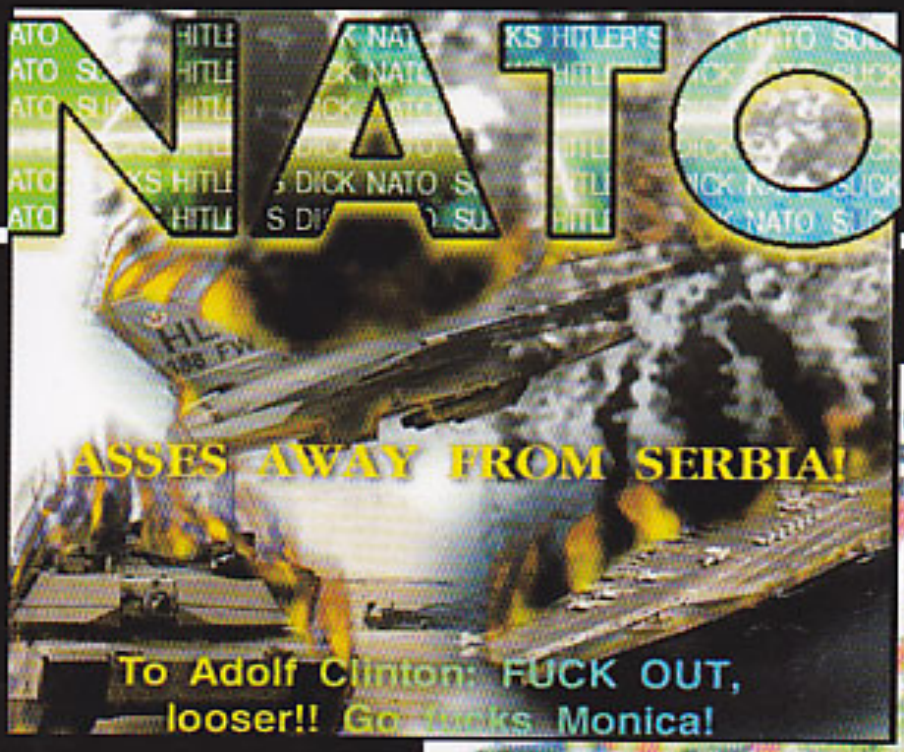
DUȘAN BAISKI

RĂZBOI PE INTERNET



Editura WALDPRESS

Duşan Baiski

Război pe Internet

Editura "Waldpress"din Timişoara 2004

Coperta: Duşan Baiski.

ISBN 973-8453-85-2

CUPRINS:

Automanipulare sau, pur şi simplu, manipulare

Crezi că vei fi îndeajuns de imparţial? – 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 şi încercat: să nu mă las pradă vreunui resentiment vizavi de americani, „eroii" şi artizanii războiului nedeclarat dus împotriva Iugoslaviei, contrar tuturor normelor juridice internaţionale în vigoare la acea dată. Oare am reuşit? Majoritatea veţi spune că nu. Autorul este de naţionalitate sârbă şi nu poate fi imparţial. Desigur, această apreciere vă aparţine. Parţial, aveţi dreptate. Cum poate fi imparţial un individ care, în timpul bombardamentelor deseori „la nimereală" ale aviaţiei N.A.T.O. ce atacă trenuri civile, convoaie umanitare şi de refugiaţi, inclusiv albanezi, şcoli, spitale, case şi blocuri de locuinţe, îi scrie preşedintelui de atunci al României, Emil Constantinescu, o scrisoare deschisă publicată în săptămânalul naţional românesc „Formula AS" şi în forumul de pe Internet al cotidianului „România liberă", intrigat de faptul că un preşedinte al unei ţări cu 23 de milioane de locuitori afirmă că bombardarea poporului sârb este „legitimă şi necesară"? Cum poate fi imparţial un român de etnie sârbă care, atunci, a trimis la forumul de discuţii „Timişoara" un mesaj în care scria că Timişoara a fost bombardată? Desigur, o glumă luată ca şi glumă, însă de unii aproape crezută. Ce uşor e să manipulezi oamenii! Îndeosebi atunci când te foloseşti de o anumită conjunctură. Dar se pare că e mai uşor să le crezi unor S.U.A. şi Marea Britanie speriate că un oarecare Saddam Husein dintr-un oarecare Irak aflat între Evul Mediu şi mileniul III deţine arme de distrugere în masă şi, ca atare, este un pericol mondial, decât să crezi un cetăţean român, fie el şi de etnie sârbă, care încearcă să facă o radiografie a primului război electronic mondial. Lăsaţi însă deoparte orice resentimente faţă de sârbi. Chiar dacă, probabil unii dintre ei s-ar fi comportat conform imaginaţiei unui individ precum Paul Goma. Nu judecaţi o întreagă naţiune în funcţie de faptele unor membri ai acesteia. Nu putem judeca românii după faptele lui Nicolae Ceauşescu. Nu putem judeca sârbii pentru faptele unui Slobodan Milošević. De fapt, ce ştie

străinătatea despre România? Dracula, Ceauşescu, Nadia Comăneci. Dar despre Iugoslavia restrânsă? Milošević, sârbi sângeroşi, gropi comune, albanezi maltrataţi... Nimic altceva decât clişee abil construite şi ulterior acceptate de minţi credule, leneşe, manipulate de indiferent cine ar deţine controlul mass-media. Deosebit de relevantă este poziţia lui Tucidide din Atena (circa 455-395 î.d.H.) faţă de război (citǎm din cartea „Război salvat" de Michael Kunczik, Editura InterGraf, 2002), membru al elitei Atenei şi chiat comandant de oşti în războiul din Peloponez, potrivit căruia războiul era un „dascăl brutal" care „reuşeşte să facă să se desfăşoare 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-aş îndrăzni să povestesc după cele relatate de primul venit, nici măcar <<după părerea mea>>, ci eu am încercat să analizez cu toată minuţiozitatea posibilă atât cele trăite de mine, cât şi ştirile de la alţii, căutând să desluşesc cât mai multe detalii. A fost o cercetare obositoare, deoarece martorii aceluiaşi eveniment nu mărturiseau aceleaşi 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 manipulaţi, ori amândouă la un loc. Din nefericire, nu sntem departe de adevăr. Aşadar, este această carte credibilă? Ar fi absurd să susţin un asemenea lucru care, potrivit logicii, pare fals de la o poştă. Mă bazez însă pe memoria şi cultura dumneavoastră generală. Ceea ce afirm eu în aceste pagini poate fi alăturat bucăţilor de mozaic din minţile dumneavoastră, legate de aceleaşi evenimente sau de evenimente similare. Rămâne în sarcina dumneavoastră să constituiţi întregul. Iar concluzia vă aparţine 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 forţelor N.A.T.O. în Kosovo şi Metohia (Iugoslavia), aprecia că atacul asupra Iugoslaviei a fost primul conflict militar din lume purtat şi prin intermediul Internetului. La un simpozion al B.N.D. (Bundesnachrichtendienst, serviciul german de informaţii, cu 6 000 de angajaţi şi 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 şi Abwehr), acelaşi general a declarat că „falsificarea datelor este o armă a războiului psihologico-propagandistic". Iar August Hanning, şeful B.N.D., a susţinut că toate guvernele „antrenează cyber-soldaţi care să atace şi să spioneze inamicul prin intermediul computerelor şi să efectueze lovituri la distanţă asupra punctelor cheie ale unei ţări". Pe de altă parte, generalul american Whesley Clark, fostul comandant al forţelor N.A.T.O. pentru Europa, a spus că „atacul asupra computerelor sârbeşti ar fi putut să întrerupă epurarea etnică şi să micşoreze numărul celor afectaţi". Numai că, după cum încă mai susţineau, la începutul lui 2001, specialiştii 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 permanenţă teama că hackerii din Iugoslavia, dar şi din alte ţări, vor ataca reţeaua informatică a Pentagonului, aşa cum s-a întâmplat,

de exemplu, cu hackerii olandezi în timpul războiului din Golf din 1991 ori a intervenţiei în Somalia. Chiar dacă oficialii americani au susţinut că site-urile sârbeşti 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 şi nicidecum o acţiune la comanda guvernului sau a armatei americane. Iată însă, potrivit publicaţiei iugoslave „Vesti", ce părere are dr. Slobodan R. Petrović, lucrător în cadrul poliţiei sârbe şi autor al cărţii „Criminalitatea digitală", despre dezinteresul guvernului american pentru atacul împotriva sistemului informatic al Serbiei: „În timpul agresiunii N.A.T.O., americanii au plănuit să înceapă cyber-atacuri asupra Serbiei, dar acest lucru nu le-a ieşit la mână întrucât tehnologia informaţională de la noi (prezentă în sistemul bancar, în poliţie, 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 instituţii americane. În 1999, aceştia au încercat de mai multe ori să pătrundă în baza de date a bazei aeriene din San Antonio, în care erau stocate date despre forţele americane din Bosnia şi în care se găseau înregistrări şi diverse documente despre atacurile aeriene asupra Irakului. Iată însă că specialişti din cadrul Centrului pentru studiul apărării din cadrul corporaţiei „Rand" afirmă că „forţe mobile mici, înarmate cu date care ajung în fiecare secundă de la sateliţi şi de la detectoarele de pe teren, vor ataca rapid locurile din care se atacă sistemul informaţional al ţării lor, acolo unde nimeni nici nu se aşteaptă."

În cadrul doctrinelor militare, războiul informaţional şi componentele sale (deci şi hacking-ul) ocupă deja un loc important. Paul Vasile, şeful Direcţiei Planificare Strategică şi 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 puţin pentru această etapă, că în sens strict militar războiul informaţional, la modul cel mai general, reprezintă totalitatea operaţiilor informaţionale, desfăşurate la nivel tactic, operativ şi strategic, pe timp de pace, criză, escaladare a crizei şi totalitatea operaţiilor informaţionale, desfăşurate la nivel tactic, conflictual, în scopul realizării unor obiective sau influenţării unor anumite ţinte. Războiul informaţional integrează forme de manifestare distincte: războiul de comandă şi control (forma strict militară), războiul bazat pe informaţii (intelligence), războiul psihologic, războiul electrosonic, războiul hackerilor (s.n.), războiul informaţiilor economice, războiul în spaţiul realităţii virtuale."

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

Primul atac al hackerilor legat de atacul terorist asupra WTC şi a Pentagonului a fost realizat asupra unui mare număr de servere pe care se găseau găzduite site-uri şi pagini web personale înregistrate la „NetNames", o organizaţie pentru înregistrarea de domenii Internet. Potrivit site-ului croat **http://active-security.org**, un oarecare „Fluffi Bunni" îl susţinea pe Osama bin Laden. Iar accesările realizate prin „NetNames" erau redirecţionate înspre o pagină de web unde se afla un pamflet la adresa intoleranţei religioase a Occidentului şi a Americii imperialiste, semnat de aşa-numitul „Fluffi Bunni". Despre acelaşi subiect va relata şi o ştire apărută la 18 septembrie 2001 pe site-ul românesc cu adresa **http://stiri.rol.ro** care, la rândul său, cita o informaţie BBC preluată

de la agenţia românească de presă „Mediafax”: „Unul dintre cele mai importante atacuri s-a produs la sfârşitul săptămânii, când un hacker autointitulat Fluffi Bunni a intrat în serverul companiei NetNames, ai cărei vizitatori erau automat îndrumaţi către o pagină cu mesajul «Dacă vreţi să vedeţi Internet din nou, daţi-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 şi Pentagon) la un apel al hackerilor croaţi din gruparea „Chaos Computer Club”. Adunaţi la aniversarea împlinirii a douăzeci de ani de la înfiinţarea grupei, aceştia, în loc să stea la taifas, au lansat un apel către hackeri din alte grupări şi/sau ţări de a se abţine de la orice atac asupra reţelelor sau site-urilor grupărilor orientate spre Islam, indiferent cât de afectaţi ar fi după atacurile asupra WTC şi Pentagon. „Îi rugăm pe oameni să-şi aducă aminte că Internetul este un sistem de comunicare”, a spus Andy Mueller-Maguhn, membru al grupării amintite. Nu aceeaşi atitudine a avut-o însă creatorul virusului „Votaţi 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 totuşi creat de un hacker care nu are nici un fel de legătură cu teroriştii sinucigaşi care au atacat New York-ul şi Washington-ul.

Senatul american a aprobat lărgirea domeniilor în care este acceptată utilizarea sistemului secret pentru supravegherea poştei 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 şi cercetările legate de terorism şi 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 lărgească modalităţile de control al Internetului şi-i va da Executivului american posibilitatea să „folosească mai bine cuceririle importante ale ştiinţei şi tehnologiei” în lupta împotriva terorismului. Din nefericire, nu există încă o definiţie unanim acceptată a acestei noţiuni.

Potrivit unei informaţii apărute pe **www.active-security.org** în septembrie 2000, compania de software „Network ICE”, în încercarea de a satisface puterea, respectiv regulamentele privind supravegherea poştei electronice, a anunţat 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 anunţat codul sursă al programului „Altivore” şi a publicat un program demo pe paginile sale web.

O altă „minune a ştiinţei şi tehnicii mondiale” este, fără îndoială, aşa-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 preşedintele american de atunci, Hary Truman, şi de care Guvernul S.U.A. nu a aflat decât în 1957), la care cooperează membrii grupului UKUSA şi anume: Governement 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 şi General Communications Security Bureau (G.C.S.B.) din Noua Zeelandă. Este lesne de observat că e vorba de ţări 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 Alianţei Nord Atlantice. Unul dintre cei care au studiat temeinic acest sistem este şi croatul Kruno Peradenić care, la un seminar derulat la Zagreb, descria „Echelon” ca fiind un sistem ce are capacitatea de a colecta şi analiza informaţiile transmise din orice colţ al lumii prin intermediul telefonului, telefaxului, e-mail-ului ori telexului. Într-un cuvânt, concluzionează acelaşi Kruno Peradenić, „Echelon este o ruşinoasă încălcare a constituţiei şi o

ameninţare a intimităţii cetăţenilor nevinovaţi din întreaga lume. Dacă agenţiile guvernamentale pot încălca, cu de la sine putere, cele mai elementare drepturi ale omului fără prea multă înţelegere, atunci s-ar putea ajunge la suspiciune generalizată şi la ruperea alianţelor între ţările 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 dovedeşte util nu doar pentru spionarea cetăţenilor din aria ţărilor UKUSA, inclusiv a politicienilor şi a organizaţiilor neguvernamentale, ci şi în spionajul tehnologic şi comercial. Un asemenea colos (doar la staţia Menwith Hill, aproape de Yorkshire?ul de Nord, Anglia, existau la un moment dat 25 de receivere, 1 400 de salariaţi ai NSA şi 350 de funcţionari pe teren) nu putea să fie desfiinţat deodată cu prăbuşirea sistemului comunist în Europa.

S-a tot pomenit în mass-media de puterea extraordinară a unor sateliţi de a realiza fotografii de o deosebită acurateţe a oricărui punct de pe glob. Scepticii afirmă însă că nu ar fi decât o gogoriţă născocită de serviciile secrete. În realitate, ar fi necesare resurse financiare uriaşe (chiar şi pentru o superputere militară cum sunt S.U.A.) pentru performanţa de a se putea urmări şi fotografia, fiindcă de fotografiat vorbeam, orice punct de pe Pământ. Şi oricând. Dacă urmăm aceeaşi logică, tot cei sceptici ar putea afirma că şi „Echelon" este o gogoriţă. În clipa de faţă, sistemul „Echelon" se foloseşte de serviciile unor sateliţi cum sunt cei trei „Orion/Vortex", produşi de compania „TRW", care au fiecare o rază de acţiune de până la 22 300 de mile şi sunt folosiţi pentru urmărirea telecomunicaţiilor. Sau cei doi „Trumpet", realizaţi de „Boeing", care au o rază de acţiune cuprinsă între 200 şi 22 300 de mile şi sunt folosiţi pentru supravegherea telefoanelor mobile. După cum vă este cunoscut, companiile de telecomunicaţii folosesc ele însele serviciile de retransmisie ale unor sateliţi, alţii decât cei pomeniţi. Aceştia însă se află sub controlul celor din sistemul „Echelon". Hacking de stat? Da. Citând cotidianul rusesc „Komsomolskaia Pravda", publicaţia „Cuget liber" (**www.cugetliber.ro**) spune că agentul F.B.I. Michael Schuler i-a invitat în Statele Unite, în 2000, pe Vasili Gorşkov şi pe Aleksei Ivanov, care l-au ajutat, în necunoştinţă de cauză, să obţină acces la reţelele serviciilor ruse de securitate. Cunoscuţi drept hackeri, cei doi i-au prezentat lui Schuler metodele lor de lucru, ceea ce a permis F.B.I. să obţină parolele de acces pentru serverele din Rusia. După care au fost arestaţi fiind acuzaţi de comiterea unor delicte informatice împotriva unor bănci americane.

Ei bine, ar comenta aceiaşi sceptici. Dar cum află americanii ce vorbeşte un român, de exemplu? „Echelon" se foloseşte de dicţionare speciale, care conţin diferite cuvinte-cheie. Din moment ce un român pronunţă 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 binişor în atenţia specialiştilor de la „Echelon". Programele de calculator de care dispun le permit să caute şi 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 aparţine acea voce. În cazul abonamentelor, companiile telefonice din România solicitau la un moment dat nu doar datele personale ale viitorului abonat, ci şi extrase de carte funciară pentru imobilele deţinute de aceştia. Faptul că, odată, pe vremea lui Ceauşescu, serviciul secret român cunoscut sub denumirea de Securitate citea scrisorile pe care le considera suspecte, încălcând deci un drept constituţional, inviolabilitatea corespondenţei, pare acum o banală glumă. Cine poate crede că aşa-zişii „băieţi buni" ne apără de aşa-zişii „băieţi răi" când clientelismul local, regional sau naţional a ajuns să fie multinaţional, iar interesele unui grup de indivizi care doresc să conducă întreaga lume dictează de unde şi până unde este democraţie, de unde şi până unde este legal şi de unde începe ilegalul? Dar să nu filosofăm. Cert este că într-o lume care se doreşte a fi tot mai sigură, devenim tot mai

nesiguri. Şi tot mai lipsiţi de intimitate din raţiuni pe care le dictează acelaşi grup de indivizi. Raţiuni care, evident, le servesc numai lor.

Sub titlul „Puterea şi slăbiciunea spionajului electronic", cotidianul sârbesc „Dnevnik" din 6 februarie 2002 aducea la cunoştinţa cititorilor săi faptul că croaţii au putut să înregistreze convorbirile telefonice ale lui Slobodan Miloševič 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). Ştirea era preluată de la publicaţia „Globus" din Zagreb, care a publicat stenograma unor convorbiri telefonice ale lui Slobodan Miloševič din Karađorđevo cu membri ai familiei sale, cu colaboratori apropiaţi, prieteni şi oameni de stat. În perioada 1996-1998, au fost înregistrate aproximativ 700 de asemenea convorbiri, acţiunea fiind condusă de Serviciul Secret Croat. Mulţi au pus însă la îndoială autenticitatea materialului, dar şi posibilitatea unei asemenea operaţiuni. Specialiştii au ajuns totuşi la concluzia că a fost posibil din cel puţin două motive. Întâi şi întâi pentru faptul că Croaţia este, cu siguranţă, dacă nu singura, atunci printre puţinele state care, pe lângă Statele Unite ale Americii, dispune de o aşa-zisă comunitate informativă şi o „construcţie umbrelă pentru comunitatea informativă". În ajunul ruperii sale de Iugoslavia, în 1990, Croaţia a primit din partea Germaniei cea mai modernă tehnică de urmărire şi 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 găseşte între Zagreb şi Sisak, o unitate specială pentru urmărirea comunicaţiilor radiotelefonice din întreaga Europă de Sud-Est. Acest centru, mai spune aceeaşi publicaţie sârbă, a fost dotat cu cea mai modernă tehnică „Johnson-Watkinson" pentru urmărirea şi înregistrarea comunicaţiilor electronice din regiune. Chiar la începutul războiului, acest centru a fost predat autorităţilor de la Zagreb de către însuşi comandantul său. Aşa a ajuns Croaţia în posesia tehnicii fostei J.N.A. Mai târziu, Croaţia a cumpărat o tehnică mai modernă.

