stat cu mâinile încrucișate nici internauții de origine slavă, îndeosebi cei din Rusia, Ucraina și Belarus. Și nici cei care, într-un fel sau altul, nu agreează politica de forță cultivată de Statele Unite, printre aceștia din urmă fiind și mulți cetățeni americani. Pe frontul celălalt s-au aflat în primul rând albanezii din diaspora, musulmanii și, evident, cei care văd în S.U.A. pe Dumnezeuul lumii. Firește, de la luptă - că doar nu se luptă pe câmpul de luptă, cu arma în mână, sub șuierul gloanțelor și în miros de praf de pușcă, ci la căldură, în fața unui monitor și cu o Coca-Cola alături – nu s-au dat la o parte nici extremiștii, cei pentru care intervenția din Iugoslavia a fost doar un pretext pentru defulare. De aceeași parte a baricadei, pe frontul împotriva S.U.A. în primul rând, s-au aflat ultranaționalistii, comuniștii și neonaziștii. Așa cum în clipa de față neonaziștii și grupările radicale islamice au făcut front comun împotriva evreilor și a americanilor. Interesant este, în acest sens, un articol scris de Ivan Ninić din Israel și apărut, în septembrie 2002, pe site-ul „Apis”

(www.2net.co.yu/apis/), care trece în revistă trecutul relațiilor dintre Germania și lumea arabă. Autorul pornește de la războiul informatic inițiat, în preajma celui de-al doilea război mondial, de către mașina propagandistică nazistă, când Germania lui Hitler s-a aliat cu fundamentalistii musulmani contra intereselor engleze, și termină prin a face următoarea remarcă: „Crearea Israelului doar amplifică intoleranța lumii arabe împotriva aliaților și, cu ajutorul fostei axe a puterii, arabii creează ei înșiși o axă antisemită, care s-a cuibărit în sânul intelectualității vest-europene de stânga, în dreapta revanșardă și într-o bună parte a Lumii a Treia. Cimentul acestei alianțe nenaturale îl constituie lupta împotriva globalizării, iar ura împotriva «Satanei mari» și a celei mici, după cum ar spune aiatollahii din Koma (Iran), capătă forme tot mai pronunțate. [...] Nazificarea unei părți a societății islamice a primit prin tehnologia de vârf o armă puternică. Perfectiunea tehnicii germane a dobândit urmași talentați în fundamentalismul islamic.” Așadar, aliații nu ți-i alegi niciodată singur. Ți-i alege conjunctura. Ori inamicul.

Portret

Chiar dacă, de curând, după ani de zile de dominație, numărul paginilor web în limba engleză a coborât sub 50%, limba Internet este în continuare considerată a fi engleza, o adevărată lingua franca a lumii moderne, așa cum, în antichitate, lingua franca a fost latina. Astfel că, pe bună dreptate, cel care dorește să pătrundă în tainele Internetului și nu știe deloc ori prea bine limba engleză trebuie să aibă neapărat în preajmă un dicționar englez-român. Și întrucât vorbim în cartea de față despre hackeri, iată și definiția de rigoare, așa cum a fost ea concepută de către anglistul Andrei Bantaș: hacker – târnăcop, topor de tăiat piatră; tăietor de piatră; salahor; muncitor care lucrează cu târnăcopul/toporul. Iar hack înseamnă cal de povară, rob, dar și a ciopârți, a tăia. Adică ceva identic sau aproape identic cu verbul românesc a hăcui, provenit din cuvântul german hacken și care înseamnă a tăia în bucăți (mici), a toca mărunț, a sfârteca, a ciopârți. Pe de altă parte, specialiștii din domeniul IT susțin faptul că hack este un cuvânt derivat din limbajul studenților de la Massachusetts Institute of Technology, utilizat pentru a defini glumele făcute de studenți și în același timp impunea respect. O legătură electrică se definea „hack simplu”, un „hack” trebuind să fie inovator, să denote stil și pricepere tehnică.

Dar cine sunt hackerii? Se spune despre ei că detestă orice individ, instrument sau lege care încearcă să împiedice cunoașterea. În lumea lor, oricine poate să demonteze un lucru pentru a-l îmbunătăți este binevenit. Însă dacă accesul la acel lucru este îngădit, dacă între hacker și informații există bariere, atunci hackerul afirmă că este vorba de birocrație, de o birocrație de-a dreptul periculoasă. De asemenea, se mai spune că, din punct de vedere al hackerilor, de pe urma libertății informației orice sistem poate trage beneficii.

Hackerii au avut un rol esențial în dezvoltarea softului, la crearea și dezvoltarea Internetului. Numai că, în timp, cele două percepțe fundamentale ale eticii lor, respectiv datoria morală de a răspândi cunoștințe scriind „software” pentru a facilita accesul la informație și la mijloacele de calcul și condamnarea vandalismului și a atentatelor la confidențialitate au început să fie în mod repetat și grosolan încălcate. Acest lucru nu a scăpat de ochiul vigilent al mass-media, care a văzut balanța înclinându-se în dezafoarea hackerilor cu respect față de etică. Drept urmare, hackerii nu mai sunt considerați a fi cei care, în epoca de pionierat, erau eroii pozitivi, ci au devenit în corpore eroi negativi.

Referindu-se la hackeri în numărul din aprilie 2002 al „PC Magazine”, Mihaela Cârstea, redactorul șef al publicației, scria în editorialul său: „Hackerii au construit Internetul. Hackerii au făcut din sistemul de operare Unix ceea ce este astăzi. Hackerii au creat Usenet-ul. Hackerii fac World Wide Web-ul să funcționeze. Dacă faci parte din această cultură, dacă te solidarizezi cu ea și dacă alte persoane care îi aparțin știu cine ești și te numesc hacker, înseamnă că ești hacker. Legendă? Adevăr? Dar chiar dacă hackerii au avut inițial un rol pozitiv la dezvoltarea Internetului, intruziunile lor forțate nu au nici o justificare.”

Dar, vă veți întreba, cine sunt de fapt acești hackeri? Răspunsul e simplu: majoritatea sunt elevi sau studenți care vor să iasă în evidență prin modificarea site-urilor, ținta lor predilectă fiind site-urile guvernamentale, militare sau ale marilor companii, așadar unele dintre cele mai des accesate și cu un mare impact la public. Cum altfel, nu-i așa, ar afla atâta lume despre faptele lor?

Demn de reținut este însă că există crackeri (acum vorbim de crackeri) care beneficiază de statut legal. L. Ivăner, autorul cărții „Lexiconul hackerului” (Editura „ProMedia Plus”, Cluj-Napoca, 1996) spune că așa-numitele „tiger teams” „...sunt echipe de crackeri profesioniști care testează sistemele de securitate ale instalațiilor de computere militare prin atacarea lor de la distanță, folosind rețele și canale comm considerate «impenetrabile». Dacă nu ar fi ținute în mare secret, am putea cu siguranță admira în programele acestor «echipe de tigri» cele mai ingenioase artificii care s-au imaginat vreodată. Ce ne împiedică să presupunem că acești crackeri profesioniști provin din rândul hackerilor care și-au înfrânat dorința de a comite infracțiuni spărgând sisteme, dorință pe care, în noua ipostază, și-o pot satisface pe cale legală.”

Dar să vedem cine sunt principalele personaje ale cărții de față. Potrivit opiniei generale, hackerii posedă un profil psihologic special. Cu cât sunt mai tineri, cu atât se laudă mai mult. Motto-ul care-i unește este „Mâncare, adăpost și un cod autentic”. O dată cu trecerea anilor, ei nu mai

sunt însă atât de interesați de ceea ce spun cei din jurul lor, ci preferă să-și păstreze un anonim deplin. Aceasta inclusiv din rațiuni de securitate.

Iată ce anume scrie despre motivarea unui atac autorul site-ului din Republica Moldova cu adresa www.ournet.md/~xguard/xsecurity/dos.html: „Motivările unui atac DoS sunt extrem de diverse. Depind multe și de maturitatea atacatorului, majoritatea începătorilor au ca motiv principal dorința de răzbunare pe un anumit utilizator, admin(istrator) sau dorința de a arăta întregii lumi ce prezintă. După aia va veni numaidecât dorința de a obține acces acolo unde nu au toți muritorii. Iar maturitatea unui atacator ar fi acționarea din motive mai serioase: motive politice, economice etc.” Așadar, dacă în timp de război hackerii tineri nu prea conștientizează ceea ce se întâmplă sau le este indiferent prin ce anume trece națiunea din care fac parte, hackerii (sau chiar foștii hackeri în tinerețe) maturi vor înțelege necesitatea implicării lor în cyberwar și vor acționa ca atare.

Pentru propria securitate vizavi de legislația în vigoare în țara lor, cei care realizează și administrează site-uri destinate hackingului au grijă să scrie că tot ceea ce fac nu este decât o prezentare a activității de hacking destinată pur și simplu... cunoașterii. Este și cazul site-ului în limba română cu adresa <http://dev-null.go.ro/cracklinks.htm>, al cărui autor, care se semnează GiaRdiA, scrie: „Informația prezentată pe acest site, programele-exemplu și alte materiale sunt DOAR în scopuri educaționale. Autorul va fi considerat în afara oricărei responsabilități dacă utilizarea acestor informații va fi în scopuri ilegale, menite să aducă pagube sau câștiguri materiale, fizice sau morale. Acest site nu încurajează deprotejarea programelor pentru folosirea lor ilegală. Metodele de protecție prezentate au ca scop îmbunătățirea modului de lucru al programatorilor dând informații asupra metodelor și variantelor de «spargere» a unui program. Acest site nu încurajează folosirea copiilor ilegale a uneltor prezentate aici. Cu alte cuvinte: dacă vrei să le folosești, cumpărați-le!”. Dar iată și descrierea aceluiași GiaRdiA pentru diverse link-uri: „Sudden Discharge Un site foarte bun de cracking. Programmers Tool's După cum spune și numele un site cu multe unelte folositoare. EternalBliss - Multe tutoriale variind de la W32dasm la VB cracking. Azrael Tutoriale de SoftIce, ASM, WinCrack, BeOS Crack si W32DASM. Romanian Cracking Force Un site românesc de crack foarte bun! Încercați-I ! Le massif central Site dedicat reverse engineering-ului. Tools, docs, links, info. Last Fravia's mirror of Reverse code engineering Cel mai tare site de reverse code engineer care a mai rămas ... Old Style Cracking.” Am încercat să accesăm unele dintre adresele de mai sus, însă nu pe toate le-am și găsit, dată fiind existența lor efemeră ori chiar teama de autorități.

Dar scum se văd a fi hackerii înșiși? O descriere foarte plastică a conceptului de hacker am găsit-o la adresa: <http://www.best.pub.ro/~traznet/nr4/hacker4.htm>: „Dacă ați mai citit ceva despre hacker, cracker, creatori de viruși și alte specimene de acest fel, probabil că sunteți deja familiarizați cu profilul psihologic atribuit acestora: «adolescenți sau tineri izolați, impotenți, incapabili să întrețină o relație socială normală...bla bla bla». Nu este deloc așa. Hackerii sunt niște băieți (sau fete) foarte de treabă - foarte inteligenți chiar dacă nu iau ei toate examenele și mai pică câte un an...”

Pentru un hacker este destul dacă nu chiar foarte greu să-și țină gura atunci când reușește să spargă un sistem protejat. Mai ales dacă se află la vârsta de cristalizare a personalității. Dar, încet-încet, grozăvia cedează locul stăpânirii de sine. Viața hackerului este lungă dacă știe să-și pună lacăt la gură. La adresa amintită mai sus se spune: „Dacă oricum ai făcut o prostie mai mare decât o poți acoperi, ai două posibilități: să apelezi la prieteni de încredere sau, dacă ești prins, să te porți ca un adult, adică: neagă tot!”

Pe www.occident.ro a fost publicat un interviu luat de Paula Bulzan informaticianului Radu D.: „- Spuneți-ne care ar fi portretul unui haker?”

- În istoriile despre hackeri am observat câteva trăsături comune, câteva caracteristici psihologice. De exemplu, nu se poate pune la îndoială faptul că majoritatea hackerilor au un nivel ridicat al inteligenței. O altă trăsătură comună este insistența, perseverența în obținerea scopului propus. Hackerii trebuie să aibă o voință puternică, deoarece de multe ori în activitatea lor este nevoie de un efort mare, este nevoie de o muncă continuă fără rezultate de încurajare pe parcurs și luarea unor decizii pe baza propriilor criterii.

Majoritatea hacker-ilor preferă lucrul individual, chiar dacă au experiența lucrului în echipă. Distanța și răceala în comunicare, predispoziția la conflict, lipsa unor emoții exprimate în exterior acestea constituie în linii mari posibilul portret al unui hacker”.

Într-un interviu publicat pe www.active-security.org, un faimos hacker canadian (din Vancouver), cunoscut în underground sub numele de K2 (numele real: A.M. Shane), a fost întrebat care sunt, după părerea lui, deosebiriile dintre un cracker și un hacker. El a dat următorul răspuns: „Păi, este efectiv un lucru subiectiv; o persoană normală (ne-tehnică) s-ar putea gândi că hacker este oricine care poate apăsa un buton și poate astfel să-și pornească unitatea de calcul. De fapt, eu efectiv nu mă gândesc atât de mult la așa ceva, acești termeni nu înseamnă nimic pentru mine. Dacă vă numiți „hacker” sau indiferent cum altcumva, unii oameni vor crede taman pe dos decât ați crezut dumneavoastră că înseamnă.”

Desigur, există deja și istorii ale hacking-ului, dar și hackeri care au intrat în istorie. Potrivit www.AimPortal.com, primii zece sunt: Richard Stallman, Dennis Ritchie, Ken Thompson, John Draper, Mark Abene, Robert Morris, Kevin Mitnick, Kevin Poulsen, Johan Helsingius și Vladimir Levin. Căroră li se adaugă Douglas Engelbart, Steve Wozniak, Clifford Stoll, Linus Torvalds și Tsutomu Shimomura. Să vedem însă cine au fost primii zece.

Richard Stallman e primul hacker fără pseudonim și care are un dosar ireproșabil. Primul contact cu computerul l-a avut la 16 ani, în Centrul științific din New York al I.B.M. În anii '70 a lucrat într-un laborator pentru inteligență artificială din cadrul Universității MIT. Este laureat al premiului „McArthur” (fond pentru persoanele geniale) care, la vremea aceea, era de 240 000 de dolari. A fost împotriva ideii ca programele de calculator să fie considerate proprietate privată, drept pentru care a înființat în ianuarie 1986 fundația „Free Software”. Este cunoscut și ca întemeietor al grupului GNU, care dezvoltă o susținere gratuită pentru sistemul de operare „Linux”. Stallman este primul luptător împotriva programelor comerciale.

Dennis Ritchie și Ken Thompson sunt cu siguranță unicii hackeri mai cunoscuți sub numele adevărate decât prin pseudonime. (dmr și Ken). Ritchie și Thompson au creat în 1969 „Unix”, un sistem operațional deschis care a schimbat radical istoria computerelor. Ritchie este cunoscut și în calitate de autor al limbajului de programare „C”. Interesant e faptul că Thompson, ca pilot amator, a avut prilejul de a pilota la Moscova un „MIG-29”.

John Draper, mai cunoscut sub numele de Cap'n Crunch, este cunoscut drept primul spărgător de sisteme telefonice. Folosind un fluier pus drept cadou în cutiile cu fulgi, a reușit să determine centrala telefonică să-i permită să telefoneze gratuit de la telefoane publice. Isprava sa a fost motiv de inspirație pentru generații întregi de hackeri pentru a se lansa în fapte asemănătoare. Mark Abene s-a întâlnit pentru prima dată cu computerele în magazinul unde lucra mama lui. A făcut experimente cu semnale telefonice și prin aceasta și-a incitat mulți „colegi” să studieze găurile din modul de lucru al companiilor telefonice. A fost unul din membrii grupului LOD, mai cunoscut sub numele de Phiber Optic. S-a certat cu „colegul” al cărui pseudonim a fost Erich Bladex. Drept pentru care Phiber a fost înlăturat din grup. Însă el a creat rapid un grup rival și anume „Masters of deception” (MOD).

În 1990, aceste două grupuri au început o acțiune care, în istoria Internetului, este cunoscută ca fiind „Marele război al hackerilor”, un conflict de doi ani care a însemnat deranjarea și ascultarea liniilor telefonice precum și pătrunderea în calculatoare străine. Acesta a fost unul dintre motivele pentru operațiunea „Diavolul înșorit” (SunDevil), cea mai mare acțiune de arestare de hackeri de până atunci.

Ținta principală au fost cei din grupul LOD, însă aceștia nu au fost prinși. Totuși, operațiunea nu a fost zadarnică - patru membri ai grupei MOD, incluzându-l aici și pe Phiber Optic, au fost băgați la închisoare, prin aceasta încheindu-se „Marele război”. După un an de închisoare, ei au ieșit ca adevărați eroi și în cinstea lor s-a organizat un chef la un club elitist din Manhattan din New York. Robert Morris (rtm) este fiul unuia dintre principalii oameni de știință din cadrul Centrului de computere al Agenției Americane pentru Securitate Națională (National Security Agency, N.S.A.). S-a întâlnit pentru prima dată cu un computer atunci când tatăl său a dus acasă una dintre mașinile criptografice pe care le-a folosit armata americană în decursul celui de-al doilea război mondial.

Ca adolescent, a procurat un act care i-a permis accesul în laboratoarele „Bell” și unde, în curând, cu ajutorul unor trucuri de programare, a dobândit statutul de administrator. Lui i se datorează inserarea în dicționarul computerelor a cuvântului „hacker”.

Cea mai importantă operă a sa apărut în perioada studiilor de științe ale computerelor la Universitatea Cornell: a fost primul virus de Internet cunoscut și sub denumirea de vierme. Pe 2 noiembrie 1988, folosindu-se de greșelile din versiunea de atunci a programului de trimitere a

poștei electronice (sendmail) și de primire a datelor despre utilizatori (finger), a scris un program care s-a multiplicat singur și s-a extins în rețea și pe care l-a denumit „vierme”. Intenția lui nu a fost să provoace perturbări ale traficului de pe Internet, ci doar să încerce unele dintre ideile sale. Din cauza unei greșeli de programare, viermele a scăpat repede de sub control, iar urmarea a însemnat un mare număr de sisteme blocate sau scoase din trafic chiar înainte ca programul să înceapă să producă pagube. Când a constatat Morris la repezeală ceea ce a făcut, s-a sfătuit cu prietenii și a expediat indicații anonime administratorilor din rețea despre ceea ce trebuie să facă pentru a opri viermele, însă era deja prea târziu. Rețeaua era într-atât de sufocată încât mesajul a ajuns prea târziu. Sistemele diferitelor universități, baze militare și fundații medicale erau deja infectate. Grupe din cadrul Universităților Berkeley și MIT lucrau de zor la decodarea viermelui pentru a descoperi ce anume face el efectiv. După douăsprezece ore de muncă, echipa de la Berkeley a găsit o soluție temporară pentru limitarea răspândirii viermelui. Între timp, sufocarea rețelei și numărul uriaș de calculatoare scoase din funcție au împiedicat recepționarea acestei informații de către toți cei cărora le era necesară. Situația s-a liniștit abia peste câteva zile. Întrucât cheltuielile cu înlăturarea pagubei ajungeau și la 50 000 de dolari de sistem, a început căutarea vinovatului. Ziariștii de la „New York Times” l-au indicat de vinovat pe Morris, astfel că a urmat arestarea acestuia și trei ani de pedeapsă plus 400 de ore în folosul comunității și 10 000 de dolari drept amendă.

Kevin Mitnick, zis Condor, a început de mic să se ocupe de comunicațiile prin calculatoare. Deoarece nu a avut bani să cumpere un computer, a apelat diverse sisteme cu ajutorul unui modem, dintr-o unitate a lanțului de magazine „Radio Shack”. El și-a câștigat locul în galeria celor mai cunoscuți hackeri datorită faptului că fotografia sa a ajuns pe lista celor mai căutați criminali urmăriți de F.B.I. În timpul celor trei ani de fugă de mâna de fier a legii, a comunicat cu prietenii prin IRC. El a fost arestat în 1995 și acuzat de falsificarea a 20 000 de numere de cărți de credit. După mai mult de un an de judecată, a recunoscut doar folosirea unor numere de telefoane mobile furate. Închiderea sa a pus capăt unei ere în care hackerii erau considerați drept o versiune modernă de Robin Hood și tuturor le-au devenit clare pericolele pe care le reprezintă asemenea indivizi. Se lucrează tot mai serios la securitatea sistemelor de rețele, iar hackerii profesioniști se retrag în ilegalitate.

Kevin Poulsen, mai cunoscut sub numele de Dark Dante, a fost primul hacker căruia hobby-ul i-a adus foloase materiale. În 1990, el a preluat toate liniile telefonice ce duceau la stația de radio KISS-FM din Los Angeles pentru a se asigura astfel că va cel de-al 102-lea ascultător care se anunță telefonic pentru a participa la o emisiune-concurs. Aceasta i-a adus un automobil Porsche-944 S2. A fost prins când au apărut fotografiile în care se vedea cum forțează punctul companiei telefonice. De altfel, fotografiile au fost făcute de un prieten de-al său, pentru a a immortaliza evenimentul. La proces a recunoscut și faptul că a pătruns în computerele F.B.I.-ului, de unde a luat o listă cu agenți aflați în misiuni speciale.

Johan Helsingius, zis și Julf, a pus în noiembrie 1992 bazele celui mai popular sistem pentru trimiterea anonimă de mesaje, Anon.Penet.Fi. Când, în 1995, Biserica scientologică a deschis proces pentru faptul că, folosindu-se de sistemul lui Julf, un anonim îi făcea publice tainele pe Internet, poliția a pătruns în spațiul de lucru al lui Helsingius.

În august 1996, tribunalul i-a ordonat să deconspire adresa adevărată a utilizatorului care era vinovat, iar el a decis să închidă sistemul. De altfel, Penet.Fi, unul dintre cele mai utilizate în Finlanda în acea perioadă, funcționa pe un calculator cu un procesor de 486 și un harddisk de 200 Mb.

Vladimir Levin este ultimul din galeria hackerilor celebri și primul hoț Internet cunoscut. Cu ajutorul computerului firmei „AO Saturn” din Petrograd, unde lucra, și a laptopului său personal, în perioada din iunie și până în august 1994, în optsprezece pătrunderi, a scos mai mult de zece milioane de dolari din sistemul „Citibank”. Interpol l-a arestat pe aeroportul londonez Heathrow în martie 1995. La începutul lui 1997, a fost în sfârșit predat americanilor, iar în august a fost condamnat la 36 de luni de închisoare și la o amendă de 250 000 de dolari.

După spectaculoasa arestare a lui Vladimir Levin din anul 1995, la opinia publică ajung doar informații nesemnificative despre atacuri temporare asupra unor prezenții Web. Faptul că sistemul de computere al ministerului american al apărării nu a rezistat atacului unui israelian de nouăsprezece ani și a celor doi complici din S.U.A. ai acestuia a tulburat opinia publică, însă nu

prea mult. Criminalitatea pe Internet a devenit o realitate, însă nimeni nu dorește să dea publicității prea multe secrete de la locul de muncă.

Hackerii deschid cyberfrontul

Este cunoscut faptul că în timpul agresiunii N.A.T.O. asupra Iugoslaviei, în 1999, au existat mai multe grupe de hackeri sârbi care au avut un rol important. Aleksandar Milosavljević, un procuror belgrădean și unul dintre puținii oameni ai legii din Serbia care se ocupă de criminalitatea prin Internet din entuziasm și din curiozitate, după cum singur declară, susține că hackerii sârbi și grupările din care fac aceștia parte se află în strânse legături cu hackerii din străinătate. Sunt îndeobște cunoscute grupările „Îngerii sârbi” („Srpski anđeli”), „Codrenii” („Šumadinci”; Šumadija” este o regiune a Serbiei, „šumadinci” fiind locuitorii acestei regiuni) și „Armata Sârbă a Internetului” („Srpska Vojska Interneta”, abreviat SVI, ceea ce înseamnă și „toți”), aceasta din urmă având și un regent și ai cărei membri le-au scris provider-ilor că, dat fiind faptul că se luptă pentru problema sârbă, să li se dea acces gratuit la Internet. Dar cine este acest Regent, zis și Kapetan Dragan (Căpitanul Dragan)? Informațiile le-am găsit la adresa <http://members.tripod.com/srbadija1/>, de unde se făcea trimitere la site-ul „Armatei Sârbe a Internetului”.

Iată cum se descrie căpitanul Dragan pe sine însuși: „Bine ați venit pe site-ul meu, de fapt pe site-ul «Reget Info». Eu sunt Regentul, cel mai mare hacker sârb și, după multe criterii, primul om al rețelei Internet iugoslave. După naționalitate sunt Om, iar după religie autoidolator (nu vă temeți, nu e vorba de nici o sectă, ci de faptul că eu cred într-un singur Dumnezeu, în mine însumi, altfel spus mă închin doar mie însumi și mă rog doar mie însumi). Sunt fondatorul și cel mai înalt funcționar al «Armatei Sârbe a Internetului» (SVI) – <http://come.to/svi> - o organizație publică a hackerilor. Potrivit spuselor altora, prin toată munca mea pe Internet am ieșit în evidență prin originalitate, rapiditate și prin efectele muncii mele. Toate faptele mele de pe Internet, chiar dacă neacceptate din punct de vedere moral și într-o oarecare măsură infraționale, le accept ca fiind ale mele!”

Iată un fragment dintr-un interviu cu căpitanul Dragan cu prilejul agresiunii N.A.T.O. asupra Iugoslaviei:

„...- Adunați din nou voluntari?

- Da, însă nu mai este vorba de aceeași categorie de voluntari care au luptat în războaiele trecute. Acum adun în forță voluntari și anume din rândul celor școliți, al tinerilor cu pregătire în domeniul computerelor, care vorbesc limbi străine, oameni cu diferite cetățenii, din diverse puncte ale globului pământesc. Asta întrucât nu e vorba de un război local, împotriva diverselor bande de teroriști, ci de un război global, împotriva Americii, a Alianței Nord-Atlantice și a slugilor acesteia.”

Pentru a fi primit în „Armata sârbă a Internetului”, cel interesat trebuia să depună următorul jurământ. „Mă jur că, sub steagul Armatei Sârbe a Internetului, mă voi lupta cinstit și drept până în ultima clipă pentru țara sârbească și poporul sârb, cu o singură dorință și anume ca SVI să controleze Internetul, iar SVI - toți sârbii, țara și lumea. Că sunt pregătit pentru a deveni membru al SVI dovedesc prin propria mea adresă de e-mail; fără teamă, mai adaug faptul că...”.

Dar cea mai cunoscută grupare de hackeri este, potrivit izvoarelor sârbe, „Crna ruka”. Înainte de toate, credem că este absolut necesar să vă oferim câteva informații despre originea acestei denumiri.

La 5 iunie 2002, www.google.com dădea 3 360 de locații pentru „crna ruka”. În limba română, „crna ruka” înseamnă „mâna neagră”. Sub această denumire a fost cunoscută organizația secretă „Unire sau moarte” („Ujedinjenje ili smrt”), înființată la Belgrad la 9 mai 1911, din care au făcut parte Gavriilo Princip, Nedeljko Čabrinović, Danilo Ilić, Trifko Grabez, Vaso Čubrilović, Veljko Čubrilović, Cvjetko Popović, Miško Jovanović, Mohammed Mehmedbašić și care a fost creată de

colonelul Dragutin Dimitrijević, cunoscut și sub numele de „Apis” (din latinescul „apis” - albină). Membrii grupului imprimau pe clădirile importante din Belgrad forma unei palme negre și de aceea lumea le-a dat numele de „Mâna neagră”. Organizația reunea ofițerii care au participat la Revolta din mai 1903 și la un atentat împotriva regelui Aleksandar Obrenović și a reginei Draga. Întrucât regina nu i-a putut dăruii soțului copii, iar ofițerii nu și-au primit salariile, atentatorii au vrut să-l proclame drept rege pe fratele acesteia. Istoricii sârbi afirmă că activitatea organizației „Crna ruka” rămâne pentru cercetători o mare taină. Este cunoscut faptul că Statul major al armatei sârbe trimitea ofițeri în Macedonia și în Serbia Veche pentru a organiza detașamente de gherilă pentru lupta împotriva forțelor Imperiului Otoman. Numai că lupta cu Turcia, iar mai târziu, cu Imperiul Austro-Ungar (sprijin logistic acordat organizației de tineret „Tânăra Bosnie” în seria de atentate asupra înalților demnitari ai Imperiului Austro-Ungar și chiar a moștenitorului tronului) nu a fost singura activitate a celor de la „Crna ruka”. Amestecul membrilor acesteia în evenimentele politice ale Serbiei a avut destui inamici, împotriva ei fiind însuși regentul Aleksandar Karađorđević și o parte a Gărzii regale, în frunte cu colonelul Živković, dar și președintele Guvernului, Nikola Pašić. După prăbușirea Serbiei, în anul 1915, colonelul Dragutin Dimitrijević a fost condamnat, la procesul de la Salonic din 1917, la moarte pentru plănuirea revoltei și a atentatului împotriva regentului Aleksandar. Numai că unii dintre membrii acestei organizații și-au continuat activitatea. Mustafa Golubić a devenit unul dintre șefii NKVD-ului (transformat mai târziu în KGB). Revizuirea procesului de la Salonic din 1953 a demonstrat că atentatul a fost înscenat de către regentul Aleksandar și de către Partidul Radical. Toți cei condamnați au fost reabilitați. Dar să revenim la Internet. Ibrahim Rugova, liderul albanezilor din Kosovo, reclama, la 20 octombrie 1998, că hackeri sârbi, membri ai „organizației teroriste Crna ruka”, au atacat indexul site-ului Centrului de Informații din Kosovo (albanez). În pagina web a albanezilor sârbi au inserat simbolurile naționale sârbe, scriind: „Bine ați venit pe pagina celor mai mari mincinoși și ucigași din lume” și „Fraților albanezi, această stemă va fi pe steagul vostru atâta timp cât va exista și steagul”.

Chiar dacă, ulterior, pagina web a fost refăcută, hackerii au revenit cu insistență, scriind: „Această pagină a fost hăcuită de către grupul de hackeri Crna Ruka. Viață lungă Serbiei Mari”. Incidentul este imediat mediatizat și de „The Associated Press” care, preluând informația de la publicația belgrădeană „Blic”, anunță că atacul a fost revendicat telefonic de un hacker membru al grupării „Crna ruka”. Site-ul www.infowar.com preia la rândul său informația și titrează două zile mai târziu, pe 22 octombrie 1998: „Serb Hackers Declare Computer War”.

Agenția independentă sârbă de știri „Beta”, citând BBC-ul, anunță că o ediție pe Internet a ziarului albanez kosovar „Zeri i Kosoves” („Glasul Kosovo-ului”), găzduită de un provider elvețian, a fost atacată de hackeri sârbi, aceștia inserând mesaje antialbaneze. Provider-ul elvețian a declarat că autor a fost un student iugoslav din Polonia (informație preluată și de mass-media germană). Hackerul l-a amenințat că, dacă mai găzduiește site-ul albanez, îi va șterge hard-disk-urile. Organizațiile internaționale pentru lupta împotriva hackerilor au oferit un premiu de 20 000 de dolari pentru prinderea acestui hacker. Dar el nu a fost prins niciodată.

Douăzeci de zile după atacul asupra ziarului kosovar albanez, scrie revista sârbească „Svet komputera” (Lumea computerelor) în numărul 11 din 1998, hackerii sârbi atacă paginile web ale publicației croate „Vjesnik”, fapt care a atras atenția mass-media din Croația și Iugoslavia, deoarece pe index a apărut un mesaj cu semnătura „Mâinii negre”. Cei de la „Vjesnik” au fost însă deosebit de satisfăcuți, deoarece au asociat numele grupei de hackeri cu acea organizație secretă sârbească, una dintre puținele organizații teroriste, spuneau ei, care s-a păstrat aproape un veac. Poliția croată a susținut că hackerii au acționat de pe teritoriul Iugoslaviei, însă nu se putea lua nici o măsură împotriva lor, Iugoslavia nefiind membră a Interpol. Drept răspuns, hackerii croați au atacat la sfârșitul lui octombrie 1998 site-ul „Bibliotecii Naționale a Serbiei”. Site-ul hackerilor croați, cu adresa <http://temat.4ever.cc>, considerat a fi cartierul general al celor două grupuri majore de hackeri – „Zadar Boyz” și „White Boyz”, a anunțat vineri, 30 octombrie 1998: „Vă informăm că organizația hackerilor croați a intrat în site-ul Bibliotecii Naționale Sârbe și a lăsat u mesaj. Este vorba despre o «răzbunare» pentru recentul atac asupra site-ului publicației «Vjesnik» și despre a vă aduce la cunoștință că nu e nici o problemă să dărâmi un site. Atacul a fost anunțat și terminat aseară la 23.00. Semnatarii sunt Positive Zero – Croatian Hackers, cu adresa de e-mail: positive0@yahoo.com.”

Redactorii revistei „Svet komputera” au căutat zile întregi pe Internet pentru a da de urma cuiva

din gruparea „Mâna neagră”. Căutarea nu le-a fost în van întrucât li s-a comunicat că, în scurt timp, vor avea prilejul să se întâlnească pe IRC cu doi dintre membrii grupei. Din discuția cu aceștia, s-a constatat că grupul „Mâna neagră” a „vizitat” în ultimul timp adresele <http://www.zik.com/>, <http://www.kosova.com/> și <http://www.vjesnik.com/>, afirmând că ei s-au ridicat în apărarea electronică a intereselor Iugoslaviei și nu vor renunța la atacuri asupra site-urilor care inserează minciuni despre situația din această țară. Cât despre „războiul electronic” cu croații, scrie în același număr al „Lumii computerelor”, ei consideră că sunt chit, întrucât sunt pentru „pace, dragoste și bunăstare pe întreaga planetă”. Drept dovadă stă și faptul că niciodată nu au șters fără a fi necesar date din paginile/site-urile web cu toate că au putut să o facă. Acesta a și fost motivul că la „Vjesnik” nu au schimbat decât indexul (pagina principală). Cei de la „Vjesnik” au susținut că hackerii sârbi nu au știut să schimbe și conținutul altor pagini web din același site.

Mai multe detalii, precum și atitudinea părții croate, le-am aflat de pe site-ul cotidianului croat „Vjesnik” (www.vjesnik.com), la rubrica „Tema zilei” din data de 29 octombrie, sub titlul „Vjesnik sub atacul Mâinii negre” – războiul informațional continuă prin atacul asupra paginilor electronice!”. În preambul scrie: „Miercuri dimineața au fost blocate temporar paginile web ale cotidianului «Vjesnik» și în locul lor a fost inserat mesajul «Mâinii negre», o organizație secretă de hackeri. Hackerii, care își spun «Mâna neagră» susțin că orice încercare de «măsluire a adevărului» despre sârbi va fi «împiedicată prin toate mijloacele». Aceeași organizație a atacat săptămâna trecută paginile publicației «Glasul Kosovo-ului» și ale Centrului informativ din Kosovo.” În locul conținutului indexului site-ului cotidianului croat a fost inserat un link către site-ul „Mâinii negre” unde, printre altele, scria că „Mâna neagră” dorește ca prin activitatea sa să schimbe imaginea falsă care înconjoară planeta și în care se vorbește despre sârbi ca fiind niște răufăcători. În finalul mesajului, „Mâna neagră” susținea că „Ultimul lucru pe care dorim e să amenințăm pe cineva, dar fiecare încercare de a falsifica adevărul vom încerca să o combatem prin toate mijloacele.” Directorul cotidianului croat, Ivan Božičević, afirma că hackerii sârbi nu doar că au atacat site-ul pentru a-și face reclamă, ci au dorit să insereze și un mesaj politic, avându-se în vedere că site-ul cu pricina avea la ora aceea peste 600 000 de vizitatori. Hackerii sârbi s-au folosit în acest atac și de lozincă „Noi nu suntem pentru război. Noi nu dorim nimănui răul”, mai scriu cei de la „Vjesnik”. De asemenea, se vrea trimitere la mass-media iugoslavă, care spunea că atacatorul a fost un student sârb în Polonia. O zi mai târziu, publicației iugoslave „Blic” (susțin tot cei de la „Vjesnik”) i s-a anunțat un membru anonim al „Mâinii negre”, confirmând că este vorba de o grupare de hackeri sârbi și anunțând continuarea „înlăturării minciunilor albaneze de pe Internet, dar și existența unor planuri asemănătoare pentru paginile Alianței Nord-Atlantice”. După spusele acestuia, „Mâna neagră” avea cinci membri, respectiv din Belgrad, Niš și din Macedonia, și că deja de un an de zile se lupta împotriva propagandei albaneze. A amintit și de faptul că în cauză nu erau membrii vreunui partid politic, ci persoane care „au găsit o metodă de luptă care le convine cel mai mult”. În același timp, spune, „Vjesnik”, cotidianul belgrădean „Politika” a publicat un amplu reportaj despre „războaiele balcanice pe Internet”, bazându-se tot pe comentariile unui asemenea hacker anonim, actualmente administrator, care „a ironizat” ideea că a fost vorba de un „student sârb în Polonia”. Croații continuă scriind cum că „Politika” amintește și de cazul atacului din Croația asupra sistemului informatic al Pentagonului, atac care, de fapt, a fost opera hackerilor sârbi pusă pe seama croaților. Tot „Vjesnik” spune că hackerii sârbi și-au făcut cunoscute telefonic intențiile și agenției „The Associated Press” care, pe 22 octombrie, a și publicat un material pe această temă.

Administratorii site-ului cu adresa <http://ds.org.yu/> anunțau miercuri, 11 noiembrie 1998: „Hackerii sârbi care-și spun «Crna ruka» au atacat site-ul Institutului «Ruđer Bošković» din Zagreb.”

Un amplu articol despre „Mâna neagră” („Die Schwarze Hand”) publică și Gerhard Mahlberg în „Frankfurter Rundschau”, în 1999, sub titlul „Cyberkrieg um das Kosovo, aus FR” (Infowar.de - <http://userpage.fu-berlin.de/~bendrath/liste.html> Quelle: FR, 31.8.1999), în care se spune că hackerii prosârbi au organizat 170 de atacuri în timpul bombardamentelor N.A.T.O. asupra Iugoslaviei. Informația este preluată din publicația londoneză „Sunday Times”.

Un atac al membrilor „Mâinii negre” este relatat câteva luni după încetarea agresiunii N.A.T.O. asupra Iugoslaviei și în numărul 282 din 7 februarie 2002 al suplimentului săptămânal „Dom i svijet” al Centrului de Informații Croat (www.hic.hr). Se spune că varianta de pe Internet a e-zinului (publicație care apare pe Internet) croat „Monitor” a fost atacată de așa-numita organizație

„Mâna neagră” din Serbia. Specialiștii în informatică croați susțin că este vorba de hackeri care cunosc excelent programul „Linux”. Se recunoaște totuși că hackerii anonimi nu au adus pagube importante acestei publicații, ci doar au dorit să arate că pot distruge paginile web ale „Monitorului”. De asemenea este amintit atacul asupra publicației „Vjesnik”.

Despre atacul hackerilor sârbi asupra cotidianului croat „Vjesnik” anunța și site-ul cu adresa www.xs4all.nl în rubrica „Balkan News”, sub titlul „Croats, Serbs Wage War on Internet”. Se mai spune că, a doua zi după atac, hackerii croați au atacat site-ul Bibliotecii Naționale Sârbe și au inserat anunțul: „Citiți Vjesnik și nu cărțile sârbești”.

O mulțime de detalii despre atacul grupării „Mâna neagră” se regăsesc în numărul din 29 octombrie al revistei iugoslave „NIN”, în articolul cu titlul „Mâna neagră pe Internet”, cu subtitlul „Apis cel virtual” și cu următorul preambul: „Războiul de pe rețeaua mondială a computerelor (Internet, n.n.) se poartă en gros. Sârbii au început (în sfârșit) să învingă.” Vizavi de site-ul publicației kosovare „Zeri i Kosoves” se spune că în locul membrilor U.C.K. („într-o poziție de eroi, cum ar spune patrioții Belgradului”) și a refugiaților albanezi udați de ploaie, pe site-ul www.zik.com a apărut un text nou: „Bine ați venit pe web site-ul celor mai mari mincinoși și criminali din lume”. Vulturul bicefal albanez a fost înlocuit cu cel sârb, iar sub el era scris: „Această stemă va rămâne pe steagul vostru atâta vreme cât voi, albanezii din Kosovo, vă veți afla în apropiere”. Provider-ul elvețian a descoperit că atacatorul este cineva care se dă drept un student sârb în Polonia, enervat de ceea ce se afla în rețea și care, în stilul lui Zorro, a hotărât să preia problema în mâinile sale. A amenințat provider-ul elvețian că dacă nu șterge site-ul kosovarilor albanezi îl va șterge el însuși. Pentru a-și susține amenințarea a distrus hard-disk-ul din biroul acestuia. Numai că necunoscutul student a lăsat o urmă: propria adresă de e-mail (poștă electronică), precum și cea a organizației „Mâna neagră”. Astfel, susține NIN, după optzeci de ani, Apis s-a aflat pentru a doua oară printre sârbi.

Dar cine sunt acești moderni „Apis”? se întreabă NIN. Pentru cazul „Glasul Kosovo-ului” elvețienii au acuzat puterea sârbă. Mass-media elvețiană a scris că „hackerii sunt apropiați ai serviciilor secrete sârbești” și că ceea ce s-a întâmplat este doar o parte a „epurării etnice” care se duce nu doar asupra albanezilor din Kosovo, ci, iată, și pe Internet. Dar, între timp, s-a făcut auzită și poziția celor de la „Mâna neagră”. NIN a reușit să-i contacteze pe doi dintre aceștia. Din motive de la sine înțelese, susține NIN, hackerii cu pricina au insistat asupra unui anonim complet. „Întâlnirea” cu ei s-a consumat prin IRC (un program pe Internet prin care se poate discuta pe viu cu alți internauți care doresc acest lucru). Pentru a demonstra că sunt ceea ce pretind, adică membri ai grupării „Mâna neagră”, ei au atacat, înainte de discuție, un site oficial din Bosnia-Herțegovina. Printre altele, hackerii au declarat că nu atacă site-urile iugoslave, cu toate că asta a fost prima lor intenție. Aceasta până când puterea nu se ia de ei. Dar dacă „...unui singur membru al Mâinii negre i se întâmplă ceva, întreg domeniul YU va zbura de pe Internet”.

Un alt atac al grupării „Crna ruka” se petrece la 20 iunie 1999, asupra portalului croat www.hr poslužitelj, deci în plină agresiune a N.A.T.O. împotriva Iugoslaviei. Iată ce scriu croații despre acest portal la adresa <http://cn.carnet.hr/arhiva>: „www.hr este unul dintre cele mai populare servicii ale CARnet. Este vorba despre catalogul consumatorilor www croați – un serviciu care este pagina neoficială de început a paginilor web din Republica Croația și care conține date despre mai mult de 3 000 de consumatori www croați”.

Tot în 1999, D. Sušanaj scria despre atacul celor de la „Crna ruka” asupra site-ului cu adresa www.hr următoarele: „Pagina de început a www.hr a fost schimbată, astfel că ea conținea stema sârbească și-i îndemna pe vizitatori «să caute adevăratul adevăr la adresa www.yu», unde, la fel, se găsește un catalog de adrese web, însă iugoslave.” Acest atac a coincis, scria același D. Sušanaj, cu acuzația celor de la CARnet și www.hr la adresa unui alt catalog croat, care ar fi copiat de la ei baza de date cu adrese de Internet.

Duminică, 28 martie 1999, cei de la www.earinfo.org.yu anunță atacuri ale hackerilor ruși asupra site-ului N.A.T.O. – www.nato.int și, respectiv, asupra celui al Marinei S.U.A. – www.nmimc1.med.navy.mil. La atacul sârbilor asupra site-ului N.A.T.O., www.nato.int, s-a folosit metoda ping. Prin această metodă se trimite spre server fișiere goale, care-l pot scoate din uz întrucât primește prea multe interogări, iar el nu le poate răspunde la toate. Sârbii au mai atacat și <http://wireless.jpl.nasa.gov/nato.html>, unde au lăsat o imagine cu Beaviss & Butthead cu un mesaj împotriva N.A.T.O.

Atacurile au fost concepute pe trei fronturi, scria Boris Ličina (www.borja.org), un jurnalist croat, la rubrica „Hack report” din magazinul informatic „Bug” și anume: hacking, spam și virusare. Citându-l pe Jamie Shea, purtătorul de cuvânt al N.A.T.O., el scria că pe adresa Alianței Nord-Atlantice soseau zilnic, la un moment dat, și câte 2 000 de e-mail-uri, în principal cu același mesaj: „F***k You!”. Pe lângă aceste e-mail-uri, existau și unele care aveau agățat și câte un virus. Chiar dacă forțele iugoslave au fost mai agile, scria același Boris Ličina, nici americanii n-au stat cu mâinile în sân. Astfel, un civil american din California, pe nume Richard Clark, a trimis în doar câteva zile, pe adresa guvernului iugoslav, 500 000 de mesaje, ceea ce l-a determinat pe provider-ul său să-i închidă contul de e-mail. Iar grupul de hackeri „Team Sp0it” a atacat și el, la rândul său, cinci site-uri sârbești. Pe de altă parte, coaliția unor hackeri europeni și albanezi, care se autointitulase „Kosovo Hackers Group”, a reușit să insereze în mai multe site-uri bannere cu textul „Free Kosova”. De atac nu a scăpat nici site-ul Universității din Novi Sad (www.unindy.ns.ac.yu), hackerul semnându-se TAC 99. Boris Ličina este de părere că, deși în spatele acestui e-război a stat mai mult mass-media decât acțiunea adevărată, asta nu înseamnă că în viitor situația nu va deveni mult mai periculoasă, cu urmări mult mai grave.

În numărul de dimineață, 28 martie 1999, publicația sârbă „Glas javnosti” scria, sub titlul: „Războiul hackerilor – până la exterminare”, următoarele: „Aseară nu a fost doborât doar «invizibilul» (aluzie la celebrul până atunci avion invizibil F-117, din care unul a fost doborât de apărarea antiaeriană iugoslavă, n.n.). Victimă a căzut și computerul central al marinei de război americane, dar și majoritatea site-urilor oficiale ale guvernelor statelor occidentale agresoare s-au trezit dimineața deosebit de afectate. Hackerii iugoslavi sunt iar stăpâni pe situație. [...] Țara noastră este atacată. Și noi, împreună cu ea! Dacă într-adevăr au existat, acum au încetat definitiv toate deosebirile ideologice. Abia acum se va vedea cât poate elita hackerilor sârbi. Și poate mult! (declara un hacker, n.n.). [...] În umbra acestei nemaivăzute agresivități, se duce din plin și celălalt – războiul virtual. Deocamdată câștigăm această bătălie.”

Luni, 29 martie 1999, www.earinfo.org.yu anunță că EuNet a pornit acțiunea denumită ALERT (http://alert.eunet.yu), iar Infosky va oferi servicii gratuite până la terminarea agresivității, aceasta pentru o mai bună informare și pentru răspândirea adevărului. În aceeași zi, tot www.earinfo.org.yu anunță că a fost atacat site-ul www.lang-bau.de și că, de această dată, a fost vorba de cineva din grupul de hackeri „Mâna neagră”.

Un an mai târziu, în martie 2000, apărea, la adresa www.landfield.com/isn/, un material scris de Ken Hyder și Nick Anning sub titlul „Serb experts hacked into Britain's Military Systems”, în care se referă la ceea ce se afirmă în The Sunday Express”, și anume că specialiștii iugoslavi au avut acces în perioada atacurilor N.A.T.O. la mari secrete militare aflate în sistemele informaționale. Răspunzând criticilor, oficialii serviciului secret britanic cunoscut sub numele de MI5 susțin că agenții săi au penetrat, la rândul lor, numeroase servere iugoslave.

Pe 6 aprilie 1999, Ellen Messmer, de la „Network World Fusion”, scria pentru CNN că, potrivit unor surse N.A.T.O., numeroasele atacuri asupra sistemelor informatice ale S.U.A. și N.A.T.O. sunt puse nu pe seama hackerilor obișnuiți, ci pe seama unor ofițeri ai armatei iugoslave („The same week a U.S. F-117A stealth fighter was lost over Yugoslavia, a NATO Web server here was shot down by denial-of-service attacks, which NATO sources strongly suspect came from the Serbian military, not independent hackers”). Independența este pusă sub semnul îndoielii și în cazul hackerilor ruși, care au atacat site-ul Orange Coast College și au inserat următoarele mesaje: „Asses out of Serbia”, “Russian hackers demand to stop terrorist aggression against Yugoslavia.” Iar de insultele lor, scrie aceeași autoare, nu scapă nici Bill Clinton și Monica Lewinsky. Și tot pe www.cnn.com a fost lansat în acea perioadă un sondaj de opinie on-line, tema fiind a se răspunde sau nu atacurilor hackerilor sârbi și prosârbi asupra S.U.A. și N.A.T.O. Au existat trei opțiuni de vot pentru acțiune: ofensiv (a hack for a hack), defensiv sau nici una, nici alta. La data documentării nu am mai putut afla rezultatele acestui sondaj, pe indexul site-ului CNN găsim un sondaj de opinie privind oportunitatea atacurilor aviației israeliene asupra orașului Gaza (pe 22 iulie 2002, majoritatea celor care au răspuns fiind împotriva atacurilor). Atacând un site albanez, un hacker sârb a lăsat următorul mesaj: „Această «pagină» a fost hăcuită de ...??? Nikita JM, MacroHard Group. Această pagină a fost prea plină de minciuni despre poporul SÂRB, de aceea a fost inevitabil a se face un asemenea lucru. De căutați adevărul, vizitați WWW.B92.NET. Mulțumiri Rusiei, grupărilor de hackeri HDT, KpZ, CHC, Legion2000, care au atacat Nimitz, și totodată mulțumiri celor de la Crna Ruka care, de

asemenea, luptă pentru adevăr în acest război media!!! SAMURAI RULLEZ ! Contactați macrohard@gmx.net sau poate - worldalbania@yahoo.com – admin mail, de asemenea hăcuit de mine”

Pe 14 aprilie 1999, BBC titra „«Serb hackers» on the rampage”

(<http://news.bbc.co.uk/1/hi/world/europe/712211.stm>), scriind apoi că alte 50 de site-uri au fost atacate, presupușii hackeri fiind, evident, cei sârbi, întrucât în paginile atacate apăreau sigla cu vulturul sârb și cuvintele „Kosovo is Serbia”. BBC mai scria că a fost atacat site-ul Ministerului Afacerilor Interne iugoslav, peste noapte apărând o versiune falsificată în limba engleză a conținutului acestuia, adăugând că oficialii iugoslavi sunt de părere că la mijloc se află propaganda americano-albaneză, atacurile pornind de pe un server american, cu un domeniu neînregistrat. În aceeași manieră au fost atacate serverele multor provideri, partide politice și firme, susținea M.A.I.-ul iugoslav. BBC mai dădea și o listă a site-urilor atacate în acea perioadă: viagra.com; eunet.com; winston.com; jamesbond.com; indianajones.com; mafia.com; kosova.com yu.com; slovenia.com; bosnia.com; sarajevo.com; warcrimesmonitor.com; arkan.com; tudjman.com, fără însă a da vreun indiciu asupra hackerilor.

Infrastructura Internet iugoslavă a fost de departe mai puțin afectată întrucât era slab dezvoltată. În plus, o agresiune militară stârnește mai multă revoltă în rândul cetățenilor țării agresate decât în rândul celor din țara/țările agresoare. CNN relatea la un moment dat, în timpul atacului N.A.T.O asupra Iugoslaviei, că un hacker olandez a reușit să „dărâme” un site iugoslav, enervat fiind de faptul că a găsit în el un text care spunea că membrii N.A.T.O. sunt noii naziști. Având pseudonimul Xoloth1, el a schimbat pagina anti-N.A.T.O. cu una pro-N.A.T.O. pe care a scris „Help Kosovo”. Site-ul atacat a fost www.pentagon.co.yu.

„În ceea ce privește activitățile hackerilor legate de ceea ce se întâmplă în clipa de față, cei mai activi sunt rușii. În deja cunoscuta pagină web cu adresa <http://www.hackzone.ru/> zilnic se inserează adrese care au avut de suferit atacuri și deseori sunt afișate și snapshot-urile browser-elor cu pagini heckerite. Trebuie observat faptul că, pe lângă hackerii ruși, în această activitate iau parte și mulți cunoscători ai computerelor din țările slave din jur. În ceea ce-i privește pe hackerii sârbi, din cauza importanței Internetului pentru Iugoslavia în acele zile, activitățile ilegale de pe domeniile YU aproape că au încetat, în caz contrar Occidentul amenințând cu sancțiuni. Însă adevărații cunoscători au avut la dispoziție, în străinătate, mijloace cu ajutorul cărora au lucrat cu hârnicie. Cineva spunea că hackerii sârbi au spart un mare număr de servere în Europa Occidentală. Francezii bine pregătiți din punct de vedere tehnic și-au dat seama că sârbi nu sunt niște sălbatici needucați, ci stăpânesc excelent noile tehnologii. Oare trebuiau să se întâmple toate acestea pentru a se ajunge la o asemenea concluzie?” - se întrebau cei de la revista sârbească de profil «Lumea computerelor?» Acest text a fost preluat de către Predrag Timotić și transmis în data de 11 mai 1999 membrilor listei de discuții „nato-agresija-na-srj” (N.A.T.O., agresiunea asupra Republicii Federative Iugoslavia) găzduită de www.eGroups.com, la „Subject” fiind trecut „[diskusije „nato-agresija-na-srj] Hakeri”.

La DefCon 8, adunarea hackerilor din iulie 2000, de la Las Vegas, adjunctul ministrului apărării S.U.A. a anunțat că sistemele de calcul guvernamentale suportă anual în jur de 21400 de încercări legale de penetrare și de atacuri, în fiecare zi șapte-opt dintre aceste atacuri arătând semne ale unui nivel mai înalt de coordonare, ceea ce demonstrează că pericolul cyberterrorismului din interior și din exterior este în creștere.

Numărul de atacuri sus-pomenit pare uriaș față de cunoscuta listă a lui Bill Wall, cunoscută și sub numele de „Bill Wall’s List of Computer Hacker Incidents” (www.totse.com), însă aceasta cuprinde cele mai cunoscute atacuri cu începere din 1961 și până în septembrie 2001. Iată pozițiile care fac referire la evenimente consumate în perioada agresiunii N.A.T.O. asupra Iugoslaviei în 1999. În 15 martie, Navy’s Medical Information Mgt Center din Bethesda este atacat de hackerii ruși, susținători ai Serbiei. Pe 24 martie, hackerii sârbi atacă site-ul N.A.T.O. din Bruxelles. În 20 aprilie, Patuxent River Naval Air Station este bombardată cu e-mail-urile trimise de un belgrădean, spam-ul conținând cuvintele „Serbia is here” („Serbia este aici”). O zi mai târziu, pe 21 aprilie, se pătrunde în serverele Aeroportului Național Washington. De 1 mai, hackerii danezi atacă un site iugoslav. În 5 mai țintă este site-ul Casei Albe (www.whitehouse.com). În 10 mai, mai multe site-uri guvernamentale americane sunt atacate de hackeri chinezi (DOE, Dep of Interior), drept represalii la atacul asupra Ambasadei Republicii Populare Chineze din Belgrad din 8 mai. Câteva ore după bombardarea ambasadei, hackerii

chinezi din grupul „Hong Kong Danger Duo“ au reușit să „doboare” site-ul www.whitehouse.com, lăsând în loc mesajul: „Protest USA’s Nazi action! Protest NATO’s brutal action”. De altfel, cu asemenea mesaje s-au trezit în acele momente mulți provideri americani. Diferite alte mesaje cu un conținut asemănător au inserat chinezii pe multe dintre site-urile care aveau legătură cu agresiunea N.A.T.O. asupra Iugoslaviei. Dar, majoritatea aveau același conținut: „Nu vom înceta până nu încetați voi.” Asiaticii au început să trimită un număr impresionant de e-mail-uri cu date nefolositoare, astfel că multe servere au fost nevoite să blocheze domeniul chinez cn.

Agresiunea asupra Iugoslaviei, scria Damjan Pelemiš în septembrie 1999, în publicația iugoslavă „Svet komputera”, i-a surprins pe informaticienii americani care se ocupă de securitatea sistemelor informaționale din S.U.A. în cea mai delicată situație, ei trebuind acum să lupte nu doar cu hackerii americani, ci și cu cei din străinătate. Cumva în același timp, F.B.I.-ul a pornit o acțiune de amploare împotriva hackerilor americani. Aceștia au înțeles însă că F.B.I.-ul a dezgropat securea războiului și au acționat ca atare. Astfel că site-urile Senatului și F.B.I.-ului au fost scoase din uz vreme de câteva zile. Site-ul Senatului a fost șters în întregime. F.B.I.-ul și-a deconectat singur serverul de la Internet, pentru siguranță. A încercat, de asemenea, să convingă lumea că pe site-ul său nu există informații secrete, ci doar publice. Aceiași hackeri au schimbat sigla „Central Intelligence Agency” cu „Central Stupidity Agency”.

Tot pe-atunci a pornit și cel de-al doilea val al atacurilor, în scenă intrând hackerii din grupul sârbesc „Srpski anđeli” (www.srpskiandjeli.org), care au luptat mai subtil. Prin site-ul lor, dar și prin lista adreselor de e-mail, peste 22 000, ei au trimis o mulțime de analize ale situației, precum și date despre distrugerile provocate de bombardamentele N.A.T.O și despre chinurile populației civile direct sau indirect afectate. Potrivit statisticilor, de pe site-ul lor au fost descărcați peste 100 GB de materiale și zilnic ajungeau peste 10 MB de mesaje prin e-mail. Asemenea site-uri au fost multe în Iugoslavia, fiecare localitate mai importantă informând prin acest mod despre evenimentele provocate pe plan local de către agresori.

Pe 26 mai urmează (din nou, scrie Bill Wall) site-ul F.B.I.-ului, iar pe 27 mai, site-ul Senatului S.U.A.. În prima zi a lunii iunie, este atacat site-ul Departamentului de Interne, iar pe 11 iunie, din nou, site-ul Senatului (atacatori fiind bulgarii din Varna Hacking Group).

Pe 12 mai 1999, pe site-ul <http://news.beograd.com/>, care preia informația de la o agenție de presă din S.U.A., se spune că hackerii din Hong Kong au reușit să pătrundă în pagini web ale Guvernului american și să insereze texte scrise în limba chineză prin care acuză S.U.A. pentru bombardarea ambasadei chineze din Belgrad.

În 1999, pe seama hackerilor sârbi sunt puse atacuri inclusiv asupra site-urilor companiei „Adidas”, respectiv a clubului de fotbal „Manchester United”. „Vjesnik”, preluând un articol de la „Internet Monitor” cu titlul „Hackerii sârbi au pornit războiul pe «rețeaua tuturor rețelelor»” și citat, la rândul său, în cadrul unui material publicat pe www.active-security.org, spune că, în urma atacului sârb asupra site-ului „Koha Ditore”, albanezii nu le-au rămas datori colegilor lor și au atacat site-ul ministerului sârb al informațiilor.

Dar cum în orice război există întotdeauna destui profitori, nici Iugoslaviei nu i-au lipsit asemenea indivizi. Sancțiunile economice, ieșirea Iugoslaviei din Interpol și agresiunea N.A.T.O. i-au încurajat pe destui hackeri sârbi să-și facă de cap. Iată ce scrie Katarina Bugajski despre acest lucru (<http://iwpr.net/>): „În vreme ce țara plângea sub povara sancțiunilor occidentale, în țară soseau pachete cu Viagra, cu bomboane de ciocolată, cu aparate foto-digitale, cu ceasuri de mână, cu tricouri și țigări cubaneze, totul mulțumită furturilor prin Internet nepedepsite. Pe de-o parte, motivul lor a fost dorința de a se răzbuna pe Occident pentru faptul de a fi izolat Iugoslavia, iar pe de-altă parte – pură distracție. Și totuși, profitul a fost pe primul loc. «De la o cutie de Viagra îmi plăteam chiria», spune zâmbind unul dintre hoții sârbi pe Internet. Furtul de Viagra a fost un adevărat hit întrucât aceasta sosea în pachete mici pentru care nu se plăteau taxe vamale.” Toate aceste lucruri erau posibile dacă intrai în posesia unui număr valid de carte de credit. „Când companiile își dădeau seama de fărădelege și refuzau să trimită în continuare cărțile, casetele video și DVD și compact-discurile în Iugoslavia, hackerii au contraatacat prin a trece la adresa expeditorului denumirea de «Serbia» în loc de «Iugoslavia». O altă metodă a fost de a se solicita expedierea pachetului la o adresă din Serbia, însă la țara de destinație se trecea «Ungaria» sau «Grecia». Când marfa ajungea în aceste țări, slujbașii poștali de acolo o redirecționau spre adresa din Serbia. [...] În timpul bombardamentelor din anul 1999, hackerii au creat intenționat haos în rețea. Ei își descriau acțiunile ca fiind «furturi patriotice» deoarece

jefuiau în exclusivitate site-uri americane și ale țărilor vest-europene care luau parte la bombardamente.”