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

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

Sistemul „Komint”, des înlocuit cu denumirea „Sigint” şi care se referă la serviciul informativ al legăturilor, adeseori înseamnă şi o clasă de sateliţi de telecomunicaţii, ce se folosesc pentru ascultarea legăturilor internaţionale prin radio, telefon, fax şi e-mail. Rolul „Komint”-ului este în permanentă creştere. Activitatea lui a fost cel mai bine scoasă în evidenţă în timpul „războiului rece”, când au fost înfiinţate serviciile statelor occidentale pentru ascultarea reţelelor de telecomunicaţii ale statelor din Pactul de la Varşovia. De la sfârşitul 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 şi este alcătuit din unităţi militare N.S.A. pentru susţinere electronică, părţi din C.I.A. pentru război electronic şi alte organizaţii. Acest sistem colaborează cu servicii de ascultare electronică ale altor state, printre care mai cunoscută este colaborarea în cadrul alianţei U.K./U.S.A. (cinci state). Totodată, se face schimb bilateral de informaţii între S.U.A. şi alte servicii naţionale de ascultare electronică. În lume, pe lângă U.K./U.S.A. există servicii de ascultare electronică în alte 30 de ţări. Un serviciu militar „Komint” în afara S.U.A. şi U.K./S.U.A. este organizaţia rusă F.A.P.S.I., care numără 54 000 de oameni. Un asemenea serviciu are şi China. Multe state din Orientul Mijlociu şi din Asia, aşa cum sunt Pakistanul şi 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 sateliţi, din care 40 sunt angajaţi în ascultarea legăturilor comerciale, 30 pentru controlul spaţiului cosmic din jurul Terrei şi pentru ascultarea legăturilor militare, în vreme ce pentru urmărirea spaţiului fostei U.R.S.S. sunt utilizaţi 50 de sateliţi.

Pomeneam mai sus de faptul că, datorită componenţei grupului care conclucrează la sistemul „Echelon”, în N.A.T.O. există o fisură. Iată însă că a apărut şi o a doua. Autor este acelaşi: S.U.A. Americanii au semnat în 2000 actele de înfiinţare ale T.P.I., însă nici administraţia Clinton, nici ulterior cea a lui Bush nu s-au obosit să solicite Senatului ratificarea acordului. Ba, mai mult, şi de aici cea de-a doua fisură, administraţia Bush a anunţat Organizaţia Naţiunilor Unite că S.U.A. îşi rezervă dreptul de a ignora orice dispoziţii ale T.P.I. – Tribunalul Penal Internaţional, prima instanţă abilitată să judece persoanele suspecte de crime de război, genocid sau crime împotriva umanităţii. Aşadar, dacă unii dintre cei 200 000 de militari americani aflaţi în 2002 în afara teritoriul S.U.A. ar fi săvârşit fapte de genul celor enumerate mai sus ei nu ar fi putut fi judecaţi de T.P.I. La insistenţele, presiunile şi, ceea ce nu este deloc exclus, şantajul americanilor, câteva state, printre care Israelul şi 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 tradiţional al S.U.A., şi Italia vor ceda presiunilor americane, nu este exclus să fie urmate şi de celelalte membre ale NA.T.O. şi atunci actuala fisură va dispărea. Însă T.P.I. ori va fi desfiinţat, ori va deveni ridicol. Şi va demonstra încă o dată că a fost înfiinţat formal, doar pentru a-i aduce pe sârbii cei indisciplinaţi în rând cu lumea. Cu lumea supusă, evident. De altfel, se cunoaşte foarte bine faptul că, în ton cu rolul pe care şi l-a impus, şi anume al celui de jandarm mondial, S.U.A. nu dau pentru prima dată dovadă de aroganţă. 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 reuşit să irite nu doar obişnuiţii săi inamici, ci şi aliaţii 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 şi unde au participat numeroşi şefi de state şi de guverne, Colin Powell, reprezentantul S.U.A., a fost huiduit copios de către chiar concetăţeni de-ai lui. Şi de această dată S.U.A. şi-au etalat aroganţa de mare putere şi de şi mai mare poluator al atmosferei. Astfel că devine de-a dreptul ridicolă mirarea americanilor în faţa 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. Iniţiatorii acestui sistem planetar de telecomunicaţii au avut se pare o imaginaţie mai puternică decât înşişi 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 deţinem despre fiecare ţară în parte. Altfel spus, doar că nu au invitat pe faţă 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 fiţuică de cartier până la radioul şi televiziunea naţională, nu care cumva să scape vreo informaţie 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 informaţii cu duiumul. Dar, mai mult, se poate influenţa un popor întreg, începând cu cel american, bineînţeles. De aici putem deja vorbi despre concepţia conflictelor de mică intensitate, despre războiul psihologico-propagandistic etc. În 2002 şi tot sub pretextul luptei împotriva terorismului, Parlamentul european adoptă şi el o lege care obligă nu doar operatorii de Internet, ci şi pe cei de telefonie fixă şi mobilă să stocheze informaţii detaliate despre convorbirile fiecărui abonat. De acum înainte, se vor arhiva numerele de telefon apelate, durata fiecărei convorbiri şi conţinutul acesteia, secunda, minutul, ora şi ziua când s-a efectuat aceasta, precum şi traseul fiecărui cetăţean 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 permanenţă cu staţiile de bază. Ratificată de parlamentele celor cincisprezece ţări membre ale U.E., legea adoptată la Bruxelles este obligatorie pentru statele candidate la aderare, deci şi pentru România. „Cu aprobarea Occidentului – spune Bogdan Chireac în editorialul „Adevărului" din 4 iunie 2002, cei care vor conduce serviciile secrete din România vor deţine o putere pe care securitatea lui Ceauşescu nu a visat-o vreodată. Dacă lucrurile vor scăpa aici de sub controlul legii, România, integrată în N.A.T.O. şi U.E., riscă să ajungă mai puţin liberă decât România lui Ceauşescu…". Iată că „Echelon" se extinde mai repede decât au crezut creatorii săi.

Nu e un secret faptul că S.U.A., Japonia şi 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 foloseşte microprocesoare pe bază de cupru în locul celor siliconice şi un program (software) pentru servicii comerciale şi de rezolvare a problemelor de inginerie de genul celor pentru design-ul avioanelor, denumit RS/6000 SP.

În China, a fost dat în folosinţă 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 ţării în domeniul apărării antiaeriene. Prin acest act, puterea de la Beijing dovedeşte că-şi dă seama de importanţa tehnologiei informatice. Cheia victoriei în războiul strategic informaţional al secolului al XXI-lea stă în suveranitatea propriei reţele informaţionale, susţin conducătorii militari chinezi. Controlul reţelei informatice naţionale chineze de către o putere, alta decât cea chineză, ar pune în primejdie interesele vitale naţionale şi ar însemna agresarea civilizaţiei chineze, se afirmă într-un studiu al staff-ului armatei chineze.

Şi, totuşi, de ce s-a derulat în 1999 primul e-război mondial? Pe de-o parte pentru că cetăţeni de etnie sârbă au existat în mai toate statele lumii şi fireşte că au fost de partea conaţionalilor lor agresaţi de forţele N.A.T.O. Pe de altă parte, pentru că nu au stat cu mâinile încrucişate nici internauţii de origine slavă, îndeosebi cei din Rusia, Ucraina şi Belarus. Şi nici cei care, într-un fel

sau altul, nu agreează politica de forţă cultivată de Statele Unite, printre aceştia din urmă fiind şi mulţi cetăţeni americani. Pe frontul celălalt s-au aflat în primul rând albanezii din diaspora, musulmanii şi, evident, cei care văd în S.U.A. pe Dumnezeul lumii. Fireşte, de la luptă - că doar nu se luptă pe câmpul de luptă, cu arma în mână, sub şuierul gloanţelor şi în miros de praf de puşcă, ci la căldură, în faţa unui monitor şi cu o Coca-Cola alături – nu s-au dat la o parte nici extremiştii, cei pentru care intervenţia din Iugoslavia a fost doar un pretext pentru defulare. De aceeaşi parte a baricadei, pe frontul împotriva S.U.A. în primul rând, s-au aflat ultranaţionaliştii, comuniştii şi neonaziştii. Aşa cum în clipa de faţă neonaziştii şi grupările radicale islamice au făcut front comun împotriva evreilor şi a americanilor. Interesant este, în acest sens, un articol scris de Ivan Ninić din Israel şi apărut, în septembrie 2002, pe site-ul „Apis" (**www.2net.co.yu/apis/**), care trece în revistă trecutul relaţiilor dintre Germania şi lumea arabă. Autorul porneşte de la războiul informatic iniţiat, în preajma celui de-al doilea război mondial, de către maşina propagandistică nazistă, când Germania lui Hitler s-a aliat cu fundamentaliştii musulmani contra intereselor engleze, şi termină prin a face următoarea remarcă: „Crearea Israelului doar amplifică intoleranţa lumii arabe împotriva aliaţilor şi, cu ajutorul fostei axe a puterii, arabii creează ei înşişi o axă antisemită, care s-a cuibărit în sânul intelectualităţii vest-europene de stânga, în dreapta revanşardă şi într-o bună parte a Lumii a Treia. Cimentul acestei alianţe nenaturale îl constituie lupta împotriva globalizării, iar ura împotriva «Satanei mari» şi a celei mici, după cum ar spune aiatolahii din Koma (Iran), capătă forme tot mai pronunţate. […] Nazificarea unei părţi a societăţii islamice a primit prin tehnologia de vârf o armă puternică. Perfecţiunea tehnicii germane a dobândit urmaşi talentaţi în fundamentalismul islamic." Aşadar, aliaţii nu ţi-i alegi niciodată singur. Ţi-i alege conjunctura. Ori inamicul.

Portret

Chiar dacă, de curând, după ani de zile de dominaţie, 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, aşa cum, în antichitate, lingua franca a fost latina. Astfel că, pe bună dreptate, cel care doreşte să pătrundă în tainele Internetului şi nu ştie deloc ori prea bine limba engleză trebuie să aibă neapărat în preajmă un dicţionar englez-român. Şi întrucât vorbim în cartea de faţă despre hackeri, iată şi definiţia de rigoare, aşa cum a fost ea concepută de către anglistul Andrei Bantaş: hacker – târnăcop, topor de tăiat piatră; tăietor de piatră; salahor; muncitor care lucrează cu târnăcopul/toporul. Iar hack înseamnă cal de povară, rob, dar şi a ciopârţi, a tăia. Adică ceva identic sau aproape identic cu verbul românesc a hăcui, provenit din cuvântul german hacken şi care înseamnă a tăia în bucăţi (mici), a toca mărunt, a sfârteca, a ciopârţi. Pe de altă parte, specialiştii din domeniul IT susţin faptul că hack este un cuvânt derivat din limbajul studenţilor de la Masachussets Institute of Technology, utilizat pentru a defini glumele făcute de studenţi şi în acelaşi timp impunea respect. O legătură electrică se definea „hack simplu", un „hack" trebuind să fie inovator, să denote stil şi pricepere tehnică.

Dar cine sunt hackerii? Se spune despre ei că detestă orice individ, instrument sau lege care încearcă să împiedice cunoaşterea. În lumea lor, oricine poate să demonteze un lucru pentru a-l îmbunătăţi este binevenit. Însă dacă accesul la acel lucru este îngrădit, dacă între hacker şi informaţii există bariere, atunci hackerul afirmă că este vorba de birocraţie, de o birocraţie de-a

dreptul periculoasă. De asemenea, se mai spune că, din punct de vedere al hackerilor, de pe urma libertăţii informaţiei orice sistem poate trage beneficii.

Hackerii au avut un rol esenţial în dezvoltarea softului, la crearea şi dezvoltarea Internetului. Numai că, în timp, cele două percepte fundamentale ale eticii lor, respectiv datoria morală de a răspândi cunoştinţe scriind „software" pentru a facilita accesul la informaţie şi la mijloacele de calcul şi condamnarea vandalismului şi a atentatelor la confidenţialitate au început să fie în mod repetat şi grosolan încălcate. Acest lucru nu a scăpat de ochiul vigilent al mass-media, care a văzut balanţa înclinându-se în devafoarea hackerilor cu respect faţă de etică. Drept urmare, hackerii nu mai sunt consideraţi a fi cei care, în epoca de pionierat, erau eroii pozitivi, ci au devenit in corpore eroi negativi.

Referindu-se la hackeri în numărul din aprilie 2002 al „PC Magazine", Mihaela Cârstea, redactorul şef al publicaţiei, 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 funcţioneze. Dacă faci parte din această cultură, dacă te solidarizezi cu ea şi dacă alte persoane care îi aparţin ştiu cine eşti şi te numesc hacker, înseamnă că eşti hacker. Legendă? Adevăr? Dar chiar dacă hackerii au avut iniţial un rol pozitiv la dezvoltarea Internetului, intruziunile lor forţate nu au nici o justificare."

Dar, vă veţi întreba, cine sunt de fapt aceşti hackeri? Răspunsul e simplu: majoritatea sunt elevi sau studenţi care vor să iasă în evidenţă prin modificarea site-urilor, ţinta lor predilectă fiind site-urile guvernamentale, militare sau ale marilor companii, aşadar unele dintre cele mai des accesate şi cu un mare impact la public. Cum altfel, nu-i aşa, ar afla atâta lume despre faptele lor? Demn de reţinut este însă că există crackeri (acum vorbim de crackeri) care beneficiază de statut legal. L. Ivaner, autorul cărţii „Lexiconul hackerului" (Editura „ProMedia Plus", Cluj-Napoca, 1996) spune că aşa-numitele „tiger teams" „...sunt echipe de crackeri profesionişti care testează sistemele de securitate ale instalaţiilor de computere militare prin atacarea lor de la distanţă, folosind reţele şi canale comm considerate «impenetrabile». Dacă nu ar fi ţinute în mare secret, am putea cu siguranţă admira în programele acestor «echipe de tigri» cele mai ingenioase artificii care s-au imaginat vreodată. Ce ne împiedică să presupunem că aceşti crackeri profesionişti provin din rândul hackerilor care şi-au înfrânat dorinţa de a comite infracţiuni spărgând sisteme, dorinţă pe care, în noua ipostază, şi-o pot satisface pe cale legală."

Dar să vedem cine sunt principalele personaje ale cărţii de faţă. Potrivit opiniei generale, hackerii posedă un profil psihologic special. Cu cât sunt mai tineri, cu atât se laudă mai mult. Motto-ul care-i uneşte este „Mâncare, adăpost şi un cod autentic". O dată cu trecerea anilor, ei nu mai sunt însă atât de interesaţi de ceea ce spun cei din jurul lor, ci preferă să-şi păstreze un anonimat deplin. Aceasta inclusiv din raţiuni 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 şi de maturitatea atacatorului, majoritatea începătorilor au ca motiv principal dorinţa de răzbunare pe un anumit utilizator, admin(istrator) sau dorinţa de a arăta întregii lumi ce prezintă. După aia va veni numaidecât dorinţa de a obţine acces acolo unde nu au toţi muritorii. Iar maturitatea unui atacator ar fi acţionarea din motive mai serioase: motive politice, economice etc." Aşadar, dacă în timp de război hackerii tineri nu prea conştientizează ceea ce se întâmplă sau le este indiferent prin ce anume trece naţiunea din care fac parte, hackerii (sau chiar foştii hackeri în tinereţe) maturi vor înţelege necesitatea implicării lor în cyberwar şi vor acţiona ca atare.

Pentru propria securitate vizavi de legislaţia în vigoare în ţara lor, cei care realizează şi administrează site-uri destinate hackingului au grijă să scrie că tot ceea ce fac nu este decât o prezentare a activităţii de hacking destinată pur şi simplu… cunoaşterii. Este şi cazul site-ului în limba română cu adresa **http://dev-null.go.ro/cracklinks.htm**, al cărui autor, care se semnează GiaRdiA, scrie: „Informaţia prezentată pe acest site, programele-exemplu şi alte materiale sunt DOAR în scopuri educaţionale. Autorul va fi considerat în afara oricărei responsabilităţi dacă utilizarea acestor informaţii va fi în scopuri ilegale, menite să aducă pagube sau câştiguri materiale, fizice sau morale. Acest site nu încurajează deprotejarea programelor pentru folosirea lor ilegală. Metodele de protecţie prezentate au ca scop îmbunătăţirea modului de lucru al programatorilor dând informaţii asupra metodelor şi variantelor de «spargere» a unui program. Acest site nu încurajează folosirea copiilor ilegale a uneltelor prezentate aici. Cu alte cuvinte: dacă vreţi să le folosiţi, cumpăraţi-le!". Dar iată şi descrierea aceluiaşi GiaRdiA pentru diverse link-uri: „Sudden Discharge Un site foarte bun de cracking. Programmers Tool's După cum spune şi 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! Încercaţi-l ! 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 şi găsit, dată fiind existenţa lor efemeră ori chiar teama de autorităţi.

Dar scum se văd a fi hackerii înşişi? O descriere foarte plastică a conceptului de hacker am găsit-o la adresa: **http://www.best.pub.ro/~traznet/nr4/hacker4.htm:** „Dacă aţi mai citit ceva despre hacker, cracker, creatori de viruşi şi alte specimene de acest fel, probabil că sunteţi deja familiarizaţi cu profilul psihologic atribuit acestora: «adolescenţi sau tineri izolaţi, impotenţi, incapabili să întreţină o relaţie socială normală...bla bla bla». Nu este deloc aşa. Hackerii sunt nişte băieţi (sau fete) foarte de treabă - foarte inteligenţi chiar dacă nu iau ei toate examenele şi mai pică câte un an..."

Pentru un hacker este destul dacă nu chiar foarte greu să-şi ţină gura atunci când reuşeşte să spargă un sistem protejat. Mai ales dacă se află la vârsta de cristalizare a personalităţii. Dar, încet-încet, grozăvia cedează locul stăpânirii de sine. Viaţa hackerului este lungă dacă ştie să-şi pună lacăt la gură. La adresa amintită mai sus se spune: „Dacă oricum ai făcut o prostie mai mare decât o poţi acoperi, ai două posibilităţi: să apelezi la prieteni de încredere sau, dacă eşti prins, să te comporţi ca un adult, adică: neagă tot!"

Pe **www.occident.ro** a fost publicat un interviu luat de Paula Bulzan informaticianului Radu D.: „- Spuneţi-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 inteligenţei. O altă trăsătura comună este insistenţa, perseverenţa în obţinerea scopului propus. Hackerii trebuie să aibă o voinţă 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 şi luarea unor decizii pe baza propriilor criterii.

Majoritatea hacker-ilor preferă lucrul individual, chiar dacă au experienţa lucrului în echipă. Distanţa şi răceala în comunicare, predispoziţia la conflict, lipsa unor emoţii 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 undergound sub numele de K2 (numele real: A.M. Shane), a fost întrebat

care sunt, după părerea lui, deosebirile dintre un cracker şi 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 şi poate astfel să-şi pornească unitatea de calcul. De fapt, eu efectiv nu mă gândesc atât de mult la aşa ceva, aceşti termeni nu înseamnă nimic pentru mine. Dacă vă numiţi „hacker" sau indiferent cum altcumva, unii oameni vor crede taman pe dos decât aţi crezut dumneavoastră că înseamnă."

Desigur, există deja şi istorii ale hacking-ului, dar şi 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 şi Vladimir Levin. Cărora li se adaugă Douglas Engelbart, Steve Wozniak, Clifford Stoll, Linus Torvalds şi Tsutomu Shimomura. Să vedem însă cine au fost primii zece. Richard Stallman e primul hacker fără pseudonim şi care are un dosar ireproşabil. Primul contact cu computerul l-a avut la 16 ani, în Centrul ştiinţific din New York al I.B.M. În anii '70 a lucrat într-un laborator pentru inteligenţă artificială din cadrul Universităţii 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 înfiinţat în ianuarie 1986 fundaţia „Free Software". Este cunoscut şi ca întemeietor al grupului GNIU, care dezvoltă o susţinere gratuită pentru sistemul de operare „Linux". Stallman este primul luptător împotriva programelor comerciale.