În „Svet kompjutera” nr. 4/1999, Slobodan Popović le propunea cititorilor o listă cu site-urile unde se puteau accesa informații legate de Kosovo și despre agresiunea N.A.T.O. asupra Iugoslaviei:

Beograd.com – www.beograd.com/ nato

YuSearch – www.yusearch.com/ kosovo.html

I*Net – www.inet.co.yu

BeoCITY – www.beocity.com

BeoNET – www.beonet.yu

SUC (Serbian Unity Congress) – www.suc.org/ kosovo_crisis

SII (Serbian Information Initiative) – www.siicom.com

Srbija danas – www.yugoslavia.com/ News

SerbiaNow! – sn-ol.com

Pančevo On-Line – www.pancevo.co.yu

Krizni centar – www.yu

Free Serbia Net – www.freenserbia.net

Dnevni Telegraf – www.dtelegraf.co.yu

Politika – www.politika.co.yu

Naša borba – www.nasa-borba.co.yu

Večernje novosti – www.vnovosti.com

Blic – www.blic.co.yu

Glas javnosti – www.glas-javnosti.co.yu

Pobjeda – www.pobjeda.co.yu

Vreme – www.vreme.com

BK Telekom – www.bktv.co.yu

Radio B92 – www.b92.net

Studio B (BeoTelNet) – www.beotel.yu

Radio Jugoslavija – www.beograd.com/ radioyu

Radio Beograd I – www.beograd.com/ radio.ram

Radio Košava – www.kosava.co.yu/ live.ram

Radio Pingvin – www.beotel.net/ radiopingvin/ pingvin.ram

Beta – www.beta-press.com

SRNA – www.suc.org/ news/ srna

Tanjug – www.suc.org/ news/ tanjug

FoNet – www.fonet.co.yu

Media Centar Beograd – www.mediacenter.open-net.org

www.srpska-mreza.com/ mlad.

Site-ul oficial al R.F.I. – www.gov.yu

Fapte din Kosovo și Metohija – www.gov.yu/ koso-vo_facts

Ministerul Informației din Serbia – www.srbija-info.yu i www.serbia-info.com

Yahoo! News (știri ale unor agenții de știri) – dailynews.yahoo.com/ headlines

The Washington Post – www.washingtonpost.com

BBC News – news.bbc.co.uk

CNN – cnn.com ili europe.cnn.com

ITAR-TASS – www.itar-tass.com/ photo/ photoba-se.htm

South China Morning Post – www.scmp.com/ news/ index.idc

WorldNet Daily (selecție de știri din diferite izvoare) – www.worldnetdaily.com

ABCNews – www.abcnews.com

Fox News – www.foxnews.com

MSNBC – www.msnbc.com

The New York Times – www.nytimes.com

Problematica propunere de acord asupra provinciei Kosovo și Metohija se putea citi la www.transnational.org/ pressinf/ pf57.html. Detalii despre avionul invizibil doborât de apărarea antiaeriană iugoslavă: F-117A Nighthawk (www.af.mil/ news/ factsheets/ F_117A_Nighthawk.html)

Cheltuieli ale S.U.A. pentru întreținerea armatei sale: www.cdi.org/ sc/ javaclock.html.

Între pagubele virtuale și cele reale

Ce se urmărește prin acest război virtual, vă veți întreba? Întâi și întâi trebuie să vedem care anume sunt țintele. Fără doar și poate, primele servere atacate sunt cele care deserveșc legăturile operative între puterea politică, de decizie, și statul major, apoi între statul major și forțele armate, apoi între diverse comandamente. Pe același plan se situează serverele guvernului și cele ale diverselor agenții de securitate și spionaj, organisme și instituții guvernamentale. Motivul îl constituie, desigur, îngreunarea pe cât posibil a traficului prin asemenea servere și, în cel mai fericit caz pentru atacatori, blocarea ori chiar scoaterea completă din uz. Pe de altă parte, sunt atacate site-uri întregi sau doar pagini web ale organizațiilor sus-amintite, cărora li se adaugă de această dată și ținte din sectorul politic și civil: parlament, partide politice, organizații civice, organizații neguvernamentale, instituții financiare, organe mass-media. Scopul acestor din urmă atacuri îl constituie în primul rând propaganda, mai cu seamă dacă este atacat site-ul vreunui organ mass-media, care va reacționa imediat și va da atacului o amploare mult mai mare decât este situația în realitate. Care sunt însă modalitățile (țintele de atac, target-urile)?

Potrivit autorului site-ului din Republica Moldova având adresa <http://www.ournet.md/~xguard/xsecurity/dos.html>, ținte ale unui atac al hackerilor pot fi, cităm: „Spațiul de swap - Majoritatea sistemelor au alocate sute de megabaiți pentru spațiul de swap destinat cererii clienților. Astfel, spațiul de swap e folosit mai mult pentru procesele fiu care au o durată mică de viață. Deci, swap-ul nu e destinat unei utilizari «din plin», un atac DoS s-ar putea baza pe «umplerea» s(pațiului); Alocare de memorie kernel - Există o oarecare limită de alocare a memoriei de către kernel. Dacă se atinge această limită, sistemul va avea nevoie să fie restartat. Utilizând un algoritm potrivit s-ar putea aduce în «down» un sistem; RAM - O modalitate de atac care ar cere alocarea unei cantități substanțiale de RAM ar cauza probleme destul de serioase sistemului. Mai vulnerabile la acest fapt ar fi serverele de e-mail care nu prea au nevoie de RAM și, de obicei, au memorie operativă mai puțină; Hard-disk-ul - Umplerea hard-disk-ului unui calculator ar fi o metodă clasică de atac. Alt aspect ar fi deterioararea discului prin suprasolicitarea lui; Serviciile - Dezactivarea serviciilor ar fi scopul principal unui atac DoS. Însă atacarea IneTD-lui ar fi ideală, deoarece ar închide tot ce a fost pornit de inetd.”

Care sunt modalitățile de lucru ale unui hacker? Cum acționează acesta? Astfel, un individ pus pe rele va scana host-urile, respectiv serverele care găzduiesc anumite site-uri, aceasta pentru a descoperi calculatoarele din rețea. Dacă va primi un răspuns, asta înseamnă că există sisteme care au adresele respective și hackerul va încerca să le atace. O altă metodă este scanarea porturilor, asta pentru a identifica porturile deschise ale aplicațiilor și a le penetra pentru a accede în sistemul respectiv. În fine, DoS (Denial of Service – blocarea serviciilor), are drept scop împiedicarea accesului la sistem a persoanelor autorizate, schimbarea parametrilor sau a configurației sistemului, blocarea serviciilor, totul până la întreruperea sistemului.

Hackerii se folosesc în mod ilegal de orice vulnerabilitate a unui sistem de operare și pătrund în rețele de calculatoare, în calculatoare, site-uri și pagini web prin ocolirea sau chiar spargerea codului de acces (password). Sistemele de operare cele mai folosite de ei sunt „Linux” și „Windows NT”. Există programe special create de hackeri („Telnet” sau „Back Oriffice”) care se instalează fără ca proprietarul (utilizatorul) să știe și din acel moment noul stăpân devine hackerul. O armă redutabilă a hackerilor sunt așa-numitele „cookies”, programele care, instalate pe un calculator vizat, îi transmit atacatorului informații despre acesta, despre tipul de browser și despre sistemul de operare. Virușii sau viermii (worm), programe care se autoreproduc la nesfârșit, afectând performanțele calculatorului (mișcorează spațiul de pe hard disk, memoria, distrug mai mult sau mai puțin datele existente în memorie) sunt și ei, alături de caii troieni (programe care rulează în background și care execută comenzile hackerului), arme de temut.

Referindu-se la țintele unui război informațional în cazul României, generalul de brigadă Paul Vasile, șeful Direcției Planificare Strategică și Controlul Armamentului din Statul Major General, afirma în 2000, în „Cotidianul”: „Forțe ostile statului român pot provoca un război informațional având ca țintă afectarea gravă a infrastructurii vitale: transporturile feroviare; transporturile aeriene; sistemele de telecomunicații; metroul; sistemul financiar-bancar; sistemul fiscal;

procesele tehnologice industriale; sistemele de aprovizionare cu energie și gaze și nu în ultimul rând a mediului ambiant etc. Afectarea gravă a infrastructurii poate fi generată de neglijență, involuntar, dar și intenționat, de forțe răuvoitoare sau potrivnice statului român. O imagine realistă a urmărilor provocate de un război informațional, în care viața cotidiană ar putea fi bulversată complet, ar putea genera cele mai diverse manifestări, cum ar fi: lipsa căldurii, a gazelor, apei și energiei electrice în locuințe și centre industriale; scăderea producției; șomajul peste limitele prevăzute; tensionarea situației sociale, greve, încercări de lovituri de stat și nesupunerea maselor în fața legilor; blocarea sistemelor financiar-bancare și scăderea rapidă a puterii de cumpărare a monedei naționale; izolarea României față de comunitatea internațională, limitarea accesului la resursele strategice; influențarea deciziilor politice și ale organelor administrației de stat de către cercuri străine de interesele statului român. “

Cum se poate riposta la o asemenea situație: Răspunsul ni-l oferă același autor: „...trebuie identificate resursele necesare pentru achiziționarea de tehnologie informațională modernă care să permită: captarea, transmiterea, procesarea rapidă a informațiilor, împiedicarea agresorului să facă același lucru, denaturarea și dezinformarea. Trebuie să avem în vedere că în proiectarea și perfecționarea structurilor organizatorice trebuie să se țină cont de misiunile specifice războiului informațional pe care acestea le vor îndeplini în cadrul sistemului, cum sunt: criptarea, autentificarea și certificarea datelor și informațiilor: controlul accesului în sistemele de informații; detectarea și eliminarea software-ului afectat; securitatea rețelelor și sistemelor C4I2; desfășurarea de campanii imagologice; operații informaționale ofensive; sustragerea sau vicierea datelor; introducerea de informații eronate sau false; interzicerea accesului neautorizat la datele proprii; distrugerea fizică a elementelor sistemelor de stocare și distribuire a datelor.”

Relevantă în acest sens este și poziția locotenentului Dan Scutaru, publicată în „Observator militar” (www.presamil.ro): „...agresiunile electronice și psihologice din prima fază a oricărui conflict își pot atinge ținta în defavoarea noastră. Mărturie stau războaiele din Golf și fosta Iugoslavie.” Pe de altă parte, susține autorul, „Un viitor conflict este de neconceput fără război electronic”. Că Armata română are în vedere un asemenea război stă mărturie și existența Centrului 147 Război Electronic. Același autor afirmă în încheierea articolului pomenit:

„Perspectivele centrului sunt promițătoare. Se vor achiziționa mai multe echipamente compatibile cu tehnica N.A.T.O. Sunt așteptate un sistem integrat de război electronic, câteva mijloace de bruij radiolocație și un sistem de interceptare emisiuni satelit. Calitatea pregătirii militarilor și așteptata venire a promoției de ofițeri de război electronic și a tehnicii de ultimă generație sunt premisele unui viitor de siguranță și liniște.”

Aceeași importanță o acordă războiului electronic și locotenent-colonelul Mircea Șuteu, comandantul Batalionului 110 Război Electronic „Feleacul”, care a făcut parte din a doua (și ultima) promoție de război electronic pregătită în Academia de Înalte Studii Militare (conform <http://www.presamil.ro>): „Astăzi, suntem în fața emergenței unui al cincilea mediu de confruntare, de această dată imaterial, și anume cel informațional, în care suportul său principal îl constituie războiul electronic. [...] ...un specialist în război electronic se formează și ajunge să dea randamentul maxim în cinci-zece ani, deoarece el trebuie să cunoască mai multe limbi străine, să fie un foarte bun utilizator al tehnicii de calcul și al celei de război electronic și să aibă cunoștințe militare de nivel operativ, uneori strategic.”

Până unde ține războiul electronic și de unde începe cel informatic? În 2002, președintele George Bush a semnat Directiva Prezidențială pentru Securitate Națională nr. 16, prin care a cerut Executivului de la Washington să pregătească un plan care să specifice liniile directoare ale unui război în cyberspațiu. În substanță, spune „Monitorul de Cluj”

(<http://arhiva.monitorulcluj.ro/2003/>), „...este vorba despre a stabili în care circumstanțe Statele Unite ar putea sau ar trebui să lanseze o ofensivă informatică împotriva rețelelor din statele inamice.”

„Washington Post” susține că încă din 1999 exista la Pentagon o structură cu o triplă sarcină: de a pune la punct arme informatice care să fie lansate împotriva inamicilor, de a realiza o apărare informatică eficientă pentru a face față eventualelor atacuri și de a antrena viitorii soldați ai cyberspațiului. Numai că folosirea programelor sau a virusurilor capabili să anihileze rețelele informatice ale inamicului nu era îndeajuns de convingătoare, întrucât un program care, de exemplu, ar scoate din uz o centrală electrică pentru alimentarea unei baze militare ar întrerupe curentul și la un spital civil (pagubă colaterală). Iar un virus „asmuțit” asupra rețelelor informatice

ale unui prezumtiv adversar ar putea scăpa și în rețeaua mondială Internet și ar putea afecta grav și rețelele ale statelor prietene sau neutre.

Iată, așadar, că se știe foarte bine țintele, dar lipsește bisturiul. Dacă atunci când e vorba despre rețelele informaționale există serioase rețineri, coaliția antiteroristă ar putea totuși depăși, pe alte planuri ale luptei, o restricție majoră, spune în articolul său „Terorismul în dreptul internațional” (<http://www.presa-mil.ro>) colonelul prof. dr. Ion Dragoman de la Academia de Înalte Studii Militare, și anume „...renunțarea la pretenția de a avea «zero pierderi» de partea sa, într-un astfel de război, așa cum s-a întâmplat în cazul represaliilor împotriva Iugoslaviei din 1999.”

Metode de luptă pe Internet

La chestionarul trimis de noi, pe 10 iulie 2002, diverselor persoane care administrează site-uri, ne-au răspuns și cei de la www.hercegbosna.org. Astfel, la întrebarea „Care ar putea fi, după părerea dumneavoastră, metodele de luptă prin intermediul Internetului?”, ei ne-au trimis următorul răspuns: a) propaganda pentru cetățenii propriei țări și propaganda pentru cetățenii străini; b) scrisori deschise mijloacelor mass-media și instituțiilor; c) cearta prin intermediul forumurilor de discuții; d) atacuri ale hackerilor. În numărul din mai 1999 al revistei iugoslave „Svet komputera” („Lumea computerelor”), Dušan Dingarac scria: „Toți oamenii care nu se află în aceste vremuri grele în primele linii de luptă, dar sunt prezenți pe Internet, contribuie la răspândirea adevărului. Metodele de luptă sunt următoarele: site-urile web, news conferințele, mesajele e-mail, chat-ul, ICQ..., dar și altele.” Revenim acum la un mesaj găsit pe Internet, în arhiva forumului de discuții cu titlul „Forum o NATO agresiji na SRJ” (<http://groups.yahoo.com/group/nato-agresija-na-srj/message/29>), adică, în traducere, „Forumul despre agresiunea N.A.T.O. asupra R.F.I.”. Adresantul este Lazar Bošković, care pe 31 martie 1999, având la „Subject” „Prin Internet, împotriva NATO”, preia și retrimite recomandările pe care le-a primit de la revista digitală lunară gratuită (în format e-mail și www) „Pretraga i prezentovanje”, realizată de Dragan Varagić din Novi Sad. Revista a început în 1997 și și-a propus să se ocupe de problematica studierii Internetului. Astfel, sub titlul „Cum se poartă un război media prin intermediul Internetului”, se recomandă următoarele. „Nu trimiteți mesaje prin CC (carbon copy, n.n.) ci prin BCC (blind carbon copy, n.n.). Indiferent de situație, nu trebuie scăpat din vedere că o asemenea trimitere poștală poate fi ulterior folosită ca SPAM. Votați pe toate locațiile importante legate de situația noastră. Data trecută i-am învins, îi vom învinge și acum. Găsiți la adresele <http://dejanews.com/> și <http://liszt.com/> un număr cât mai mare de news grupuri și liste e-mail care se ocupă de politică generală și cu tematica Iugoslaviei și Kosovo-ului și participați la discuții. Aveți în vedere regulamentele acestor grupuri de discuții și trimiteți mesaje cu fapte care există îndeajuns în favoarea noastră. Fiecare discuție argumentată pe news grupurile serioase și pe listele de e-mail înseamnă foarte mult. De cum găsiți asemenea grupuri de discuții, schimbați-le cu toți cei care cunosc bine limba engleză. Trimiteți reacții la materiale la toate marile ziare și reviste de pe Internet care se ocupă de țara noastră. Sunt în vigoare aceleași reguli ca în cazul news grupurilor și a listelor de e-mail. Listele mijloacelor mass-media mai importante le puteți găsi la adresele <http://www.mediacentar.opennet.org/> și <http://www.totalnews.com/>. La <http://pretraga.co.yu/yuguide/> puteți găsi un director al motoarelor noastre de căutare, dacă doriți să găsiți adresele noastre cu cele mai actuale informații, din mai multe locuri. Utilizați mIRC și alte locuri pe Web unde se poate polemiza pe această temă. Recomandarea este să fie găsite discuții serioase, care cu siguranță există. Pe prezentările oficiale ale statelor găsiți adresele de e-mail ale politicienilor importanți și scrieți-le. Acest lucru nu vă va face poate plăcere, însă poate le va atrage atenția un (oarecare, n.n.) număr de scrisori. Într-un cuvânt, tot ceea ce găsiți și poate eventual să folosească în oprirea bombardamentelor, folosiți! Autor: Dragan Varagić.” Același e-mail conține câteva adrese ale liderilor americani (președinte, vicepreședinte, secretar de stat, prima doamnă etc.) și recomandarea ca mesajele

să fie scurte și clare: „No NATO in Kosovo!”. După care sunt date câteva recomandări pentru sârbii și aliații care sunt cetățeni americani, adresele de e-mail ale tuturor senatorilor americani și textul care li se poate trimite. Mesajul atrage atenția asupra faptului că: planul administrației Clinton constă în promovarea unor grupuri ale căror interese sunt terorismul, traficul cu stupefiante și destabilizarea unei întregi regiuni; atacul asupra Iugoslaviei este un atac asupra unui stat suveran, finanțat de contribuabilii americani etc.

Pe 7 aprilie 1999, Jovan Kurbalija le scria abonaților „Forumului despre agresiunea N.A.T.O. asupra R.F.I.” următoarele: „Vă invit să luați parte la acțiunea istorică, să participați la cel mai puternic de până acum atac asupra centrelor occidentale ale minciunii. În cadrul războiului convențional împotriva poporului sârb și a cetățenilor Iugoslaviei, așa după cum știți, se poartă și un război mediatic de satanizare a sârbilor și împotriva tuturor acelor care apără suveranitatea Iugoslaviei. Ținta atacurilor N.A.T.O. este ca întotdeauna să ne prezinte drept persoane fără chip și fără suflet. Ușor le este lor atunci să ne ucidă așa, fără chip. Nouă ne revine sarcina să arătăm că avem o față, că avem un obraz și că avem un suflet. Nouă ne revine sarcina să arătăm (lumii, n.n.) minciunile și propaganda lor. Treaba este foarte simplă, noi am pregătit totul pentru a se începe munca. Principalul meu consilier pentru probleme tehnice și principalul organizator al acestui proiect este americanul Paul Kneisel. Paul este editorul publicației «Internet antifascist». Este foarte priceput în luptele mediatic electronice și a reputat victorii importante împotriva organizațiilor fasciste de pe Internet. Își cunoaște jobb-ul.

Metoda este verificată, cu succes:

Trebuie ca în fiecare zi să trimiteți un scurt raport despre evenimentele din Iugoslavia la (propunerile de mai jos):

- 1) Lista principalelor publicații occidentale;
- 2) Lista grupurilor Usenet alese cu grijă;
- 3) Lista publicațiilor occidentale de mai mică importanță;

Despre ce trebuie scris: despre lucruri cotidiene, obișnuite, în legătură cu actuala situație. Despre cum suportați voi, oamenii obișnuiți, aceste evenimente. Vorbiți despre nenorociri, dar dați dovadă și de mândrie și de faptul că veți trece peste toate acestea. Vorbiți despre obiectivele civile distruse. Descrieți clipele grele prin care au trecut vecinii sau prietenii dumneavoastră civili. Evident că nu trebuie să le scriem despre obiectivele militare distruse și nici despre cel mai mic semn de scădere a moralului poporului. Vă rog ca în scrisorile dumneavoastră să nu atacați poporul american obișnuit. Tocmai pe americanul de rând dorim să-l atragem de partea noastră. Nu sunt ei de vină, ci Clinton și banda lui. Jumătate din locuitorii Americii sunt deja împotriva bombardării Iugoslaviei. Noi trebuie să păstrăm această jumătate și să-i atragem și pe alții. Nu luați în seamă o adunătură de idioți (care se pot găsi oriunde) și care-și vor exprima satisfacția că poporul Iugoslaviei este bombardat. Nu vă impacientați că engleza vă este (probabil) relativ inaccesibilă. Autenticitatea va transpare din fiecare cuvânt al nostru. Vă rog să trimiteți o copie a scrisorii dumneavoastră la adresa: Protiv-NATA@Yahoo.com. Noi vă vom informa despre cum evoluează proiectul. Invitați și prietenii (din Iugoslavia) să se implice. Cu cât suntem mai mulți – cu atât mai bine.

Iată acum câteva adrese la care ați putea să începeți a trimite imediat corespondența dumneavoastră.

Vă rog să trimiteți mesaje la toate adresele pe care vi le dăm. Valoarea publicațiilor de mai mică importanță este că, cu siguranță, vor lua în seamă acest atac al nostru și, prin articolele lor vor influența și marile publicații.”

Urmează adresele de e-mail ale publicațiilor de mare și mai mică importanță din Occident și ale news-grupurilor USENET.

Tot pe „Forumul despre agresiunea N.A.T.O. asupra R.F.I.”, Predrag Timotić scria la 16 aprilie 1999, având la „Subject” „Re: Apărarea țării prin Internet”, următoarele: „De la începutul agresiunii N.A.T.O. asupra Iugoslaviei, prin Internet se poartă un adevărat război. Un mare număr de patrioți îi «bombardează» cu e-mail-uri pe președintele american, pe vicepreședinte, pe senatori... Cei care se pricep atacă site-urile agresoare, le șterg și lasă mesaje cu adevărul despre Kosovo. În aceasta ne ajută foarte mult și frații ruși. Dacă doriți să ajutați și dumneavoastră în apărarea electronică a Iugoslaviei, votați pe site-urile unde s-a început votul asupra situației din Kosovo (de exemplu, dacă trebuie sau nu început un atac terestru asupra R.F.I.) ori bombardați-le cu e-mail-uri (programe care vă vor ajuta în aceasta puteți găsi pe

yu.forum.erotika). Vă atragem atenția să nu purtați pe Internet un război media greșit (în primul rând prin bombardarea cu e-mail-uri – scrisorile personalizate având un mult mai mare efect). La adresa alert.eunet.yu se află un îndrumar excelent. Îl redăm integral și vă rugăm să-l respectați.” Pe de altă parte, administratorii site-ului iugoslav <http://www.oaza.co.yu/> solicită implicarea tuturor celor interesați în realizarea unei cât mai bune pagini web. „Pe această pagină – spuneau ei – nu veți găsi minciuni CNN, ci veți găsi doar adevărul despre bombele N.A.T.O. și despre rezistența sârbă împotriva agresorului. Așteptăm și ajutorul dumneavoastră – trimiteți-ne informații verificate. Concetățenii noștri și prietenii din întreaga lume sunt bineveniți cu fiecare informație despre acțiunile oamenilor noștri din diaspora. Vom deschide o pagină cu scrisorile dumneavoastră, iar părerile le puteți expedia și la forum. De asemenea, avem nevoie și de ajutor în traduceri pentru a ține în același timp și o pagină în limba engleză, cu știri de ultimă oră. Dacă aveți posibilitatea de a insera pagina noastră web pe servere mai rapide și mai sigure din străinătate, anunțați-ne.”

Întrucât, în mod logic, majoritatea celor care asigură servicii internet (provideri) angajează pentru administrarea sistemului persoane cu oarecare experiență în domeniu, putem deduce că sfaturi de bon ton pe Internet nu pot da nici cei fără experiență, nici cei prea emotivi în situații cum a fost momentul Kosovo. Astfel că nici cei de la www.alert.eunet.yu nu puteau să sfătuiască cyber-războinicii decât așa cum au făcut-o. Textul care urmează vorbește de la sine.

„Vă rugăm să citiți și, în cele din urmă, să luați în serios conținutul acestui mesaj: de reacția dumneavoastră ar putea să depindă multe lucruri.

Ceea ce știți și singuri este faptul că poporul sârb se găsește în război cu cea mai puternică și mai bine pregătită din lume națiune din punct de vedere tehnic.

Aportul dumneavoastră la situația actuală din țară poate să fie constructiv. Pe de altă parte, modul greșit de acțiune poate fi deosebit de periculos. Nimeni din Iugoslavia nu are dreptul să ofere vreun motiv pentru a ne fi întrerupt accesul la Internet, rețeaua globală care ne poate ajuta să facem auzită și cealaltă parte a conflictului.

Pe lângă războiul cu bombe și rachete de croazieră, împotriva noastră se poartă și unul dintre cele mai perfide războaie mediatice înregistrate în acest secol (XX, n.n.). Războiul se poartă pe toate canalele media, dar cel mai mult prin televiziune și pe Internet. Vă atenționăm asupra mai multor lucruri.

SPAM pe Internet

Emoțiile sunt mai puternice decât o gândire rațională, lucru de care nu ne putem mira. Nu se pune în discuție nici apărarea țării. Dar, în intenția de a dovedi mărinimia noastră, suntem câteodată în situația de a pierde măsura. O parte din utilizatorii locali de Internet încearcă să-și exprime dezgustul față de agresiunea N.A.T.O. asupra țării noastre, astfel că trimit un mare număr de mesaje de revoltă la multe forumuri de discuții (newsgroups), inclusiv la cele care sunt specializate pe anumite probleme. Chiar dacă în esență suntem de acord cu mesajele și conținutul lor, trebuie să vă atragem atenția asupra unei situații deosebit de periculoase: Iugoslavia este pândită de realul pericol al decuplării de la Internet!

În principal, se întâmplă două lucruri:

- dacă sunt expediate spre adrese nesemnificative, asemenea mesaje se consideră a fi SPAM-uri – cu conținuturi nedorite care încalcă regulile bon tonului pe Internet (așa-zisul netiquette). A persevera într-un asemenea comportament poate să pună sub semnul întrebării toate domeniile, ba chiar întreg domeniul yu pe «lista neagră», ceea ce se află doar la un pas depărtare de deconectarea de pe Internet a domeniilor (noastre, n.n.) de pe Internet;

Chiar și atunci când mesajele sunt expediate la forumurile de discuții și la «anumite» adrese de poștă electronică, asta poate deranja mass-media celeilalte părți. De exemplu: CNN a început «să piardă» în multe votări (on-line, n.n.) pe care le organizează cu prilejul așa-zisei «campanii îndreptățite în Iugoslavia», mulțumită în principal voturilor trimise din țara noastră. Aceasta, dar și multe alte case de editură, cărora li se întâmplă lucruri similare (de pildă CBS, Sky, BBC și altora asemenea), au o audiență suficientă pentru a solicita deconectarea Iugoslaviei de la Internet sub masca SPAM-urilor.

Asta nu putem permite!

Expedierea mesajelor electronice

Da sau nu

Să nu dăm prilej deconectării! Dacă utilizăm forumuri de discuții pentru a ne exprima gândurile,

(ceea ce trebuie să facem oricum), atunci să respectăm niște reguli:

Atenție! – Aveți grijă la munca pe Internet.

Este posibil ca, de un e-mail, cineva să vă trimită agățat un virus în vederea punerii în execuție a unui program. Virusul nu poate să se activeze dacă vă veți limita la citirea mesajului. Pentru a rula programul care v-a fost trimis, trebuie activat de dumneavoastră înșivă printr-un click asupra fișierului agățat, fie imediat, fie mai târziu. Prin aceasta oferiți posibilitatea accesului la fișierele de pe calculatorul dumneavoastră sau folosirea în sensul rău a calculatorului dumneavoastră pentru «atacul» asupra altor sisteme. Cel mai bine este ca mesajele dubioase pe care le-ați primit de la necunoscuți să le ștergeți de îndată.

NU – nu încercați să expediați viruși ori programe asemănătoare oamenilor care se află de cealaltă parte a baricadei, îndeosebi la adresele guvernului american ori ale instituțiilor militare. Există apărare împotriva unor asemenea lucruri și nu va fi nici un folos de pe urma încercării dumneavoastră. Aidoma altor acțiuni, și aceasta va contribui la o posibilă deconectare a țării noastre de la Internet.

DA- să folosim în exclusivitate grupurile de discuții pentru expedierea unor asemenea mesaje. Un grup care se ocupă de competiții de Formula 1 ori de programarea în programul Java nu sunt nicidecum bune pentru asemenea mesaje.

DA – să dovedim că suntem umani: apelurile noastre împotriva uciderilor și a distrugerilor din țara noastră trebuie să le exprimăm utilizând un vocabular decent și nicidecum vulgar, expresii gâlcevitoare ori umilitoare; să dăm dovadă de verticalitate și cultură în utilizarea Internetului ca mijloc mass-media.

NU – să nu expediem un număr mai mare de mesaje cu același conținut la aceeași adresă, SPAM-uri, oricum nu persoanelor ori organizațiilor care se află în afara cercurilor politice. Aceasta se numește și bombardament cu e-mail-uri, însă efectele nu sunt importante ci, dimpotrivă, după saturarea de scurtă durată a sistemului de e-mail a destinatarului să fie limitat acceptul unor asemenea mesaje «înainte» de a ajunge la serverul destinatarului. Oricât ne-ar fi de greu din cauza a ceea ce ni se întâmplă, să nu uităm că în lume există totuși și dintr-aceia cărora puțin le pasă de chinul nostru. Să respectăm cu demnitate o asemenea atitudine străină. Să trimitem e-mail-uri în exclusivitate la adresele care sunt deschise pentru gândire.

DA – încercați să găsiți corespondenți care sunt dispuși să asculte ori sunt însărcinați să-i asculte pe alții (mass-media etc.), uitați-vă la listele anexate.

DA – Pentru corespondență utilizați limba engleză. Cea mai mare parte a corespondenților vor primi astfel mai ușor și mai rapid informația dumneavoastră. Dacă aveți probleme în a scrie în engleză, rugați pe cineva mai pregătit în această problemă.

DA – străduiți-vă să scrieți mesaje scurte și pline de esență, care să aibă un mesaj anume. Evitați ca în mesajele dumneavoastră să săriți de la o temă la alta.

NU- nu permiteți ca durerea și mânia dumneavoastră să fie exprimate prin cuvinte indecente.

NU – nu arătați că evenimentele afectează totul în Iugoslavia și concentrați-vă asupra suferințelor omenesii.

DACĂ – vă adresați mai multor oameni, din indiferent ce motiv, folosiți «Bcc» (blind carbon copy) și nu «Cc» (carbon copy). Astfel se evită folosirea abuzivă (întâmplătoare sau intenționată) a adreselor de e-mail pe care utilizatorul le poate primi și pe care nu le-a primit mai înainte – în măsura în care e-mail-ul pe care l-ați trimis cuiva nu este efectiv transmis și pentru că nu este transmis primiți un mesaj pe care nu l-ați mai primit anterior, contactați-vă provider-ul [...].

ATENȚIE! – Toate e-mail-urile care ajung la cunoștința dumneavoastră sunt cu siguranță notate undeva ori sunt mai târziu supuse analizei. Aveți grijă să nu-i compromiteți pe oamenii noștri care trăiesc ori lucrează temporar în străinătate. Nu socotiți niciodată că asemenea mesaje sunt sigure, iar conținutul lor să nu fie legat de situația actuală: poate asemenea mesaje vor determina cheltuirea de resurse umane și materiale ale agresorului. Conținuturile ideale ale unor asemenea mesaje sunt: poezia, rețetele culinare, istoria ș.a.m.d.

DA – căutați locații pe care există posibilitatea de a se vota pentru sau împotriva folosirii forței în Iugoslavia; încercați să găsiți informații care ne folosesc, îndeosebi pe locațiile principalelor case de editură din Occident. Vizitați toate site-urile guvernamentale și militare ale statelor N.A.T.O.

Trebuie și nu trebuie să le vedeți în detaliu, țelul este înregistrarea fiecărui «hit» de pe un asemenea site și determinarea administratorului să cheltuiască timp pentru analizarea logo-urilor.

NU – nu vizitați prezentațiile iredentiștilor albanezi și mass-media UCK și celelalte (vezi anexa).

Administratorii acestor site-uri trebuie să știe că sunt vizitați de puține persoane!

Dacă realizați prezentări (web, n.n.)

- Siliți-vă ca prezentările dumneavoastră să fie cât mai puțin colorate. Pentru fundal să predomine culoarea neagră ori o alta, tot întunecată.

- Puneți link-uri spre site-urile pe care considerați că trebuie să le vadă oamenii sau cel mai bine puneți un link către <http://alert.eunet.yu>, iar utilizatorului alert@Eunet.yu trimiteți-i link-urile recomandate.

- Vedeți recomandările detaliate pentru realizarea de prezentări în condițiile de dinainte de campania antirăzboi.

Ne urmăresc, ne observă și ne ascultă!

Nu puneți sub semnul îndoielii informațiile despre „coloana a cincea”. Nu e vorba despre paranoia și despre vânătoarea de vrăjitoare, așa cum probabil v-ați gândit în prima clipă, ci de fapte.

Mărturie sunt mutarea masivă a locatoarelor în Kosovo și în alte părți ale țării și bruierea sistemelor noastre de legătură cu ajutorul stațiilor de brujaș găsite în interiorul R.F.I.

Agentura străină se află și acționează aici.

Pe lângă confruntarea militară directă și vizibilă, împotriva țării noastre se poartă deci și un război „nevăzut”, cuprinzător, de informare și de spionaj. Informațiile de pe teren sunt de un interes vital pentru planificarea atacurilor aeriene și nu numai, precum și a formelor agresiunii. Fără rapoarte de pe teren, N.A.T.O., ca oricare alt agresor, este „orb” și îi sunt îngreunate planificările și realizarea unor noi acțiuni.

De aceea, aveți grijă de știrile pe care trimiteți le prin intermediul poștei electronice și a convorbirilor telefonice cu familia și prietenii, acasă ori în străinătate.

Nu dați detalii despre obiectivele lovite, despre gradul de distrugere, despre momentul lovirii și alte informații asemănătoare. Asemenea date sunt neprețuite pentru informatorii N.A.T.O., îndeosebi când le primesc regulat și gratuit.

În toate aceste comunicații încercați să fiți cât mai indeciși. Părinților, prietenilor și cunoscuților dumneavoastră le va fi îndeajuns să afle că sunteți bine.

E posibil, dar și credibil ca serviciul american de spionaj să asculte convorbirile telefonice (inclusiv rețelele de telefonie mobilă GSM și NMT, sistemele de paging etc.) și să filtreze toate mesajele electronice între sârbi și restul lumii.

Nu vă încredeți în algoritmii de cifrare RSA/PGP, cu atât mai mult în (compactarea, n.n.) zip și arj cu parolă și în alte metode «la îndemână».

Chiar dacă trebuie să transmiteți o știre care i-ar putea fi de folos inamicului pentru a afla dacă și în ce măsură și-a dus la îndeplinire planurile, atunci faceți-o în cea mai ocolitoare, asociativă și inaccesibilă manieră. În aceste zile am demonstrat că suntem un popor care are ceva mai mult decât agresorul.

Totuși, cel mai bine este să vă abțineți de la asemenea metode de informare.

Evitați publicarea oricăror informații care ar putea fi de folos inamicului!

Dacă primiți un e-mail jignitor:

În primul rând nu vă enervați. E-adevărat, nu e ceva prea ușor în timpurile când emoțiile vă potopesc, însă este exact scopul pentru trimiterea unor asemenea mesaje!

Despre ce este vorba? Pesemne că asemenea mesaje de e-mail sunt trimise de utilizatorii de diferite naționalități, cu adrese fictive (Yahoo, Hotmail etc.). Asemenea mesaje se trimit în mod automat, cu mesaje identice, la mii de adrese, cu intenția de a sufoca legăturile noastre prin Internet.

Dacă le răspundeți, înseamnă că și-au atins scopul.

Așadar, nu răspundeți la asemenea mesaje. Trebuie doar să le ignorați, mai exact să le ștergeți imediat.

Un al doilea motiv e că nu există o rațiune pentru a răspunde întrucât eventualele dumneavoastră replici nu le citește nimeni. Chiar de primiți vreun „răspuns” este vorba despre un text pregătit dinainte, «generic», trimis de computer și nu de o persoană anume.

Răspunzând la asemenea mesaje ne facem nouă înșine rău întrucât sufocăm Internetul prin comunicații sterile, care se pot mult mai bine utiliza.

Încheiere

Cu siguranță că nu este necesar să vă explicăm cât de mare este puterea Internetului. Fiți conștienți că agresorul a angajat resurse însemnate în intenția de a influența utilizatorii de

Internet din Iugoslavia, având în vedere faptul că ne consideră un grup țintă de elită. Nu puneți la îndoială faptul că, în viitorul apropiat, se va ajunge la o escaladare a evenimentelor «și» pe Internet. Aceasta este o sursă majoră pe care trebuie să o utilizăm în campania intensivă de chemare împotriva agresiunii pactului N.A.T.O., însă totodată trebuie ca prin acest mijloc să păstrăm cu orice preț legătura cu lumea.

Să nu permitem ca purtarea noastră să fie considerată drept motiv pentru deconectarea Iugoslaviei de la Internet.

Să nu dăm ocazia serviciilor de informații ale pactului N.A.T.O. să se folosească în interesul lor de informațiile pe care le plasăm pe Internet.

Să nu le permitem să ne dea afară din rețea.

Dacă tot cred că suntem o elită intelectuală, să le arătăm că și suntem cu adevărat!

Nu vă zgârciți să trimiteți acest mesaj prietenilor, utilizatorilor de Internet din Iugoslavia. Războiul se poartă pe Internet.

Un război pe care nu avem voie să-l pierdem.” (sublinierea ne aparține, n.a.).

În continuare, au fost date adresele unde se putea vota împotriva agresiunii N.A.T.O. (browser sau e-mail): <http://cgi.pathfinder.com/time/daily/poll/; 0,2637,kosovous,00.html>;

<http://cgi.pathfinder.com/time/daily/poll/; 0,2637,groundtroops,00.html>;

<http://cgi.pathfinder.com/time/daily/poll/; 0,2637,serbiabomb,00.html>;

<http://www.cnn.com/CNN/Programs/TalkBack/>; http://www.canoe.ca/CNEWSKosovo/990330_kosovo.html;

<http://www.cnn.com/>; <http://www.express.de/extra/umfrage/>

<http://www.centraleurope.com/>; <http://www.cbs.com/navbar/news.html> <http://abcnews.go.com/>;

<http://www.cgi-world.com/>; <http://www.businessweek.com/1998/11/b3569104.htm>;

<http://witi.com/Newsrec/Polls/090596/>; <http://cgi.pathfinder.com/time/daily/poll/drug.html>.

Prin e-mail se putea vota la următoarele adrese: yourcall@sky.co.uk; vijesti@hrt.hr;

<http://www.cbs.com/navbar/feedback.html>; <http://www.coil.com/~ggorka/media.html>.

Din păcate, astăzi la aceste adrese nu mai putem vedea rezultatele voturilor. De asemenea, au mai fost date adresele browser ale principalelor publicații mass-media din țările ce făceau parte din N.A.T.O.

Site-uri care țin evidența principalelor atacuri ale hackerilor pe Internet și unde se pot găsi referiri la multe din atacurile din perioada agresiunii N.A.T.O. asupra Iugoslaviei sunt următoarele:

www.2600.com; www.attrition.org; www.hackzone.ru.

Sub titlul „Cu Internetul împotriva bombelor”, Dušan Dingarac scria în numărul din aprilie 1999 al revistei iugoslave „Svet komputera” următoarele: „Prin Internet s-a răspândit și vestea că agențiile americane de spionaj controlează întregul trafic pe Internet pentru a descoperi informații despre țintele atinse. Pe lângă această știre a urmat și un apel pentru evitarea descrierii țintelor lovite, pentru ca dușmanul să rămână dezorientat”.

În timp ce lucram la cartea de față, l-am întâlnit întâmplător, la o conferință de presă ținută la Timișoara, pe publicistul Sorin Bogdan, corespondent de război pentru una din televiziunile din România în timpul agresiunii N.A.T.O. asupra Iugoslaviei. Ne-a confirmat faptul că nu a fost nici o greutate să cunoască în timp util, el sau alți corespondenți de război aflați pe vremea aceea la Belgrad, de la relațiile lor dintr-un loc sau altul de pe teritoriul iugoslav, care au fost efectele unui bombardament sau al altuia. Cum „Echelon” nu dormea 24 de ore din 24, atacatorii puteau ști ușor dacă rachetele sau bombele lor și-au atins ținta ori nu și care au fost pagubele. E lesne de înțeles că în tot timpul agresiunii N.A.T.O. o mare parte din personalul și tehnica utilizate de sistemul de spionaj global sus-pomenit au fost cu ochii și urechile la Iugoslavia. De aici și atacurile repetate asupra unor ținte, despre care s-a aflat imediat, de ce nu și din citirea e-mail-urilor, ținte care nu au fost distruse la primul ori la următoarele bombardamente.

La 10 decembrie 1998, Irina și Slobodan Stojičević lansează pe forumul de discuții „Serbian Forum”, găzduit de groups.yahoo.com/group, ideea că, cităm: „...Acesta este primul război din istorie în care se utilizează și Internetul”. Tot ei fac apel la o coordonare a luptei prin acest modern sistem de comunicare și, totodată, de propagandă. Iată și textul acestui mesaj: „Câte mai poate omul să asculte și să vadă! Păi acesta nu e războiul privat al fiecăruia dintre noi. Nu, fraților și domnilor, nu este nici cuminte și nici eficient ca fiecare dintre noi să se joace de-a războiul atunci când i se pare lui interesant.

Unii recomandă să fie trimise «spam»-uri, iar alții, cu atât mai mult, ne roagă să trimitem doar ceea ce este cel mai urgent întrucât și așa sunt serverele supraaglomerate...

Propun...

Să ne organizăm și să contactăm statul major ori să găsim pe cineva anume (propunerile sunt binevenite) și să cădem de comun acord asupra unei anumite strategii pe care să o aplicăm cu toții.

Dacă ne închid domeniul (de Internet, n.n.) YU (sincer să fiu eu personal nu cred că ar face un asemenea lucru), vom fi cu toții în pierdere, însă o pierdere cu mult mai mare va suferi Serbia. În afară de asta, nu știu dacă i-a mai picat cuiva în minte:

Acesta este primul război din istorie în care se utilizează Internetul.

Cred că inamicul a și pus la punct (teoretic și practic) atât strategia, cât și partea practică și, pe Dumnezeu meu, chiar și tactica întrebuițării noului armament.

Poate i se va părea cuiva că a face un asemenea lucru este o exagerare, însă o asemenea metodă de comunicare poate (și este) să fie folosită ca o armă.

Trebuie oare să stăm și să așteptăm să ne fie țintiți providerii asemenea televiziunilor?

Există pregătite locații de rezervă pentru servere (ordine de război)?

Există vreo instituție care să coordoneze munca pe Internet în condițiile «stării de război»?

Mie mi se pare logică și organizarea de secțiuni în cadrul Comandamentului Suprem...

Mijlocul de comunicare căruia îi aparține viitorul, dar și o parte din actualitate (iar cu ele viețile noastre și ale copiilor noștri) nu trebuie să ajungă a fi jucăria oricui...

Acestea sunt doar câteva gânduri pe această temă.

Propunerile sunt binevenite.

Slobodan

P.S. Armata noastră are un site al ei?"

Cu siguranță că ați observat o anumită inadvertență: deși mesajul a fost trimis pe 10 decembrie 1998, autorul deja spune: „Trebuie oare să stăm și să așteptăm să ne fie țintiți providerii asemenea televiziunilor?” Ori atacul asupra radioreleelor și a sediilor televiziunilor publice s-a întâmplat abia în 1999, când experții N.A.T.O. au considerat că radioul și televiziunea s-au transformat în arme propagandistice periculoase pentru succesul acțiunii aliaților. Ca atare, este evident că e vorba despre un tânăr (posibil student) care folosea programe de calculator copiate de pe Internet sau de la prieteni și care aveau un anumit termen pentru testare (și apoi de comandare). Pentru a evita ajungerea la termenul final de utilizare, cea mai simplă metodă este fixarea ceasului intern al calculatorului la o dată anterioară datei reale. Așadar, timpul real al expedierii mesajului de mai sus este cu certitudine situat undeva după primele bombardamente ale N.A.T.O. asupra releelor radioteleviziunii iugoslave din primăvara lui 1999. Altfel nu se putea face o paralelă între țintirea releelor de televiziune și atacul asupra providerilor din Iugoslavia. Cert este și faptul că autorul a exagerat ori nu a putut cuprinde realitatea: una este să distrugi rețeaua de telecomunicații clasice a inamicului, alta e să-i întrerupi accesul la rețeaua de sateliți pentru servicii Internet (aflați majoritatea în proprietatea țărilor membre ale N.A.T.O.). Fiindcă una e să bombardezi releele de radioteleviziune, aflate, de regulă, izolate de zonele rezidențiale, și alta e să ataci sediile providerilor, aflate în copleșitoarea majoritate a cazurilor în cele mai aglomerate zone citadine. Or N.A.T.O. adoptase deja ideea loviturilor chirurgicale, ineficiente totuși în asemenea zone, dovadă fiind și miile de „pagube colaterale”.

Afirmația noastră precum că este vorba de un „pirat” de software sunt și mesajele la care autorul de mai sus a replicat și care sunt toate datate 23 aprilie, respectiv 22 aprilie 1999.

Astfel, un anonim ce semna cu „ex Singidunum” (Singidunum, denumirea antică a Belgradului), îndemnând la o companie de lovituri mobile, propunea un alt soi de atacuri: „Îi invităm pe toți membrii lui exSingidunum să ni se alăture în campania loviturilor mobile. SerbSaver este un program [...] care permite alegerea telefoniei mobile [...], se stabilește contingentul de numere care vor fi contactate (numere de 6 cifre, fără introducerea prefixului) și atunci se apasă pe buton: «Haideți cu toții la atac», apoi «Văzduhul vibrează de parcă arde cerul. Se pregătește furtuna.»

O.K. Nu vă impacientați. El (telefonul mobil, n.n.) transmite următorul mesaj: «Have you killed your Serb today». După comentariile actuale, are efect asupra generației de silicon CNN (americani), dar și asupra celorlalți. Încercați și alegeți o țară fascistă în care este zi, astfel încât să aibă la ce să mediteze până la sfârșitul zilei (garantează vise rele). Opinia publică este deosebit de importantă în țările fasciste, iar dacă aceasta își intensifică presiunea asupra guvernului său, cu atât mai bine pentru noi. Dacă le reușește această campanie, atunci se știe cine este următorul și următorul... Această misiune nu e doar pentru a contribui la apărarea

sârbilor, ci a tuturor popoarelor [...]. Distribuți-l (programul CompuSerb, n.n.) prietenilor dumneavoastră din toată lumea deoarece dacă ne întrerup (domeniul YU, n.n.), ori dacă ne distrug infrastructura în cadrul căreia intră și telefonica, nu vom putea acționa cu toate forțele, astfel că toți cei din afara domeniului nostru ne vor fi o prelungire a mâinii. Nu vor putea ei (dușmanii, n.n.) să întrerupă și toate celelalte domenii în care există măcar și un singur sârb sau prieten.”

Dar iată și... aspectul tehnic al problemei: „Pentru un singur contact sunt necesare 10 secunde, ceea ce înseamnă 360 de contacte într-o oră, iar cu trei programe lansate în același timp, aproximativ 1 100 de contacte. Închipuiți-vă că acționăm în medie măcar trei ore pe zi (deci 3 300), ceea ce ar fi la 200 de utilizatori, de exemplu, în jur de 650 000 pe zi, ceea ce nu e chiar o cifră de lepădat.”

Autorul mesajului mai scrie și un P.S.: „Am contactat câțiva webmasteri, astfel că în curând îl vom putea aștepta pe vreuna din paginile web.”

În aceeași zi, Vasja Bojanić scria: „1. Vă recomand tuturor acelorora care existați să citiți cartea lui Noam Chomsky «Ce dorește de fapt America». Puteți afla cu cine avem de-a face și ce mai vor să facă, astfel că nu trebuie să vă surprindă. 2. În loc de a striga lozinci pe la manifestațiile de protest, vă propun un cântec. Un cântec frumos și solidar. Unul pentru celălalt. Poate așa am putea să atragem mai multă atenție.

Colega mea din școala medie este una dintre cei uciși în timpul serviciului la R.T.S. (Radioteleviziunea sârbă).

Nu putem aproba venirea forțelor N.A.T.O. în țara noastră, întrucât nu dispunem de destulă armată pentru a le asigura securitatea.”

Pe de altă parte, sârbii din Canada, respectiv din Ottawa, au pornit o campanie de strângere de fonduri pentru publicitate antibombardamente în publicația „Ottawa Citizen”. Nu mai puțin de 80% dintre cei care și-au oferit ajutorul au și făcut-o, astfel că s-a ajuns chiar la un excedent financiar (deși au fost necesari 14 851 de dolari, s-au strâns aproape 22 000 de dolari, la acțiune participând inclusiv grecii canadieni). De unde s-a ajuns la ideea continuării campaniei publicitare în publicații de importanță națională în Canada („Globe & Mail” sau „National Post”). Bran Selic scria la 22 aprilie 1999: „Tuturor celor care urmăresc CNN, CBC și altele asemenea le este limpede că în lumea contemporană comercializantă acțiunea în planul «public relations» este una dintre cele mai eficiente metode de luptă.” A se vedea în acest sens impactul pe care l-a avut pentru opinia publică americană și îndeosebi asupra minorității evreiești din Statele Unite ale Americii compania americană „Ruder Finn”, plătită de diaspora albaneză.

Împotriva agresiunii NATO asupra Iugoslaviei se putea vota pe Internet la următoarele adrese:

www.centraleurope.com; www.msnbc.com/; www.cnn.com/; news.ninensn.com.au/;

www.cbsnews.com/. E greu de crezut că oficialitățile S.U.A. sau N.A.T.O. au luat în considerare rezultatele acestor voturi, dar cu siguranță le-au monitorizat evoluția pas cu pas, pentru cu totul alte scopuri, unul fiind cu siguranță realizarea de baze de date cu adresele de e-mail și țările de unde veneau voturile împotriva agresiunii N.A.T.O.

„Războiul cibernetic a sosit cu toate implicațiile sale și i-a surprins complet nepregătiți, chiar și pe americani. Îndeosebi când e vorba despre implicații etice”, scria corespondentul din Washington al publicației iugoslave „NIN” (www.nin.co.yu) în numărul din 4 septembrie 1999, preluând afirmația unui profesor de la Academia Marină din Monterrey, California. La un simpozion organizat la Washington s-a spus că ceea ce a fost lansat în primăvara lui 1999 în Balcani este „similar, după importanță, cu bombardamentul aerian în primul război mondial și cu atacul cu bomba nucleară asupra Hiroshimei, în 1945.” Adică „războiul cibernetic”, despre care se apreciază că a jucat un rol cheie în predarea neașteptată a lui Milošević pe 7 iunie și acceptarea, practic, a retragerii necondiționate din Kosovo. Același profesor californian, consilier al Pentagonului și unul din experții de frunte americani în probleme de luptă informatică, a declarat că rușii i-au atenționat pe americani că vor reacționa „prin toate mijloacele” (ceea ce, în limbaj diplomatic, include și armamentul nuclear) dacă vor fi atacați cibernetic de către Occident. Detalii despre faza finală a agresiunii N.A.T.O. asupra Iugoslaviei se află în continuare la „strict secret”, însă acum este clar că S.U.A. au atacat cibernetic sistemele vitale iugoslave, „în prima ofensivă cibernetică de masă de care se știe în istoria războiului”, scria același corespondent al publicației iugoslave. Cităm din același articol (apărut sub titlul „Duhul în afara sticlei”): „Din alte izvoare de aici (S.U.A., n.n.) se poate concluziona la modul general că în faza finală a intervenției împotriva

Iugoslaviei direcția principală de atac a fost îndreptată spre perturbarea rețelei de computere pentru comandă și control a Statului Major al Armatei Iugoslave. Cu deosebire în această operație a fost țintit sistemul integrat de computere al apărării antiaeriene a Armatei Iugoslaviei, în ideea ca prima acțiune militară în jumătatea de secol de existență a N.A.T.O. să se termine așa cum a început: fără nici o jertfă din partea piloților din cadrul armatei care a acționat zi și noapte asupra Serbiei, Kosovo-ului și (uneori) a Muntenegrului. Pe lângă apărarea antiaeriană, în vizorul intervenției cibernetice americane s-au găsit în această perioadă și sistemul telefonic și celelalte comunicații de care s-a servit Statul Major al Armatei Iugoslave. Ideea - cum se explică neoficial - a fost de a se distruge acest sistem în măsura în care va obliga conducerea de la Belgrad să treacă la sistemul de comunicații cu comandanții de pe teren prin legătura radio și prin telefoanele mobile - care se urmăresc și se ascultă mai ușor." Oficialii de la Pentagon susțin că prin aceste acțiuni s-a obținut un „succes important”, însă operațiunile cibernetice au fost utilizate cu întârziere și cu reținere. Altfel spus, S.U.A. au utilizat în acțiunea lor în Balcani doar zece la sută din capacitățile pe care le posedă. Nici nu e de mirare, mai ales dacă se are în vedere faptul că în S.U.A. se află aproape jumătate din computerele existente la ora actuală în întreaga lume. Despre un asemenea stil de luptă, americanii cred că ar fi ideal pentru pedepsire, fiindcă se află undeva între sancțiunile economice și un atac cu armament convențional. Crearea haosului prin mijloace electronice în tabăra adversarului este o alternativă întru totul acceptabilă, deoarece permite evitarea vărsării de sânge. Numai că un atac cibernetic va produce reacția părții adverse, care va recurge la acțiuni teroriste ori la angajarea hackerilor individuali. Escaladarea unui conflict cibernetic până la dimensiuni inimaginabile, care pot scăpa de sub orice control, reprezintă însă o realitate de care trebuie să se țină cont, scrie „NIN”. Despre războiul cibernetic între S.U.A., pe de o parte, și sârbi, pe de altă parte, a vorbit la un simpozion al specialiștilor informaticieni din cadrul armatei și unul din șefii forțelor aeriene americane. „Am consemnat câteva încercări de distrugere a rețelelor noastre (informative). Din fericire, acțiunile sârbești de acest fel nu au fost cu nimic mai puțin eficiente decât acțiunile apărării lor antiaeriene.” Același general a declarat că și specialiștii americani au atacat, la rândul lor, sistemele informatice sârbești, printre care și cel al apărării antiaeriene, însă nu a precizat care a fost impactul acestor atacuri. În cele 78 de zile de atac asupra Iugoslaviei, forțele americane au încercat să dezvolte un sistem de război electronic care va fi o parte a doctrinei militare în viitor. În atacurile asupra R.F.I. s-au folosit de cinci ori mai multe tehnologii informatice decât în războiul din Golf. N.A.T.O. a recunoscut că hackerii sârbi i-au blocat în martie 1999 sistemele informatice cu viruși și cu un mare număr de mesaje electronice, însă oficialii ai Alianței au precizat că pagube au fost doar pe site-uri și în sistemele de distribuire a e-mail-urilor. Nu s-a consemnat nici un atac reușit asupra computerelor militare. Scopurile urmărite de către un hacker pot fi mai puține ori mai multe, în funcție de ceea ce-l motivează pe acesta să atace. În numărul său din noiembrie 2000, revista „PC Report” trece în revistă posibilele scopuri ale unui atacator, fără însă a le epuiza. Iată și lista:

- 1) îngreunarea sau încetinirea activității normale a unui serviciu prin mărirea timpilor de răspuns la cereri sau prin perturbarea accesului la resurse, mergând până la blocarea completă a activității;
- 2) inserarea de secvențe denaturate în datele trimise de un serviciu către utilizatori mergând până la deturnarea completă a serviciului către o resursă controlată de atacator;
- 3) obținerea de acces nelegitim la servicii private sau cu acces limitat;
- 4) capturarea informațiilor vehiculate de servicii cu caracter privat sau secret;
- 5) modificarea configurației mașinilor care oferă anumite servicii;
- 6) instalarea de programe speciale, care execută pe serverele atacate diverse acțiuni în interesul atacatorului, cum ar fi colectarea de parole etc.;
- 7) înlocuirea unor programe ce fac parte din instalarea mașinii atacate, altele care par a executa aceleași acțiuni ca și cele originale, dar de fapt lucrează pentru atacator;
- 8) ștergerea pur și simplu a unor programe și/sau informații de pe serverele atacate, mergând până la distrugerea completă din punct de vedere software a mașinilor atacate sau chiar până la distrugerii hardware (improbabil, dar nu imposibil).

Așadar, orice calculator aflat în rețeaua Internet devine automat vulnerabil. Însă vulnerabilitatea poate fi mai mare sau mai mică, totul fiind în funcție de sistemele de protecție ale calculatorului. Pentru a ataca, un hacker va utiliza întâi „Host Scan” pentru identificarea calculatoarelor din rețea. Dacă primește un răspuns de la unul din computere, hackerul va trece fără doar și poate la

atac. Următoarea fază o constituie scanarea prin care se urmărește identificarea porturilor deschise ale aplicațiilor pentru a fi utilizate pentru accesul în sistem. După ce pătrunde în sistem, atacatorul va bloca serviciile existente pe mașina respectivă prin schimbarea parametrilor sau a configurației sistemului ori prin instalarea unui program propriu, care are drept scop generarea unui trafic uriaș în sistemul vizat. Această acțiune poartă numele de DoS - Denial of Service. Dat fiind faptul că protocolul Internet TCP/IP gestionează mesajele foarte mari prin fragmentarea lor. Acestea sunt trimise prin rețea în pachete optime, iar la destinație sunt asamblate la loc. Ce fac hackerii? Ei trimit fragmente foarte mici care simulează un pachet foarte mare, imposibil de asamblat. În contextul aceleiași metode, spune Petre Rău în cartea sa „Infraționalitatea pe calculator” (vezi www.rap.freehosting.net/Infra/P3.html), „...unii procedează la «stârnirea» tuturor calculatoarelor active dintr-o rețea, pentru a trimite, într-un trafic foarte mare, răspunsuri pe adresa unei victime alese în prealabil, până la obținerea unei blocări complete.” Blocarea unor servere ce oferă servicii importante, de exemplu Web, spune același autor, este o altă tehnică utilizată frecvent. Ea constă în simularea unei sesiuni TCP, o dată cu expedierea unui număr foarte mare de mesaje, la care nu se mai generează răspunsurile la informațiile de confirmare, paralizând astfel activitatea calculatorului, destinație care nu mai poate deschide nici o conexiune legitimă.

Sub titlul „Mesaje dușmănoase”, pe Internet a circulat și un asemenea text: „Știm cu toții foarte bine că ne aflăm în război. Știm foarte bine și cine anume ne sunt dușmanii. În aceste zile grele aceștia ne scriu și se bucură de chinurile noastre. De aceea am decis să le facem publice adresele de e-mail, iar voi faceți ceea ce urmează: potopiți-i cu e-mail-uri nefolositoare de mărime apreciabile, de sute de kb. Mail box-ul le va fi în curând supraîncărcat; trimiteți-le viruși. Aveți grijă ca virusul să fie împachetat într-un mesaj nevinovat; trimiteți mai departe adresele lor de e-mail.” După text urmau e-mail-urile respective.