Dennis Ritchie şi Ken Thompson sunt cu siguranţă unicii hackeri mai cunoscuţi sub numele adevărate decât prin pseudonime. (dmr şi Ken). Ritchie şi Thompson au creat în 1969 „Unix", un sistem operaţional deschis care a schimbat radical istoria computerelor. Ritchie este cunoscut şi 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 reuşit să determine centrala telefonică să-i permită să telefoneze gratuit de la telefoane publice. Isprava sa a fost motiv de inspiraţie pentru generaţii 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 şi prin aceasta şi-a incitat mulţi „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 şi anume „Masters of deception" (MOD).

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

Ţinta principală au fost cei din grupul LOD, însă aceştia nu au fost prinşi. Totuşi, operaţiunea nu a fost zadarnică - patru membri ai grupei MOD, incluzându-l aici şi pe Phiber Optic, au fost băgaţi la închisoare, prin aceasta încheindu-se „Marele război". După un an de închisoare, ei au ieşit ca adevăraţi eroi şi 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 ştiinţă din cadrul Centrului de computere al Agenţiei Americane pentru Securitate Naţională (National Security Agency, N.S.A.). S-a întâlnit pentru prima dată cu un computer atunci când tatăl său a dus acasă una dintre maşinile 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" şi unde, în curând, cu ajutorul unor trucuri de programare, a dobândit statutul de administrator. Lui i se datorează inserarea în dicţionarul computerelor a cuvântului „hacker".

Cea mai importantă operă a sa apărut în perioada studiilor de ştiinţe ale computerelor la Universitatea Cornell: a fost primul virus de Internet cunoscut şi sub denumirea de vierme. Pe 2 noiembrie 1988, folosindu-se de greşelile din versiunea de atunci a programului de trimitere a poştei electronice (sendmail) şi de primire a datelor despre utilizatori (finger), a scris un program care s-a multiplicat singur şi s-a extins în reţea şi pe care l-a denumit „vierme". Intenţia lui nu a fost să provoace perturbări ale traficului de pe Internet, ci doar să încerce unele dintre ideile sale. Din cauza unei greşeli 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 şi a expediat indicaţii anonime administratorilor din reţea despre ceea ce trebuie să facă pentru a opri viermele, însă era deja prea târziu. Reţeaua era într-atât de sufocată încât mesajul a ajuns prea târziu. Sistemele diferitelor universităţi, baze militare şi fundaţii medicale erau deja infectate. Grupe din cadrul Universităţilor Berkeley şi 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 soluţie temporară pentru limitarea răspândirii viermelui. Între timp, sufocarea reţelei şi numărul uriaş de calculatoare scoase din funcţie au împiedicat recepţionarea acestei informaţii de către toţi cei cărora le era necesară. Situaţia s-a liniştit abia peste câteva zile. Întrucât cheltuielile cu înlăturarea pagubei ajungeau şi la 50 000 de dolari de sistem, a început căutarea vinovatului. Ziariştii de la „New York Times" l-au indicat de vinovat pe Morris, astfel că a urmat arestarea acestuia şi trei ani de pedeapsă plus 400 de ore în folosul comunităţii şi 10 000 de dolari drept amendă.

Kevin Mitnick, zis Condor, a început de mic să se ocupe de comunicaţiile prin calculatoare. Deoarece nu a avut bani să cumpere un computer, a apelat diverse sisteme cu ajutorul unui modem, dintr-o unitate a lanţului de magazine „Radio Shack". El şi-a câştigat locul în galeria celor mai cunoscuţi hackeri datorită faptului că fotografia sa a ajuns pe lista celor mai căutaţi criminali urmăriţi 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 şi acuzat de falsificarea a 20 000 de numere de cărţi 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 consideraţi drept o versiune modernă de Robin Hood şi tuturor le-au devenit clare pericolele pe care le reprezintă asemenea indivizi. Se lucrează tot mai serios la securitatea sistemelor de reţele, iar hackerii profesionişti 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 staţia de radio KISS-FM din Los Angeles pentru a se asigura astfel că va cel de-al 102-lea ascultător care se anunţă telefonic pentru a participa la o emisiune-concurs. Aceasta i-a adus un automobil Porsche-944 S2. A fost prins când au apărut fotografii în care se vedea cum forţează punctul companiei telefonice. De altfel, fotografiile au fost făcute de un prieten de-al său, pentru a a

imortaliza evenimentul. La proces a recunoscut şi faptul că a pătruns în computerele F.B.I.-ului, de unde a luat o listă cu agenţi aflaţi în misiuni speciale.

Johan Helsingius, zis şi 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, poliţia a pătruns în spaţiul 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, funcţiona pe un calculator cu un procesor de 486 şi un harddisk de 200 Mb.

Vladimir Levin este ultimul din galeria hackerilor celebri şi primul hoţ Internet cunoscut. Cu ajutorul computerului firmei „AO Saturn" din Petrograd, unde lucra, şi a laptopului său personal, în perioada din iunie şi 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 Heatrow în martie 1995. La începutul lui 1997, a fost în sfârşit predat americanilor, iar în august a fost condamnat la 36 de luni de închisoare şi la o amendă de 250 000 de dolari. După spectaculoasa arestare a lui Vladimir Levin din anul 1995, la opinia publică ajung doar informaţii nesemnificative despre atacuri temporare asupra unor prezentaţii Web. Faptul că sistemul de computere al ministerului american al apărării nu a rezistat atacului unui israelian de nouăsprezece ani şi 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 doreşte să dea publicităţii prea multe secrete de la locul de muncă.

Hackerii deschid cyberfrontul

Este cunoscut faptul că în timpul agresiunii N.A.T.O. asupra Iugoslavei, în 1999, au existat mai multe grupe de hackeri sârbi care au avut un rol important. Aleksandar Milosavljević, un procuror belgrădean şi unul dintre puţinii oameni ai legii din Serbia care se ocupă de criminalitatea prin Internet din entuziasm şi din curiozitate, după cum singur declară, susţine că hackerii sârbi şi grupările din care fac aceştia parte se află în strânse legături cu hackeri din străinătate. Sunt îndeobşte cunoscute grupările „Îngerii sârbi" („Srpski anđeli"), „Codrenii" („Šumadinci"; Šumadija" este o regiune a Serbiei, „šumadinci" fiind locuitorii acestei regiuni) şi „Armata Sârbă a Internetului" („Srpska Vojska Interneta", abreviat SVI, ceea ce înseamnă şi „toţi"), aceasta din urmă având şi un regent şi 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 şi Kapetan Dragan (Căpitanul Dragan)? Informaţiile 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 însuşi: „Bine aţi venit pe site-ul meu, de fapt pe site-ul «Reget Info». Eu sunt Regentul, cel mai mare hacker sârb şi, după multe criterii, primul om al reţelei Internet iugoslave. După naţionalitate sunt Om, iar după religie autoidolatru (nu vă temeţi, 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 şi mă rog doar mie însumi). Sunt fondatorul şi cel mai înalt funcţionar al «Armatei Sârbe a Internetului« (SVI) – **http://come.to/svi** - o organizaţie publică a

hackerilor. Potrivit spuselor altora, prin toată munca mea pe Internet am ieşit în evidenţă prin originalitate, rapiditate şi prin efectele muncii mele. Toate faptele mele de pe Internet, chiar dacă neacceptate din punct de vedere moral şi într-o oarecare măsură infracţionale, le accept ca fiind ale mele!"

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

„…- Adunaţi din nou voluntari?

- Da, însă nu mai este vorba de aceeaşi categorie de voluntari care au luptat în războaiele trecute. Acum adun în forţă voluntari şi anume din rândul celor şcoliţi, al tinerilor cu pregătire în domeniul computerelor, care vorbesc limbi străine, oameni cu diferite cetăţenii, 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 Alianţei Nord-Atlantice şi 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 şi drept până în ultima clipă pentru ţara sârbească şi poporul sârb, cu o singură dorinţă şi anume ca SVI să controleze Internetul, iar SVI - toţi sârbii, ţara şi 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 informaţii despre originea acestei denumiri.

La 5 iunie 2002, **www.google.com** dădea 3 360 de locaţii pentru „crna ruka". În limba română, „crna ruka" înseamnă „mâna neagră". Sub această denumire a fost cunoscută organizaţia secretă „Unire sau moarte" („Ujedinjenje ili smrt"), înfiinţată la Belgrad la 9 mai 1911, din care au făcut parte Gavrilo Princip, Nedeljko Čabrinović, Danilo Ilić, Trifko Grabez, Vaso Čubrilović, Veljko Čubrilović, Cvjetko Popović, Miško Jovanović, Mohammed Mehmedbašić şi care a fost creată de colonelul Dragutin Dimitrijević, cunoscut şi sub numele de „Apis" (din latinescul „apis" - albină). Membrii grupului imprimau pe clădirile importante din Belgrad forma unei palme negre şi de aceea lumea le-a dat numele de „Mâna neagră". Organizaţia reunea ofiţerii care au participat la Revolta din mai 1903 şi la un atentat împotriva regelui Aleksandar Obrenović şi a reginei Draga. Întrucât regina nu i-a putut dărui soţului copii, iar ofiţerii nu şi-au primit salariile, atentatorii au vrut să-l proclame drept rege pe fratele acesteia. Istoricii sârbi afirmă că activitatea organizaţiei „Crna ruka" rămâne pentru cercetători o mare taină. Este cunoscut faptul că Statul major al armatei sârbe trimitea ofiţeri în Macedonia şi în Serbia Veche pentru a organiza detaşamente de gherilă pentru lupta împotriva forţelor Imperiului Otoman. Numai că lupta cu Turcia, iar mai târziu, cu Imperiul Austro-Ungar (sprijin logistic acordat organizaţiei de tineret „Tânăra Bosnie" în seria de atentate asupra înalţilor demnitari ai Imperiului Austro-Ungar şi chiar a moştenitorului 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 însuşi regentul Aleksandar Karađorđević şi o parte a Gărzii regale, în frunte cu colonelul Živković, dar şi preşedintele Guvernului, Nikola Pašić. După prăbuşirea Serbiei, în anul 1915, colonelul Dragutin Dimitrijević a fost condamnat, la procesul de la Salonic din 1917, la moarte pentru plănuirea revoltei şi a atentatului împotriva regentului Aleksandar. Numai că unii dintre membrii acestei organizaţii şi-au continuat activitatea. Mustafa Golubić a devenit unul dintre şefii 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 şi de către Partidul Radical. Toţi cei condamnaţi au fost reabilitaţi.

Dar să revenim la Internet. Ibrahim Rugova, liderul albanezilor din Kosovo, reclama, la 20 octombrie 1998, că hackeri sârbi, membri ai „organizaţiei teroriste Crna ruka", au atacat indexul site-ului Centrului de Informaţii din Kosovo (albanez). În pagina web a albanezilor sârbii au inserat simbolurile naţionale sârbe, scriind: „Bine aţi venit pe pagina celor mai mari mincinoşi şi ucigaşi din lume" şi „Fraţilor albanezi, această stemă va fi pe steagul vostru atâta timp cât va exista şi steagul".

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

Agenţia independentă sârbă de ştiri „Beta", citând BBC-ul, anunţa că o ediţie pe Internet a ziarului albanez kosovar „Zeri i Kosoves" („Glasul Kosovo-ului"), găzduită de un provider elveţian, a fost atacată de hackeri sârbi, aceştia inserând mesaje antialbaneze. Provider-ul elveţian a declarat că autor a fost un student iugoslav din Polonia (informaţie preluată şi de mass-media germană). Hackerul l-a ameninţat că, dacă mai găzduieşte site-ul albanez, îi va şterge hard-disk-urile. Organizaţiile internaţionale 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 publicaţiei croate „Vjesnik", fapt care a atras atenţia mass-media din Croaţia şi Iugoslavia, deoarece pe index a apărut un mesaj cu semnătura „Mâinii negre". Cei de la „Vjesnik" au fost însă deosebit de satisfăcuţi, deoarece au asociat numele grupei de hackeri cu acea organizaţie secretă sârbească, una dintre puţinele organizaţii teroriste, spuneau ei, care s-a păstrat aproape un veac. Poliţia croată a susţinut că hackerii au acţionat de pe teritoriul Iugoslavei, însă nu se putea lua nici o măsură împotriva lor, Iugoslavia nefiind membră a Interpol. Drept răspuns, hackerii croaţi au atacat la sfârşitul lui octombrie 1998 site-ul „Bibliotecii Naţionale a Serbiei".

Site-ul hackerilor croaţi, cu adresa **http://temat.4ever.cc**, considerat a fi cartierul general al celor două grupuri majore de hackeri – „Zadar Boyz" şi „White Boyz", a anunţat vineri, 30 octombrie 1998: „Vă informăm că organizaţia hackerilor croaţi a intrat în site-ul Bibliotecii Naţionale Sârbe şi a lăsat u mesaj. Este vorba despre o «răzbunare« pentru recentul atac asupra site-ului publicaţiei «Vjesnik« şi despre a vă aduce la cunoştinţă că nu e nici o problemă să dărâmi un site. Atacul a fost anunţat şi 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 discuţia cu aceştia, s-a constatat că grupul „Mâna neagră a „vizitat" în ultimul timp adresele **http://www.zik.com/**, **http://www.kosova.com/** şi **http://www.vjesnik.com/**, afirmând că ei s-au ridicat în apărarea electronică a intereselor Iugoslaviei şi nu vor renunţa la atacuri asupra site-urilor care inserează minciuni despre situaţia din această ţară. Cât despre „războiul electronic" cu croaţii, scrie în acelaşi număr al „Lumii computerelor", ei consideră că sunt chit, întrucât sunt pentru „pace, dragoste şi bunăstare pe întreaga planetă". Drept dovadă stă şi faptul că niciodată nu

au şters fără a fi necesar date din paginile/site-urile web cu toate că au putut să o facă. Acesta a şi fost motivul că la „Vjesnik" nu au schimbat decât indexul (pagina principală). Cei de la „Vjesnk" au susţinut că hackerii sârbi nu au ştiut să schimbe şi conţinutul altor pagini web din acelaşi site.

Mai multe detalii, precum şi atitudinea părţii 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 informaţional continuă prin atacul asupra paginilor electronice!". În preambul scrie: „Miercuri dimineaţa au fost blocate temporar paginile web ale cotidianului «Vjesnik» şi în locul lor a fost inserat mesajul «Mâinii negre», o organizaţie secretă de hackeri. Hackerii, care îşi spun «Mâna neagră» susţin că orice încercare de «măsluire a adevărului» despre sârbi va fi «împiedicată prin toate mijloacele». Aceeaşi organizaţie a atacat săptămâna trecută paginile publicaţiei «Glasul Kosovo-ului» şi ale Centrului informativ din Kosovo." În locul conţinutului indexului site-ului cotidianului croat a fost inserat un link către site-ul „Mâinii negre" unde, printre altele, scria că „Mâna neagră" doreşte ca prin activitatea sa să schimbe imaginea falsă care înconjoară planeta şi în care se vorbeşte despre sârbi ca fiind nişte răufăcători. În finalul mesajului, „Mâna neagră" susţinea că „Ultimul lucru pe care dorim e să ameninţăm 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-şi face reclamă, ci au dorit să insereze şi 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 şi de lozinca „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, publicaţiei iugoslave „Blic" (susţin tot cei de la „Vjesnik") i s-a anunţat un membru anonim al „Mâinii negre", confirmând că este vorba de o grupare de hackeri sârbi şi anunţând continuarea „înlăturării minciunilor albaneze de pe Internet, dar şi existenţa unor planuri asemănătoare pentru paginile Alianţei Nord-Atlantice". După spusele acestuia, „Mâna neagră" avea cinci membri, respectiv din Belgrad, Niš şi din Macedonia, şi că deja de un an de zile se lupta împotriva propagandei albaneze. A amintit şi 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 acelaşi 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". Croaţii continuă scriind cum că „Politika" aminteşte şi de cazul atacului din Croaţia asupra sistemului informatic al Pentagonului, atac care, de fapt, a fost opera hackerilor sârbi pusă pe seama croaţilor. Tot „Vjesnik" spune că hackerii sârbi şi-au făcut cunoscute telefonic intenţiile şi agenţiei „The Associated Press" care, pe 22 octombrie, a şi publicat un material pe această temă.

Administratorii site-ului cu adresa **http://ds.org.yu/** anunţau miercuri, 11 noiembrie 1998: „Hackerii sârbi care-şi spun «Crna ruka» au atacat site-ul Institutului «Ruđer Bošković» din Zagreb."

Un amplu articol despre „Mâna neagră" („Die Schwarze Hand") publică şi 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. Informaţia este preluată din publicaţia londoneză „Sunday Times".

Un atac al membrilor „Mâinii negre" este relatat câteva luni după încetarea agresiunii N.A.T.O. asupra Iugoslaviei şi în numărul 282 din 7 februarie 2002 al suplimentului săptămânal

„Dom i svijet" al Centrului de Informaţii Croat (**www.hic.hr**). Se spune că varianta de pe Internet a e-zin-ului (publicaţie care apare pe Internet) croat „Monitor" a fost atacată de aşa-numita organizaţie „Mâna neagră" din Serbia. Specialiştii în informatică croaţi susţin că este vorba de hackeri care cunosc excelent programul „Linux". Se recunoaşte totuşi că hackerii anonimi nu au adus pagube importante acestei publicaţii, ci doar au dorit să arate că pot distruge paginile web ale „Monitorului". De asemenea este amintit atacul asupra publicaţiei „Vjesnik".

Despre atacul hackerilor sârbi asupra cotidianului croat „Vjesnik" anunţa şi 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 croaţi au atacat site-ul Bibliotecii Naţionale Sârbe şi au inserat anunţul: „Citiţi Vjesnik şi nu cărţile sârbeşti".

O mulţime 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" şi cu următorul preambul: „Războiul de pe reţeaua mondială a computerelor (Internet, n.n.) se poartă en gros. Sârbii au început (în sfârşit) să învingă." Vizavi de site-ul publicaţiei kosovare „Zeri i Kosoves" se spune că în locul membrilor U.C.K. („într-o poziţie de eroi, cum ar spune patrioţii Belgradului") şi a refugiaţilor albanezi udaţi de ploaie, pe site-ul **www.zik.com** a apărut un text nou: „Bine aţi venit pe web site-ul celor mai mari mincinoşi şi 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 veţi afla în apropiere". Provider-ul elveţian a descoperit că atacatorul este cineva care se dă drept un student sârb în Polonia, enervat de ceea ce se afla în reţea şi care, în stilul lui Zorro, a hotărât să preia problema în mâinile sale. A ameninţat provider-ul elveţian că dacă nu şterge site-ul kosovarilor albanezi îl va şterge el însuşi. Pentru a-şi susţine ameninţarea a distrus hard-disk-ul din biroul acestuia. Numai că necunoscutul student a lăsat o urmă: propria adresă de e-mail (poştă electronică), precum şi cea a organizaţei „Mâna neagră". Astfel, susţine NIN, după optzeci de ani, Apis s-a aflat pentru a doua oară printre sârbi.

Dar cine sunt aceşti moderni „Apis"?, se întreabă NIN. Pentru cazul „Glasul Kosovo-ului" elveţienii au acuzat puterea sârbă. Mass-media elveţiană a scris că „hackerii sunt apropiaţi ai serviciilor secrete sârbeşti" şi că ceea ce s-a întâmplat este doar o parte a „epurării etnice" care se duce nu doar asupra albanezilor din Kosovo, ci, iată, şi pe Internet. Dar, între timp, s-a făcut auzită şi poziţia celor de la „Mâna neagră". NIN a reuşit să-i contacteze pe doi dintre aceştia. Din motive de la sine înţelese, susţine NIN, hackerii cu pricina au insistat asupra unui anonimat complet. „Întâlnirea" cu ei s-a consumat prin IRC (un program pe Internet prin care se poate discuta pe viu cu alţi internauţi care doresc acest lucru). Pentru a demonstra că sunt ceea ce pretind, adică membri ai grupării „Mâna neagră", ei au atacat, înainte de discuţie, un site oficial din Bosnia-Herţegovina. Printre altele, hackerii au declarat că nu atacă site-urile iugoslave, cu toate că asta a fost prima lor intenţie. 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** posluzitelj, deci în plină agresiune a N.A.T.O. împotriva Iugoslaviei. Iată ce scriu croaţii 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 croaţi – un serviciu care este pagina neoficială de început a paginilor web din Republica Croaţia şi care conţine date despre mai mult de 3 000 de consumatori www croaţi".