Hackingul, între patriotism și terorism

În timpul agresiunii N.A.T.O. asupra Iugoslaviei, atacurile și pătrunderile neautorizate efectuate de către sârbi într-o mulțime de pagini și site-uri web au cunoscut o nouă dimensiune, opinia publică iugoslavă și o bună parte a lumii acceptând ideea că există și un alt fel de hacking și anume hackingul patriotic. În permanență, însă, rămâne în prim-plan același semn de întrebare: unde se află granița între legal și ilegal? În mod clar, totul depinde de partea de baricadă unde se află hackerul/crackerul, respectiv cel atacat. În acest context, americanii, cei mai vânați de iugoslavi, au catalogat atacurile drept crackuri, ilegalități etc. De partea cealaltă, iugoslavii au etichetat acțiunile respective drept hackuri perfect legale, mai cu seamă că acțiunea în forță a N.A.T.O. nu a fost decât o grosolană agresiune, fără nici un temei legal. Așadar, dacă facem apel la etică, trebuie să aplicăm același standard atât pentru acțiunile forțelor N.A.T.O., cât și pentru atacurile digitale ale iugoslavilor și aliaților lor: ori amândouă au fost legale, ori amândouă au fost ilegale. Dublul standard este încă, din nefericire, frecvent utilizat în relațiile internaționale, dreptate având cel puternic, câinele (democrația nefiind pentru căței). Scena politică internațională pare mai curând un teatru de luptă între bandele mafioate din New York, de exemplu. Iar democrația pare mai curând praf în ochii celor slabi.

Iată că, astfel, chiar și crackerul cel mai înrăit poate deveni un erou popular dacă, în timpul unei confruntări militare, intră în luptă de partea poporului său și atacă, printr-o metodă sau alta, pagini și site-uri web ale dușmanului. Desigur, într-o lume normală, el ar fi un proscris vânat inclusiv de poliția țării sale. În plin război, însă, atacurile sale pot servi o cauză mai mult sau mai puțin dreaptă. Iar el, hackerul, respectiv crackerul, așa cum spuneam și în rândurile de mai sus, poate fi un erou popular.

Hackingul patriotic a ajuns o temă extrem de generoasă pentru cei care studiază fenomenul Internet. Ne vom limita totuși la studiul noțiunii de bază: hackingul, dar și la practicienii săi,

hackerii, respectiv crackerii.

În general, hackerii acuză mass-media de faptul că-i confundă cu crackerii, cei care, în accepțiunea hackerilor, sunt adevărații pirați informatici. Ei, hackerii, susțin că respectă un fel de cod cavaleresc: niciodată să nu faci pagube, niciodată să nu furi și niciodată să nu te lași descoperit. „Doar o provocare a inteligenței (vezi www.munty.150m.com/Hack/intro-htm, care preia materialul de la Cyberwarrior). Niciodată cu intenție criminală. Cultura hacker este legată de numele marilor universități americane (Harvard, Berkley, Stanford) unde, de regulă, toți studenții sunt hackeri.” Ceea ce însă uită acești teoreticieni ai hackingului este una dintre legile fundamentale ale democrației: respectul față de proprietate. Dacă un hacker pătrunde în sistemul meu informatic el este un hacker. Dacă același individ începe să-mi fure date sau să-mi șteargă fișierele, el este un cracker. Numai că în ambele cazuri este vorba în primul rând de o intrare neautorizată, deci de o violare a proprietății. Chiar dacă hackerul declară că doar a vrut să studieze, să învețe. Prin urmare, fără intenția de a polemiza cu hackerii, ne vom asuma punctul de vedere al mass-media și vom pomeni de crackeri doar acolo și când va fi neapărat cazul. Pe lângă hackingul patriotic există și cel politic, în care un hacker demonstrează prin fapta sa, evident, că nu este de acord cu ideile propagate de un om sau un partid politic și decide să atace o pagină web, de regulă cea de început (indexul), sau chiar un site întreg. Pe de altă parte, se mai poate vorbi de un hacking antistatal, când un hacker atacă paginile web sau site-urile unor instituții de stat pentru că nu este de acord cu una sau cu mai multe laturi ale politicii unui stat dintr-un domeniu sau altul. Sau ia atitudine împotriva celor care au pedepsit un alt hacker, caz în care se poate crea chiar un curent internațional de pedepsire a pedepsitorului, aici celebru fiind cazul lui Michnik. După atacul asupra World Trade Center din 11 septembrie 2001, a apărut așa-numitul terorism cibernetic și care, susține mass-media, ar consta din folosirea Internetului de către grupările teroriste de tip Al-Qaeda pentru comunicații, recrutare și colectare de fonduri. „Chiar și acum – scria cotidianul bucureștean «România Liberă» la 11 septembrie 2002 -, în condiții de securitate sporită, Al-Qaeda se folosește de internet pentru a pune la cale noi atacuri. Experții au ajuns la concluzia că teroriștii au studiat cu mare atenție sistemul telefonic american, alimentarea cu apă, serviciile publice, dirijate computerizat.” Același cotidian citează un oficial de la Centrul de protecție a infrastructurii din cadrul F.B.I. care afirmase că „Nu pot să dorm de teama unui atac clasic, fizic, combinat cu un atac cibernetic care ar distruge sistemele noastre de intervenție în caz de situații de urgență”. Pare totuși de necrezut nu faptul că nu ar putea exista pe viitor asemenea atacuri, ci faptul că, deși previzibile, asemenea riscuri sunt efectiv acceptate. A lăsa la îndemâna hackerilor, crackerilor ori a altor persoane controlul asupra, să zicem, alimentării cu apă a unui oraș este nebunie curată atâta vreme cât se poate izola complet de exterior orice rețea de calculatoare. Nu este departe în urma noastră virusul mileniului, care aproape că a isterizat o planetă întreagă și nu a fost decât un bluf. Ce anume se urmărește prin crearea unor asemenea stări de panică nu e ușor de ghicit. Însă, în mod cert, cineva câștigă din asemenea manipulări în masă.

În 1997, televiziunea rusă anunța: „încercările repetate ale hackerilor de a pătrunde în sistemele informatice ale instituțiilor de stat”. Șeful agenției federale pentru comunicații afirma că folosirea cu rea intenție a tehnologiei moderne de telecomunicații poate „influența psihologia unor întregi națiuni”. Nu se cunoaște ce efect a avut în Belarus atacul hackerilor asupra site-ului președintelui Belarusului, Lukașenko, în care fotografia acestuia din urmă începea să se transforme în portretul lui Hitler, apoi în cel al lui Stalin, pentru a redeveni la chipul președintelui, dar cu siguranță a provocat cel puțin o mulțime de zâmbete.

În ultimii ani, s-a constatat că grupurile care activează în domeniul politicului organizează tot mai multe atacuri de tip hacker din ce în ce mai sofisticate. Aici este vorba despre agende politice naționale, internaționale și transnaționale. Astfel, o grupare de hackeri care activa sub denumirea de „Mossad”, a atacat site-ul oficial al președintelui iranian Mohammed Khatani.

În 1998, în Australia, în pragul alegerilor, un hacker necunoscut a modificat pagina oficială a Partidului Liberal, ministrul liberal al afacerilor externe, Alexander Downer, devenind, în opinia hackerului, „ministrul pentru umilința externă”. Mai mult decât atât, intrusul a legat pagina ministrului cu cea a Disneyland-ului, iar paginile altor miniștri, cu pagini porno de pe Internet. Ministrul pentru relații de muncă, Peter Reith, a devenit „ministrul distrugerii locului de muncă și a dreptății, pentru Gestapo și propagandă”.

Kashmirul, provincia indiană dorită atât de mult de islamiștii pakistanezi, a fost nu o dată mărul

discordiei și pe Internet. După ce armata indiană a lansat un site dedicat Kashmirului, hackerii pakistanezi l-au și atacat. Agenția indiană de presă PTI a anunțat că atacul l-au înfăptuit „persoane suspectate a fi membri ai serviciilor de spionaj pakistaneze”. Armata a refăcut site-ul, însă hackerii l-au atacat din nou, chiar de mai multe ori. Conflictul este anunțat și pe site-ul BBC-ului (<http://www.monitor.bbc.co.uk/>), la 25 octombrie 1998, sub titlul „Războiul lumilor pe Internet”. Se presupune că multe din atacurile pakistaneze aparțin hackerilor din grupul intitulat WFD. În mod cert, conflictul digital indo-pakistanez nu va înceta atâta timp cât problema Kashmirului nu va fi rezolvată convenabil pentru ambele părți.

Un an mai târziu, în 1999, Republica Populară Chineză a lansat un site dedicat drepturilor omului. Reacția nu a întârziat să apară, hackerii care optează pentru libertăți mai mari decât cele oferite de Beijing atacând imediat după aceea.

Sub titlul „Pentaguard, cel mai puternic grup de hackeri???” la adresa <http://silviu.4t.com/hack.htm> a apărut o adevărată radiografie a unui puternic grup de hackeri români. La un moment dat, aceștia declarau: „Ne-am întors... după o lungă perioadă de tăcere, Pentaguard s-a întors. Cu un nou echipaj format din: Diablo (membru fondator), Halo, Killtec și G-man. Ca întotdeauna, principalele ținte sunt serverele militare și guvernamentale (pentru că acolo se găsește marfă). Ieri, 26.10.1999, am început un nou război numit: Războiul WWW... un război împotriva Statelor Unite și a celorlalte state care se cred puternice atunci când luptă cu un adversar mai slab, dar care se sperie când ar trebui să lupte cu un inamic de talia lor...”

Autorul articolului, bun cunoscător al evoluției celor de la „Pentaguard”, aproape că spune în ce oraș activează aceștia: „Nu se știe cu exactitate când au apărut, cert este doar că cel care a pus bazele acestui grup de «haiduci ai Internetului» e Diablo. De asemenea, componența Pentaguard s-a schimbat permanent, însă, printre cei mai cunoscuți se numără G-man, n0nam3, Light, H3X0r (alias Andripopa sau Linuxman), Beculetz (alias joaka cruce) și BM-Freak. [...] De multe ori, paginile modificate conțineau mențiunea «Copyright WRHC (West Romanian Hackers Corporation)»”. În textul de mai sus apare un nume care te duce cu gândul la una dintre melodiile lui „Phoenix”, legendara formație de muzică din Timișoara, și anume „Andripopa”. La fel și mențiunea: „Copyright WRHC (West Romanian Hackers Corporation)”. Dar cel mai convingător argument nu este că Pentaguard s-a aliat cu hackerii ruși, ci faptul că membrii săi au început un „război WWW” împotriva Statelor Unite ale Americii. Or se știe că în Banat trăiesc cei mai mulți etnici sârbi din România, iar timișorenii au înțeles poate cel mai bine nedreptatea ce li s-a făcut sârbilor prin agresiunea N.A.T.O. asupra Iugoslaviei. În colaborare cu hackerii ruși de la „KpZ”, cei de la „Pentaguard” au atacat în câteva săptămâni 21 de servere militare ale SUA. Dar iată încă un fragment din textul de pe <http://silviu.4t.com/hack.htm>: „Anul 1999 a reprezentat însă un adevărat coșmar pentru americani, după ce Pentaguard s-a aliat cu KpZ, un grup de hackeri din Rusia. Cele mai mari succese le-au avut conducătorii acestora, Diablo și Windows 95, care în câteva săptămâni au atacat 21 de servere militare ale SUA. Mesajele lăsate, uneori pline de umor, se referă, în general, la politica practică de anumite state și la încălcarea drepturilor omului. De exemplu, pe un site al US Navy apare următorul mesaj: «Motivul pentru care am spart acest server este următorul: Când Miloșevici a început să omoare albanezi în propria lui țară (Kosovo este o parte a Serbiei) ați început războiul împotriva lui pentru a-l pedepsi. Foarte bine! Acum vine întrebarea: Rusia a început să omoare civili ceceni. Unde este armata SUA? Unde sunt faimoasele bombardiere F117? Unde sunt rachetele Tomahawk? Auuuuu... vă temeți de Al Treilea Război Mondial! În cazul acesta va trebui să vă descurcați cu Războiul WWW. Pentaguard, cu o nouă echipă condusă de Diablo, pornește noul război pentru a arăta lumii că unii oameni au curajul de a înfrunta orice putere de pe glob. Nu contează de unde este sau cât de mare este armata sa. Vom câștiga acest război!»”

Exemplul de mai sus le conferă celor de la „Pentaguard” o aureolă de eroi. Iar acțiunile lor par firești într-un context în care marile puteri aplică diferite standarde în relațiile interstatale.

În octombrie 2002, motorul de căutare www.google.com dădea nu mai puțin de 900 de adrese conținând numele de „Pentaguard”. Poate cea mai completă istorie despre acest cel mai cunoscut grup de hackeri români se găsește la adresa www.halbasus.go.ro și este, probabil, realizată de unul dintre membrii grupului. Autorul descrie, succint, momentele nașterii grupării, în 1998, fără a numi orașul. Potrivit www.transindex.ro, acesta ar fi Oradea. Un capitol care avea să „consacre” acest grup a început în ianuarie 1999, când guvernul chinez a condamnat la moarte doi hackeri care au spart o bancă și au furat 10 000 de dolari. Cităm: „Era o încălcare grosolană a

drepturilor omului. Întreg underground-ul a ripostat... Hackeri de peste tot atacau serverele chinezilor... PentaGuardul nu a făcut excepție și câteva site-uri ale guvernului chinez au fost sparte ca semn de protest față de legile lor stupide.” Dacă e să ne luăm după informațiile din www.halbasus.go.ro, episodul KpZ a fost mai mult un concurs între Diablo, cel care a pus bazele grupului românesc, și hackerul rus care-și spunea Windows 95, cei doi întâlnindu-se în timp ce Diablo spărgea o pagină anonimă. Cităm din nou: „...cei doi au ajuns la o oarecare prietenie și Windows 95 a lansat o provocare. Site-uri .gov si .mil... un subiect tabu la acea oră... nimeni nu se atingea de ele (nu știu din ce motiv). Cine sparge mai multe pagini .gov si .mil... Și cursa a început... La sfârșitul zilei, KpZ a spart 3 site-uri... Diablo 18... oricum site-urile aveau aproximativ același text (KpZ and PentaGuard forever :))... atunci a intrat PentaGuardul în atenția presei... și după acea colaborare ciudată PG-ul nu a mai făcut alte colaborări.

Acest moment a fost unul care a format stilul PG... de aici încolo PG a spart (cu mici excepții) doar site-uri .gov și .mil... pentru a demonstra că și ele sunt site-uri la fel de vulnerabile... și un nume că NASA sau US Air Force nu poate proteja un server. De aici încolo au urmat o grămadă de hackuri... de la nasa.gov-uri până la [.navy.mil](http://navy.mil) și [.af.mil](http://af.mil)-uri nimic nu a fost lăsat neatins...” În 2000, Diablo îl întâlnește pe [LiGHT], din același oraș, apoi pe n0_nam3, „colegul, prietenul și verișorul lui [LiGHT]”. La rândul său. [LiGHT] „...întâlnise câțiva tipi din Timișoara... BM-Freak, beculetz și H3X03...” Cei șase vor băga spaima în administratorii de pe Internet. Cităm din nou: „... la turma de .gov-uri si .mil-uri care a dat culoarea PG-ului acum s-au adăugat noi victime autohtone... ministerul finanțelor (de multe ori), romtelecom (numa' de vreo 2 ori), RASDAQ, eximbank, porsche.ro, europeandrinks, și altele (cateva ISP-uri, etc...). PG era deja un nume binecunoscut pentru presa română și cea străină, s-au scris articole, interviuri (mai mult sau mai puțin corecte:), etc. poate acesta a fost apogeul grupului...” Între timp, BM-Freak este obligat să părăsească grupul, locul său fiind luat de către Jaymzu, „administrator și hacker liber profesionist”. În 2001, Diablo și [LiGHT] pun la cale ceea ce mai târziu a fost declarat, cităm: „cel mai sistematic atac asupra unor servere guvernamentale din toata lumea”. Scenariul a fost simplu, povestește autorul istoriei grupului: „[LiGHT] și Diablo, închiși într-o cameră cu țigări, beri și două calculatoare legate la net printr-un dial-up. Operațiunea a început la 10 seara și s-a terminat pe la 6 dimineața... Rezultatul? O grămadă de servere sparte. Ziarele vuiiau... PG (Pentaguard, n.n.) era din nou în atenția presei... era deja timpul să reîntre în underground.” Acum, pentaguarzii s-au liniștit, unii fiind la facultate, iar alții ocupându-se de lucruri mai cuminiți. Scurta și interesanta istorie a grupului se încheie cu un șir cuprinzând adresele unora dintre site-urile atacate, precum și adresele la care se pot vedea și rezultatele de la vremea respectivă ale atacurilor (mirror) din 2000 și 2001. Printre adresele atacate și menționate pe site-ul www.attrition.org (54 de poziții) se află și următoarele: US Naval Hospital, Yokosuka Japan (<http://www.nhyoko.med.navy.mil>), NASA COTS Year 2000 Software Compliance Tracking Database (cotserver.lerc.nasa.gov), #2 Fe-deral Maritime Commission (<http://www.fmc.gov/>), Department of the Treasury - CSM (<http://www.ots.treas.gov/>), McGhee Tyson Air National Guard Base, Knoxville (<http://www.tnknnox.ang.af.mil/>), #2 Ministry of Foreign Affairs of Georgia (<http://www.mfa.gov.ge/>), US Courts, District of Idaho (<http://www.id.uscourts.gov/>), US Courts (<http://www.idd.uscourts.gov/>), US Office of Surface Mining (U.S. Department of the Interior) (<http://www.coh.osmre.gov/>), US Department of the Interior, Alaskan Office (<http://www.ak.doi.gov/>), Australian Institute of Marine Science (<http://www.aims.gov.au/>), Naval Air Facility in Washington (<http://www.nafwash.navy.mil/>).

Lista unei părți a site-urilor sparte de către membrii Pentaguard se găsește la adresa <http://www.attrition.org/mirror/attrition/pentaguard.html>. Un interviu cu Diablo a fost accesibil pe site-ul www.epress.ro. Ce anume se putea citi la un moment dat pe site-ul Ministerului Finanțelor din România, spart de același grup, se poate citi la adresa <http://floweros.tripod.com>. Taxa pe prostie, instituită de „Noua coalitie guvernamentală formată din: Pentaguard, Getto Daci și Institutul Român de Cercetări Alcoolice”, care a preluat controlul Ministerului Finanțelor, a făcut furori în România: „Pentru a spori veniturile bugetare, Ministerul Finanțelor introduce taxa pe prostie... Această taxă poate aduce venituri nelimitate pt că știm de la chimie că în lume există 2 elemente omniprezente: hidrogenul și proștii... Această taxă va crește proporțional cu mărirea funcției... deci dacă un măturător de stradă va plăti 100.000 lei, un președinte prost poate ajunge să plătească o sumă de: 10.000.000.000.000.000 lei.... Deci avertizăm pe domnul Ion Iliescu ca să se gândească de 2 ori sau de 3 ori înainte de a candida pentru că dacă vine el la putere

România va putea trăi numai din impozitul pe care îl plătește domnia sa pe prostia pe care are tupeul de a o afișa.”

„Monitorul de Braşov” (www.brasov.monitorul.ro) titra pe 5 noiembrie 1999: „Noi năzbâții ale hackerilor români”, în cauză fiind, evident, grupul Pentaguard, format din „patru băieți și două fete”. Referindu-se la Diablo, ziarul scria că „... s-a aliat în luna ianuarie cu Windows '95, liderul organizației «Kp2» din Rusia, declarând World Wide Web War sub deviza «Russia and Romania For Ever». În primele două luni de alianță, cele două organizații au reușit să distrugă 21 de servere guvernamentale sau militare americane sau chinezești.”

Pe site-ul www.chip.ro, sub titlul „Atacul hackerilor și contraatacul providerilor”, apare un text în care se face referire și la Pentaguard: „Un alt exemplu convingător referitor la vulnerabilitatea pe Internet îl reprezintă acțiunile hackerilor români Pentaguard; aceștia susțin că hackurile au motivație politică, dar fac acest lucru și din pură distracție. Considerați de CNN ca fiind pe locul I, precum și atenția deosebită pe care le-o poartă americanii, sunt lucruri datorate faptului că grupul Pentaguard a spart site-ul trezoreriei Statelor Unite în 15 secunde, precum și o serie de site-uri românești oficiale: Romtelecom, Universitatea din Timișoara, TVR, Ministerul de Finanțe.”

Referire la acel loc I deținut la un moment dat de către cei din Pentaguard, clasificare realizată de CNN, face și site-ul www.transindex.ro/magazin/ în 19 februarie 2001. După Pentaguard, cu 154 de site-uri sparte (din care 78 gov. și mil.) urmau: grupurile de hackeri AntiChrist, cu 136 de spargerii, Global Hell (111), hV2K (53), Level Seven (59), KpZ (48), forPaxe (62), Team Spl0it (42).

În 1999, după nouă luni de căutare a unei fisuri în sistemul providerului irlandez „Connect Ireland”, au avut loc optsprezece atacuri simultane, astfel că proprietarul a fost nevoit să întrerupă temporar serviciile de profil către toți clienții săi și să-și instaleze un hard disk mai puternic și programe performante. Dar cine au fost furioșii atacatori? Se crede că organizatorul a fost guvernul indonezian, iar hackerii au atacat din diverse locuri, din S.U.A până la Australia. Motivul atacurilor l-a constituit găzduirea de către „Connect Ireland” a site-ului conducătorilor luptei pentru independență a Timorului de Est (până de curând aflat sub stăpânirea Indoneziei), respectiv Ramos Horta și episcopul catolic Carlos Belo, care au primit împreună, în 1996, premiul Nobel pentru pace.

De serviciile hackerilor se folosesc inclusiv guvernele și partidele politice. Un exemplu concludent în acest sens este isprava unor hackeri mexicani care, la comanda Partidului Democrat Revoluționar, de opoziție în anul 2000, au spart codul de acces și au pătruns în serverele guvernului, aflând astfel de fărădelegile de ordin financiar ale acestuia și pe care a trebuit să le acopere statul mexican prin împrumuturi la diferite organisme financiare străine.

Scriind în articolul cu titlul „Hackerii pakistanezi au atacat locația web a guvernului american”, publicat pe Internet pe 26 octombrie 2001, despre atacul hackerilor pakistanezi asupra serverului NOAA (National Oceanic & Atmospheric Administration), inaccesibil câteva ore, publicația iugoslavă „Mikro online” cita mesajul hackerilor și anume: „Cu toate că guvernul Pakistanului condamnă atacul asupra S.U.A., noi susținem Al Qaeda. Deținem câteva informații strict secrete ale guvernului american pe care le vom preda organizației Al Qaeda. Dați-ne pace pentru a avea pace”. Hackerii solicitau S.U.A. să-și retragă forțele armate din Arabia Saudită, să înceteze bombardamentele asupra Afganistanului și să limiteze susținerea Israelului. De menționat că serverul atacat era unul de rezervă pentru datele meteo pe care NOAA le asigură Direcției federale pentru zboruri.

Unul dintre războaiele cibernetice din Europa a început în 2001, când un ieșean, cu pseudonimul Igu Uiorean, student la Facultatea de Automatizări și Calculatoare din Cluj-Napoca, a atacat pagina www.nemnemsoha.hu, un site naționalist maghiar (vezi www.sinaia.globtel.ro și www.rdr.go.ro). Titlul paginii maghiare face referire la faptul că membrii grupului nu vor accepta niciodată decizia de la Trianon. Atacul se repetă. Ba, mai mult, românii sunt gata să plătească alte atacuri asupra site-ului. În ajutor le vin, gratuit, hackerii slovaci. Maghiarii apelează la cei mai buni ingineri IT pentru a-și apăra informațiile. Apare o pagină nouă cu titlul „olahhak”, un cuvânt compus din „olah” și „hacker”. În vara aceluiași an, românii reușesc să spargă canalul de comunicații maghiar și intră în posesia unor date secrete privind codurile de siguranță ale site-ului adversarilor. În noiembrie, site-ul este spart, iar conținutul paginilor – modificat. Coaliția româno-slovacă, scrie „Ziua”, reușește să descarce documente cu date concrete anti-românești. Membrii grupului românesc au declarat că în intenția lor a fost să predea serviciilor secrete românești

„prada de război”. Pe fir intră Poliția română. Grupul lui Uiorean își încetează activitatea. Însă războiul continuă, hackerii naționaliști români aflându-se în continuare la vânătoare de pagini naționaliste maghiare. Un grup de hackeri conștanțeni a anunțat pe un „chat” al crackerilor că intenționează să spargă serverul Clubului Trianon. Maghiarii au luat și ei măsuri, anunțând Poliția maghiară.

Pe 11 septembrie, cotidianul bucureștean „Adevărul” anunța: „Cel mai mare site antiromânesc – spart de hackeri”. În material, autorii scriau, printre altele: „Una dintre paginile tapetate cu lozinci și imagini revizioniste a fost acoperită cu un uriaș steag românesc sub care scrie «Transilvania este a României». Este a doua oară când hackerii români – cunoscuți mai mult drept «carderi» (spărgători de cărți de credit) – se implică «ideologic»”. Site-ul antiromânesc atacat nu era altul decât același pomenit mai sus, adică site-ul cu adresa www.nemnemsoha.hu.

Acest război a luat amploare atunci când românii și maghiarii nu s-au limitat la a sparge site-urile naționaliste și revizioniste, ci au trecut și la spargerea căsuțelor poștale personale. Ziarul „Ziua”, care a urmărit îndeaproape luptele, susține că redactorii săi au primit însă și mesaje prin care o serie de hackeri români și maghiari și-au exprimat dezacordul față de acțiunile colegilor lor. Un membru al R.H.C. - Romanian Hacking Community, a scris: „Sunt membrul celui mai mare grup de hackeri din România [...]. Vă scriu referitor la războiul declarat împotriva hackerilor unguri de către hackerii români, război care practic nu există, deoarece cei 4 sau 5 care au spart site-ul guvernului Ungariei nu pot fi numiți o grupare. [...] Grupul nostru are scopul de a ajuta și nu a distruge, nu de a crea probleme și conflicte între cele două țări. Nu ne place să fim numiți «piraiți», deoarece grupul nostru are un scop benefic, prin securizarea serverelor care ar putea cădea pe mâini «criminale»”. Dar, scria în același cotidian, grupării lui Uiorean i s-au alăturat cei din „TeamBucTm”, care s-au angajat să ajute grupul clujeanului și să facă ravagii prin paginile maghiare: „...sper să putem să ne ținem de cuvânt și să pice multe. să vadă și iei ce înseamnă adevărat «război» cu românii în domeniul internetului.” Reacția hackerilor maghiari nu s-a lăsat mult așteptată, scria Laszlo Kallai în „Ziua”. Într-un e-mail, un oarecare Miki scrisese: „stiu foarte bine ca gasca Ta a spart site-ul unguresc ai sa suporti consecintele in vigoare muiistule. hai ca vom face o vizita in bucuresti si va vom arunca in aer cind nici nu gindesti mincatorule de lebada sinteti lepadatura europeii.”

În mai 2001, cei de la <http://pcnen.cg.yu> preluau o știre apărută în publicația londoneză „Independent” și potrivit căreia orașul Priština din Kosovo a fost paralizat întrucât numeroase organizații internaționale și neguvernamentale, cyber-café-uri și oameni de afaceri au fost deconectați de la Internet. Unicul provider, IPKO, acuza pentru aceasta Serbia, întrucât în ultimele 18 luni hackerii sârbi au atacat de nenumărate ori sistemul IPKO, ceea ce a determinat provider-ul american „Interpacket” să întrerupă, la rândul său, colaborarea cu IPKO pentru a-și proteja propriul sistem. În ajutorul kosovarilor a sărit un provider norvegian, care a încercat fără succes să salveze rețeaua kosovară. „Independent” arată că este vorba despre unul dintre cele mai noi episoade în îndelungatul război electronic balcanic. Dacă, după multe confruntări pe Internet, Serbia și Croația au încheiat pacea, incidentele au devenit tot mai numeroase între războinicii electronici din Kosovo și Macedonia.

În primăvara lui 2001, coliziunea dintre un avion american de spionaj și un avion chinezesc de vânătoare s-a soldat cu moartea pilotului chinez. Rapid, hackerii chinezi au solicitat mobilizare generală în mediul lor și atacul asupra „șintelor” Internet americane.

Doar în luna mai 2001, site-ul Casei Albe a fost spart de hackeri de cel puțin trei ori și aceasta în același fel: prin atacuri DoS. A treia oară, site-ul atacat a fost inaccesibil mai mult de șase ore, suspectați de atac fiind hackerii chinezi. La începutul lunii mai, hackerii chinezi au realizat, așa cum, de fapt, au și anunțat înainte, sute de atacuri asupra site-urilor americane, printre altele fiind grav afectat și serverul de e-mail al Camerei Reprezentanților. Responsabili ai atacurilor asupra a numeroase ste-uri guvernamentale și comerciale americane s-au declarat a fi cei din grupul autointitulat „Uniunea Hackerilor din China” (Hongke Union) care, la un moment dat, au anunțat prin pagina web „ChinaByte” că după ce au atacat mai mult de o mie de site-uri americane și-au îndeplinit țelurile contraatacurilor și că următoarele atacuri antiamericane nu mai sunt acțiunea lor. În final, au declarat că „Prin această acțiune am dovedit că sentimentul patriotic încă mai există în inimile chinezilor”. Desigur, fiind vorba de China, ești foarte tentat să afirmi că în spatele acestor atacuri nu poate să stea decât o grupă de specialiști IT chinezi, fie aflați în solda Guvernului comunist, fie informaticienii din cadrul armatei chineze. Cum tot atât de bine nu este

exclus ca hackerii din „Hongke Union” să fie totuși tineri chinezi puternic îndoctrinați cu ideologia comunistă. Prea puțini ar crede că, totuși, nu puțini oameni, din indiferent ce țară aflată sub indiferent ce sistem politic, pot da dovadă de patriotism când e vorba de relația țării lor cu o alta, percepută ca fiind agresoare.

Printre site-urile atacate se număra și www.leg.wa.gov, unde se aflau informații despre executivul și legislația americană și unde, după un atac al hackerilor, s-au ivit mesaje scrise în limba chineză. Între timp, pilotul american al avionului de spionaj EP-3E, mai norocos decât nefericitul său coleg chinez, s-a decis să scrie o carte despre incidentul prin care a trecut și despre cele 11 zile de prizonierat la chinezi.