Tot în 1999, D. Sušanj 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 conţinea

stema sârbească şi-i îndemna pe vizitatori «să caute adevăratul adevăr la adresa **www.yu»**, unde, la fel, se găseşte un catalog de adrese web, însă iugoslave." Acest atac a coincis, scria acelaşi D. Sušanj, cu acuzaţia celor de la CARnet şi **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** anunţă atacuri ale hackerilor ruşi asupra site-ului N.A.T.O. – **www.nato.int** şi, 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 trimit spre server fişiere goale, care-l pot scoate din uz întrucât primeşte prea multe interogări, iar el nu le poate răspunde la toate. Sârbii au mai atacat şi **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" şi anume: hacking, spam şi virusare. Citându-l pe Jamie Shea, purtătorul de cuvânt al N.A.T.O., el scria că pe adresa Alianţei Nord-Atlantice soseau zilnic, la un moment dat, şi câte 2 000 de e-mail-uri, în principal cu acelaşi mesaj: „F***k You!". Pe lângă aceste e-mail-uri, existau şi unele care aveau agăţat şi câte un virus. Chiar dacă forţele iugoslave au fost mai agile, scria acelaşi 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 şi el, la rândul său, cinci site-uri sârbeşti. Pe de altă parte, coaliţia unor hackeri europeni şi albanezi, care se autointitulase „Kosovo Hackers Group", a reuşit să insereze în mai multe site-uri bannere cu textul „Free Kosova". De atac nu a scăpat nici site-ul Universităţii din Novi Sad (**www.unindy.ns.ac.yu**), hackerul semnându-se TAC 99. Boris Ličina este de părere că, deşi în spatele acestui e-război a stat mai mult mass-media decât acţiunea adevărată, asta nu înseamnă că în viitor situaţia nu va deveni mult mai periculoasă, cu urmări mult mai grave.

În numărul de duminică, 28 martie 1999, publicaţia 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 şi computerul central al marinei de război americane, dar şi majoritatea site-urilor oficiale ale guvernelor statelor occidentale agresoare s-au trezit dimineaţa deosebit de afectate. Hackerii iugoslavi sunt iar stăpâni pe situaţie. […] Ţara noastră este atacată. Şi 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. Şi poate mult! (declara un hacker, n.n.). […] În umbra acestei nemaivăzute agresiuni, se duce din plin şi celălalt – războiul virtual. Deocamdată câştigăm această bătălie."

Luni, 29 martie 1999, **www.earinfo.org.yu** anunţă că EuNet a pornit acţiunea denumită ALERT (**http://alert.eunet.yu**), iar Infosky va oferi servicii gratuite până la terminarea agresiunii, aceasta pentru o mai bună informare şi pentru răspândirea adevărului. În aceeaşi zi, tot **www.earinfo.org.yu** anunţă că a fost atacat site-ul **www.lang-bau.de** şi 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 şi 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", şi anume că specialiştii iugoslavi au avut acces în perioada atacurilor N.A.T.O. la mari secrete militare aflate în sistemele

informaţionale. Răspunzând criticilor, oficialii serviciului secret britanic cunoscut sub numele de MI5 susţin că agenţii 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. şi N.A.T.O. sunt puse nu pe seama hackerilor obişnuiţi, ci pe seama unor ofiţeri 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”.). Independenţa este pusă sub semnul îndoielii şi în cazul hackerilor ruşi, care au atacat site-ul Orange Coast College şi au inserat următoarele mesaje: „Asses out of Serbia”, “Russian hackers demand to stop terrorist aggression against Yugoslavia.” Iar de insultele lor, scrie aceeaşi autoare, nu scapă nici Bill Clinton şi Monica Lewinsky. Şi 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 şi prosârbi asupra S.U.A. şi N.A.T.O. Au existat trei opţiuni de vot pentru acţiune: 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 găsindu-se un sondaj de opinie privind oportunitatea atacurilor aviaţiei israeliene asupra oraşului 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 căutaţi adevărul, vizitaţi **WWW.B92.NET**. Mulţumiri Rusiei, grupărilor de hackeri HDT, KpZ, CHC, Legion2000, care au atacat Nimitz, şi totodată mulţumiri celor de la Crna Ruka care, de asemenea, luptă pentru adevăr în acest război media!!! SAMURAI RULLEZ ! Contactaţi **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, presupuşii hackeri fiind, evident, cei sârbi, întrucât în paginile atacate apăreau sigla cu vulturul sârb şi 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 conţinutului 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 aceeaşi manieră au fost atacate serverele multor provideri, partide politice şi firme, susţinea M.A.I.-ul iugoslav. BBC mai dădea şi 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 puţin afectată întrucât era slab dezvoltată. În plus, o agresiune militară stârneşte mai multă revoltă în rândul cetăţenilor ţării agresate decât în rândul celor din ţara/ţările agresoare. CNN relata la un moment dat, în timpul atacului N.A.T.O asupra Iugoslaviei, că un hacker olandez a reuşit 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 nazişti. 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 priveşte activităţile hackerilor legate de ceea ce se întâmplă în clipa de faţă, cei mai activi sunt ruşii. În deja cunoscuta pagină web cu adresa **http://www.hackzone.ru/** zilnic se inserează adrese care au avut de suferit atacuri şi deseori sunt afişate şi snapshot-urile browser-

elor cu pagini heckerite. Trebuie observat faptul că, pe lângă hackerii ruşi, în această activitate iau parte şi mulţi cunoscători ai computerelor din ţările slave din jur. În ceea ce-i priveşte pe hackerii sârbi, din cauza importanţei Internetului pentru Iugoslavia în acele zile, activităţile ilegale de pe domeniile YU aproape că au încetat, în caz contrar Occidentul ameninţând cu sancţiuni. Însă adevăraţii cunoscători au avut la dispoziţie, în străinătate, mijloace cu ajutorul cărora au lucrat cu hărnicie. Cineva spunea că hackerii sârbi au spart un mare număr de servere în Europa Occidentală. Francezii bine pregătiţi din punct de vedere tehnic şi-au dat seama că sârbii nu sunt nişte sălbatici needucaţi, 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 şi transmis în data de 11 mai 1999 membrilor listei de discuţii „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 anunţat că sistemele de calcul guvernamentale suportă anual în jur de 21400 de încercări legale de penetrare şi de atacuri, în fiecare zi şapte-opt dintre aceste atacuri arătând semne ale unui nivel mai înalt de coordonare, ceea ce demonstrează că pericolul cyberterorismului din interior şi din exterior este în creştere.

Numărul de atacuri sus-pomenit pare uriaş faţă de cunoscuta listă a lui Bill Wall, cunoscută şi 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 şi până în septembrie 2001. Iată poziţiile 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 ruşi, susţinători 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 conţinând cuvintele „Serbia is here" („Serbia este aici"). O zi mai târziu, pe 21 aprilie, se pătrunde în serverele Aeroportului Naţional Washington. De 1 mai, hackerii danezi atacă un site iugoslav. În 5 mai ţintă 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 reuşit 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 mulţi provideri americani. Diferite alte mesaje cu un conţinut asemănător au inserat chinezii pe multe dintre site-urile care aveau legătură cu agresiunea N.A.T.O. asupra Iugoslaviei. Dar, majoritatea aveau acelaşi conţinut: „Nu vom înceta până nu încetaţi 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 publicaţia iugoslavă „Svet komputera", i-a surprins pe informaticienii americani care se ocupă de securitatea sistemelor informaţionale din S.U.A. în cea mai delicată situaţie, ei trebuind acum să lupte nu doar cu hackerii americani, ci şi cu cei din străinătate. Cumva în acelaşi timp, F.B.I.-ul a pornit o acţiune de amploare împotriva hackerilor americani. Aceştia au înţeles însă că F.B.I.-ul a dezgropat securea războiului şi au acţionat ca atare. Astfel că site-urile Senatului şi F.B.I.-ului au fost scoase din uz vreme de câteva zile. Site-ul Senatului a fost şters în întregime. F.B.I.-ul şi-a deconectat

singur serverul de la Internet, pentru siguranţă. A încercat, de asemenea, să convingă lumea că pe site-ul său nu există informaţii secrete, ci doar publice. Aceiaşi hackeri au schimbat sigla „Central Intelligence Agency" cu „Central Stupidity Agency".

Tot pe-atunci a pornit şi 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 şi prin lista adreselor de e-mail, peste 22 000, ei au trimis o mulţime de analize ale situaţiei, precum şi date despre distrugerile provocate de bombardamentele N.A.T.O şi despre chinurile populaţiei civile direct sau indirect afectate. Potrivit statisticilor, de pe site-ul lor au fost descărcaţi peste 100 GB de materiale şi 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 informaţia de la o agenţie de presă din S.U.A., se spune că hackerii din Hong Kong au reuşit să pătrundă în pagini web ale Guvernului american şi 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 «reţeaua tuturor reţelelor»" şi 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 şi au atacat site-ul ministerului sârb al informaţiilor.

Dar cum în orice război există întotdeauna destui profitori, nici Iugoslaviei nu i-au lipsit asemenea indivizi. Sancţiunile economice, ieşirea Iugoslaviei din Interpol şi agresiunea N.A.T.O. i-au încurajat pe destui hackeri sârbi să-şi facă de cap. Iată ce scrie Katarina Bugajski despre acest lucru (**http://iwpr.net/**): „În vreme ce ţara plângea sub povara sancţiunilor occidentale, în ţară soseau pachete cu Viagra, cu bomboane de ciocolată, cu aparate foto-digitale, cu ceasuri de mână, cu tricouri şi ţigări cubaneze, totul mulţumită furturilor prin Internet nepedepsite. Pe de-o parte, motivul lor a fost dorinţa de a se răzbuna pe Occident pentru faptul de a fi izolat Iugoslavia, iar pe de-altă parte – pură distracţie. Şi totuşi, profitul a fost pe primul loc. «De la o cutie de Viagra îmi plăteam chiria», spune zâmbind unul dintre hoţii sârbi pe Internet. Furtul de Viagra a fost un adevărat hit întrucât aceasta sosea în pachete micuţe 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 îşi dădeau seama de fărădelege şi refuzau să trimită în continuare cărţile, casetele video şi DVD şi 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 ţara de destinaţie se trecea «Ungaria» sau «Grecia». Când marfa ajungea în aceste ţări, slujbaşii poştali de acolo o redirecţionau spre adresa din Serbia. [..] În timpul bombardamentelor din anul 1999, hackerii au creat intenţionat haos în reţea. Ei îşi descriau acţiunile ca fiind «furturi patriotice» deoarece jefuiau în exclusivitate site-uri americane şi ale ţărilor 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 informaţii legate de Kosovo şi 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.freeserbia.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 şi Metohija – **www.gov.yu/** koso-vo_facts
Ministerul Informaţiei din Serbia – **www.srbija-info.yu** i www.serbia-info.com
Yahoo! News (ştiri ale unor agenţii de ştiri) – 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 (selecţie de ştiri 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 şi 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 întreţinerea armatei sale: **www.cdi.org/** sc/ javaclock.html.

Între pagubele virtuale şi cele reale

Ce se urmăreşte prin acest război virtual, vă veţi întreba? Întâi şi întâi trebuie să vedem care anume sunt ţintele. Fără doar şi poate, primele servere atacate sunt cele care deservesc legăturile operative între puterea politică, de decizie, şi statul major, apoi între statul major şi forţele armate, apoi între diverse comandamente. Pe acelaşi plan se situează serverele guvernului şi cele ale diverselor agenţii de securitate şi spionaj, organisme şi instituţii guvernamentale. Motivul îl constituie, desigur, îngreunarea pe cât posibil a traficului prin asemenea servere şi, 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 organizaţiilor sus-amintite, cărora li se adaugă de această dată şi ţinte din sectorul politic şi civil: parlament, partide politice, organizaţii civice, organizaţii neguvernamentale, instituţii 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 reacţiona imediat şi va da atacului o amploare mult mai mare decât este situaţia în realitate. Care sunt însă modalităţile (ţintele de atac, target-urile)?

Potrivit autorului site-ului din Republica Moldova având adresa **http://www.ournet.md/~xguard/xsecurity/dos.html**, ţinte ale unui atac al hackerilor pot fi, citãm: „Spaţiul de swap - Majoritatea sistemelor au alocate sute de megabaiţi pentru spaţiul de swap destinat cererii clienţilor. Astfel, spaţiul de swap e folosit mai mult pentru procesele fiu care au o durată mică de viaţă. Deci, swap-ul nu e destinat unei utilizari «din plin», un atac DoS s-ar putea baza pe «umplerea» s(paţiului); 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 cantităţi substanţiale 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 şi, de obicei, au memorie operativă mai puţină; 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 modalităţile de lucru ale unui hacker? Cum acţionează acesta? Asfel, un individ pus pe rele va scana host-urile, respectiv serverele care găzduiesc anumite site-uri, aceasta pentru a descoperi calculatoarele din reţea. Dacă va primi un răspuns, asta înseamnă că există sisteme care au adresele respective şi hackerul va încerca să le atace. O altă metodă este scanarea porturilor, asta pentru a identifica porturile deschise ale aplicaţiilor şi 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 configuraţiei sistemului, blocarea serviciilor, totul până la întreruperea sistemului.

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

Referindu-se la ţintele unui război informaţional în cazul României, generalul de brigadă Paul Vasile, şeful Direcţiei Planificare Strategică şi Controlul Armamentului din Statul Major General, afirma în 2000, în „Cotidianul": „Forţe ostile statului român pot provoca un război informaţional având ca ţintă afectarea gravă a infrastructurii vitale: transporturile feroviare; transporturile aeriene; sistemele de telecomunicaţii; metroul; sistemul financiar-bancar; sistemul fiscal; procesele tehnologice industriale; sistemele de aprovizionare cu energie şi gaze şi nu în ultimul rând a mediului ambiant etc. Afectarea gravă a infrastructurii poate fi generată de neglijenţă, involuntar, dar şi intenţionat, de forţe răuvoitoare sau potrivnice statului român. O imagine realistă a urmărilor provocate de un război informaţional, în care viaţa cotidiană ar putea fi bulversată complet, ar putea genera cele mai diverse manifestări, cum ar fi: lipsa căldurii, a gazelor, apei şi energiei electrice în locuinţe şi centre industriale; scăderea producţiei; şomajul peste limitele prevăzute; tensionarea situaţiei sociale, greve, încercări de lovituri de stat şi nesupunerea maselor în fata legilor; blocarea sistemelor financiar-bancare şi scăderea rapidă a puterii de cumpărare a monedei naţionale; izolarea României faţă de comunitatea internaţională, limitarea accesului la resursele strategice; influenţarea deciziilor politice şi ale organelor administraţiei de stat de către cercuri străine de interesele statului român. "

Cum se poate riposta la o asemenea situaţie: Răspunsul ni-l oferă acelaşi autor: „...trebuie identificate resursele necesare pentru achiziţionarea de tehnologie informaţională modernă care să permită: captarea, transmiterea, procesarea rapidă a informaţiilor, împiedicarea agresorului să facă acelaşi lucru, denaturarea şi dezinformarea. Trebuie să avem în vedere că în proiectarea şi perfecţionarea structurilor organizatorice trebuie să se ţină cont de misiunile specifice războiului informaţional pe care acestea le vor îndeplini în cadrul sistemului, cum sunt: criptarea, autentificarea şi certificarea datelor şi informaţiilor: controlul accesului în sistemele de informaţii; detectarea şi eliminarea software-ului afectat; securitatea reţelelor şi sistemelor C412; desfăşurarea de campanii imagologice; operaţii informaţionale ofensive; sustragerea sau vicierea datelor; introducerea de informaţii eronate sau false; interzicerea accesului neautorizat la datele proprii; distrugerea fizică a elementelor sistemelor de stocare şi distribuire a datelor."

Relevantă în acest sens este şi poziţia locotenentului Dan Scutaru, publicată în „Observator militar" (**www.presamil.ro**): „...agresiunile electronice şi psihologice din prima fază a oricărui conflict îşi pot atinge ţinta în defavoarea noastră. Mărturie stau războaiele din Golf şi fosta Iugoslavie." Pe de altă parte, susţine autorul, „Un viitor conflict este de neconceput fără război electronic". Că Armata română are în vedere un asemenea război stă mărturie şi existenţa Centrului 147 Război Electronic. Acelaşi autor afirmă în încheierea articolului pomenit: „Perspectivele

centrului sunt promiţătoare. Se vor achiziţiona mai multe echipamente compatibile cu tehnica N.A.T.O. Sunt aşteptate un sistem integrat de război electronic, câteva mijloace de bruiaj radiolocaţie şi un sistem de interceptare emisiuni satelit. Calitatea pregătirii militarilor şi aşteptata venire a promoţiei de ofiţeri de război electronic şi a tehnicii de ultimă generaţie sunt premisele unui viitor de siguranţă şi linişte."

Aceeaşi importanţă o acordă războiului electronic şi locotenent-colonelul Mircea Şuteu, comandantul Batalionului 110 Război Electronic „Feleacul", care a făcut parte din a doua (şi ultima) promoţie de război electronic pregătită în Academia de Înalte Studii Militare (conform **http://www.presamil.ro**): „Astăzi, suntem în faţa emergenţei unui al cincilea mediu de confruntare, de această dată imaterial, şi anume cel informaţional, în care suportul său principal îl constituie războiul electronic. [...] ...un specialist în război electronic se formează şi 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 şi al celei de război electronic şi să aibă cunoştinţe militare de nivel operativ, uneori strategic."

Până unde ţine războiul electronic şi de unde începe cel informatic? În 2002, preşedintele George Bush a semnat Directiva Prezidenţială pentru Securitate Naţională nr. 16, prin care a cerut Executivului de la Washington să pregătească un plan care să specifice liniile directoare ale unui război în cyberspaţiu. În substanţă, spune „Monitorul de Cluj" (**http://arhiva.monitorulcluj.ro/2003/**), „...este vorba despre a stabili în care circumstanţe Statele Unite ar putea sau ar trebui să lanseze o ofensivă informatică împotriva reţelelor din statele inamice."

„Washington Post" susţine 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 faţă eventualelor atacuri şi de a antrena viitorii soldaţi ai cyberspaţiului. Numai că folosirea programelor sau a viruşilor capabili să anihileze reţelele 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 şi la un spital civil (pagubă colaterală). Iar un virus „asmuţit" asupra reţelelor informatice ale unui prezumtiv adversar ar putea scăpa şi în reţeaua mondială Internet şi ar putea afecta grav şi reţele ale statelor prietene sau neutre.

Iată, aşadar, că se ştiu foarte bine ţintele, dar lipseşte bisturiul. Dacă atunci când e vorba despre reţele informaţionale există serioase reţineri, coaliţia antiteroristă ar putea totuşi depăşi, pe alte planuri ale luptei, o restricţie majoră, spune în articolul său „Terorismul în dreptul internaţional" (**http://www.presa-mil.ro**) colonelul prof. dr. Ion Dragoman de la Academia de Înalte Studii Militare, şi anume „...renunţarea la pretenţia de a avea «zero pierderi» de partea sa, într-un astfel de război, aşa 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 şi 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 cetăţenii propriei ţări şi propaganda pentru cetăţeni

străini; b) scrisori deschise mijloacelor mass-media şi instituţiilor; c) cearta prin intermediul forumurilor de discuţii; d) atacuri ale hackerilor. În numărul din mai 1999 al revistei iugoslave „Svet komputera" („Lumea computerelor"), Dušan Dingarac scria: „Toţi oamenii care nu se află în aceste vremuri grele în primele linii de luptă, dar sunt prezenţi pe Internet, contribuie la răspândirea adevărului. Metodele de luptă sunt următoarele: site-urile web, news conferinţele, mesajele e-mail, chat-ul, ICQ…, dar şi altele." Revenim acum la un mesaj găsit pe Internet, în arhiva forumului de discuţii cu tilul „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 şi retrimite recomandările pe care le-a primit de la revista digitală lunară gratuită (în format e-mail şi www) „Pretraga i prezentovanje", realizată de Dragan Varagić din Novi Sad. Revista a început în 1997 şi şi-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 trimiteţi mesaje prin CC (carbon copy, n.n.) ci prin BCC (blind carbon copy, n.n.). Indiferent de situaţie, nu trebuie scăpat din vedere că o asemenea trimitere poştală poate fi ulterior folosită ca SPAM. Votaţi pe toate locaţiile importante legate de situaţia noastră. Data trecută i-am învins, îi vom învinge şi acum. Găsiţi la adresele **http://dejanews.com/** şi **http://liszt.com/** un număr cât mai mare de news grupuri şi liste e-mail care se ocupă de politică generală şi cu tematica Iugoslaviei şi Kosovo-ului şi participaţi la discuţii. Aveţi în vedere regulamentele acestor grupuri de discuţii şi trimiteţi mesaje cu fapte care există îndeajuns în favoarea noastră. Fiecare discuţie argumentată pe news grupurile serioase şi pe listele de e-mail înseamnă foarte mult. De cum găsiţi asemenea grupuri de discuţii, schimbaţi-le cu toţi cei care cunosc bine limba engleză. Trimiteţi reacţii la materiale la toate marile ziare şi reviste de pe Internet care se ocupă de ţara noastră. Sunt în vigoare aceleaşi reguli ca în cazul news grupurilor şi a listelor de e-mail. Listele mijloacelor mass-media mai importante le puteţi găsi la adresele **http://www.mediacentar.opennet.org/** şi **http://www.totalnews.com/**.
La **http://pretraga.co.yu/yuguide/** puteţi găsi un director al motoarelor noastre de căutare, dacă doriţi să găsiţi adresele noastre cu cele mai actuale informaţii, din mai multe locuri. Utilizaţi mIRC şi alte locuri pe Web unde se poate polemiza pe această temă. Recomandarea este să fie găsite discuţii serioase, care cu siguranţă există. Pe prezentările oficiale ale statelor găsiţi adresele de e-mail ale politicienilor importanţi şi scrieţi-le. Acest lucru nu vă va face poate plăcere, însă poate le va atrage atenţia un (oarecare, n.n.) număr de scrisori. Într-un cuvânt, tot ceea ce găsiţi şi poate eventual să folosească în oprirea bombardamentelor, folosiţi! Autor: Dragan Varagić." Acelaşi e-mail conţine câteva adrese ale liderilor americani (preşedinte, vicepreşedinte, secretar de stat, prima doamnă etc.) şi recomandarea ca mesajele să fie scurte şi clare: „No NATO in Kosovo!". După care sunt date câteva recomandări pentru sârbii şi aliaţii care sunt cetăţeni americani, adresele de e-mail ale tuturor senatorilor americani şi textul care li se poate trimite. Mesajul atrage atenţia asupra faptului că: planul administraţiei Clinton constă în promovarea unor grupuri ale căror interese sunt terorismul, traficul cu stupefiante şi destabilizarea unei întregi regiuni; atacul asupra Iugoslaviei este un atac asupra unui stat suveran, finanţat de contribuabilii americani etc.

Pe 7 aprilie 1999, Jovan Kurbalija le scria abonaţilor „Forumului despre agresiunea N.A.T.O. asupra R.F.I." următoarele: „Vă invit să luaţi parte la acţiunea istorică, să participaţi la cel mai puternic de până acum atac asupra centrelor occidentale ale minciunii. În cadrul războiului convenţional împotriva poporului sârb şi a cetăţenilor Iugoslaviei, aşa după cum ştiţi, se poartă şi un război mediatic de satanizare a sârbilor şi împotriva tuturor acelora care apără suveranitatea Iugoslaviei. Ţinta atacurilor N.A.T.O. este ca întotdeauna să ne prezinte drept persoane fără chip

şi fără suflet. Uşor le este lor atunci să ne ucidă aşa, fără chip. Nouă ne revine sarcina să arătăm că avem o faţă, că avem un obraz şi că avem un suflet. Nouă ne revine sarcina să arătăm (lumii, n.n.) minciunile şi propaganda lor. Treaba este foarte simplă, noi am pregătit totul pentru a se începe munca. Principalul meu consilier pentru probleme tehnice şi principalul organizator al acestui proiect este americanul Paul Kneisel. Paul este editorul publicaţiei «Internet antifascist». Este foarte priceput în luptele mediatice electronice şi a repurtat victorii importante împotriva organizaţiilor fasciste de pe Internet. Îşi cunoaşte jobb-ul.

Metoda este verificată, cu succes:

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

1) Lista principalelor publicaţii occidentale;

2) Lista grupurilor Usenet alese cu grijă;

3) Lista publicaţiilor occidentale de mai mică importanţă;

Despre ce trebuie scris: despre lucruri cotidiene, obişnuite, în legătură cu actuala situaţie. Despre cum suportaţi voi, oamenii obişnuiţi, aceste evenimente. Vorbiţi despre nenorociri, dar daţi dovadă şi de mândrie şi de faptul că veţi trece peste toate acestea. Vorbiţi despre obiectivele civile distruse. Descrieţi clipele grele prin care au trecut vecinii sau prietenii dumneavoastră civili. Evident că nu trebuie să le scriem despre obiectivele militare distruse şi nici despre cel mai mic semn de scădere a moralului poporului. Vă rog ca în scrisorile dumneavoastră să nu atacaţi poporul american obişnuit. Tocmai pe americanul de rând dorim să-l atragem de partea noastră. Nu sunt ei de vină, ci Clinton şi banda lui. Jumătate din locuitorii Americii sunt deja împotriva bombardării Iugoslaviei. Noi trebuie să păstrăm această jumătate şi să-i atragem şi pe alţii. Nu luaţi în seamă o adunătură de idioţi (care se pot găsi oriunde) şi care-şi vor exprima satisfacţia că poporul Iugoslaviei este bombardat. Nu vă impacientaţi că engleza vă este (probabil) relativ inaccesibilă. Autenticitatea va transpare din fiecare cuvânt al nostru. Vă rog să trimiteţi o copie a scrisorii dumneavoastră la adresa: **Protiv-NATA@Yahoo.com**. Noi vă vom informa despre cum evoluează proiectul. Invitaţi şi prietenii (din Iugoslavia) să se implice. Cu cât suntem mai mulţi – cu atât mai bine.

Iată acum câteva adrese la care aţi putea să începeţi a trimite imediat corespondenţa dumneavoastră.

Vă rog să trimiteţi mesaje la toate adresele pe care vi le dăm. Valoarea publicaţiilor de mai mică importanţă este că, cu siguranţă, vor lua în seamă acest atac al nostru şi, prin articolele lor vor influenţa şi marile publicaţii."

Urmează adresele de e-mail ale publicaţiilor de mare şi mai mică importanţă din Occident şi 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 ţării prin Internet", următoarele: „De la începutul agresiunii N.A.T.O. asupra Iugoslaviei, prin Internet se poartă un adevărat război. Un mare număr de patrioţi îi «bombardează» cu e-mail-uri pe preşedintele american, pe vicepreşedinte, pe senatori… Cei care se pricep atacă site-urile agresoare, le şterg şi lasă mesaje cu adevărul despre Kosovo. În aceasta ne ajută foarte mult şi fraţii ruşi. Dacă doriţi să ajutaţi şi dumneavoastră în apărarea electronică a Iugoslaviei, votaţi pe site-urile unde s-a început votul asupra situaţiei din Kosovo (de exemplu, dacă trebuie sau nu început un atac terestru aspra R.F.I.) ori bombardaţi-le cu e-mail-uri (programe care vă vor ajuta în aceasta puteţi găsi pe yu.forum.erotika). Vă atragem atenţia să nu purtaţi pe Internet un război media greşit (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 şi vă rugăm să-l respectaţi."

Pe de altă parte, administratorii site-ului iugoslav **http://www.oaza.co.yu/** solicită implicarea tuturor celor interesaţi în realizarea unei cât mai bune pagini web. „Pe această pagină – spuneau ei – nu veţi găsi minciuni CNN, ci veţi găsi doar adevărul despre bombele N.A.T.O. şi despre rezistenţa sârbă împotriva agresorului. Aşteptăm şi ajutorul dumneavoastră – trimiteţi-ne informaţii verificate. Concetăţenii noştri şi prietenii din întreaga lume sunt bineveniţi cu fiecare informaţie despre acţiunile oamenilor noştri din diaspora. Vom deschide o pagină cu scrisorile dumneavoastră, iar părerile le puteţi expedia şi la forum. De asemenea, avem nevoie şi de ajutor în traduceri pentru a ţine în acelaşi timp şi o pagină în limba engleză, cu ştiri de ultimă oră. Dacă aveţi posibiliatea de a insera pagina noastră web pe servere mai rapide şi mai sigure din străinătate, anunţaţi-ne."

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

„Vă rugăm să citiţi şi, în cele din urmă, să luaţi în serios conţinutul acestui mesaj: de reacţia dumneavoastră ar putea să depindă multe lucruri.

Ceea ce ştiţi şi singuri este faptul că poporul sârb se găseşte în război cu cea mai puternică şi mai bine pregătită din lume naţiune din punct de vedere tehnic.

Aportul dumneavoastră la situaţia actuală din ţară poate să fie constructiv. Pe de altă parte, modul greşit de acţiune poate fi deosebit de periculos. Nimeni din Iugoslavia nu are dreptul să ofere vreun motiv pentru a ne fi întrerupt accesul la Internet, reţeaua globală care ne poate ajuta să facem auzită şi cealaltă parte a conflictului.

Pe lângă războiul cu bombe şi rachete de croazieră, împotriva noastră se poartă şi 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 şi pe Internet. Vă atenţionăm asupra mai multor lucruri.

SPAM pe Internet

Emoţiile sunt mai puternice decât o gândire raţională, lucru de care nu ne putem mira. Nu se pune în discuţie nici apărarea ţării. Dar, în intenţia de a dovedi mărinimia noastră, suntem câteodată în situaţia de a pierde măsura. O parte din utilizatorii locali de Internet încearcă să-şi exprime dezgustul faţă de agresiunea N.A.T.O. asupra ţării noastre, astfel că trimit un mare număr de mesaje de revoltă la multe forumuri de discuţii (newsgroups), inclusiv la cele care sunt specializate pe anumite probleme. Chiar dacă în esenţă suntem de acord cu mesajele şi conţinutul lor, trebuie să vă atragem atenţia asupra unei situaţii 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 conţinuturi nedorite care încalcă regulile bon tonului pe Internet (aşa-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 şi atunci când mesajele sunt expediate la forumurile de discuţii şi la «anumite» adrese de poştă electronică, asta poate deranja mass-media celeilalte părţi. De exemplu: CNN a început

«să piardă» în multe votări (on-line, n.n.) pe care le organizează cu prilejul aşa-zisei «campanii îndreptăţite în Iugoslavia», mulţumită în principal voturilor trimise din ţara noastră. Aceasta, dar şi multe alte case de editură, cărora li se întâmplă lucruri similare (de pildă CBS, Sky, BBC şi altora asemenea), au o audienţă 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 discuţii pentru a ne exprima gândurile, (ceea ce trebuie să facem oricum), atunci să respectăm nişte reguli:

Atenţie! – Aveţi grijă la munca pe Internet.

Este posibil ca, de un e-mail, cineva să vă trimită agăţat un virus în vederea punerii în execuţie a unui program. Virusul nu poate să se activeze dacă vă veţi limita la citirea mesajului. Pentru a rula programul care v-a fost trimis, trebuie activat de dumneavoastră înşivă printr-un click asupra fişierului agăţat, fie imediat, fie mai târziu. Prin aceasta oferiţi posibilitatea accesului la fişierele 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-aţi primit de la necunoscuţi să le ştergeţi de îndată.

NU – nu încercaţi să expediaţi viruşi ori programe asemănătoare oamenilor care se află de cealaltă parte a baricadei, îndeosebi la adresele guvernului american ori ale instituţiilor militare. Există apărare împotriva unor asemenea lucruri şi nu va fi nici un folos de pe urma încercării dumneavoastră. Aidoma altor acţiuni, şi aceasta va contribui la o posibilă deconectare a ţării noastre de la Internet.

DA- să folosim în exclusivitate grupurile de discuţii pentru expedierea unor asemenea mesaje. Un grup care se ocupă de competiţii 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 şi a distrugerilor din ţara noastră trebuie să le exprimăm utilizând un vocabular decent şi nicidecum vulgar, expresii gâlcevitoare ori umilitoare; să dăm dovadă de verticalitate şi cultură în utilizarea Internetului ca mijloc mass-media.

NU – să nu expediem un număr mai mare de mesaje cu acelaşi conţinut la aceeaşi adresă, SPAM-uri, oricum nu persoanelor ori organizaţiilor care se află în afara cercurilor politice. Aceasta se numeşte şi 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 totuşi şi dintr-aceia cărora puţin 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 – încercaţi să găsiţi corespondenţi care sunt dispuşi să asculte ori sunt însărcinaţi să-i asculte pe alţii (mass-media etc.), uitaţi-vă la listele anexate.

DA – Pentru corespondenţă utilizaţi limba engleză. Cea mai mare parte a corespondenţilor vor primi astfel mai uşor şi mai rapid informaţia dumneavoastră. Dacă aveţi probleme în a scrie în engleză, rugaţi pe cineva mai pregătit în această problemă.

DA – străduiţi-vă să scrieţi mesaje scurte şi pline de esenţă, care să aibă un mesaj anume. Evitaţi ca în mesajele dumneavoastră să săriţi de la o temă la alta.

NU- nu permiteţi ca durerea şi mânia dumneavoastră să fie exprimate prin cuvinte indecente.

NU – nu arătaţi că evenimentele afectează totul în Iugoslavia şi concentraţi-vă asupra suferinţelor omeneşti.

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

ATENŢIE! – Toate e-mail-urile care ajung la cunoscuţii dumneavoastră sunt cu siguranţă notate undeva ori sunt mai târziu supuse analizei. Aveţi grijă să nu-i compromiteţi pe oamenii noştri care trăiesc ori lucrează temporar în străinătate. Nu socotiţi niciodată că asemenea mesaje sunt sigure, iar conţinutul lor să nu fie legat de situaţia actuală: poate asemenea mesaje vor determina cheltuirea de resurse umane şi materiale ale agresorului. Conţinuturile ideale ale unor asemenea mesaje sunt: poezia, reţetele culinare, istoria ş.a.m.d.

DA – căutaţi locaţii pe care există posibilitatea de a se vota pentru sau împotriva folosirii forţei în Iugoslavia; încercaţi să găsiţi informaţii care ne folosesc, îndeosebi pe locaţiile principalelor case de editură din Occident. Vizitaţi toate site-urile guvernamentale şi militare ale statelor N.A.T.O. Trebuie şi nu trebuie să le vedeţi în detaliu, ţelul este înregistrarea fiecărui «hit» de pe un asemenea site şi determinarea administratorului să cheltuie timp pentru analizarea logo-urilor.

NU – nu vizitaţi prezentaţiile iredentiştilor albanezi şi mass-media UCK şi celelalte (vezi anexa). Administratorii acestor site-uri trebuie să ştie că sunt vizitaţi de puţine persoane!

Dacă realizaţi prezentări (web, n.n.)

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

- Puneţi link-uri spre site-urile pe care consideraţi că trebuie să le vadă oamenii sau cel mai bine puneţi un link către **http://alert.eunet.yu**, iar utilizatorului **alert@Eunet.yu** trimiteţi-i link-urile recomandate.

- Vedeţi recomandările detaliate pentru realizarea de prezentări în condiţiile de dinainte de campania antirăzboi.

Ne urmăresc, ne observă şi ne ascultă!

Nu puneţi sub semnul îndoielii informaţiile despre „coloana a cincea”. Nu e vorba despre paranoia şi despre vânătoarea de vrăjitoare, aşa cum probabil v-aţi gândit în prima clipă, ci de fapte. Mărturie sunt mutarea masivă a locatoarelor în Kosovo şi în alte părţi ale ţării şi bruierea sistemelor noastre de legătură cu ajutorul staţiilor de brujaj găsite în interiorul R.F.I.

Agentura străină se află şi acţionează aici.

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

De aceea, aveţi grijă de ştirile pe care trimiteţi le prin intermediul poştei electronice şi a convorbirilor telefonice cu familia şi prietenii, acasă ori în străinătate.

Nu daţi detalii despre obiectivele lovite, despre gradul de distrugere, despre momentul lovirii şi alte informaţii asemănătoare. Asemenea date sunt nepreţuite pentru informatorii N.A.T.O., îndeosebi când le primesc regulat şi gratuit.

În toate aceste comunicaţii încercaţi să fiţi cât mai indecişi. Părinţilor, prietenilor şi cunoscuţilor dumneavoastră le va fi îndeajuns să afle că sunteţi bine.

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

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

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

Totuşi, cel mai bine este să vă abţineţi de la asemenea metode de informare.

Evitaţi publicarea oricăror informaţii care ar putea fi de folos inamicului!

Dacă primiţi un e-mail jignitor:

În primul rând nu vă enervaţi. E-adevărat, nu e ceva prea uşor în timpurile când emoţiile 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 naţionalităţi, cu adrese fictive (Yahoo, Hotmail etc.). Asemenea mesaje se trimit în mod automat, cu mesaje identice, la mii de adrese, cu intenţia de a sufoca legăturile noastre prin Internet.

Dacă le răspundeţi, înseamnă că şi-au atins scopul.

Aşadar, nu răspundeţi la asemenea mesaje. Trebuie doar să le ignoraţi, mai exact să le ştergeţi imediat.

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

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

Încheiere

Cu siguranţă că nu este necesar să vă explicăm cât de mare este puterea Internetului. Fiţi conştienţi că agresorul a angajat resurse însemnate în intenţia de a influenţa utilizatorii de Internet din Iugoslavia, având în vedere faptul că ne consideră un grup ţintă de elită. Nu puneţi la îndoială faptul că, în viitorul apropiat, se va ajunge la o escaladare a evenimentelor «şi» 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 preţ 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 informaţii ale pactului N.A.T.O. să se folosească în interesul lor de informaţiile pe care le plasăm pe Internet.

Să nu le permitem să ne dea afară din reţea.

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

Nu vă zgârciţi să trimiteţi 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 aparţine, 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/CNEWSKoso-vo/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 publicaţii mass-media din ţările ce făceau parte din N.A.T.O.

Site-uri care ţin evidenţa principalelor atacuri ale hackerilor pe Internet şi 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 şi vestea că agenţiile americane de spionaj controlează întregul trafic pe Internet pentru a descoperi informaţii despre ţintele atinse. Pe lângă această ştire a urmat şi un apel pentru evitarea descrierii ţintelor lovite, pentru ca duşmanul să rămână dezorientat".

În timp ce lucram la cartea de faţă, l-am întâlnit întâmplător, la o conferinţă de presă ţinută la Timişoara, 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 alţi corespondenţi de război aflaţi pe vremea aceea la Belgrad, de la relaţiile 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 şti uşor dacă rachetele sau bombele lor şi-au atins ţinta ori nu şi care au fost pagubele. E lesne de înţeles că în tot timpul agresiunii N.A.T.O. o mare parte din personalul şi tehnica utilizate de sistemul de spionaj global sus-pomenit au fost cu ochii şi urechile la Iugoslavia. De aici şi atacurile repetate asupra unor ţinte, despre care s-a aflat imediat, de ce nu şi din citirea e-mail-urilor, ţinte care nu au fost distruse la primul ori la următoarele bombardamente.

La 10 decembrie 1998, Irina şi Slobodan Stojičević lansează pe forumul de discuţii „Serbian Forum", găzduit de groups.yahoo.com/group, ideea că, citäm: „…Acesta este primul război din istorie în care se utilizează şi Internetul". Tot ei fac apel la o coordonare a luptei prin acest modern sistem de comunicare şi, totodată, de propagandă. Iată şi textul acestui mesaj: „Câte mai poate omul să asculte şi să vadă! Păi acesta nu e războiul privat al fiecăruia dintre noi. Nu, fraţilor şi domnilor, nu este nici cuminte şi 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 alţii, cu atât mai mult, ne roagă să trimitem doar ceea ce este cel mai urgent întrucât şi aşa sunt serverele supraaglomerate…

Propun…

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

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 toţii în pierdere, însă o pierdere cu mult mai mare va suferi Serbia.

În afară de asta, nu ştiu dacă i-a mai picat cuiva în minte:

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

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

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

Trebuie oare să stăm şi să aşteptăm să ne fie ţintiţi providerii asemenea televiziunilor?

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

Există vreo instituţie care să coordoneze munca pe Internet în condiţiile «stării de război»?