Din nefericire, Internetul poate fi foarte ușor un mijloc de dezinformare în masă, cu efecte la nivel global. Cititorul poate să-și imagineze diverse scenarii având drept punct de plecare un eveniment deosebit, petrecut în 12 iulie 2000. Site-ul cunoscutului cotidian belgrădean „Politika” a fost atacat, în el fiind inserată o notă prin care se anunța faptul că președintele Slobodan Milošević a fost atacat de un grup de teroriști la reședința sa din cartierul rezidențial belgrădean Dedinje. Rănit fiind, a fost de urgență dus la spital. După câteva ore în care medicii au încercat să-i salveze viața, președintele Iugoslaviei a decedat. „Așteptăm în continuare informații. Urmăriți programul nostru și site-ul nostru de pe Internet pentru a afla vești noi în acest moment greu pentru poporul nostru.”, scriseseră hackerii pe site-ul cotidianului „Politika”. Trebuie reținut și faptul că trustul de presă „Politika” dispune, în afară de cotidianul sus-amintit, de un post de radio și de unul de televiziune. Cei care au avut curiozitatea să dea curs invitației hackerilor ar fi avut surpriza să constate că atât radioul, cât și televiziunea Politika emiteau obișnuitele lor programe și nicidecum muzica clasică, normală pentru asemenea momente. Știrea a fost preluată de publicația belgrădeană în limba engleză „Bilten” și de corespondentul agenției de presă „Reuters”.

În 14 iulie 2000, apărea și pe site-ul cu adresa <http://vojvodina.com> știrea că hackerii au reușit să spargă site-ul publicației belgrădene „Politika” și să insereze informația cum că președintele Iugoslaviei, Slobodan Milošević, a fost ucis de explozia unei bombe. Buletinul independent „VIP” a dat și el publicității conținutul informației: „Președintele iugoslav Slobodan Milošević a decedat din cauza rănilor cauzate de explozia unei bombe amplasate în buncărul său de pe Dedinje”.

Evident că lumea, îndeosebi ziariștii și diplomații, a dat năvală să vadă informația cu pricina pe site-ul „Politika”. Numai că izvorul notei mincinoase nu mai exista, site-ul fiind repede refăcut de către proprietari, de unde și concluzia că fusese doar o acțiune de hacking. Dar acest lucru l-ar fi putut presupune și cei care au preluat informația privind moartea lui Milošević, mai cu seamă că Internetul ar fi fost ultimul loc unde să apară o asemenea informație. Așadar, iată că pe Internet nu este nimic sigur nici din acest punct de vedere, o informație abil strecurată pe un site oficial, prin hacking, evident, sau o informație falsă inserată dinadins pe un site oficial pot să inducă în eroare. Pornind de la această premisă, scepticii ar putea spune că Internetul nu prezintă nici un fel de garanție dacă informațiile pot fi atât de ușor falsificate. Dar putem oare spune cu mâna pe inimă că celelalte mijloace de informare în masă, cum ar fi televiziunea, radioul, publicațiile sunt mai sigure? Parțial da, fiindcă în aceste cazuri informația falsă poate fi introdusă doar de cel care lucrează la unul dintre aceste mijloace de informare în masă și nicidecum de vreun hacker. Se întâmplă deseori ca hackerul să fie unul dintre angajații cu acces la site-ul companiei unde lucrează. În „hacker” nu se poate însă transforma și angajatul unei televiziuni, de exemplu? Dincolo de toate aceste speculații rămâne valabil unul singur și același lucru: mijloacele de comunicare/informare în masă nu sunt și nici nu pot fi sută la sută sigure și nu pot ele însele garanta veridicitatea unei informații. Să renunțăm la mass-media? La Internet? Desigur că nu. Doar că trebuie să avem întotdeauna rezerve îndeosebi când e vorba de informații importante sau extrem de importante și să le verificăm pe mijloace de comunicare în masă diferite. Abia după aceea putem trage concluzia dacă informația este sau nu autentică.

Pe 18 septembrie, pe site-ul românesc cu adresa <http://stiri.rol.ro> apărea o știre preluată de la BBC și care spunea că, cităm: „Hackeri autointitulați «patrioți» au «spart» mai multe site-uri web, între care și al talibanilor, pirații informatici încercând să pericliteze activitatea organizațiilor și țărilor pe care le consideră vinovate pentru atacurile teroriste de marți.” În aceeași știre se amintea despre un grup de hackeri autointitulat „Dispatchers” și care anunțase că plănuiește un atac coordonat asupra infrastructurii computerizate a țărilor care s-ar putea afla în spatele atentatelor comise pe 11 septembrie asupra Statelor Unite. Ba, mai mult, membri ai grupului

amintit s-au și lăudat că au distrus deja câțiva provideri palestinieni.

O notă nesemnată, publicată în cotidianul național „România liberă” în data de 3 octombrie 2002, relatează despre faptul că „S.U.A. au lichidat un site web al Al-Qaeda” la numai 12 ore de la apariția acestuia. Site-ul respectiv conținea informații referitoare la Osama bin Laden, o declarație a secretarului de presă al rețelei Al-Qaeda și un mesaj către prizonierii de la baza americană Guantanamo din Cuba, prin care aceștia erau îndemnați să reziste. Tot S.U.A. au lichidat și site-ul „Jihadul on-line”, însă acesta a reapărut în octombrie 2002, primele informații fiindu-i dedicate lui Khattab, liderul mujahedinilor arabi în Cecenia ucis de forțele armate rusești.

Site-ul Ministerului de Interne al Iranului, cu adresa www.moi.gov.ir, a fost și el atacat. Indexul (prima pagină) a fost înlocuit cu mesajul „Owned! Ya biatch!”, precum și de diverse imagini dintre care se remarcă poza lui Osama bin Laden cu două pistoale îndreptate spre capul acestuia, se precizează pe www.div.ro. Autorii au fost cei din „The Dispatchers”, care au declarat război teroriștilor din întreaga lume.

Pe 1 aprilie 1999, un anume Adrian le trimitea membrilor unei liste de discuții un mesaj preluat de la o agenție internațională de știri, cu subiectul „despre hackerii iugoslavi”, în care se vorbea despre atacurile hackerilor iugoslavi asupra serverelor oficiale ale unor state membre ale N.A.T.O. În finalul textului în limba engleză, același Adrian încheie: „Patrioti baietii, n-am ce zice :-). Răspunzând la acest mesaj, un anume Sabin spunea: „... corect...a propos de patriotism, ati auzit ca Djeordjevici , jucator de fotbal de la Metz si-a luat «concediu» pe perioada razboiului si s-a dus la Belgrad pentru a fi alaturi de compatriotii lui. imputiti rau de tot americanii astia ca isi baga nasul si bombele pe unde au kef, nu?”

Numărul atacurilor informatice a crescut doar în perioada ianuarie - iunie 2002, față de întregul an 2001, cu 64% (www.zidezi.ro). Această informație a fost publicată de către compania Riptech, care a încercat să sublinieze faptul că atacurile hackerilor au tendința de a deveni din ce în ce mai sofisticate. Din numărul total al atacurilor date de hackeri în perioada ianuarie-iunie 2002, 4/5 au fost date de către „piraiți” din: Statele Unite ale Americii, Germania, Coreea de Sud, China, Franța, Canada, Italia, Taiwan, Marea Britanie și Japonia. Elan Yoram, unul dintre autorii acestui raport, a ținut să facă precizarea că aceste cyber-atacuri pot proveni și din țări cunoscute ca fiind adăpostul anumitor grupări teroriste. Printre aceste țări au fost menționate Iran, Pakistan, Kuweit și Indonezia. „Este aproape imposibil să se stabilească o linie de demarcație clară între atacurile hackerilor și cyber-terorism, deoarece ambele tipuri de atacuri se fac tranzitând spațiul internetic, folosind de cele mai multe ori serverele publice”, a ținut să sublinieze Yoram.

„Cooperare «împotriva naturii» între neonaziști și extremiștii evrei”, titrează cotidianul timișorean „Agenda zilei” în vara lui 2003, preluând un articol de la Agenția „Reuters”. Iar în subtitlu, aceeași publicație scrie: „Alianța a inundat rețeaua mondială cu mesaje de ură la adresa arabilor”.

Așadar, și mișcarea neonazistă pare că suferă de păcatul numit „aripi”. De la colaborarea dintre naziști și musulmani împotriva evreilor, iată că există naziști „dispuși să-și uite propriile vederi antisemite pentru a pune la cale o cooperare uluitoare cu grupări extremiste evreiești din țară (Franța, n.n.). Această colaborare, prin Internet, i-a ajutat pe neonaziștii francezi să-și transplanteze mesaje de ură împotriva arabilor și musulmanilor în Orientul Mijlociu, iar pe extremiștii evrei să știe mai multe despre atacurile prin rețea împotriva site-urilor arabe.” Evident, o asemenea situație nu putea să-i scape lui Mouloud Aounit, directorul unei organizații antirasiste din capitala Franței. Acesta a dat publicității un raport de 170 de pagini cu privire la paradoxala cooperare născută din ura comună a celor două forme de extremism. Potrivit acestuia, nu mai puțin de 26 de site-uri aparținând extremei drepte franceze și grupărilor extremiste evreiești din Franța plătesc găzduirea paginilor web pe același server din S.U.A. cu începere din 1999, anul primului război electronic mondial. Dar, în cele din urmă, scrie publicația timișoreană, partajarea comună a spațiului pe serverul american a luat sfârșit. Motivul: puncte de vedere diferite referitoare la campania americano-engleză în Irak. Pur și simplu, unii dintre neonaziști (o altă aripă?) nu au fost de acord cu atacul aliat împotriva Irakului. „Pe site-urile respective există și îndemnuri de asasinare a președintelui Jacques Chirac, menționat cu numele de «Ben Shirak»”, încheie „Agenda zilei”.

Că Internetul poate fi transformat în armă o dovedește și activitatea cibernetică a așa-zisului anacronic Phenian. Tot „Agenda zilei” scria pe 17 mai 2003: „Phenianul are o armată de hackeri pricepuți - Războiul informațional e în toi”. Potrivit Agenției „Reuters”, al cărei material este preluat de publicația bănățeană, „...singurul server care susține site-urile oficiale nord-coreene se

află în Japonia. Dar realitatea este cu totul alta. În Coreea de Nord sunt antrenați anual circa 100 de tineri transformați în hackeri, soldații informaționali ai regimului.” Vecina din sud, Coreea soră, nu se află așadar amenințată numai de rachetele fraților comuniști din nord (posibil chiar atomice), ci și de cyber-atacuri. „La începutul acestui an, un virus a contaminat rapid aproape toate rețelele de calculatoare din Coreea de Sud, blocând și traficul pe Internet. A fost pentru prima dată când serviciile rețelilor din această țară au fost afectate într-o asemenea măsură. Se crede că a fost vorba despre un «exercițiu» de atac lansat de nord-coreeni.” Hoțul nepris este negustor cinstit, spune un proverb românesc. Cel care a afectat traficul pe Internet al sud-coreenilor putea să fie un frate nord-coreean, dar tot atât de bine putea să fie chiar un student sud-coreean. Numai că nu ar fi fost „politic” să nu se profite de o asemenea ocazie pentru a se crea „imagine”. Referindu-se la sud-coreeni în cartea sa „Lacrima - Orient și occident” (Ed. „Anthropos” Timișoara, 2000, versiune în limba română: Dușan Baiski), scriitoarea taiwaneză Chang Shiang Hua spune la un moment dat: „... o cunoscută mișcare de rezistență a studenților coreeni, o mișcare a sentimentelor naționale profunde, a luptei împotriva guvernării, împotriva Americii, poartă pecetea unui fanatism de puber care, de cum trece perioada exaltării tinerești, deseori se stinge de la sine. Așa că, la terminarea universității, o mulțime de asemenea activiști studenți extremiști caută de urgență debutul în «ape liniștite», ajungând astfel până la companiile americane, care oferă un salariu bun.” Și cum Coreea de Sud este una dintre cele mai informatizate țări din lume, cum și în această țară pot exista informaticieni cu păreri pro-nord-coreene, nu este obligatoriu de crezut că unul din cei o sută de nord-coreeni pregătiți pentru atacuri cibernetice este teroristul care a afectat Internetul sud-coreean.

În baza reclamațiilor primite de Centrul Împotriva Fraudelor pe Internet din S.U.A. pe parcursul anului 2002, pe primul loc la nivelul țărilor de pe teritoriul cărora au fost inițiate fraude se situează Statele Unite, susține cotidianul „The Sidney Morning Herald”. De ce nu ar fi fost posibil ca „înghețarea” Internetului sud-coreean să fi fost realizată de S.U.A., tocmai pentru a menține încordată situația din cele două Corei? Desigur, este doar o ipoteză, dar dacă americanii au fost în stare să mituiască generali „loiali” lui Saddam Husein pentru a intra apoi victorioși în Irak, de ce nu am accepta o asemenea ipoteză și în cazul la care ne-am referit? Din păcate, doar Dumnezeu știe care este adevărul. Împreună cu războinicii implicați. Referitor la clasamentul întocmit de cotidianul australian, „Renașterea bănățeană” din Timișoara enumera și celelalte țări din tristul clasament: după S.U.A. urmau Nigeria, Canada, Africa de Sud, România și Spania. Nu știm pe ce loc erau situați superhackerii singurului abonat nord-coreean la Internet, Kim Jong-il, dar e cam greu de crezut că providerul japonez ar fi lăsat nesupravegheată activitatea centurionilor comuniști din Peninsula. O activitate susținută, menită a bloca serverele Coreei de Sud, ar fi fost depistată imediat. Dar politica e politică.

În 2002, relatează presa internațională, președintele George W. Bush a semnat o directivă prin care stabilea datele lansării unor atacuri asupra rețelilor de calculatoare ale unor țări ostile Statelor Unite ale Americii. Acest ordin a fost deconspirat de cotidianul „The Washington Post”. Regulile pentru războiul informațional au fost pregătite în timp ce Pentagonul lua deja în considerare lansarea unor asemenea atacuri împotriva țărilor-țintă, scria „Reuters”. Mecanismul acestui război invizibil și tăcut s-ar putea să-și demonstreze capacitatea cu prilejul campaniei militare din Golf, a afirmat un oficial al Pentagonului, citat de cotidianul din capitala S.U.A. Alți oficiali cu funcții importante au declarat că S.U.A. nu au lansat niciodată atacuri informaționale (terorism de stat recunoscut indirect?) pe scară largă, însă de acum Pentagonul a început să lucreze la armele cele mai potrivite pentru atac. „Un scenariu posibil - scria „Agenda zilei” în 2003 - arată cum specialiștii armatei S.U.A., așezați în fața terminalelor de calculator, neutralizează cu câteva apăsări de tastă rețelele computerizate ale unei țări ostile «stingându-i» radarele, sistemul energetic național și întreaga rețea telefonică. Asta doar pentru deschidere...”

Cum vine asta, vă veți întreba? Orice om normal se întreabă de ce este necesar ca sistemele informatice sensibile să fie interconectate. De aceea pare stupefiantă afirmația că un atac terorist ar putea paraliza Internetul. Autori sunt nimeni alții decât cercetători din cadrul Universității din Ohio - S.U.A. Aceștia au demonstrat că principalele orașe vor avea acces la Internet chiar și în cazul în care rețeaua va funcționa la capacitate redusă, în vreme ce orașele mijlocii și mici vor fi deconectate. Costurile relativ mari pentru transmisia prin satelit, dar și pentru cea prin magistralele din fibră optică obligă providerii mai mici să se „aboneze” la cei cu putere financiară mai mare. Astfel că rețeaua seamănă cu o caracatiță. Dacă este distrus centrul, adică providerul

puternic, automat „pică” și providerii mărunți. Unul dintre universitarii din Ohio, Tony Grubestic, compara consecințele unui asemenea scenariu cu acelea care pot interveni în traficul aerian: „În cazul în care condițiile atmosferice opresc sau întârzie traficul pe un aeroport, ca O'Hare din Chicago, pasagerii din întreaga țară vor resimți consecințele. Acest lucru este valabil și pentru Internet.” Universitarii americani arată într-un studiu că, după atentatele teroriste din 11 septembrie, mai multe zone din jurul metropolei New York au fost deconectate de la Internet, iar portalurile nu au putut fi accesate timp de două zile. Același Grubestic este de părere că, din motive de securitate, rețelele de Internet nu trebuie concentrate în marile orașe și cere o mai mare descentralizare a Internetului. Ceea ce este echivalent cu a solicita încălcarea regulilor economiei de piață prin intervenția statului care fie sprijină prin fonduri publice întreținerea unor servere, fie introduce reguli speciale pentru providerii de Internet.

Atotprezentul „Reuters” este din nou citat masiv pe mapamond la sfârșitul lui octombrie 2002. Astfel, „România liberă” din București titra pe 30 octombrie 2002: „Hackerii proislamici pregătesc un război cibernetic”. O banală previziune a cuiva de la cunoscuta agenție de știri sau doar o bucățică dintr-un scenariu mai amplu de război psihologic? O picătură informațională în campania de pregătire psihologică a agresiunii americano-engleze împotriva Irakului? Nu știm, nu putem răspunde. Putem doar specula. Răspunsurile pot fi, în mod firesc, afirmative. Același „Reuters”, citând experți în probleme de Internet, preluat de cotidianul național românesc, spune că „Hackerii proislamici se află în prima linie a unui potențial război cibernetic după decizia așanumiților «hacktiviști» și a creatorilor de viruși de a rupe armistițiul autoimpus după atentatele din 11 septembrie 2001 din S.U.A.”. Pirații ciberneticii proislamici și-au intensificat atacurile împotriva țărilor care sprijină războiul dus de S.U.A. împotriva terorismului și campania sa împotriva Irakului, în timp ce virusul „bugbear” și atacul eşuat asupra Internetului demonstrează că hackerii au ieșit din nou la vânătoare. Firma britanică „MI2G” din Londra a anunțat că octombrie 2002 poate concura la titlul de cea mai neprielnică lună din cauza atacurilor electronice - 16 559 la număr. Aceeași companie - care oferă consultanță privind securitatea pentru bănci și firme de asigurare și reasigurare, a subliniat că atacurile motivate politic au crescut semnificativ. „România liberă” citează responsabili ai acestei companii: „Am remarcat că din ce în ce mai multe grupuri de hackeri care sprijină interese islamice au început să se unească, urmărind o agendă comună antiamericană, antibritanică, antiaustraliană, antiindiană și antiisraeliană.” Dean White, coordonatorul Centrului Sans (dedicat Internetului) pentru Asia-Pacific, referindu-se la părerea experților în domeniul Internetului, afirma: „Trebuie să ne așteptăm la un atac și să fim pregătiți, a fost liniște prea mult timp, mai mult ca sigur că urmează să se întâmple ceva.” Potrivit „MI2G”, dintre grupurile de hackeri active în octombrie 2002 trei erau proislamice (din păcate, nu se dă numărul total pentru a ne face o părere clară asupra proporției grupărilor proislamice). Cităm din „România liberă” din 30 octombrie 2002: „Unul dintre ele (dintre cele trei grupuri proislamice, n.n.) se numește «Unix Security Guards» (USG), un grup de hackeri format în mai 2002 și despre care se crede că este compus din alte entități mai mici, variind de la «EgyptianFighter» până la hackerii din fostele republici sovietice musulmane și până în Maroc. USG și-a înzecit atacurile în interval de o lună, de la 21 înregistrate în august, și până la 207, în septembrie. Numai în octombrie USG, se poate «lăuda» cu 1 511 atacuri. Alte grupuri active de hackeri sunt «FBH» (Federal Bureau of Hackers - biroul federal al hackerilor), bănuie că ar avea sediul în Pakistan, și «The Bugz» majoritar pakistanez. Creșterea atacurilor virtuale proislamice coincide cu atacul fără precedent de săptămâna trecută pe 9 din cele 13 servere principale care formează coloana vertebrală a rețelei Internet. Oficialitățile de la Washington au încercat să minimalizeze incidentul și sugestiile că ar fi vorba de «cyberterrorism», însă experții informaticieni spun că, indiferent de vinovat, acest atac a evidențiat vulnerabilitatea infrastructurii de comandă și control.”

O concluzie (de ce nu, sugerată) ce se poate trage este că, dacă se întâmplă ceva rău, indiferent ce, pro-islamicii vor fi de vină și nicidecum o eroare pur umană sau un atac din interior. Ce se întâmplă însă dincolo de fosta „cortină de fier”? O știre provenind de la aceeași atotștiutoare agenție de știri „Reuters” (?!), citând o sursă din cadrul fostului K.G.B., este preluată pe 16 octombrie 2002 de „Renașterea bănățeană”: „Hackerii au încercat, în 2002, de un milion de ori să acceseze, în mod ilegal, site-ul oficial al F.S.B. (Serviciul Federal de Securitate rus)... Numărul tentativelor de piraterie informatică s-a dublat în comparație cu anul trecut, la data de 1 septembrie depășind cifra de 760.000 de cazuri, a precizat aceeași sursă. Potrivit oficialului din cadrul F.S.B., «nu este vorba de activitatea serviciilor străine», ci de încercările tinerilor

preocupați de Internet, de a-și «dovedi îndrăzneala». Hackerii sunt, «cel mai adesea minori, iar dat fiind că nu reușesc să spargă codurile, nu există vreo acțiune de urmărire», a explicat sursa din cadrul F.S.B..” Așadar, nici pomeneală de atacuri cibernetice din partea cecenilor sau a aliaților acestora. O „omisiune” calculată din partea oficialului F.S.B. citat de „Reuters” sau chiar realitatea? Sau să fi suferit americanii adevărate traume psihice după 11 septembrie și acum văd în jur doar dușmani? „România liberă” din 11 septembrie 2002 scria, exact la un an după atacul terorist asupra S.U.A.: „Atacurile teroriste împotriva Statelor Unite din 11 septembrie 2001 au atras atenția asupra unui alt fenomen periculos: folosirea Internetului de către grupările teroriste, pentru comunicații, recrutare și colectare de fonduri. Chiar și acum, în condiții de securitate sporită, AL-Qaeda se folosește de Internet pentru a pune la cale noi atacuri. Experții au ajuns la concluzia că teroriștii au studiat cu mare atenție sistemul telefonic american, alimentarea cu apă, serviciile publice, dirijate computerizat. [...] De altfel, avertismente cu privire la un posibil atac cibernetic s-au înregistrat destul de des după 11 septembrie 2001. Astfel de atacuri sunt greu de prevăzut, iar efectele lor ar fi devastatoare, în condițiile în care mare parte din servicii - de la tranzacții financiare la asigurări sociale - se bazează pe Internet și utilizează baze de date computerizate.” Parcă totul aduce cu isteria provocată de virusul mileniului, care s-a dovedit un mare fâș susținut cu abilitate de către cei interesați. Iată ce scria în 1990 cunoscutul autor de science fiction Arthur C. Clarke în cartea sa „The ghost from the grand banks” (apărută în limba română sub titlul „Fantoma adâncurilor”, Ed. Valdo, 1992): „Până în 1960, din ce în ce mai multe calcule ale lumii fuseseră preluate de computere și procesul se încheiase acum definitiv. Milioane de memorii optice și electronice înmagazinaseră trilioane de tranzacții - practic toate afacerile planetei. Și, desigur, multe din aceste intrări purtau o dată. Când a început ultimul deceniu al secolului, ceva ca o undă de șoc a străbătut lumea financiară. Și deodată, dar tardiv, au realizat că celor mai multe dintre aceste date le lipsea componenta vitală. Funcționarii umani de bancă, cei care țineau ceea ce încă se mai numea «contabilitatea», arareori se oboseau să scrie «19» înaintea următoarelor două cifre. Acestea erau luate drept bune, era o chestiune de bun simț. Iar bunul simț, din păcate, era vădit că le lipsea computerelor. Și, în primii zori ai lui '00, miriade de îndobitociți de electronică își ziceau «00 este mai mic decât 99 ». Așa că astăzi este mai devreme decât ieri - cu exact 99 de ani. Recalculați toate depășirile de cont, ipotecile, operațiile curente pe această bază...”

Evident, uneori nu mai știi unde se termină imaginația și începe realitatea, însă e greu de crezut că omul se poate lăsa pe mâna computerelor fără a-și lua toate măsurile de protecție. Imaginați-vă doar o banală pană de curent care să întrerupă un serviciu vital într-un oraș cu două milioane de locuitori. Ar fi o dovadă de prostie crasă pentru un manager să accepte un asemenea lucru. Un banal circuit electric casnic este prevăzut cu siguranțe în caz de scurtcircuit. Darămite un serviciu vital controlat de computer. Da, veți spune, dar dușmanul poate avea implantați oameni în interiorul sistemului. Deci mai rămân 50% șanse pentru un reușit atac terorist cibernetic. Însă așa cum înșiși oamenii din cadrul C.I.A., F.S.B. sau S.R.I. sunt, la rândul lor supravegheați, și în serviciile publice vitale, teoretic, ar trebui să existe supervizori. Așadar, șansele unui atac se reduc la 25%. Ei bine, calculele pot duce chiar până la un 0,001%, ceea ce înseamnă că un atac tot ar fi posibil. Este evident că da. Dar fără a minimaliza rolul controlului cibernetic asupra unor procese din cadrul serviciilor publice, nu putem crede că vreo națiune este atât de naivă încât să nu dubleze sau să tripleze măsurile de securitate. Și atunci, la ce bun atâta isterie vizavi de posibilele efecte catastrofale ale unui atac cibernetic? Ne temem oare de calitatea forței de muncă? Să fie tehnica mai presus de om? Nu mai există nici o fărâmbă de patriotism la cei puși să ne apere? Cercetători ruși prost plătiți, ajunși în slujba lui fitecine, valize atomice vândute pe-un pachet de mahorcă... Totul este posibil. Dar să nu disperăm. Drobul de sare poate fi coborât. Practică însă și americanii hacking-ul patriotic? Se pare că da. „România liberă” din 3 octombrie 2002 scria că S.U.A. au lichidat site-ul „Cercetări islamice” al organizației teroriste internaționale Al-Qaeda la numai 12 ore de la apariția acestuia în rețeaua Internet. „În cele câteva ore de existență, pe site au apărut informații cu privire la Osama bin Laden, o declarație a secretarului de presă al rețelei Al-Qaeda și un mesaj către prizonieri de la baza Guantanamo, prin care aceștia erau îndemnați să reziste.” Numai că, asemenea unei hidre cu o mie de capete, de tai un cap, răsare altul. Același cotidian românesc continuă: „Marți a reapărut însă pe Internet site-ul «Jihadul on-line», închis de S.U.A. anterior și care îi aparține - potrivit ziarului saudit «As Sharq Al Ausat» - lui Abdurrahman Ar-Rashid, cetățean al unuia dintre statele din Golf. Primele informații

au fost dedicate în totalitate lui Khattab - liderul ucis al mujahedinilor arabi din Cecenia.” Iată însă și o altă știre publicată în mass-media românească, de data aceasta în 2003. Site-ul postului de televiziune prin satelit „Al-Jazeera”, al cărui sediu se găsește în micul stat arab Qatar, a fost blocat în urma a mai multor atacuri. Oficialii postului, citați de A.F..P., au dat vina pe americani. Abdel Aziz Al-Mahmud, redactorul șef al ediției electronice al „Al-Jazeera”, a declarat că este vorba despre „atacuri masive” declanșate după ce acest cunoscut post de televiziune a difuzat imagini cu cadavrele soldaților americani uciși sau executați de irakieni.

Imediat după atacul terorist asupra World Trade Center din New York, hackeri neidentificați au blocat aproape toate paginile oficiale de pe Internet ale Afganistanului, în vreme ce în multe pagini dedicate lui Osama bin Laden și talibanilor au fost inserate alte conținuturi. De asemenea, a fost lansat și un virus denumit „WTC”. Acesta era transmis prin poșta electronică, emițătorul anunțând în corpul mesajului că fișierul atașat conține informații despre distrugerea turnurilor gemene (www.danas.org, 18 septembrie 2001).

Un grup de hackeri pakistanezi a atacat pe 17 octombrie 2001 serverul Administrației Naționale pentru Ocean și Atmosferă (S.U.A.). În mesajul trimis, hackerii spuneau: „Chiar dacă guvernul pakistanez condamnă atacul asupra S.U.A., noi susținem Al Qaeda. Deținem niște informații secrete aparținând guvernului american pe care le vom preda organizației Al Qaeda. Lăsați-ne în pace și vă vom lăsa în pace.” După cum scria pe www.sksu.net, hackerii solicitau S.U.A. să-și retragă forțele armate din Arabia Saudită, să înceteze să bombardeze Afganistanul și să înceteze să susțină Israelul. De asemenea, mai amenințau că vor schimba fața altor site-uri, însă nu vor fura date întrucât acest lucru nu este etic.

Interesant este însă faptul că, prin atacul din 11 septembrie 2001 asupra turnurilor gemene World Trade Center, Al Qaeda devine cea dintâi organizație ca fiind „statul virtual” „Statul virtual, scrie Philip Bobbitt în «Time», citat de publicația croată «Vjesnik» (www.vjesnik.com), are multe trăsături ale altor state (o armată și o inteligență antrenate, trezorerie și surse de venituri, structură administrativă și un fel de asigurări sociale pentru familiile luptătorilor săi), însă el nu are granițe, declară războaie, încheie alianțe cu alte state și, prin țelurile sale are un caracter global, nu are un loc definit pe harta globului pământesc. [...] În secolul 21, statele naționale ar putea fi înlocuite cu ceva ce s-ar putea numi «state economice». Statele economice vor avea frontiere și structuri administrative similare cu cele ale statelor naționale, însă răspunderile cheie vor fi trecute de la guverne la sectorul privat; corporațiile multinaționale vor prelua rolurile pe care un guvern nu le mai poate îndeplini și vor șterge granițele dintre liderul politici și liderul corporativ. Tocmai pentru că economia este particulară, globală și transnațională, statele economice vor putea mai bine decât cele naționale să se descurce cu un război care în parte este particular, o parte multinațional și o parte de apărare, așa cum vor fi războaiele în viitor... [...] La fel ca moartea, războiul va veni când va veni. S.U.A. ar putea ajuta în stabilirea a ce fel de Război lung va veni. Acest război poate fi caracterizat de către statele naționale cu o populație din ce în ce mai bătrână care încearcă să se opună tot mai puternicelor state economice, în vreme ce statele virtuale se vor înclina când înspre o parte, când spre alta. Cu siguranță că vom vedea conflicte între forme concurențiale ale statelor economice. Poate fi vorba și de un război cronic, cu intervenții de mică intensitate - acțiuni polițienești cu motive umanitare; [...] Războiul s-ar putea purta și între anumite regiuni sau poate între marile puteri care pun în mișcare atacuri virtuale acoperite - pentru ca apoi atacurile hackerilor să degenereze în declanșarea unui conflict armat.” Într-un raport al Consiliului Național de Cercetare din S.U.A. intitulat „Computere în criză”, se spune că „Teroristul zilei de mâine ar putea fi capabil să provoace daune mai mari cu un keyboard decât cu o bombă”. Internetul este intens folosit de diverse grupări teroriste întrucât este mijlocul perfect pentru a organiza și a conduce acțiuni de la distanță, în perfect anonim și în perfectă siguranță. Prin utilizarea unor tehnici de criptografiere tot mai sofisticate și folosind specialiști în informatică dintre cei mai buni, organizațiile teroriste le transmit subordonaților nu doar ordine, ci și planuri de acțiune, fotografiile ale celor vizați pentru a fi lichidați, instrucțiuni, coduri și hărți.