Mie mi se pare logică şi organizarea de secţiuni în cadrul Comandamentului Suprem…

Mijlocul de comunicare căruia îi aparţine viitorul, dar şi o parte din actualitate (iar cu ele vieţile noastre şi ale copiilor noştri) 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 siguranţă că aţi observat o anumită inadvertenţă: deşi mesajul a fost trimis pe 10 decembrie 1998, autorul deja spune: „Trebuie oare să stăm şi să aşteptăm să ne fie ţintiţi providerii asemenea televiziunilor?” Ori atacul asupra radioreleelor şi a sediilor televiziunilor publice s-a întâmplat abia în 1999, când experţii N.A.T.O. au considerat că radioul şi televiziunea s-au transformat în arme propagandistice periculoase pentru succesul acţiunii aliaţilor. 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 şi care aveau un anumit termen pentru testare (şi 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. Aşadar, 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 ţintirea releelor de televiziune şi atacul asupra providerilor din Iugoslavia. Cert este şi faptul că autorul a exagerat ori nu a putut cuprinde realitatea: una este să distrugi reţeaua de telecomunicaţii clasice a inamicului, alta e să-i întrerupi accesul la reţeaua de sateliţi pentru servicii Internet (aflaţi majoritatea în proprietatea ţărilor membre ale N.A.T.O.). Fiindcă una e să bombardezi releele de radioteleviziune, aflate, de regulă, izolate de zonele rezidenţiale, şi alta e să ataci sediile providerilor, aflate în copleşitoarea majoritate a cazurilor în cele mai aglomerate zone citadine. Or N.A.T.O. adoptase deja ideea loviturilor chirurgicale, ineficiente totuşi în asemenea zone, dovadă fiind şi miile de „pagube colaterale”.

Afirmaţia noastră precum că este vorba de un „pirat” de software sunt şi mesajele la care autorul de mai sus a replicat şi 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 toţi membrii lui exSingidunum să ni se alăture în campania loviturilor mobile. SerbSaver este un program […] care permite alegerea telefoniei mobile […], se stabileşte contingentul de numere care vor fi contactate (numere de 6 cifre, fără introducerea prefixului) şi atunci se apasă pe buton: «Haideţi cu toţii la atac», apoi «Văzduhul vibrează de parcă arde cerul. Se pregăteşte furtuna.» O.K. Nu vă impacientaţi. El (telefonul mobil, n.n.) transmite următorul mesaj: «Have you killed your Serb today». După comentariile actuale, are efect asupra generaţiei de silicon CNN (amerii[cani]), dar şi asupra celorlalţi. Încercaţi şi alegeţi o ţară fascistă în care este zi, astfel încât să aibă la ce să mediteze până la sfârşitul zilei (garantează vise rele). Opinia publică este deosebit de importantă în ţările fasciste, iar dacă aceasta îşi intensifică presiunea asupra guvernului său, cu atât mai bine pentru noi. Dacă le reuşeşte această campanie, atunci se ştie cine este următorul şi următorul…Această misiune nu e doar pentru a contribui la apărarea sârbilor, ci a tuturor popoarelor […]. Distribuiţi-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 şi telefonia, nu vom putea acţiona cu toate forţele, astfel că toţi cei din afara domeniului nostru ne vor fi o prelungire a mâinii. Nu vor putea ei (duşmanii, n.n.) să întrerupă şi toate celelalte domenii în care există măcar şi un singur sârb sau prieten."

Dar iată şi… 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 acelaşi timp, aproximativ 1 100 de contacte. Închipuiţi-vă că acţionăm 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 şi un P.S.: „Am contactat câţiva webmasteri, astfel că în curând îl vom putea aştepta pe vreuna din paginile web."

În aceeaşi zi, Vasja Bojanić scria: „1. Vă recomand tuturor acelora care existaţi să citiţi cartea lui Noam Chomsky «Ce doreşte de fapt America». Puteţi afla cu cine avem de-a face şi ce mai vor să facă, astfel că nu trebuie să vă surprindă. 2. În loc de a striga lozinci pe la manifestaţiile de protest, vă propun un cântec. Un cântec frumos şi solidar. Unul pentru celălalt. Poate aşa am putea să atragem mai multă atenţie.

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

Nu putem aproba venirea forţelor N.A.T.O. în ţara 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 publicaţia „Ottawa Citizen". Nu mai puţin de 80% dintre cei care şi-au oferit ajutorul au şi făcut-o, astfel că s-a ajuns chiar la un excedent financiar (deşi au fost necesari 14 851 de dolari, s-au strâns aproape 22 000 de dolari, la acţiune participând inclusiv grecii canadieni). De unde s-a ajuns la ideea continuării campaniei publicitare în publicaţii de importanţă naţională în Canada („Globe & Mail" sau „National Post"). Bran Selić scria la 22 aprilie 1999: „Tuturor celor care urmăresc CNN, CBC şi altele asemenea le este limpede că în lumea contemporană comercializantă acţiunea 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 şi îndeosebi asupra minorităţii evreieşti 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.ninemsn.com.au/; **www.cbsnews.com/**. E greu de crezut că oficialităţile S.U.A. sau N.A.T.O. au luat în considerare

rezultatele acestor voturi, dar cu siguranţă le-au monitorizat evoluţia pas cu pas, pentru cu totul alte scopuri, unul fiind cu siguranţă realizarea de baze de date cu adresele de e-mail şi ţările de unde veneau voturile împotriva agresiunii N.A.T.O.

„Războiul cibernetic a sosit cu toate implicaţiile sale şi i-a surprins complet nepregătiţi, chiar şi pe americani. Îndeosebi când e vorba despre implicaţii etice", scria corespondentul din Washington al publicaţiei iugoslave „NIN" (**www.nin.co.yu**) în numărul din 4 septembrie 1999, preluând afirmaţia 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 importanţă, cu bombardamentul aerian în primul război mondial şi cu atacul cu bomba nucleară asupra Hiroshimei, în 1945." Adică „războiul cibernetic", despre care se apreciază că a jucat un rol cheie în predarea neaşteptată a lui Milošević pe 7 iunie şi acceptarea, practic, a retragerii necondiţionate din Kosovo. Acelaşi profesor californian, consilier al Pentagonului şi unul din experţii de frunte americani în probleme de luptă informatică, a declarat că ruşii i-au atenţionat pe americani că vor reacţiona „prin toate mijloacele" (ceea ce, în limbaj diplomatic, include şi armamentul nuclear) dacă vor fi atacaţi 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 ştie în istoria războiului", scria acelaşi corespondent al publicaţiei iugoslave. Citǎm din acelaşi 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 intervenţiei împotriva Iugoslaviei direcţia principală de atac a fost îndreptată spre perturbarea reţelei de computere pentru comandă şi control a Statului Major al Armatei Iugoslave. Cu deosebire în această operaţie a fost ţintit sistemul integrat de computere al apărării antiaeriene a Armatei Iugoslaviei, în ideea ca prima acţiune militară în jumătatea de secol de existenţă a N.A.T.O. să se termine aşa cum a început: fără nici o jertfă din partea piloţilor din cadrul armadei care a acţionat zi şi noapte asupra Serbiei, Kosovo-ului şi (uneori) a Muntenegrului. Pe lângă apărarea antiaeriană, în vizorul intervenţiei cibernetice americane s-au găsit în această perioadă şi sistemul telefonic şi celelalte comunicaţii 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 comunicaţii cu comandanţii de pe teren prin legătura radio şi prin telefoanele mobile - care se urmăresc şi se ascultă mai uşor." Oficialii de la Pentagon susţin că prin aceste acţiuni s-a obţinut un „succes important", însă operaţiunile cibernetice au fost utilizate cu întârziere şi cu reţinere. Altfel spus, S.U.A. au utilizat în acţiunea lor în Balcani doar zece la sută din capacităţile 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 sancţiunile economice şi un atac cu armament convenţional. 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 reacţia părţii adverse, care va recurge la acţiuni 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 ţină cont, scrie „NIN". Despre războiul cibernetic între S.U.A., pe de o parte, şi sârbi, pe de altă parte, a vorbit la un simpozion al specialiştilor informaticieni din cadrul armatei şi unul din şefii forţelor aeriene americane. „Am consemnat câteva încercări de distrugere a reţelelor noastre (informative). Din fericire, acţiunile sârbeşti de acest fel nu au fost cu nimic mai puţin eficiente decât acţiunile apărării lor antiaeriene." Acelaşi general a declarat că şi specialiştii

americani au atacat, la rândul lor, sistemele informatice sârbeşti, printre care şi cel al apărării antiaeriene, însă nu a precizat care a fost impactul acestor atacuri. În cele 78 de zile de atac asupra Iugoslaviei, forţele 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 viruşi şi cu un mare număr de mesaje electronice, însă oficiali ai Alianţei au precizat că pagube au fost doar pe site-uri şi în sistemele de distribuire a e-mail-urilor. Nu s-a consemnat nici un atac reuşit asupra computerelor militare.

Scopurile urmărite de către un hacker pot fi mai puţine ori mai multe, în funcţie 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 şi lista:

1) îngreunarea sau încetinirea activităţii normale a unui serviciu prin mărirea timpilor de răspuns la cereri sau prin perturbarea accesului la resurse, mergând până la blocarea completă a activităţii;

2) inserarea de secvenţe denaturate în datele trimise de un serviciu către utilizatori mergând până la deturnarea completă a serviciului către o resursă controlată de atacator;

3) obţinerea de acces nelegitim la servicii private sau cu acces limitat;

4) capturarea informaţiilor vehiculate de servicii cu caracter privat sau secret;

5) modificarea configuraţiei maşinilor care oferă anumite servicii;

6) instalarea de programe speciale, care execută pe serverele atacate diverse acţiuni în interesul atacatorului, cum ar fi colectarea de parole etc.;

7) înlocuirea unor programe ce fac parte din instalarea maşinii atacate, altele care par a executa aceleaşi acţiuni ca şi cele originale, dar de fapt lucrează pentru atacator;

8) ştergerea pur şi simplu a unor programe şi/sau informaţii de pe serverele atacate, mergând până la distrugerea completă din punct de vedere software a maşinilor atacate sau chiar până la distrugeri hardware (improbabil, dar nu imposibil).

Aşadar, orice calculator aflat în reţeaua Internet devine automat vulnerabil. Însă vulnerabilitatea poate fi mai mare sau mai mică, totul fiind în funcţie de sistemele de protecţie ale calculatorului. Pentru a ataca, un hacker va utiliza întâi „Host Scan" pentru identificarea calculatoarelor din reţea. Dacă primeşte un răspuns de la unul din computere, hackerul va trece fără doar şi poate la atac. Următoarea fază o constituie scanarea prin care se urmăreşte identificarea porturilor deschise ale aplicaţiilor pentru a fi utilizate pentru accesul în sistem. După ce pătrunde în sistem, atacatorul va bloca serviciile existente pe maşina respectivă prin schimbarea parametrilor sau a configuraţiei sistemului ori prin instalarea unui program propriu, care are drept scop generarea unui trafic uriaş în sistemul vizat. Această acţiune 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 reţea în pachete optime, iar la destinaţie sunt asamblate la loc. Ce fac hackerii? Ei trimit fragmente foarte mici care simulează un pachet foarte mare, imposibil de asamblat. În contextul aceleiaşi metode, spune Petre Rău în cartea sa „Infracţionalitatea pe calculator" (vezi **www.rap.freehosting.net/Infract/P3.html**), „...unii procedează la «stârnirea» tuturor calculatoarelor active dintr-o reţea, pentru a trimite, într-un trafic foarte mare, răspunsuri pe adresa unei victime alese în prealabil, până la obţinerea unei blocări complete." Blocarea unor servere ce oferă servicii importante, de exemplu Web, spune acelaşi 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

informaţiile de confirmare, paralizând astfel activitatea calculatorului, destinaţie care nu mai poate deschide nici o conexiune legitimă.

Sub titlul „Mesaje duşmănoase”, pe Internet a circulat şi un asemenea text: „Ştim cu toţii foarte bine că ne aflăm în război. Ştim foarte bine şi cine anume ne sunt duşmanii. În aceste zile grele aceştia ne scriu şi se bucură de chinurile noastre. De aceea am decis să le facem publice adresele de e-mail, iar voi faceţi ceea ce urmează: potopiţi-i cu e-mail-uri nefolositoare de mărimi apreciabile, de sute de kb. Mail box-ul le va fi în curând supraîncărcat; trimiteţi-le viruşi. Aveţi grijă ca virusul să fie împachetat într-un mesaj nevinovat; trimiteţi mai departe adresele lor de e-mail.” După text urmau e-mail-urile respective.

Hakingul, între patriotism şi terorism

În timpul agresiunii N.A.T.O. asupra Iugoslaviei, atacurile şi pătrunderile neautorizate efectuate de către sârbi într-o mulţime de pagini şi site-uri web au cunoscut o nouă dimensiune, opinia publică iugoslavă şi o bună parte a lumii acceptând ideea că există şi un alt fel de hacking şi anume hackingul patriotic. În permanenţă, însă, rămâne în prim-plan acelaşi semn de întrebare: unde se află graniţa între legal şi ilegal? În mod clar, totul depinde de partea de baricadă unde se află hackerul/crackerul, respectiv cel atacat. În acest context, americanii, cei mai vânaţi de iugoslavi, au catalogat atacurile drept crackuri, ilegalităţi etc. De partea cealaltă, iugoslavii au etichetat acţiunile respective drept hackuri perfect legale, mai cu seamă că acţiunea în forţă a N.A.T.O. nu a fost decât o grosolană agresiune, fără nici un temei legal. Aşadar, dacă facem apel la etică, trebuie să aplicăm acelaşi standard atât pentru acţiunile forţelor N.A.T.O., cât şi pentru atacurile digitale ale iugoslavilor şi aliaţilor lor: ori amândouă au fost legale, ori amândouă au fost ilegale. Dublul standard este încă, din nefericire, frecvent utilizat în relaţiile internaţionale, dreptate având cel puternic, câinele (democraţia nefiind pentru căţei). Scena politică internaţională pare mai curând un teatru de luptă între bandele mafiote din New York, de exemplu. Iar democraţia pare mai curând praf în ochii celor slabi.

Iată că, astfel, chiar şi crackerul cel mai înrăit poate deveni un erou popular dacă, în timpul unei confruntări militare, intră în luptă de partea poporului său şi atacă, printr-o metodă sau alta, pagini şi site-uri web ale duşmanului. Desigur, într-o lume normală, el ar fi un proscris vânat inclusiv de poliţia ţării sale. În plin război, însă, atacurile sale pot servi o cauză mai mult sau mai puţin dreaptă. Iar el, hackerul, respectiv crackerul, aşa cum spuneam şi 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 totuşi la studiul noţiunii de bază: hackingul, dar şi la practicienii săi, hackerii, respectiv crackerii.

În general, hackerii acuză mass-media de faptul că-i confundă cu crackerii, cei care, în accepţiunea hackerilor, sunt adevăraţii piraţi informatici. Ei, hackerii, susţin că respectă un fel de cod cavaleresc: niciodată să nu faci pagube, niciodată să nu furi şi niciodată să nu te laşi descoperit. „Doar o provocare a inteligenţei (vezi **www.munty.150m.com/Hack/intro-htm**, care preia materialul de la Cyberwarrior). Niciodată cu intenţie criminală. Cultura hacker este legată de numele marilor universităţi americane (Harvard, Berkley, Stanford) unde, de regulă, toţi studenţii sunt hackeri.” Ceea ce însă uită aceşti teoreticieni ai hackingului este una dintre legile

fundamentale ale democraţiei: respectul faţă de proprietate. Dacă un hacker pătrunde în sistemul meu informatic el este un hacker. Dacă acelaşi individ începe să-mi fure date sau să-mi şteargă fişierele, el este un cracker. Numai că în ambele cazuri este vorba în primul rând de o intrare neautorizată, deci de o violare a proprietăţii. Chiar dacă hackerul declară că doar a vrut să studieze, să înveţe. Prin urmare, fără intenţia de a polemiza cu hackerii, ne vom asuma punctul de vedere al mass-media şi vom pomeni de crackeri doar acolo şi când va fi neapărat cazul.

Pe lângă hackingul patriotic există şi 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 şi 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 instituţii 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 internaţional de pedepsire a pedepsitorului, aici celebru fiind cazul lui Michnik. După atacul asupra World Trade Center din 11 septembrie 2001, a apărut aşa-numitul terorism cibernetic şi care, susţine mass-media, ar consta din folosirea Internetului de către grupările teroriste de tip Al-Qaeda pentru comunicaţii, recrutare şi colectare de fonduri. „Chiar şi acum – scria cotidianul bucureştean «România Liberă» la 11 septembrie 2002 -, în condiţii de securitate sporită, Al-Qaeda se foloseşte de internet pentru a pune la cale noi atacuri. Experţii au ajuns la concluzia că teroriştii au studiat cu mare atenţie sistemul telefonic american, alimentarea cu apă, serviciile publice, dirijate computerizat.” Acelaşi cotidian citează un oficial de la Centrul de protecţie 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 intervenţie în caz de situaţii de urgenţă”. Pare totuşi de necrezut nu faptul că nu ar putea exista pe viitor asemenea atacuri, ci faptul că, deşi 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 oraş este nebunie curată atâta vreme cât se poate izola complet de exterior orice reţea de calculatoare. Nu este departe în urma noastră virusul mileniului, care aproape că a isterizat o planetă întreagă şi nu a fost decât un bluf. Ce anume se urmăreşte prin crearea unor asemenea stări de panică nu e uşor de ghicit. Însă, în mod cert, cineva câştigă din asemenea manipulări în masă.

În 1997, televiziunea rusă anunţa: „încercările repetate ale hackerilor de a pătrunde în sistemele informatice ale instituţiilor de stat”. Şeful agenţiei federale pentru comunicaţii afirma că folosirea cu rea intenţie a tehnologiei moderne de telecomunicaţii poate „influenţa psihologia unor întregi naţiuni”. Nu se cunoaşte ce efect a avut în Belarus atacul hackerilor asupra site-ului preşedintelui Belarusului, Lukaşenko, 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 preşedintelui, dar cu siguranţă a provocat cel puţin o mulţime 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 naţionale, internaţionale şi transnaţionale. Astfel, o grupare de hackeri care activa sub denumirea de „Mossad”, a atacat site-ul oficial al preşedintelui 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 umilinţa externă”. Mai mult decât atât, intrusul a legat pagina ministrului cu cea a Disneyland-ului, iar paginile altor miniştri, cu pagini porno de pe Internet. Ministrul pentru relaţii de muncă, Peter Reith, a devenit „ministrul distrugerii locului de muncă şi a dreptăţii, pentru Gestapo şi propagandă”.

Kashmirul, provincia indiană dorită atât de mult de islamiştii pakistanezi, a fost nu o dată mărul discordiei şi pe Internet. După ce armata indiană a lansat un site dedicat Kashmirului, hackerii pakistanezi l-au şi atacat. Agenţia indiană de presă PTI a anunţat 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 anunţat şi 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 aparţin 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 părţi.

Un an mai târziu, în 1999, Republica Populară Chineză a lansat un site dedicat drepturilor omului. Reacţia nu a întârziat să apară, hackerii care optează pentru libertăţi 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, aceştia 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 şi G-man. Ca întotdeauna, principalele ţinte sunt serverele militare şi guvernamentale (pentru că acolo se găseşte marfă). Ieri, 26.10.1999, am început un nou război numit: Războiul WWW... un război împotriva Statelor Unite şi 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 evoluţiei celor de la „Pentaguard", aproape că spune în ce oraş activează aceştia: „Nu se ştie cu exactitate când au apărut, cert este doar că cel care a pus bazele acestui grup de «haiduci ai Internetului» e Diablo. De asemenea, componenţa Pentaguard s-a schimbat permanent, însă, printre cei mai cunoscuţi se numără G-man, n0nam3, Light, H3X0r (alias Andripopa sau Linuxman), Beculetz (alias joaka cruce) si BM-Freak. […] De multe ori, paginile modificate conţineau menţiunea «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 formaţie de muzică din Timişoara, şi anume „Andripopa". La fel şi menţiunea: „Copyright WRHC (West Romanian Hackers Corporation)". Dar cel mai convingător argument nu este că Pentaguard s-a aliat cu hackerii ruşi, ci faptul că membrii săi au început un „război WWW" împotriva Statelor Unite ale Americii. Or se ştie că în Banat trăiesc cei mai mulţi etnici sârbi din România, iar timişorenii au înţeles poate cel mai bine nedreptatea ce li s-a făcut sârbilor prin agresiunea N.A.T.O. asupra Iugoslaviei. În colaborare cu hackerii ruşi 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 coşmar 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 şi 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 practicată de anumite state şi 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 Miloşevici a început să omoare albanezi în propria lui ţară (Kosovo este o parte a Serbiei) aţi 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 temeţi de Al Treilea Război Mondial! În cazul acesta va trebui să vă descurcaţi cu Războiul WWW. Pentaguard, cu o nouă echipă condusă de Diablo, porneşte 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 câştiga acest război!»"

Exemplul de mai sus le conferă celor de la „Pentaguard" o aureolă de eroi. Iar acţiunile lor par fireşti într-un context în care marile puteri aplică diferite standarde în relaţiile interstatale.

În octombrie 2002, motorul de căutare **www.google.com** dădea nu mai puţin de 900 de adrese conţinând numele de „Pentaguard". Poate cea mai completă istorie despre acest cel mai cunoscut grup de hackeri români se găseşte la adresa **www.halbasus.go.ro** şi este, probabil, realizată de unul dintre membrii grupului. Autorul descrie, succint, momentele naşterii grupării, în 1998, fără a numi oraşul. 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 şi au furat 10 000 de dolari. Citäm: „Era o încălcare grosolană a drepturilor omului. Întreg underground-ul a ripostat... Hackeri de peste tot atacau serverele chinezilor... PentaGuardul nu a făcut excepţie şi câteva site-uri ale guvernului chinez au fost sparte ca semn de protest faţă de legile lor stupide." Dacă e să ne luăm după informaţiile din **www.halbasus.go.ro**, episodul KpZ a fost mai mult un concurs între Diablo, cel care a pus bazele grupului românesc, şi hackerul rus care-şi spunea Windows 95, cei doi întâlnindu-se în timp ce Diablo spărgea o pagină anonimă. Citäm din nou: „…cei doi au ajuns la o oarecare prietenie şi Windows 95 a lansat o provocare. Site-uri .gov si .mil... un subiect tabu la acea oră... nimeni nu se atingea de ele (nu ştiu din ce motiv). Cine sparge mai multe pagini .gov si .mil... Şi cursa a început... La sfârşitul zilei, KpZ a spart 3 site-uri... Diablo 18... oricum site-urile aveau aproximativ acelaşi text (KpZ and PentaGuard forever :))... atunci a intrat PentaGuardul în atenţia presei... şi 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 excepţii) doar site-uri .gov şi .mil... pentru a demonstra că şi ele sunt site-uri la fel de vulnerabile... şi 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 şi .af.mil-uri nimic nu a fost lăsat neatins..."

În 2000, Diablo îl întâlneşte pe [LiGHT], din acelaşi oraş, apoi pe n0_nam3, „colegul, prietenul şi verişorul lui [LiGHT]". La rândul său. [LiGHT] „…întâlnise câţiva tipi din Timişoara… BM-Freak, beculetz şi H3X03…" Cei şase vor băga spaima în administratorii de pe Internet. Citäm din nou: „... la turma de .gov-uri si .mil-uri care a dat culoarea PG-ului acum s-au adăugat noi victime autohtone... ministerul finanţelor (de multe ori), romtelecom (numa' de vreo 2 ori), RASDAQ, eximbank, porsche.ro, europeandrinks, şi altele (cateva ISP-uri, etc...). PG era deja un nume binecunoscut pentru presa română şi cea străină, s-au scris articole, interviuri (mai mult sau mai puţin 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 şi hacker liber profesionist". În 2001, Diablo şi [LiGHT] pun la cale ceea ce mai târziu a fost declarat, citäm: „cel mai sistematic atac asupra unor servere guvernamentale din toata lumea". Scenariul a fost simplu, povesteşte autorul istoriei grupului: „[LiGHT] şi Diablo, închişi într-o cameră cu ţigări, beri şi două calculatoare legate la net printr-un dial-up. Operaţiunea a început la 10 seara şi s-a terminat pe la 6 dimineaţa... Rezultatul? O grămadă de servere sparte. Ziarele vuiau... PG (Pentaguard, n.n.) era din nou în atenţia presei... era deja timpul să reintre în underground." Acum, pentaguarzii s-au liniştit, unii fiind la facultate, iar alţii ocupându-se de lucruri mai cuminţi. Scurta şi interesanta istorie a grupului se încheie cu un şir cuprinzând adresele unora dintre site-urile atacate, precum şi adresele la care se pot vedea şi rezultatele de la vremea respectivă ale atacurilor (mirror) din 2000 şi 2001. Printre adresele atacate şi menţionate pe site-ul **www.attrition.org** (54 de poziţii) se află şi 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.tnknox.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 părţi a site-urilor sparte de către membrii Pentaguard se găseşte 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 Finanţelor din România, spart de acelaşi grup, se poate citi la adresa **http://floweros.tripod.com**. Taxa pe prostie, instituită de „Noua coaliţie guvernamentală formată din: Pentaguard, Getto Daci şi Institutul Român de Cercetări Alcoolice", care a preluat controlul Ministerului Finanţelor, a făcut furori în România: „Pentru a spori veniturile bugetare, Ministerul Finanţelor introduce taxa pe prostie... Această taxă poate aduce venituri nelimitate pt că ştim de la chimie că în lume există 2 elemente omniprezente: hidrogenul şi proştii... Această taxă va creşte proporţional cu mărimea funcţiei... deci dacă un măturător de stradă va plăti 100.000 lei, un preşedinte 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 plăteşte domnia sa pe prostia pe care are tupeul de a o afişa."

„Monitorul de Braşov" (**www.brasov.monitorul.ro**) titra pe 5 noiembrie 1999: „Noi năzbâtii ale hackerilor români", în cauză fiind, evident, grupul Pentaguard, format din „patru băieţi şi două fete". Referindu-se la Diablo, ziarul scria că „… s-a aliat în luna ianuarie cu Windows '95, liderul organizaţiei «Kp2» din Rusia, declanşând World Wide Web War sub deviza «Russia and Romania For Ever». În primele două luni de alianţă, cele două organizaţii au reuşit să distrugă 21 de servere guvernamentale sau militare americane sau chinezeşti."

Pe site-ul **www.chip.ro**, sub titlul „Atacul hackerilor şi contraatacul providerilor", apare un text în care se face referire şi la Pentaguard: „Un alt exemplu convingător referitor la vulnerabilitatea pe Internet îl reprezintă acţiunile hackerilor români Pentaguard; aceştia susţin că hackurile au motivaţie politică, dar fac acest lucru şi din pură distracţie. Consideraţi de CNN ca fiind pe locul I, precum şi atenţia 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 şi o serie de site-uri româneşti oficiale: Romtelecom, Universitatea din Timişoara, TVR, Ministerul de Finanţe." Referire la acel loc I deţinut la un moment dat de către cei din Pentaguard, clasificare realizată de CNN, face şi site-ul **www.transindex.ro/magazin/** în 19 februarie 2001. După Pentaguard, cu 154 de site-uri sparte (din care 78 gov. şi mil.) urmau: grupurile de hackeri AntiChrist, cu 136 de spargeri, 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 toţi clienţii săi şi să-şi instaleze un hard disk mai puternic şi programe performante. Dar cine au fost furioşii 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 independenţă a Timorului de Est (până de curând aflat sub stăpânirea Indoneziei), respectiv Ramos Horta şi episcopul catolic Carlos Belo, care au primit împreună, în 1996, pemiul Nobel pentru pace.

De serviciile hackerilor se folosesc inclusiv guvernele şi partidele politice. Un exemplu concludent în acest sens este isprava unor hackeri mexicani care, la comanda Partidului Democrat Revoluţionar, de opoziţie în anul 2000, au spart codul de acces şi au pătruns în serverele guvernului, aflând astfel de fărădelegile de ordin financiar ale acestuia şi 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 locaţia web a guvernului american”, publicat pe Internet pe 26 octombrie 2001, despre atacul hackerilor pakistanezi asupra serverului NOOA (National Oceanic & Atmospheric Administration), inaccesibil câteva ore, publicaţia iugoslavă „Mikro online” cita mesajul hackerilor şi anume: „Cu toate că guvernul Pakistanului condamnă atacul asupra S.U.A., noi susţinem Al Qaeda. Deţinem câteva informaţii strict secrete ale guvernului american pe care le vom preda organizaţiei Al Qaeda. Daţi-ne pace pentru a avea pace”. Hackerii solicitau S.U.A. să-şi retragă forţele armate din Arabia Saudită, să înceteze bombardamentele asupra Afganistanului şi să limiteze susţinerea Israelului. De menţionat că serverul atacat era unul de rezervă pentru datele meteo pe care NOAA le asigură Direcţiei federale pentru zboruri.

Unul dintre războaiele cibernetice din Europa a început în 2001, când un ieşean, cu pseudonimul Igu Uiorean, student la Facultatea de Automatizări şi Calculatoare din Cluj-Napoca, a atacat pagina **www.nemnemsoha.hu**, un site naţionalist maghiar (vezi **www.sinaia.globtel.ro** şi 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-şi apăra informaţiile. Apare o pagină nouă cu titlul „olahhak”, un cuvânt compus din „olah” şi „hacker”. În vara aceluiaşi an, românii reuşesc să spargă canalul de comunicaţii maghiar şi intră în posesia unor date secrete privind codurile de siguranţă ale site-ului adversarilor. În noiembrie, site-ul este spart, iar conţinutul paginilor – modificat. Coaliţia româno-slovacă, scrie „Ziua”, reuşeşte să descarce documente cu date concrete anti-româneşti. Membrii grupului românesc au declarat că în intenţia lor a fost să predea serviciilor secrete româneşti „prada de război”. Pe fir intră Poliţia română. Grupul lui Uiorean îşi încetează activitatea. Însă războiul continuă, hackerii naţionalişti români aflându-se în continuare la vânătoare de pagini naţionaliste maghiare. Un grup de hackeri constănţeni a anunţat pe un „chat” al crackerilor că intenţionează să spargă serverul Clubului Trianon. Maghiarii au luat şi ei măsuri, anunţând Poliţia maghiară.

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

Acest război a luat amploare atunci când românii şi maghiarii nu s-au limitat la a sparge site-urile naţionaliste şi revizioniste, ci au trecut şi la spargerea căsuţelor poştale personale. Ziarul „Ziua”, care a urmărit îndeaproape luptele, susţine că redactorii săi au primit însă şi mesaje prin care o serie de hackeri români şi maghiari şi-au exprimat dezacordul faţă de acţiunile 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 numiţi o grupare. [...]. Grupul nostru are scopul de a ajuta şi nu a distruge, nu de a crea probleme şi conflicte între cele două ţări. Nu ne place să fim numiţi «piraţi», deoarece grupul nostru are un scop benefic, prin securizarea serverelor care ar putea cădea pe mâini «criminale»". Dar, scria în acelaşi cotidian, grupării lui Uiorean i s-au alăturat cei din „TeamBucTm", care s-au angajat să ajute grupul clujeanului şi să facă ravagii prin paginile maghiare: „...sper să putem să ne ţinem de cuvânt şi să pice multe. să vadă şi iei ce înseamnă adevărat «război» cu românii în domeniul internetului." Reacţia hackerilor maghiari nu s-a lăsat mult aşteptată, 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 europei."

În mai 2001, cei de la **http://pcnen.cg.yu** preluau o ştire apărută în publicaţia londoneză „Independent" şi potrivit căreia oraşul Priština din Kosovo a fost paralizat întrucât numeroase organizaţii internaţionale şi neguvernamentale, cyber-caffé-uri şi oameni de afaceri au fost deconectaţi 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-şi proteja propriul sistem. În ajutorul kosovarilor a sărit un provider norvegian, care a încercat fără succes să salveze reţeaua 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 şi Croaţia au încheiat pacea, incidentele au devenit tot mai numeroase între războinicii electronici din Kosovo şi Macedonia.

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

Doar în luna mai 2001, site-ul Casei Albe a fost spart de hackeri de cel puţin trei ori şi aceasta în acelaşi fel: prin atacuri DoS. A treia oară, site-ul atacat a fost inaccesibil mai mult de şase ore, suspectaţi de atac fiind hackerii chinezi. La începutul lunii mai, hackerii chinezi au realizat, aşa cum, de fapt, au şi anunţat înainte, sute de atacuri asupra site-urilor americane, printre altele fiind grav afectat şi serverul de e-mail al Camerei Reprezentanţilor. Responsabili ai atacurilor asupra a numeroase ste-uri guvernamentale şi comerciale americane s-au declarat a fi cei din grupul autointitulat „Uniunea Hackerilor din China" (Hongke Union) care, la un moment dat, au anunţat prin pagina web „ChinaByte" că după ce au atacat mai mult de o mie de site-uri americane şi-au îndeplinit ţelurile contraatacurilor şi că următoarele atacuri antiamericane nu mai sunt acţiunea lor. În final, au declarat că „Prin această acţiune am dovedit că sentimentul patriotic încă mai există în inimile chinezilor". Desigur, fiind vorba de China, eşti foarte tentat să afirmi că în spatele acestor atacuri nu poate să stea decât o grupă de specialişti IT chinezi, fie aflaţi în solda Guvernului comunist, fie informaticieni din cadrul armatei chineze. Cum tot atât de bine nu este exclus ca hackerii din „Hongke Union" să fie totuşi tineri chinezi puternic îndoctrinaţi cu ideologia comunistă. Prea puţini ar crede că, totuşi, nu puţini oameni, din indiferent ce ţară aflată sub indiferent ce sistem politic, pot da dovadă de patriotism când e vorba de relaţia ţării lor cu o alta, percepută ca fiind agresoare.

Printre site-urile atacate se număra şi **www.leg.wa.gov**, unde se aflau informaţii despre executivul şi legislaţia americană şi 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 şi despre cele 11 zile de prizonierat la chinezi.

Din nefericire, Internetul poate fi foarte uşor un mijloc de dezinformare în masă, cu efecte la nivel global. Cititorul poate să-şi 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 anunţa faptul că preşedintele Slobodan Milošević a fost atacat de un grup de terorişti la reşedinţa sa din cartierul rezidenţial belgrădean Dedinje. Rănit fiind, a fost de urgenţă dus la spital. După câteva ore în care medicii au încercat să-i salveze viaţa, preşedintele Iugoslaviei a decedat. „Aşteptăm în continuare informaţii. Urmăriţi programul nostru şi site-ul nostru de pe Internet pentru a afla veşti noi în acest moment greu pentru poporul nostru.", scriseseră hackerii pe site-ul cotidianului „Politika". Trebuie reţinut şi faptul că trustul de presă „Politika" dispune, în afară de cotidianul sus-amintit, de un post de radio şi de unul de televiziune. Cei care au avut curiozitatea să dea curs invitaţiei hackerilor ar fi avut surpriza să constate că atât radioul, cât şi televiziunea Politika emiteau obişnuitele lor programe şi nicidecum muzica clasică, normală pentru asemenea momente. Ştirea a fost preluată de publicaţia belgrădeană în limba engleză „Bilten" şi de corespondentul agenţiei de presă „Reuters".

În 14 iulie 2000, apărea şi pe site-ul cu adresa **http://vojvodina.com** ştirea că hackerii au reuşit să spargă site-ul publicaţiei belgrădene „Politika" şi să insereze informaţia cum că preşedintele Iugoslaviei, Slobodan Milošević, a fost ucis de explozia unei bombe. Buletinul independent „VIP" a dat şi el publicităţii conţinutul informaţiei: „Preşedintele iugoslav Slobodan Milošević a decedat din cauza rănilor cauzate de explozia unei bombe amplasate în buncărul său de pe Dedinje".

Evident că lumea, îndeosebi ziariştii şi diplomaţii, a dat năvală să vadă informaţia cu pricina pe site-ul „Politica". Numai că izvorul notei mincinoase nu mai exista, site-ul fiind repede refăcut de către proprietari, de unde şi concluzia că fusese doar o acţiune de hacking. Dar acest lucru l-ar fi putut presupune şi cei care au preluat informaţia privind moartea lui Milošević, mai cu seamă că Internetul ar fi fost ultimul loc unde să apară o asemenea informaţie. Aşadar, iată că pe Internet nu este nimic sigur nici din acest punct de vedere, o informaţie abil strecurată pe un site oficial, prin hacking, evident, sau o informaţie 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 nci un fel de garanţie dacă informaţiile pot fi atât de uşor falsificate. Dar putem oare spune cu mâna pe inimă că celelalte mijloace de informare în masă, cum ar fi televiziunea, radioul, publicaţiile sunt mai sigure? Parţial da, fiindcă în aceste cazuri informaţia falsă poate fi introdusă doar de cel care lucrează la unul dintre aceste mijloace de informare în masă şi nicidecum de vreun hacker. Se întâmplă deseori ca hackerul să fie unul dintre angajaţii cu acces la site-ul companiei unde lucrează. În „hacker" nu se poate însă transforma şi angajatul unei televiziuni, de exemplu? Dincolo de toate aceste speculaţii rămâne valabil unul singur şi acelaşi lucru: mijloacele de comunicare/informare în masă nu sunt şi nici nu pot fi sută la sută sigure şi nu pot ele însele garanta veridicitatea unei informaţii. Să renunţăm la mass-media? La Internet? Desigur că nu. Doar că trebuie să avem întotdeauna rezerve îndeosebi când e vorba de informaţii importante sau extrem de importante şi să le verificăm pe mijloace de comunicare în masă diferite. Abia după aceea putem trage concluzia dacă informaţia este sau nu autentică.

Pe 18 septembrie, pe site-ul românesc cu adresa **http://stiri.rol.ro** apărea o ştire preluată de la BBC şi care spunea că, citătm: „Hackeri autointitulaţi «patrioţi» au «spart» mai multe site-uri web, între care şi al talibanilor, piraţii informatici încercând să pericliteze activitatea organizaţiilor

şi ţărilor pe care le consideră vinovate pentru atacurile teroriste de marţi." În aceeaşi ştire se amintea despre un grup de hackeri autointitulat „Dispatchers" şi care anunţase că plănuieşte un atac coordonat asupra infrastructurii computerizate a ţărilor care s-ar putea afla în spatele atentatelor comise pe 11 septembrie asupra Statelor Unite. Ba, mai mult, membri ai grupului amintit s-au şi lăudat că au distrus deja câţiva provideri palestinieni.

O notă nesemnată, publicată în cotidianul naţional „România liberă" în data de 3 octombrie 2002, relata despre faptul că „S.U.A. au lichidat un site web al Al-Qaeda" la numai 12 ore de la apariţia acestuia. Site-ul respectiv conţinea informaţii referitoare la Osama bin Laden, o declaraţie a secretarului de presă al reţelei Al-Qaeda şi un mesaj către prizonierii de la baza americană Guantanamo din Cuba, prin care aceştia erau îndemnaţi să reziste. Tot S.U.A. au lichidat şi site-ul „Jihadul on-line", însă acesta a reapărut în octombrie 2002, primele informaţii fiindu-i dedicate lui Khattab, liderul mujahedinilor arabi în Cecenia ucis de forţele armate ruseşti.

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

Pe 1 aprilie 1999, un anume Adrian le trimitea membrilor unei liste de discuţii un mesaj preluat de la o agenţie internaţională de ştiri, 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, acelaşi Adrian încheia: „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 Belgradpentru 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, faţă de întregul an 2001, cu 64% (**www.zidezi.ro**). Această informaţie a fost publicată de către compania Riptech, care a încercat să sublinieze faptul că atacurile hackerilor au tendinţa 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 „piraţi" din: Statele Unite ale Americii, Germania, Coreea de Sud, China, Franţa, Canada, Italia, Taiwan, Marea Britanie şi Japonia. Elan Yoram, unul dintre autorii acestui raport, a ţinut să facă precizarea că aceste cyber-atacuri pot proveni şi din ţări cunoscute ca fiind adăpostul anumitor grupări teroriste. Printre aceste ţări au fost menţionate Iran, Pakistan, Kuweit şi Indonezia. „Este aproape imposibil să se stabilească o linie de demarcaţie clară între atacurile hackerilor şi cyber-terorism, deoarece ambele tipuri de atacuri se fac tranzitând spaţiul internetic, folosind de cele mai multe ori serverele publice", a ţinut să sublinieze Yoram.