Pe de altă parte, Internetul este ideal pentru răspândirea unei ideologii sau alteia. În lucrarea lor intitulată „Internetul, criminalitatea și dreptul”, prof. univ. dr. Dan Banciu și conf. univ. dr. Ion Vlăduț scriu: „Un exemplu în acest sens îl reprezintă organizația teroristă Drumul luminos din Peru, care, dispunând de un site pe Web, își promovează propria ideologie extremistă. Interesant este faptul că, așa după cum constata fostul șef al operațiunilor F.B.I., Buck Revell, atâta timp cât

mesajele acestor grupări fac numai propagandă pentru ideologia lor, fără să treacă la acțiuni criminale, teroriștii pot desfășura liberi activități, astfel încât Internetul a devenit un adevărat «rai» pentru ei.”

Simpatizanții diverselor organizații teroriste construiesc site-uri de simpatie. După ce gruparea teroristă „Tupac Amaru” a ocupat reședința ambasadorului Japoniei în Peru, în decembrie 1996, luând ostateci membrii ambasadei și pe invitații acestora, simpatizanții din S.U.A. și Canada ai organizației amintite au realizat o serie de site-uri de simpatie.

Dar Internetul este foarte utilizat și pentru diseminarea mesajelor de ură și incitare la violență. Nu puține sunt site-urile antisemite și antioccidentale. Numai că, susțin autorii amintiți mai înainte, „...în S.U.A. se consideră că informațiile difuzate pe Internet țin de dreptul la liberă exprimare, riposta autorităților față de construirea site-urilor de către grupările teroriste fiind destul de delicată. Astfel, în această țară, deși paginile Web ale grupărilor teroriste sunt publice, F.B.I.-ul nu are voie să facă dosare cu fișierele respective decât atunci când investighează un anumit caz care a fost aprobat de procuror.” Astfel că, concluzionează aceiași autori, „... grupărilor teroriste nu le-a trebuit prea mult timp să înțeleagă faptul că un mijloc de presiune la fel de spectaculos, dacă nu mai mult, decât plasarea unor bombe în diferite locuri publice, îl reprezintă distrugerea infrastructurilor informatice și periclitarea vaselor rețele.”

În acest context, se cuvine să amintim faptul că în timpul agresiunii N.A.T.O. asupra Iugoslaviei, au devenit foarte active grupările antisemite și antisemiții individuali, vinovați pentru atacul N.A.T.O. asupra Iugoslaviei fiind considerați evreii americani prezenți în structurile de conducere ale S.U.A. Pe listele de discuții sârbești și-a făcut apariția și lista conținând numele și poziția acestora. Iat-o:

1. Secretary of State - Madeleine Albright
2. Secretary of the Treasury - Robert Rubin
3. Secretary of Defense - William Cohen
4. CIA chief - George Tenet
5. Head of Nat. Sec. Council - Samuel Berger
6. Secretary of Agriculture - Dan Glickman
7. Chairman of the Fed. Res. Board - Alan Greenspan
8. Health Care Chief - Sandy Kristoff
9. Head of Voice of America - Evelyn Lieberman
10. Under Secretary of State for Europe - Stuart Elsenstat
11. U.S. Trade Representative - Charlene Barshefsky
12. Chief Aide to the First Lady - Susan Thomases
13. Heads National Economic Council - Gene Sperling
14. Heads National Health Care Policy - Ira Magaziner
15. Deputy Secretary of State - Peter Tarnoff
16. Ass. Sec. of State for Congressional Affairs - Wendy Sherman
17. On Board of Economic Council - Alice Rivlin
18. On Board of Economic Council - Janet Yellen
19. Presidential Advisor - Rahm Emanuel
20. Council to the President - Doug Sosnik
21. Deputy National Security Council - Jim Steinberg
22. NSC Senior Director for Speechwriting - Anthony Blinken
23. Drug Policy Coordinator - Robert Weiner
24. Special Liaison to the Jewish Community - Jay Footlik
25. Presidential Personal Chief - Robert Nash
26. Presidential Attorney - Jane Sherburne
27. Asian Expert on Security Council - Mark Penn
28. Communications Aide - Robert Boorstine
29. Communications Aide - Keith Boykin
30. Special Assistant to the President - Jeff Eller
31. National Health Care Advisor - Tom Epstein
32. National Security Council Member - Judith Feder
33. Asst. Sec. of Veterans Affairs - Richard Feinberg
34. Deputy Head of Food and Drug Admin. - Herschel Gober

35. White House council - Steve Kessler
36. Asst. Secretary of Education - Ron Klein
37. Director of Press Conferences - Margaret Hamburg
38. Director of St. Dept. Policy - Karen Alder
39. Member National Security Council - Samuel Lewis
40. Member of the National Security Council - Stanley Ross
41. Director of the Peace Corps - Dan Shifter
42. Deputy Chief of Staff - Eli Segal
43. Dep. Director of Man. and Budget - Jack Lew
44. Under Secretary of State - James P. Rubin
45. Under Secretary of the Treasury - David Lipton
46. Special Council to the President - Lanny P. Breuer
47. Special Representative to NATO - Richard Holbrooke
48. Chief of Social Security - Kenneth Apfel
49. Deputy White House Council - Joel Klein
50. Special Advisor to the First Lady - Sidney Blumenthal
51. Chief of Food and Drug Administration - David Kessler
52. Acting Solicitor General - Seth Waxman
53. Presidential Pollster - Mark Penn
54. Special Middle East Representative - Dennis Ross
55. General Counsel for the FBI - Howard Shapiro
56. White House Special Counsel - Lanny Davis
57. Secretary of Management and Budget - Sally Katzen
58. Heads FBI Equal Opportunity Office - Kathleen Koch
59. Deputy Chief of Staff - John Podesta
60. Vice Chairman of Federal Reserve Board - Alan Blinder
61. Heads Council of Economic Advisors - Jane Yellen

Lista am preluat-o din site-ul lui Boris Pribich, un cetățean american de origine sârbă, foarte activ în materie de antisemitism. Contactându-l pentru a-i cere aprobarea pentru preluarea unor fragmente din paginile sale web (vezi <http://MediaLies.com/>; <http://CompuSerb.com/>; <http://VoteForUSA.com/>; <http://SerbianDefenseLeague.com/>; <http://AmericanDefenseLeague.com/>), ne-a solicitat imperios să nu trecem sub tăcere implicarea evreilor americani în agresiunea N.A.T.O. asupra Iugoslaviei. Câtă dreptate are acest om va decide doar istoria. Cert este însă faptul că, interesându-ne mai îndeaproape de activitatea sa, am dat peste o listă de discuții a evreilor de pe Yahoo, respectiv „EEJH” Jewish History, unde Pribich este considerat „...Mr. alias Boris Primich's Organization, should be investigated by FBI and State Department, as Terrorist Fascist/Hitlerist Organization”, opinia fiind a semnatarului e-mail-ului și anume un anume dr. Sigmund Mittler, M.D. Professor.

Tot pe unul din site-urile lui Pribich am dat și peste un text intitulat „Cine controlează media din S.U.A.”, unde autorul face o radiografie a mijloacelor de informare și divertisment din Statele Unite din punctul de vedere al naționalității fondatorilor, proprietarilor sau actualilor conducători, concluzia fiind clară: evreii conduc media în S.U.A. și pot influența și/sau manipula extrem de ușor opinia publică în favoarea lor sau împotriva persoanelor și/sau statelor considerate inamice. Unul dintre principalii vinovați de agresiunea din 1999 asupra Iugoslaviei este considerată Madeleine Albright, pe atunci secretarul de stat al S.U.A. Tot pe unul din site-urile lui Boris Pribich am dat și peste un text dedicat acesteia și intitulat „Dosar secret: Zilele belgrădene ale lui Madeleine Albright. Cum a uitat limba sârbă.” Autorul articolului, scris în 1997, pe când Albright era ambasadorul S.U.A. la O.N.U. este Momir Ilić, un ziarist care a stat de vorbă cu foștii ei prieteni și colegi de școală din Belgrad. Trebuie reținut că Joseph Korbel, tatăl lui Madeleine Albright, a fost ambasadorul Cehoslovaciei la Belgrad pe timpul președinției la Praga a lui Benes, iar viitorul secretar de stat al S.U.A. și-a petrecut aici o bună parte a tinereții. Cu atât mai ciudată devine din acest punct de vedere aversiunea ei ulterioară față de sârbi. Faptul că familia de evrei cehi Korbel a părăsit la un moment dat Cehoslovacia, de teama de a nu fi exterminată de naziști, și a ajuns în Iugoslavia pentru a fi ajutată să plece de aici în America, cu ajutorul sârbilor, nu a mai contat în acțiunile din 1999 ale lui Madeleine Albright. Poreclită pe Internet „baba cu coaie de oțel”, Albright a fost, este și va rămâne în memoria sârbilor drept una din maleficele ființe umane

din istoria acestuia.

Dacă ar fi să tragem câteva concluzii, nici nu e de mirare că sentimentele antisemite ale multor sârbi par a fi perfect justificate: media americană, controlată de evrei, a jucat un rol esențial în istoria deciziei de atac asupra Iugoslaviei, iar faptul că Executivul american a fost la timpul respectiv plin de evrei, cu Madeleine Albright în frunte (nu mă lăsa să mor că n-o să te las să trăiești...) poate duce și la ideea unei conspirații bine concertate a evreilor împotriva poporului sârb. Câtă dreptate au sau nu antisemiții declarați ori chiar simpli sârbi care cred asemenea lucruri, doar Dumnezeu poate ști.

Internetul ca mijloc de propagandă

Miloš Urošević scria pentru membrii listei de discuții serbianforum (<http://www.eGroups.com/list/serbianforum>): „Pe CNN au publicat faptul că Pentagonul are probleme cu identificarea țintelor pe care le-au nimerit sau nu. Pentru aceasta se folosesc de orice izvor de informație, oricum și de acesta de față (lista de discuții, n.n.). Vă rog, fraților din Iugoslavia, nu descrieți detaliat ceea ce a fost nimerit (de bombe, n.n.), ci doar din ce direcție s-au auzit detonațiile. Cu cât sunteți mai nehotărâți, cu atât mai bine.” Nu cumva era vorba de un ordin prin CNN pentru spionii americani aflați în acel timp pe teritoriul Iugoslaviei să-și facă mai bine treaba și să trimită detalii despre efectele bombardamentelor? Sau să fi fost însuși individul cu numele de Miloš Urošević cel care a retransmis acest ordin, spionii americani fiind cuplați la lista de discuții serbianforum? Evident, totul este posibil. Nu există mijloc mai facil pentru transmiterea de informații decât Internetul, mai cu seamă că poșta electronică poate transporta de la expeditor către destinatar nu doar un banal text, ci și imagini statice ori în mișcare și fișiere audio. Este adevărat că în Timișoara, în zilele fierbinți ale lui decembrie 1989 și chiar în ianuarie 1990 era relativ periculos să fii văzut pe stradă fotografiind ori filmând. Însă pe-atunci încă mai persistau prejudecățile și ferocea teamă de Securitate. În 1999, însă, când existau aparate digitale de fotografiat și filmat miniaturale, nu era greu să filmezi un pod distrus la Novi Sad, să fugi în apartament și să transmiți imaginea direct din aparat, prin e-mail, către cel care te-a angajat să spionezi. Chiar și într-o Iugoslavia cum era cea de sub Milošević, aflată în plin război. În același mesaj, Miloš Urošević îi sfătuia pe membrii listei de discuții să viziteze site-urile albaneze, citând „Kosova press” care dădea informații despre pozițiile exacte ale forțelor iugoslave la Drenica și în alte localități din Kosovo, și să anunțe cele mai apropiate posturi de miliție care, la rândul lor, să anunțe armata că se află în pericol. În încheiere, Urošević scria: „Acțiunea: Toți suntem ținte!”

Brazilianul Leo Villanova scria la lista de discuții nato-agresija-na-srj, găzduită de www.egroups.com, despre transmisiile TV prin cablu prin care americanii solicitau ajutor umanitar pentru victimele tornadelor, aceasta în vreme ce tot ei, americanii, ucideau în Iugoslavia mii de civili, iar costul unei rachete „Tomahawk” era de 1 000 000 USD.

Nenad Čuturić din Sundsvall, Suedia, scria tot pentru nato-agresija-na-srj cum că în casa prietenului său Joseph s-a întâlnit cu un individ în civil care s-a prezentat a fi ofițer în Bundeswehr. Acesta i-a adus la cunoștință că a văzut într-o bază militară aeriană faptul că militarii care încărcău materialele de propagandă (fluturași) în avioane erau cu toții îmbrăcați în costume speciale împotriva microorganismelor. Drept urmare, Nenad îi atenționa pe cei din țară să nu pună mâna pe fluturașii aruncați pe teritoriul Iugoslaviei, deoarece exista pericolul să fie contaminați. Dacă e să ne gândim la faptul că forțele NATO au bombardat Iugoslavia și cu bombe ce conțineau în componența lor și uraniu, nu este exclus ca necunoscutul din casa lui Joseph să fi fost într-adevăr ofițer Bundeswehr. Desigur, este o simplă speculație, însă care poate avea în sine un grăunte de adevăr.

Astăzi – e-politie, mâine – cyberwarior

Donald Rumsfeld, ministru american al apărării, a declarat în primăvara lui 2002 că armata americană se pregătește pentru un răspuns rapid și ferm în cazul unui atac cibernetic. „Provocările noului secol sunt deosebite de acelea ale secolului abia încheiat” – a afirmat el în cadrul unei conferințe despre apărarea națională, ținută la Washington (www.klik.hr/). „Am învățat multe de la primul război al secolului 21, însă nu trebuie să credem că teroriștii sunt unica amenințare. Viitoare amenințări cu care se va confrunta America pot fi teroriștii, un conflict tradițional între două state ori ceva cu totul altfel – un război cibernetic de amploare.” Armata Statelor Unite ale Americii a realizat un site intern prin care generalii aflați pe teren și echipa din S.U.A. vor aduce hotărâri importante, dacă nu cumva vor conduce chiar un război. Toate informațiile și conținuturile comunicațiilor vor fi adunate într-un singur loc, iar prin intermediul chat-ului se vor transmite ordinele. Întreaga infrastructură, respectiv partea principală a acesteia, se va afla într-un cort. Cheia constă în faptul că doar cu două click-uri de mouse se poate ajunge la orice informație importantă. Site-ul este pe deplin sigur vizavi de atacurile hackerilor și ale celorlalți răufăcători din domeniul IT.

La rândul său, pentru a ține pasul cu progresul tehnologic, poliția britanică a înființat o unitate națională de luptă împotriva criminalității cibernetice. Obiectivul acesteia este vânatoarea a tot mai multor criminali care-și conduc afacerile prin intermediul Internetului. Pentru dezvoltarea unității, spun cei de la www.becki-informator.at, s-au cheltuit mai mult de 25 de milioane de lire sterline. În componență intră 40 de specialiști care-și vor desfășura activitatea într-un sediu secret din Londra. S-a concluzionat, potrivit ultimelor studii, că Internetul a devenit cel mai bun loc unde bandele organizate utilizează calculatorul pentru tot soiul de fărâdelegi, de la pedofilie până la hackeri, care amenință utilizatorii și sistemele din întreaga lume. Alarmant este și faptul că mai mult de 60% din afacerile on-line britanice au fost ținte ale atacurilor hackerilor.

Nu mult timp după agresiunea NATO asupra Iugoslaviei, dr. Slobodan R. Petrović, polițistul iugoslav de care am mai pomenit în această carte, își exprima temerea că, după readmiterea oficială a poliției iugoslave în Interpol, crackerii și carderii iugoslavi vor fi urmăriți de societățile de asigurări străine care au acoperit pagubele produse de aceștia diferitelor companii, îndeosebi din S.U.A. Iar pe lângă problemele cu mașinile furate, lumea va insista pe criminalitatea pe Internet.

În cyberspațiu totul e posibil

Nu, nu este o afirmație atât de gratuită precum pare dacă avem în vedere faptul că Internetul își are deja și un patron spiritual: Sfântul Isidor de Sevilla.

Pe 13 aprilie 2002, cotidianul românesc „Ziua” titra: „«Papa a murit» au scris hackerii pe site-ul RAI”. Știrea, apărută pe site-ul televiziunii italiene RAI, cu toate că era falsă, a fost preluată și de alte site-uri, care au adăugat și un necrolog dedicat Papei Wojtyła.

Ion Iliescu, președintele României, vizitând în 2001 compania românească „Romsys”, unul dintre cei mai importanți furnizori de servicii informatice din România folosite în domeniile financiar-bancar, medical, învățământ și guvernamental, afirma că hackerii „pot deveni factori constructivi” și că „Acum ei își folosesc inteligența pentru șmecherii, dar pot fi folosiți”. Pe de altă parte, Victor Grădinescu, directorul serviciilor informatice din cadrul firmei sus-amintite, era de părere că este bine „să-i angajăm pe hackeri pentru sistemele de securitate și pentru testarea lor” (sursa: <http://cicero.kappa.ro/arhive/2001/07/19>).

Beta-AFP scria, la 26 iunie 2002, despre un protest original al proprietarilor de Internet-café-uri din Grecia. Supărați că Executivul elen plănuia să interzică distracția electronică în locurile publice, membrii Asociației Naționale a Proprietarilor de Internet-café-uri din Grecia a organizat

un Internet-caffé în piața centrală din orașul Salonic, instalând acolo mai mult de 300 de computere. Guvernul grec a decis să facă un asemenea pas întrucât a constatat că în tot mai multe cazuri jocurile electronice se transformă în jocuri de noroc.

Aceeași agenție de presă se referea, în aceeași zi, și la închiderea a 200 de Internet-caffé-uri la Shangaj, după ce 24 de persoane au murit într-un incendiu provocat la un asemenea club din Beijing de către tineri nemulțumiți că li se interzice accesul. În capitala chineză au fost închise, din aceeași cauză, toate Internet-caffé-urile (din cele 2 400 existente aproximativ 2 200 nu aveau autorizații de funcționare).

Politicienii își fac campanie prin spam-uri. Candidatul californian Bill Jones, în timpul campaniei sale electorale, s-a folosit din plin de Internet, însă într-un mod greșit. Politicianul a trimis e-mail-uri utilizând servere din Coreea de Sud. Aceasta i-a fost cea de-a doua campanie în care s-a folosit de spam-uri, deoarece doar cu un an înainte a utilizat o asemenea metodă pentru a câștiga voturi. Purtătorul de cuvânt al politicianului a recunoscut că pentru campania prin intermediul e-mail-urilor au folosit o a treia parte, pe care nu a dorit să o nominalizeze. Activiștii împotriva spam-urilor și utilizatorii care au primit asemenea e-mail-uri au fost deosebit de furioși, ceea ce, cu siguranță, a avut un efect deosebit de negativ asupra campaniei politicianului în cauză.

Cu atacuri DoS împotriva naziștilor. Aceasta era, la un moment dat, în 2001, esența unei informații publicate în publicația germană „Der Spiegel” și preluată de mass-media internațională. Otto Schily, ministrul german al afacerilor interne, a găsit o soluție viabilă pentru a opri atacurile din partea site-urilor naziste: atacurile DoS (Denial of Service). Pentru a apăra infrastructura germană de Internet, același Otto Schilly a înființat în cadrul ministerului condus de el o secție specială care se ocupă cu apărarea părții germane a cyber-spațiului.

Nu întotdeauna hackerii pătrund într-un sistem informațional din proprie inițiativă. Dovadă este și invitația lansată de către doi sponsori americani deloc anonimi, respectiv „Infosec” și „Argus Systems Group”, la participarea la un concurs dotat cu un premiu 35000 de lire sterline pentru cel care reușește să „spargă” „PitBull”, un software de securitate. Câștigător trebuia să fie acela care reușește să pătrundă în servere și să modifice paginile web ale companiilor xType Moto-Rockets și xCursion Adventure Travel. Câștigători au fost hackerii polonezi, membri ai grupului autointitulat „LSD” (Last Stage of Delirium).

„La capitolul absurdități legislative, România a fost detașat depășită de Grecia”, scria la un moment dat Eugen Secmerein în 2002, în publicația românească „eWeek”. Dar despre ce este vorba? Citând „ZDNet”, autorul pomenește despre faptul că Parlamentul de la Atena a aprobat Legea nr. 3037/2002 prin care se interzice explicit practicarea oricăror jocuri „care conțin mecanisme electronice și software” la domiciliu sau în locuri publice. Altfel spus, cei surprinși că joacă diverse jocuri pe computer, video, X-Box, console, telefoane mobile PDA etc. puteau fi pedepsiți cu amenzi usturătoare cuprinse între 5 000 și 75 000 de euro, dar, într-o fază ulterioară, și cu închisoare de la o lună la 12 luni.

Din aprilie 2001, austriecii au o întreprindere de stat care regularizează și plătește expedierea de e-mail-uri. „Austria Email”, scria „BOL”, înregistrează fiecare e-mail trimis și, prin ISP-urile locale, plătește utilizatorilor finali câte un șiling/e-mail-ul, din care 10% se duc spre compania prin al cărei software a fost trimis e-mail-ul. Această măsură nu a întâmpinat aproape nici un fel de probleme din partea internauților. Reprezentantul guvernului a afirmat că, cităm: „Comunicația prin e-mail este același lucru cu distribuția apei ori a energiei electrice și trebuie să fie regularizată de către stat.”

Sub presiunea atacurilor cotidiene din partea hackerilor din întreaga lume – scria „Klik” în mai 2001, guvernul american s-a gândit cum să-și îmbunătățească sistemele de securitate informațională și anume prin atragerea de partea sa a hackerilor care doresc burse de studiu. Prin colaborarea dintre Guvern și National Science Foundation – NSF, câte 200 de studenți vor beneficia de astfel de burse, urmând ca la terminarea studiilor să lucreze doi ani de zile pentru guvernul federal. Pentru aceste burse au fost alocați 8,6 de milioane de dolari.

În mai 2001, www.active-security.org anunța, preluând o informație de pe site-ul www.attrition.org, cum că www.attrition.org, pe care se află o importantă bază de date privind securitatea pe Internet, își va întrerupe rubrica unde apăreau deja de doi ani de zile adresele paginilor și site-urilor atacate de hackeri, munca fiind preluată de către aldas.de. Verificând link-ul către „Attrition”, o pagină web a lui www.active-security.org, am constatat că pagina respectivă

fusese ștearsă. Am căutat apoi adresa <http://aldas.de>. Nici vorbă de ceea ce mă așteptam, ALDAS fiind literele de început de la „Analytisches Labor Dr. Axel Schumann (...ein Labor für chemisch analytische Prüfungen. Wir untersuchen Boden, Wasser, Abwasser, Luft, Bodenluft und Material-Proben, Fertigprodukte...)”. Este aceasta încă o dovadă că pe Internet nimic nu e veșnic și nici sigur.

În septembrie 2001, Singapore și Belgia au semnat un document prin care se angajau să se atenționeze reciproc în ceea ce privește virușii, pentru a se apăra cu succes de pagubele pe care le creează virușii în domeniile economic și financiar.

Statele nu stau cu mâinile încrucișate în lupta cu hackerii, ele adoptând tot felul de legi, unele mai eficiente, altele total ineficiente. La rândul lor, anunțau cei de la thebu-siness.vnunet.com, hackerii grupului cDc (The Cult of the Dead Cow), cunoscut pentru „Back Orifice”, lucrau în 2001 la un browser care trebuia să se opună cenzurii. Acest grup dezvoltă P2P (peer to peer), un soft de rețea care trebuia să învingă cenzura corporațiilor și a guvernelor. Marea problemă consta însă în faptul că un asemenea browser putea fi utilizat de către criminali și pedofili pentru a-și ascunde fărâdelegile.

În iunie 2002, www.suonline.net anunța faptul că tehnicianul însărcinat cu întreținerea arhivei electronice conținând cele mai importante documente istorice ale Norvegiei a murit fără a încredința cuiva parola de acces. De la moartea acestuia au trecut deja mai mulți ani și angajații „Centrului Național Norvegian pentru Limbă și Cultură” tot nu au acces la arhivă, astfel că directorul Centrului a făcut apel prin radio la toți hackerii care ar putea ajuta la spargerea parolei de acces. Evident că s-au anunțat mult mai mulți hackeri decât s-ar fi așteptat. Această întâmplare a readus în centrul atenției utilizarea programului „Dead Man’s Switch”, care este astfel scris încât, dacă nu se resetează în mod regulat, trece automat la executarea comenzilor setate în prealabil, cum ar fi trimiterea de e-mail-uri la adresele stabilite și la securizarea bazelor de date prin cifrare ori chiar la ștergerea lor.

O interesantă situație, amintită de același www.suonline.net, s-a petrecut în Coreea de Sud, după ce compania de software de securitate „KDWorks” a organizat o competiție prin care hackerii erau invitați să spargă un anumit server, pe învingători așteptându-i premii bănești importante. Numai că doi hackeri au pătruns în chiar serverul lui „KDWorks” și și-au inserat datele de identificare în locul datelor fiecărui potențial câștigător al concursului. În mesajul lor de pe hackers.com ei au scris că serverul desemnat pentru a fi atacat în cadrul concursului nu rula decât un număr redus de aplicații și nu reprezenta o situație reală, astfel că s-au hotărât să „aranjeze” serverul principal. Pe de altă parte, „KDWorks” a susținut că serverul pentru concurs, care rula pe Smoothwall Linux, a fost o momelă pentru hackeri și a constatat dintr-un server fals și din software pentru urmărirea și identificarea celor care pătrund în sistem.

Despre un concurs... legal de hacking relatează Vladimir Ciolan în „Chip online” (www.chip.ro) din 6 august 2003. „În timp ce marii oficiali americani nu mai prididesc să condamne hacking-ul și inclusiv pe hackeri, undeva în deșert se organizează DefCon, un concurs în cadrul căruia sunt testate abilitățile de a sparge, dar și de a proteja o rețea. Ca dovadă că asocierea termenului de «hacker» cu cel de «răufăcător» este greșită, printre participanți se numără și angajați ai unor agenții federale. [...] Concursul întărește regula conform căreia cea mai bună cale de a apăra un server este de a ști cum să îl ataci. «Unelte pentru hacking nu ar trebui să fie ilegale, dar dacă le folosesc pentru a pătrunde în calculatorul tău, atunci devin un răufăcător» a mai declarat Crispin Cowan (Chief Scientist la Immunix, companie ce furnizează servicii de securitate Linux și căpitan al echipei din concursul DefCon cu același nume, n.n.), subliniind încă o dată diferența dintre hackeri și crackeri.”

Căutând cu www.google.com, un puternic motor de căutare pe Internet, adrese de pagini web care să conțină cuvintele-cheie „hacker” (haker, potrivit ortografiei sârbo-croate), am ajuns și la domeniul www.elitesecurity.org, întreținut de bosniaci și care conține o serie de forumuri de discuții. Atenția ne-a fost atrasă de mesajul membrului cu numărul 12119, de loc din Sarajevo, însă care nu și-a dat și numele real. El făcea cunoscut celorlalți membri din forumul despre hackeri și hacking faptul că EC-Council (www.eccouncil.org/index.htm) permite certificarea hackerilor în domeniile metodologiei și eticii hackingului. „Oamenii care au cunoștințe în hacking pot primi pentru cunoștințele lor un certificat și, evident, pot accesa un loc de muncă în calitate de consultanți” - scria bosniacul. Credeam că este vorba despre o banală glumă a unui adolescent pus pe șotii, însă accesând, la rândul nostru, www.eccouncil.org, ne-am convins că acesta nu

mințea. Cel care dorește să intre în posesia unui certificat din partea lui EC-Council, deci să devină un „Certified Ethical Hacker”, trebuie să treacă 21 de teste și anume; Ethics and Legal Issues, Footprinting, Scanning, Enumeration, System Hacking, Trojans and Backdoors, Sniffers, Denial of Service, Social Engineering, Session Hijacking, Hacking Web Servers, Web Application Vulnerabilities, Web Based Password Cracking Techniques, SQL Injection, Hacking Wireless Networks, Virus and Worms, Hacking Novell; Hacking Linux, IDS, Firewalls and Honeypots, Buffer Owerflows, Cryptography.

La capitolul „curiozități” poate fi trecut, în mod evident, și „Muzeul fraudei pe Internet” înființat de către compania „Ad Cops”, care conține deocamdată o colecție de exponate pentru ajutor împotriva fraudei prin e-commerce.

Mass-media și agresiunea asupra Iugoslaviei

Războiul mediatic, îndeosebi cel de la televiziune și de pe Internet, i-a prins și pe români. Majoritatea populației nu era neapărat împotriva alianței nord-atlantice și a americanilor, însă simpatiza cu sârbii. Doar puterea politică a momentului, din dorința de a fi pe placul S.U.A. și N.A.T.O., de-a dreptul a excelat în a susține acțiunile militare împotriva țării vecine (și "prietene", ar completa, zeflemitor, un cunoscut "analist politic"). A rămas proverbială afirmația președintelui de atunci al României, Emil Constantinescu, cum că bombardarea Iugoslaviei este necesară și legitimă, afirmație criticată de mass-media românească. "Avea România interesul ca președintele țării să declare că un război împotriva Iugoslaviei este "necesar și legitim" chiar înainte de a începe bombardamentele? Și de ce legitim, dacă ONU nici după sistarea bombardamentelor nu a legitimat intervenția militară a NATO?" - scria Corneliu Vlad (www.lumeam.ro, site-ul "Lumea magazin"). "Nu am fost capabili să înțelegem că, în numele democrației și al drepturilor omului, era necesar și legitim să moară copii și bătrâni, să fie bombardate spitale, case, trenuri, poduri. Ei, politicienii, sunt singurii care știu ce e bine pentru noi și pentru țară" - scria, la rândul său, și Marian Oprea (www.lumeam.ro).

Iar în 1999, în timpul războiului, un cunoscut disident român, aflat la Paris, este vorba despre Paul Goma, scria cu o ură nedisimulată: "Nu, Sârbul nu este capabil să facă deosebirea între victimă și călău decât la modul sârbesc: când el persecută, violentează, jefuiește, violează, omoară ne-sârbi, boje moi, nu face vreun rău - dovadă: majka lui nu i-a spus o singură vorbă grea, necum să-i zmulgă urechile când a constatat că și-a început cariera de cetnik gâtuind mâța (vecinului), și a sfârșit prin a tortura, a arde de vii femei și copii (dar ne-uitând ca, în elanuri patriotice - și ortodox - mai întâi să-i ceară albanezului 1.500 mărci germane, "pretul vietii", apoi să-l oblige să scoată, să dea tot; în final zmulgînd verighetele, inelele, cerceii, brățările, lăntușoarele de aur de pe cadavre)". La prima citire, te înfiori de grozăviile de care sunt în stare sârbii. Numai că un om sănătos la minte și fără interese de-o parte ori de alta nu poate lua în serios asemenea aberații. Iar de Paul Goma, pe care, cândva, în timpul lui Ceaușescu, îl admiram, ți se face de-a dreptul milă pentru cât de mult s-a lasat prins în mrejele propagandistice țesute cu atâta abilitate de către N.A.T.O. Dar acesta a fost primul e-razboi mondial și Paul Goma a luptat de partea N.A.T.O. Despre ce e-n mintea acestui individ, doar psihologii ar putea spune mult mai multe. Cert este însă un alt lucru. Mașina propagandistică a lucrat excelent. Din păcate, în joc s-au prins destui intelectuali români cărora, acum, când Kosovo se află sub protecția N.A.T.O. (care se pare că mai mult protejează mafia albaneză și traficul de droguri și nicidecum enclavile cu sârbii care au mai rămas), când copiii sârbilor merg la școală sub escortă, iar obiective culturale și religioase sârbești, destule aflate pe lista UNESCO, sunt aruncate în aer, distruse și scârnavite de albanezi, nu mai dau dovadă de același zel în apărarea drepturilor omului.

Evident, războiul propagandistic prin mass-media a fost folosit din plin și de către R.T.S., televiziunea națională sârbă, și de alte televiziuni iugoslave din acea perioadă. Cât despre

epitetele cu care gratulau aceste posturi atât Alianța Nord-Atlantică, cât și diverse personalități occidentale, ele au fost tema colecției lui Predrag Timotić, care le-a făcut cunoscute pe lista de discuții nato-agresija-na-srj.

Pentru N.A.T.O.: hoarde de gangsteri, pirați ai văzduhului, haimanale fasciste, forță mecanică brutală, hoarde bestiale, sălbăticiunile N.A.T.O., monștri N.A.T.O., agresori însetați de sânge, falanși fasciste N.A.T.O., N.A.T.O. - alianța răului, armada răului, seniorii războiului în imperiul ucigașilor, democrația tomahawk într-o aventură războinică, ceată de sălbatici, canibali gigantici, tirani cu creier liliputan, monștri mongoloizi, conglomerat mongoloid, autoproclamați apostoli ai democrației în rolul celor mai periculoși ucigași, businessmani cu pușcă, o urâtă amintire istorică, galeria de tipi ai lui Freud, vrăjitoarele N.A.T.O.-ului, maniaci îmbătați cu forța, monștri ucigași însetați de sânge și mașina lor de propagandă a minciunii, puternică mașină media prevăzută cu turbo-manipulatoarele CNN-ului, răufăcători impotenți, semănătorii morții, călăreții apocalipsei, mutații, camarila militară regională, corporație internațională monstruoasă, bandă războinică de fasciști, răufăcătorii încăpățânați ai lui Goebbels, cei mai mari vandali ai secolului al XX-lea, sălbăticiunile lui Clinton, semănătoarele de fier ale morții, proiectile răufăcătoare, satrapii întregii lumi, atacurile brutale și răufăcătoare ale lașilor din America, gealații văzduhului, crimă a bestialilor piloți N.A.T.O., dinaintea a cândva casei albe, iar acum a casei negre din Washington, hoardele aeriene ale răufăcătoarei alianțe N.A.T.O., nocturni ucigași cu sânge rece, nu știm cum să le mai spunem.

Pentru Bill Clinton: bolnavul războiului, pedofilul bolnav, nestăpânitul barbar, amoretul mincinos, Adolf Goebbels Hitler Clinton, creatura Washingtonului, greșeală biologică, șeriful legii junglei, sălbaticul cu zâmbet rușinos, președintele al cărui centru este în șliț, răufăcătorul nervos.

Pentru Xavier Solana: un răufăcător în fruntea agresorilor, o nouă perversă creație a războinicilor voaieri lipsiți de scrupule, cretinul general al N.A.T.O., gunoiul american.

Pentru Koffi Anan: cel nu îndeajuns de informat, cel care nu citește știrile.

Pentru Madeleine Albright: uliul american, pocitania cu chip de femeie, șarpele perfid cu cizme de cowboy, secretar de stat ca o femeie de serviciu la hotelul "Red Roof".

Jacques Chirac: completarea jalnică a lui Clinton, sluga europeană a N.A.T.O., unul dintre conducătorii genocidului.

Umor de război

Bancurile, caricaturile, montajele fotografice, graffiti, iată câteva dintre cele mai... umane mijloace de luptă împotriva răului. Este, dacă vreți, un fel de... întoarcere, după palma primită, a celui alt obraz. Un fel de rezistență sub teroarea Satanei. Românii știu perfect ce rol au jucat bancurile politice în timpul dictaturii comuniste. Sârbii și-au întors și ei obrazul. Și ce anume a rezultat? Acum, când totul pare a se fi terminat, putem spune cu mâna pe inimă: mai multe și splendide colecții de bancuri, caricaturi, montaje fotografice și graffiti. Cu autori mai mult sau mai puțin cunoscuți. Dar care, datorită Internetului, și-au îndeplinit pe deplin rolul de supapă psihică.

Aforisme:

o Țigani flutură o lozincă pe care scrie: "NATO, predă-te, vom muri cu toții!"

o Când ataci spitalele cu bombe, ori ești un criminal conștient, ori un ucigaș nebun, ori un ... "american umanitar".

o Ai grijă, acum, Bill (Clinton), că l-ai supărat și pe Bruce Lee!

o Solana, nu te mai obosi, Clinton are deja un câine!

o Închiriez teren pe Vodna - pentru căderea avioanelor N.A.T.O.

o Schimb doi piloți americani cu o bicicletă!

o Clinton, de vei continua astfel, Hitler se va alege cu complexul inferiorității!

o Fraților ruși, nu mai filosofați atât, treceți la răfuiala fizică!

- o Avem și noi minte și putere, numai că ne lipsesc 300 de dolari.
- o N.A.T.O. se comportă ca un huligan. Noi îi azvârlim pe-alde ăștia afară din cafenea!
- o Aceasta este o lovitură dată umanității cu democrația americană.
- o Amerii vor să preia mass-media noastră... probabil cred că tuturor le plac desenele animate!
- o Ei își au creaturile, noi, caricaturile!
- o Nu putem primi trupele N.A.T.O., nu avem destule forțe să le asigurăm securitatea!
- o Billy, te așteptăm la ora 20, pe Podul Brankovo.
- o Dați poporului comici, nu politicieni!
- o Vino repede, Bill... s-a sculat!
- o Clinton, te iubesc... mort!
- o Billy, te aștept pe tine și compania ta la un pahar de vorbă...
- o Hillary, nu-l lăsa să se înmulțească!
- o Bill, tu ești cea mai mare catastrofă umanitară!
- o Dintre toate limbile, Clinton o cunoaște cel mai bine pe-a Monicăi!
- o Bill, azi-noapte am visat că nu mai ești!
- o Chelsea, aruncă-l pe tata din tren!
- o Billy, de ce nu ți se mai întorc avioanele! Dresează-le!
- o Pentru războiul împotriva sârbilor, Pentagonul solicită Congresului alte cinci-șase miliarde. De ar fi avut sârbii acești bani ar fi ajuns deja la Washington!
- o Cum se simt Clinton și restul politicienilor care deja de o lună de zile nu au mai fost la WC din cauza situației din Kosovo? Plini de sine!
- o De-ar avea tomahawk-ul capul lui Madeleine Albright ar fi fost și mai oribil!
- o Dostoievski a fost un clarvăzător. A scris cartea "Idiotul" înainte de nașterea lui Clinton.
- o Proletari din toate țările, unde sunteți?
- o Criza kosovară este o criză de domeniul trecutului, N.A.T.O. este criza viitorului!
- o CNN. Cinic. Neargumentat. Noutăți.
- o Am demonstrat că Pământul e rotund: ne-am căcat prin Orient, iar rahatul a ajuns până-n Occident!
- o Boris, păi nu ți-am spus să trimiți popi, ci tunuri! Sloba.
- o Iată rezolvarea: Milošević - secretar general al O.N.U.
- o Noi suntem în realitate ceea ce doriți voi să fiți în filme.
- o Doamne, să nu-i ierți, au știut ce fac!
- o Dacă avionul a fost invizibil, iar noi nu l-am văzut, cine a cheltuit muniție pe degeaba?
- o Doar hoții, curvele și N.A.T.O. lucrează noaptea!
- o Frați sârbi, rezistați! Sârbii sunt alături de voi!
- o Pacifiști din toată lumea, uniți-vă... bombardați Serbia!
- o Două luni mai târziu: Pace, pace, pace, nu e nimeni vinovat.
- o Trimiteți-ne trupe. Să umplem gropile.
- o După război, Clinton și Milošević se întâlnesc pe o insulă pustie. Clinton, bucuros: - Vezi, Milo, ce mică-i lumea! La care Milošević îi răspunde: - Nu e mică lumea, ci e mare Serbia.
- o N.A.T.O., țintește vaca vecinului, în zona 44,12 pe 38,13. Nu are importanță cât costă.
- o Garantăm ieșirea soldaților N.A.T.O. din Serbia pe orizontală.
- o Albright, nu te-aș ciocăni nici măcar cu o piatră-n cap.
- o America mai trimite trei sute de avioane. Înseamnă că atâtea au fost doborâte.
- o Nu bombe inteligente sunt proaste, ci proști sunt piloții N.A.T.O.
- o Cum să înapoiem un tomahawk neexplodat celor care l-au trimis?
- o Albright nu are nimic împotriva sârbilor. Ea ne iubește și ne respectă atât de mult încât ne-a anunțat în limba sârbă că o să ne bombardeze
- o Vorbește sârbește, să te bombardeze toată lumea.
- o Monica, de fapt ce-ai fumat?
- o Vom face YUGO F 117 GTI. Zastava, Kragujevac.
- o Cumpăr F-117, se poate și pe bucăți.
- o Clinton, tu ești Monica noastră.
- o America este o superputere; l-a clonat pe Adolf în Clinton.
- o New Albanian Terrorist Organization (N.A.T.O., n.n.)
- o Bombă ziua. Bun adăpost.

- o Celui care doboară un B2 îi voi fi Monică.
- o De vânzare F-117, avariat, puțin trecut, vopsit original.
- o Americanii au avut F-117. Acum au F-114.
- o Serbia, până la Casa Albă.
- o Albania a mobilizat 75% din comanșii. Unul a fost bolnav.
- o Radioamatorii nu vor mai întoarce tomahawk-urile în Albania..., ci în Italia.
- o Un minor dintr-un zgârie-nori belgrădean a fost pedepsit de judecător pentru o infracțiune: punga cu gunoi pe care a aruncat-o de pe terasă a nimerit o rachetă de croazieră.
- o Feministele cehe au respins ideea că Albright a fost membra lor. Directorul Grădinii zoologice din Praga s-a alăturat acestui protest.
- o Jos bombele N.A.T.O.!
- o Mi s-a defectat televizorul. Va trebui să privesc bombardamentele de pe terasă.
- o Felicitări, Bill! Al tău Adolf.
- o Să se salveze cine poate - vin sârbii.
- o Voi aveți avionul invizibil, noi avem dioptrii.
- o Azi au decolat de la Aviano mai multe avioane. S-au întors și mai multe.
- o Moarte lui Clinton, Monica - poporului!
- o Clinton, F-117 nu e bun. Încearcă un MIG!
- o Clinton, să dea Dumnezeu să-ți nască Chelsea un sârb.
- o Ați avut avioane invizibile, acum aveți piloți miopi.
- o Intrarea în Serbia e liberă - ieșirea se plătește cu capul.
- o Monica, a lui Sloba e mai tare.
- o Hei... arde aripa avionului dumneavoastră!
- o Dacă pentru dumneavoastră a fost invizibil, vă vom trimite o fotografie.
- o Frați ruși, în numele lui Hristos, trimiteți rachete S-300.
- o Iartă-i, Doamne, au mâncat vaci nebune.
- o N-aveți nici o șansă, Serbia e-n transă.
- o Cine nu are nimic în cap, are în bombe.
- o Bill, și eu am pățit la fel. Murat.
- o Serbia, cel mai mare consumator de avioane americane.
- o Victor Cernomârdin + Bill Clinton = Cernobîl sârbesc.
- o Europa, dormi liniștită! Serbia veghează.
- o Monica, strânge din dinți!
- o Nu e bine să zbori până nu cresc aripile.
- o Monica e bună, dar Tony e și mai bun.
- o Diferența dintre Hitler și Clinton e că Hitler i-a fost credincios Evei Braun.
- o Tony Bleeeeeer, oaie neagră!
- o Scuzați, nu am știut că e invizibil!
- o Hei, cow-boy Bill, descalecă de pe Balcani!
- o Dumnezeu vede mai bine decât Awacs.
- o Un Clinton bun este un Clinton mort.
- o CNN minte mai bine decât RTS.
- o Prognoza meteo: în Serbia vor cădea și mâine avioane.
- o Clinton, cel mai bun lucru care ți se poate întâmpla în viață este să rămână Hilary văduvă.
- o Americanii au primit două milioane de albanezi. Noi, un singur Kosovo. Nu înțeleg de ce se revoltă atât?
- o Al meu e vizibil, dar nu cade.
- o N.A.T.O., mai păstrează câte-o bombă pentru irlandezi, kurzi și basci!
- o De ce nu reușește N.A.T.O. să nimerească rezervoarele de benzină din Serbia Centrală, ci în principal case țărănești? Tacticienii au priceput că rezervoarele de țuică sunt un factor mult mai important al apărării și o țintă potențial mai mare.
- o Sloba: îți mulțumesc, Clinton, pentru că în 20 de zile ai făcut ceea ce eu încerc de zece ani!
- o Cum reacționează "verzii" în Germania vizavi de participarea țării lor în agresiunea asupra Iugoslaviei? Își schimbă denumirea în "verzi-măslină".
- o Nu arunca gunoi, nu hrăni animalele sălbatice și piloți pierduți!
- o Poate că americanii știu să facă bombe inteligente, dar nu și politicieni deștepți.

- o Departe ideea că sârbii sunt un popor celest. Ei caută salvarea îndeosebi sub pământ.
- o Cum te poți răzbuna cel mai bine pe țările N.A.T.O.? Bucurându-te sincer să primească refugiați din Kosovo cât mai mulți.
- o Raportul institutului meteorologic: deasupra Iugoslaviei este în continuare vreme frumoasă; plouă cu găleata.
- o Monica, acum lasă-mă și pe mine puțin! Tony Blair.
- o Dacă începe aici cel de-al treilea război mondial, poate ne vor recunoaște drepturile de autor.
- o "Titanic", mândria Flotei a VI-a.
- o Cel mai nou blestem: Dar-ar Dumnezeu să-ți fie casa pe CNN!
- o CNN + BBC = CARTOON NETWORK
- o Albright, întoarce-te în locul tău natal (Belgrad), să ne plimbăm pe Corso!
- o V-au spus că este invizibil, însă am descoperit dioptria cea bună!
- o Întrebare: ce are Clinton între picioare? Un invizibil și două locatoare.
- o Poate ar trebui să se strângă bani pentru a le da piloților posibilitatea să vadă pe cine și pe ce aruncă bombe: cumpărați-le ochelari, iar testul la alcool să fie obligatoriu!
- o Fratele meu îi ajută pe albanezi: le trimite regulat muniție prin țevă!
- o Tot mi se pare că Bill are deficit de minte și suficit de piloți.
- o Lui Clinton îi lipsește Princip (Gavrilo).
- o F-117 suferă de epilepsie. Dr. Freud.
- o Ei nu înțeleg nimic. Noi vrem în N.B.A. nu în N.A.T.O.
- o Eu sunt pacifist. Serbia până la Pacific.
- o N.A.T.O.! Ucid, deci exist.

România și e-pirateria

„Rata anuală a pirateriei software în România a atins, la sfârșitul lui 2003, nivelul de 73%, iar valoarea programelor utilizate ilegal s-a ridicat la 49,3 de milioane de dolari, a anunțat miercuri, Business Software Alliance (B.S.A.), care citează un studiu realizat de International Data Corporation (I.P.R.)“, precizează Agenția românească „Mediafax“ în data de 7 iulie 2004. Reamintim că B.S.A., înființată în 1988, la Washington (S.U.A.), reprezintă interesele producătorilor locali de software, printre care se numără „GeCad“, „Ciel Romania“, „Softwin“, „Kepler Software Development“ și „Romsym Data“, dar și companiile internaționale „Adobe“, „Autodesk“, „Macromedia“, „Microsoft“, „Bentley Systems“ și „Symantec“. B.S.A. are ca principale domenii de interes reducerea ratei pirateriei software, informarea și educarea utilizatorilor de programe, sprijinirea instituțiilor guvernamentale responsabile cu aplicarea legilor din domeniul dreptului de autor și desfășurarea de activități de lobby pentru adoptarea unei legislații corespunzătoare în domeniul proprietății intelectuale.

Tot „Mediafax“ precizează că „Organismul (B.S.A., n.n.) a semnalat că regiunea Asia-Pacific, Europa de Est și America Latină continuă să fie «punctele fierbinți ale pirateriei de pe glob, mai mult de jumătate din software-ul instalat pe computerele din aceste regiuni fiind versiuni piratate»“. Care ar fi răspunsul la întrebarea de ce este atât de ridicată rata pirateriei în Europa de Est, deci și în România? Directorul general al B.S.A. EMEA (Europa, Orientul Mijlociu și Africa), Steven Frantzen, spunea în iunie 2004: „Regiunea Europei Centrale și de Est se confruntă cu provocarea creșterii economice și cu tradiționalul respect redus pentru drepturile de proprietate intelectuală. De aceea, nu este surprinzător că această regiune înregistrează cea mai ridicată rată a pirateriei software. Totuși, trebuie luați în considerație unii factori care vor ameliora această situație, cel mai important fiind aderarea la Uniunea Europeană a unor state din regiune, fapt care va determina aplicarea mai eficientă a legislației dreptului de autor“. La rândul său, Nicolae Burchel, reprezentant legal al B.S.A. pentru România, declara: „Strategia europeană a B.S.A. este aplicabilă și în România și se înscrie în linia generală a activităților derulate până în

prezent. Planul în cinci puncte poate reuși numai cu sprijinul Guvernului, al administrației locale, al asociațiilor profesionale și al altor instituții și autorități. Îmbunătățiri reale pot să apară numai printr-un cadru legal modern și aplicarea legislației, cu ajutorul sprijinului public, la toate nivelurile, pentru proprietatea intelectuală și industriile din domeniile de creație a proprietății intelectuale.“

De unde, brusc, atâta pornire împotriva răufăcătorilor din domeniul IT din România? Vă vom oferi, în cele ce urmează, câteva exemple care au pus pe jar autoritățile românești.

Cotidianul național „România liberă“ scria pe 16 septembrie 2002, cu titlul „Șapte hackeri craioveni au furat 15.800 USD“, sub semnătura lui C. Vilău: „Cinci firme din SUA, Marea Britanie și Thailanda au fost prejudiciate cu suma de 15.800 USD de șapte hackeri din Craiova. Tinerii, cu vârste cuprinse între 16 și 22 de ani, au comis fraudele prin Internet, utilizând calculatoarele unor cluburi din municipiul Craiova. [...] Pentru achitarea bunurilor comandate, hackerii au utilizat cărți de credit aparținând unor cetățeni americani și israelieni, intrând în posesia acestora prin spargerea site-urilor unor magazine virtuale, unde anterior titularii acestor instrumente de plată le utilizau legal.“

Iată, așadar, un alt fel de război, un război în domeniul comercial, unde metoda de luptă folosită le este foarte bine cunoscută și multor hackeri sârbi. Cotidianul bucureștean „Adevărul“ scria la un moment dat: „Bijuterii și tablouri de mii de dolari - achiziționate fraudulos prin Internet“. Și anume: „Trei adolescenți craioveni au fost prinși în flagrant la Vama Băneasa, în timp ce ridicau un inel de aur cu diamant în valoare de 5.600 dolari, trimis de un cetățean american în urma unei licitații pe Internet. [...] Anchetatorii au stabilit că Dima și Câmpean accesau, dintr-un Cafe-Internet din Craiova, site-uri de licitații, cumpărând bijuterii, tablouri [...] pe care le primeau în țară, fără a plăti vreodată aceste bunuri.“

„România liberă“ scria despre un „Hacker albaulian, maestru în «țepe virtuale»“ care, abia ieșit din liceu, a scos aproape 30 000 USD de la „fraieri americani“. „Fost elev al unui liceu cu profil informatic din județul Alba, tânărul în vârstă de 20 de ani este acuzat că a accesat fără drept, prin sustragerea parolelor de acces, mai multe conturi ale unor utilizatori legali ai site-ului de licitații on-line «e-Bay», sub identitatea cărora ar fi indus în eroare mai mulți cetățeni americani. [...] Păgubiții plăteau între 200 și 700 USD prin serviciul «Western Union», pentru produse ce nu au ajuns niciodată în posesia lor.“

În numărul său de luni, 3 martie 2003, cotidianul bucureștean „România liberă“ titra: „Pirații informatici reușesc să scape cu pedepse derizorii sau chiar basma curată“. De unde și până unde o asemenea concluzie la autorul articolului, respectiv o cunoscută ziaristă din Timișoara pe nume Laura M. Forțiu. Ne permitem să preluăm un fragment din acest material: „Instanțele timișorene s-au confruntat în ultima vreme cu o adevărată «explozie» de cauze având ca obiect fraude prin Internet. Startul, să spunem așa, a fost dat de celebrul deja Mircea Harapu, un tânăr de 24 de ani, care a reușit să spargă parolele unei pagini web a unei importante firme newyorkeze.

Societatea americană avea ca obiect de activitate vânzarea de produse on-line, astfel că românul a intrat în posesia unor informații confidențiale, în care apăreau inclusiv seriile cărților de credit ale persoanelor care au avut relații de afaceri cu firma. Așadar, după ce a extras 15 fișiere ce conțineau date confidențiale despre clienții companiei, timișoreanul a contactat conducerea firmei și i-a solicitat suma de 5 000 de dolari pentru a nu face cunoscute informațiile obținute.

Reprezentanții companiei au anunțat însă imediat FBI, care a luat legătura cu specialiștii Centrului Zonal pentru Combaterea Crimei Organizate și Antidrog Timișoara. Harapu a fost prins în flagrant tocmai când s-a prezentat la bancă pentru a ridica o parte din banii preținși. Deferit justiției sub acuzația comiterii infracțiunilor de șantaj și violarea secretului corespondenței, Mircea Harapu a fost condamnat de Judecătoria Timișoara la trei ani închisoare. Surpriză însă! Tribunalul Timiș, o instanță-campion la achitări cu cântec, a admis recent apelul așa-zisului hacker și l-a scos în final nevinovat.“

Nici Iașul nu se lasă mai prejos. „România liberă“ scria, sub semnătura Deliei Ștefănoaie: „Cyber-spărgătorii de mașini au îngenuncheat Poliția Iași“, cu subtitlul: „O bandă de informaticieni sparge cele mai sofisticate sisteme de alarmă cu ajutorul laptopurilor și al dispozitivelor de ultimă generație, lăsând limuzinele încuiate“. În context, un polițist de la Secția 3 Poliție din Iași declara: „Vin cu laptopurile și un dispozitiv special de spargere a codurilor de acces, care substituie comenzile. Ușile se deschid și infractorii pătrund în interior. Poartă mănuși chirurgicale și nu lasă nici o urmă. Taie cu clești speciali cablurile casetofonelor și ale CD-playerelor sofisticate și le scot din locașurile lor. Golesc torpedourile și apoi încuie la loc mașinile. Lucrează extrem de

curat. Suntem depășiți de tehnica lor.“

Numai că răufăcătorii din România nu acționează doar în țara lor natală. O dată cu desființarea vizelor pentru Europa Occidentală, ei s-au orientat chiar foarte rapid. Andrei Bădin scria în „România liberă”: „Filiere românești de clonat carduri în Italia și Spania“. Ce făceau, de fapt, aceștia? Pur și simplu clonau carduri. Prin intermediul acestora, cumpărau parfumuri și haine scumpe, electronică performantă, telefoane mobile, echipament de schi etc.

Luni, 12 mai 2003, cotidianul bucureștean „Adevărul“ titra: „Pentru a pune capăt valului de fraude comise prin Internet, IGP a înființat un serviciu de luptă împotriva infracționalității cibernetice“. Oricare dintre metodele de luptă utilizate pe Internet în 1999, în timpul agresiunii NATO asupra Iugoslaviei, poate fi considerată infracționalitate cibernetică. După ce dă drept exemple negative faptele comise la București, Brașov, Cluj-Napoca, Craiova, Argeș și Timișoara, „Adevărul“ spune că „Valul de fraude prin Internet, puse la cale în special de tinerii pasionați de calculatoare, au pus pe jar conducerea IGP (Inspectoratul General al Poliției, n.n.), care a decis să înființeze un serviciu specializat în combaterea infracționalității cibernetice. Noua structură va funcționa în cadrul Direcției Generale de Combatere a Crimei Organizate și Antidrog (DGCCOA) și va avea polițiști în fiecare centru zonal al Direcției.“ Referindu-se la victimele predilecte ale fraudelor cibernetice înfăptuite de români, autorul articolului spune că e vorba de cetățeni din S.U.A. și Europa Occidentală.

În cotidianul timișorean „Agenda zilei“ din 22 mai 2004, Daniela A. Budici scria: „Hacker condamnat. El a trebuit să plătească 10 000 USD“. În 2003, acesta, împreună cu un alt individ rămas neidentificat, a atacat site-ul IPJ Timiș și a distrus întreaga bază de date. „Moise, care a folosit porecla DarkHate, a lăsat și un mesaj: «Lăsați lumea să bea în scara blocului! Că așa-i frumos! Promitem să ne cumișim și ne lăsăm de hacking și vă lăsăm site-ul în pace.»” Este vorba despre bucureșteanul Valentin Moise, care a fost acuzat de acces fără drept la un sistem informatic, prin încălcarea măsurilor de securitate și perturbare gravă, inacceptabilă, a funcționării unui sistem informatic, prin ștergerea datelor informatice. El a fost condamnat la doi ani de închisoare cu suspendare condiționată a executării pedepsei. Totodată, el a fost obligat să plătească IPJ Timiș 10 000 USD cu titlu de despăgubiri. Tot Daniela A. Budici scria în cotidianul timișorean „Agenda zilei”: „Cinci tineri timișoreni care au tras pe sfoară peste 60 de cetățeni americani cu câteva zeci de mii de dolari au fost condamnați de către Judecătoria Timișoara.“ Și dacă tot suntem la Timișoara... Laura M. Forțiu titra în „România liberă“ din 16 februarie 2004: „Costel Balint, acuzat de complicitate la o înșelăciune de proporții“. Iar în subtitlu: „51 de americani au fost trași pe sfoară, plătind sume grele în dolari pentru produse electronice... inexistente; misiunea revoluționarului era aceea de a ridica valuta din bancă și a o transforma apoi în lei, serviciu pentru care era recompensat corespunzător de capii afacerii“. Articolul se încheia astfel: „Se pare însă că probele în acuzare, ca și cele în apărare nu au fost (cel puțin pe moment) suficiente pentru a convinge instanța de judecată de vinovăția sau nevinovăția revoluționarului acuzat de complicitate la înșelăciune astfel încât magistrații să poată da un verdict.“

Tot în Timișoara, fiul unui polițist (!), domiciliat aproape de centrul orașului, avea un studio de piratare a CD-urilor și DVD-urilor. La descinderea polițiștilor în casă s-au găsit 7 000 de CD-uri și DVD-uri cu muzică, jocuri, filme și aparatură de înregistrare. Tânărul s-a ales cu o amendă de șapte milioane de lei, cu toate că prejudiciul făcut prin neplata drepturilor de autor se cifra la aproximativ două miliarde de lei.

Se pare că, totuși, ceva începe să se miște și în România. În aprilie 2004, a fost lansat la Iași primul comitet local de inițiativă al Coaliției „proIntellect“ (www.prointellect.ro). Acesta reunește personalități din diferite medii (universitar, de afaceri, administrație, procuratură, poliție) interesate să facă ceva pentru a pune capăt furtului uriaș și generalizat din domeniul proprietății intelectuale, care afectează economia, dar și statul în același timp. Printre scopurile sale se numără și informarea asupra riscurilor pirateriei și a gravității fenomenului de furt din domeniul proprietății intelectuale din România. Coaliția își propune să atragă atenția tuturor românilor că furtul de proprietate intelectuală este o infracțiune la fel de gravă ca și furtul de bunuri, care poate fi pedepsit atât civil, cât și penal, iar cei care continuă să pirateze se expun unor pedepse grave, dar și faptul că rata pirateriei este unul dintre elementele care dau măsura societății românești. Inițiativa ieșenilor a avut ecou la Cluj-Napoca, iar apoi, la 30 iunie 2004, și la Timișoara. Fiecare comitet local al Coaliției „proIntellect“ va edita un buletin lunar. Din păcate, dacă membrii coaliției

nu vor da dovadă de maximă agresivitate în lupta lor împotriva pirateriei IT, dacă nu-i vor „urechea” cu fermitate pe cei puși și plătiți să aplice o legislație deja existentă pentru apărarea dreptului de autor, nu vor fi altceva decât încă o mișcare/grupare ai cărei membri își plâng unul altuia pe umăr fără a fi în stare să dea jos drobul de sare.