„Cooperare «împotriva naturii» între neonazişti şi extremiştii evrei", titrează cotidianul timişorean „Agenda zilei" în vara lui 2003, preluând un articol de la Agenţia „Reuters". Iar în subtitlu, aceeaşi publicaţie scrie: „Alianţa a inundat reţeaua mondială cu mesaje de ură la adresa arabilor". Aşadar, şi mişcarea neonazistă pare că suferă de păcatul numit „aripi". De la colaborarea dintre nazişti şi musulmani împotriva evreilor, iată că există nazişti „dispuşi să-şi uite propriile vederi antisemite pentru a pune la cale o cooperare uluitoare cu grupări extremiste evreieşti din ţară (Franţa, n.n.). Această colaborare, prin Internet, i-a ajutat pe neonaziştii francezi să-şi transplanteze mesaje de ură împotriva arabilor şi musulmanilor în Orientul Mijlociu, iar pe extremiştii evrei să ştie mai multe despre atacurile prin reţea împotriva site-urilor arabe." Evident, o asemenea situaţie nu putea să-i scape lui Mouloud Aounit, directorul unei organizaţii antirasiste

din capitala Franţei. Acesta a dat publicităţii 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 puţin de 26 de site-uri aparţinând extremei drepte franceze şi grupărilor extremiste evreieşti din Franţa plătesc găzduirea paginilor web pe acelaşi server din S.U.A. cu începere din 1999, anul primului război electronic mondial. Dar, în cele din urmă, scrie publicaţia timişoreană, partajarea comună a spaţiului pe serverul american a luat sfârşit. Motivul: puncte de vedere diferite referitoare la campania americano-engleză în Irak. Pur şi simplu, unii dintre neonazişti (o altă aripă?) nu au fost de acord cu atacul aliat împotriva Irakului. „Pe site-urile respective există şi îndemnuri de asasinare a preşedintelui Jacques Chirac, menţionat cu numele de «Ben Shirak»", încheie „Agenda zilei".

Că Internetul poate fi transformat în armă o dovedeşte şi activitatea cibernetică a aşa-zisului anacronic Phenian. Tot „Agenda zilei" scria pe 17 mai 2003: „Phenianul are o armată de hackeri pricepuţi - Războiul informaţional e în toi". Potrivit Agenţiei „Reuters", al cărei material este preluat de publicaţia bănăţeană, „...singurul server care susţine site-urile oficiale nord-coreene se află în Japonia. Dar realitatea este cu totul alta. În Coreea de Nord sunt antrenaţi anual circa 100 de tineri transformaţi în hackeri, soldaţii informaţionali ai regimului." Vecina din sud, Coreea soră, nu se află aşadar ameninţată numai de rachetele fraţilor comunişti din nord (posibil chiar atomice), ci şi de cyber-atacuri. „La începutul acestui an, un virus a contaminat rapid aproape toate reţelele de calculatoare din Coreea de Sud, blocând şi traficul pe Internet. A fost pentru prima dată când serviciile reţelelor din această ţară au fost afectate într-o asemenea măsură. Se crede că a fost vorba despre un «exerciţiu» de atac lansat de nord-coreeni." Hoţul neprins 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 creea „imagine". Referindu-se la sud-coreeni în cartea sa „Lacrima - Orient şi occident" (Ed. „Anthropos" Timişoara, 2000, versiune în limba română: Duşan Baiski), scriitoarea taiwaneză Chang Shiang Hua spune la un moment dat: „... o cunoscută mişcare de rezistenţă a studenţilor coreeni, o mişcare a sentimentelor naţionale profunde, a luptei împotriva guvernării, împotriva Americii, poartă pecetea unui fanatism de puber care, de cum trece perioada exaltării tinereşti, deseori se stinge de la sine. Aşa că, la terminarea universităţii, o mulţime de asemenea activişti studenţi extremişti caută de urgenţă debutul în «ape liniştite», ajungând astfel până la companiile americane, care oferă un salariu bun." Şi cum Coreea de Sud este una dintre cele mai informatizate ţări din lume, cum şi în această ţară pot exista informaticieni cu păreri pro-nord-coreene, nu este obligatoriu de crezut că unul din cei o sută de nord-coreeni pregătiţi pentru atacuri cibernetice este teroristul care a afectat Internetul sud-coreean.

În baza reclamaţiilor primite de Centrul Împotriva Fraudelor pe Internet din S.U.A. pe parcursul anului 2002, pe primul loc la nivelul ţărilor de pe teritoriul cărora au fost iniţiate fraude se situează Statele Unite, susţine cotidianul „The Sidney Morning Herald". De ce nu ar fi fost posibil ca „îngheţarea" Internetului sud-coreean să fi fost realizată de S.U.A., tocmai pentru a menţine încordată situaţia 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 victorioşi în Irak, de ce nu am accepta o asemenea ipoteză şi în cazul la care ne-am referit? Din păcate, doar Dumnezeu ştie care este adevărul. Împreună cu războinicii implicaţi. Referitor la clasamentul întocmit de cotidianul australian, „Renaşterea bănăţeană" din Timişoara enumera şi celelalte ţări din tristul clasament: după S.U.A. urmau Nigeria, Canada, Africa de Sud, România şi Spania. Nu ştim pe ce loc erau situaţi superhackerii singurului abonat nord-coreean la Inernet, Kim Jong-il, dar e cam greu de crezut că providerul japonez ar fi lăsat nesupravegheată activitatea centurionilor

comunişti din Peninsulă. O activitate susţinută, menită a bloca serverele Coreei de Sud, ar fi fost depistată imediat. Dar politica e politică.

În 2002, relatează presa internaţională, preşedintele George W. Bush a semnat o directivă prin care stabilea datele lansării unor atacuri asupra reţelelor de calculatoare ale unor ţări ostile Statelor Unite ale Americii. Acest ordin a fost deconspirat de cotidianul „The Washington Post". Regulile pentru războiul informaţional au fost pregătite în timp ce Pentagonul lua deja în considerare lansarea unor asemenea atacuri împotriva ţărilor-ţintă, scria „Reuters". Mecanismul acestui război invizibil şi tăcut s-ar putea să-şi demonstreze capacitatea cu prilejul campaniei militare din Golf, a afirmat un oficial al Pentagonului, citat de cotidianul din capitala S.U.A. Alţi oficiali cu funcţii importante au declarat că S.U.A. nu au lansat niciodată atacuri informaţionale (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 specialiştii armatei S.U.A., aşezaţi în faţa terminalelor de calculator, neutralizează cu câteva apăsări de tastă reţelele computerizate ale unei ţări ostile «stingându-i» radarele, sistemul energetic naţional şi întreaga reţea telefonică. Asta doar pentru deschidere..."

Cum vine asta, vă veţi întreba? Orice om normal se întreabă de ce este necesar ca sistemele informatice sensibile să fie interconectate. De aceea pare stupefiantă afirmaţia că un atac terorist ar putea paraliza Internetul. Autori sunt nimeni alţii decât cercetători din cadrul Universităţii din Ohio - S.U.A. Aceştia au demonstrat că principalele oraşe vor avea acces la Internet chiar şi în cazul în care reţeaua va funcţiona la capacitate redusă, în vreme ce oraşele mijlocii şi mici vor fi deconectate. Costurile relativ mari pentru transmisia prin satelit, dar şi pentru cea prin magistralele din fibră optică obligă providerii mai mici să se „aboneze" la cei cu putere financiară mai mare. Astfel că reţeaua seamănă cu o caracatiţă. Dacă este distrus centrul, adică providerul puternic, automat „pică" şi providerii mărunţi. Unul dintre universitarii din Ohio, Tony Grubesic, compara consecinţele unui asemenea scenariu cu acelea care pot interveni în traficul aerian: „În cazul în care condiţiile atmosferice opresc sau întârzie traficul pe un aeroport, ca O'Hare din Chicago, pasagerii din întreaga ţară vor resimţi consecinţele. Acest lucru este valabil şi 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. Acelaşi Grubesic este de părere că, din motive de securitate, reţelele de Internet nu trebuie concentrate în marile oraşe şi cere o mai mare descentralizare a Internetului. Ceea ce este echivalent cu a solicita încălcarea regulilor economiei de piaţă prin intervenţia statului care fie sprijină prin fonduri publice întreţinerea unor servere, fie introduce reguli speciale pentru providerii de Internet.

Atotprezentul „Reuters" este din nou citat masiv pe mapamond la sfârşitul lui octombrie 2002. Astfel, „România liberă" din Bucureşti titra pe 30 octombrie 2002: „Hackerii proislamici pregătesc un război cibernetic". O banală previziune a cuiva de la cunoscuta agenţie de ştiri sau doar o bucăţică dintr-un scenariu mai amplu de război psihologic? O picătură informaţională în campania de pregătire psihologică a agresiunii americano-engleze împotriva Irakului? Nu ştim, nu putem răspunde. Putem doar specula. Răspunsurile pot fi, în mod firesc, afirmative. Acelaşi „Reuters", citând experţi în probleme de Internet, preluat de cotidianul naţional românesc, spune că „Hackerii proislamici se află în prima linie a unui potenţial război cibernetic după decizia aşa-numiţilor «hacktivişti» şi a creatorilor de viruşi de a rupe armistiţiul autoimpus după atentatele din 11 septembrie 2001 din S.U.A.". Piraţii cibernetici prislamici şi-au intensificat atacurile împotriva ţărilor care sprijină războiul dus de S.UA. împotriva terorismului şi campania sa împotriva Irakului, în timp ce virusul „bugbear" şi atacul eşuat asupra Internetului demonstrează că hackerii

au ieşit din nou la vânătoare. Firma britanică „MI2G" din Londra a anunţat că octombrie 2002 poate concura la titlul de cea mai neprielnică lună din cauza atacurilor electronice - 16 559 la număr. Aceeaşi companie - care oferă consultanţă privind securitatea pentru bănci şi firme de asigurare şi 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 şi antiisraeliană." Dean White, coordonatorul Centrului Sans (dedicat Internetului) pentru Asia-Pacific, referindu-se la părerea experţilor în domeniul Internetului, afirma: „Trebuie să ne aşteptăm la un atac şi să fim pregătiţi, a fost linişte 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 proporţiei grupărilor proislamice). Citäm din „România liberă" din 30 octombrie 2002: „Unul dintre ele (dintre cele trei grupuri proislamice, n.n.) se numeşte «Unix Security Guards» (USG), un grup de hackeri format în mai 2002 şi despre care se crede că este compus din alte entităţi mai mici, variind de la «EgyptianFighter» până la hackerii din fostele republici sovietice musulmane şi până în Maroc. USG şi-a înzecit atacurile în interval de o lună, de la 21 înregistrate în august, şi 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), bănuit că ar avea sediul în Pakistan, şi «The Bugz» majoritar pakistanez. Creşterea atacurilor virtuale proislamice coincide cu atacul fără precedent de săptămâna trecută pe 9 din cele 13 servere principale care formează coloana vertebrală a reţelei Internet. Oficialităţile de la Washington au încercat să minimalizeze incidentul şi sugestiile că ar fi vorba de «cyberterorism», însă experţii informaticieni spun că, indiferent de vinovat, acest atac a evidenţiat vulnerabilitatea infrastructurii de comandă şi 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 şi nicidecum o eroare pur umană sau un atac din interior.

Ce se întâmplă însă dincolo de fosta „cortină de fier"? O ştire provenind de la aceeaşi atotştiutoare agenţie de ştiri „Reuters" (?!), citând o sursă din cadrul fostului K.G.B., este preluată pe 16 octombrie 2002 de „Renaşterea bănăţeană": „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 comparaţie cu anul trecut, la data de 1 septembrie depăşind cifra de 760.000 de cazuri, a precizat aceeaşi sursă. Potrivit oficialului din cadrul F.S.B., «nu este vorba de activitatea serviciilor străine», ci de încercările tinerilor preocupaţi de Internet, de a-şi «dovedi îndrăzneala». Hackerii sunt, «cel mai adesea minori, iar dat fiind că nu reuşesc să spargă codurile, nu există vreo acţiune de urmărire», a explicat sursa din cadrul F.S.B.." Aşadar, nici pomeneală de atacuri cibernetice din partea cecenilor sau a aliaţilor 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 şi acum văd în jur doar duşmani? „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 atenţia asupra unui alt fenomen periculos: folosirea Internetului de către grupările teroriste, pentru comunicaţii, recrutare şi colectare de fonduri. Chiar şi acum, în condiţii de securitate sporită, AL-Qaeda se foloseşte de Internet pentru a pune la cale noi atacuri. Experţii au ajuns la concluzia că teroriştii au studiat cu mare atenţie 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 condiţiile în care mare parte din servicii - de la tranzacţii financiare la asigurări sociale - se bazează pe Internet şi utilizează baze de date computerizate." Parcă totul aduce cu isteria provocată de virusul mileniului, care s-a dovedit un mare fâs susţinut cu abilitate de către cei interesaţi. 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 şi procesul se încheiase acum definitiv. Milioane de memorii optice şi electronice înmagazinaseră trilioane de tranzacţii - practic toate afacerile planetei. Şi, desigur, multe din aceste intrări purtau o dată. Când a început ultimul deceniu al secolului, ceva ca o undă de şoc a străbătut lumea financiară. Şi deodată, dar tardiv, au realizat că celor mai multe dintre aceste date le lipsea componenta vitală. Funcţionarii umani de bancă, cei care ţineau 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 simţ. Iar bunul simţ, din păcate, era vădit că le lipsea computerelor. Şi, în primii zori ai lui '00, miriade de îndobitociţi de electronică îşi ziceau «00 este mai mic decât 99 ». Aşa că astăzi este mai devreme decât ieri - cu exact 99 de ani. Recalculaţi toate depăşirile de cont, ipotecile, operaţiile curente pe această bază..."

Evident, uneori nu mai ştii unde se termină imaginaţia şi începe realitatea, însă e greu de crezut că omul se poate lăsa pe mâna computerelor fără a-şi lua toate măsurile de protecţie. Imaginaţi-vă doar o banală pană de curent care să întrerupă un serviciu vital într-un oraş 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 siguranţe în caz de scurtcircuit. Darămite un serviciu vital controlat de computer. Da, veţi spune, dar duşmanul poate avea implantaţi oameni în interiorul sistemului. Deci mai rămân 50% şanse pentru un reuşit atac terorist cibernetic. Însă aşa cum înşişi oamenii din cadrul C.I.A., F.S.B. sau S.R.I. sunt, la rândul lor supravegheaţi, şi în serviciile publice vitale, teoretic, ar trebui să existe supervizori. Aşadar, şansele 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 naţiune este atât de naivă încât să nu dubleze sau să tripleze măsurile de securitate. Şi atunci, la ce bun atâta isterie vizavi de posibilele efecte catastrofale ale unui atac cibernetic? Ne temem oare de calitatea forţei de muncă? Să fie tehnica mai presus de om? Nu mai există nici o fărâmă de patriotism la cei puşi să ne apere? Cercetători ruşi prost plătiţi, ajunşi 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 şi 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 organizaţiei teroriste internaţionale Al-Qaeda la numai 12 ore de la apariţia acestuia în reţeaua Internet. „În cele câteva ore de existenţă, pe site au apărut informaţii cu privire la Osama bin Laden, o declaraţie a secretarului de presă al reţelei Al-Qaeda şi un mesaj către prizonieri de la baza Guantanamo, prin care aceştia erau îndemnaţi să reziste." Numai că, asemenea unei hidre cu o mie de capete, de tai un cap, răsare altul. Acelaşi cotidian românesc continuă: „Marţi a reapărut însă pe Internet site-ul «Jihadul on-line», închis de S.U.A. anterior şi care îi aparţine - potrivit ziarului saudit «As Sharq Al Ausat» - lui Abdurrahman Ar-Rashid, cetăţean al unuia dintre statele din Golf. Primele informaţii au fost dedicate în totalitate lui Khattab - liderul ucis al mujahedinilor arabi din Cecenia."

Iată însă şi o altă ştire publicată în mass-media românească, de data aceasta în 2003. Site-ul postului de televiziune prin satelit „Al-Jazeera", al cărui sediu se găseşte în micul stat arab Qatar,

a fost blocat în urma a mai multor atacuri. Oficialii postului, citaţi de A.F..P., au dat vina pe americani. Abdel Aziz Al-Mahmud, redactorul şef al ediţiei electronice al „Al-Jazeera", a declarat că este vorba despre „atacuri masive" declanşate după ce acest cunoscut post de televiziune a difuzat imagini cu cadavrele soldaţilor americani ucişi sau executaţi de irakieni.

Imediat după atacul terorist asupra World Trade Center din New York, hackeri neidentificaţi au blocat aproape toate paginile oficiale de pe Internet ale Afganistanului, în vreme ce în multe pagini dedicate lui Osama bin Laden şi talibanilor au fost inserate alte conţinuturi. De asemenea, a fost lansat şi un virus denumit „WTC". Acesta era transmis prin poşta electronică, emiţătorul anunţând în corpul mesajului că fişierul ataşat conţine informaţii despre distrugerea turnurilor gemene (**www.danas.org**, 18 septembrie 2001).

Un grup de hackeri pakistanezi a atacat pe 17 octombrie 2001 serverul Administraţiei Naţionale pentru Ocean şi Atmosferă (S.U.A.). În mesajul trimis, hackerii spuneau: „Chiar dacă guvernul pakistanez condamnă atacul asupra S.U.A., noi susţinem Al Qaeda. Deţinem nişte informaţii secrete aparţinând guvernului american pe care le vom preda organizaţiei Al Qaeda. Lăsaţi-ne în pace şi vă vom lăsa în pace." După cum scria pe **www.sksu.net**, hackerii solicitau S.U.A. să-şi retragă forţele armate din Arabia Saudită, să înceteze să bombardeze Afganistanul şi să înceteze să susţină Israelul. De asemenea, mai ameninţau că vor schimba faţa altor site-uri, însă nu vor fura date întrucât acest lucru nu este etic.

Interesant este însă faptul că, prin atacul din11 septembrie 2001 asupra turnurilor gemene World Trade Center, Al Qaeda devine cea dintâi organizaţie ca fiind „statul virtual" „Statul virtual, scrie Philip Bobbitt în «Time», citat de publicaţia croată «Vjesnik» (**www.vjesnik.com**), are multe trăsături ale altor state (o armată şi o inteligenţie antrenate, trezorerie şi surse de venituri, structură administrativă şi un fel de asigurări sociale pentru familiile luptătorilor săi), însă el nu are graniţe, declară războaie, încheie alianţe cu alte state şi, prin ţelurile sale are un caracter global, nu are un loc definit pe harta globului pământesc. [..] În secolul 21, statele naţionale ar putea fi înlocuite cu ceva ce s-ar putea numi «state economice». Statele economice vor avea frontiere şi structuri administrative similare cu cele ale statelor naţionale, însă răspunderile cheie vor fi trecute de la guverne la sectorul privat; corporaţiile multinaţionale vor prelua rolurile pe care un guvern nu le mai poate îndeplini şi vor şterge graniţele dintre liderul politici şi liderul corporativ. Tocmai pentru că economia este particulară, globală şi transnaţională, statele economice vor putea mai bine decât cele naţionale să se descurce cu un război care în parte este particular, o parte multinaţional şi o parte de apărare, aşa 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 naţionale cu o populaţie 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 siguranţă că vom vedea conflicte între forme concurenţiale ale statelor economice. Poate fi vorba şi de un război cronic, cu intervenţii de mică intensitate - acţiuni poliţieneşti cu motive umanitare; [...] Războiul s-ar putea purta şi între anumite regiuni sau poate între marile puteri care pun în mişcare atacuri virtuale acoperite - pentru ca apoi atacurile hackerilor să degenereze în declanşarea unui conflict armat."

Într-un raport al Consiliului Naţional 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 şi a conduce acţiuni de la distanţă, în perfect anonimat şi în perfectă siguranţă. Prin utilizarea unor tehnici de criptografiere tot mai sofisticate şi folosind specialişti în informatică dintre cei mai buni, organizaţiile teroriste le transmit subordonaţilor nu

doar ordine, ci şi planuri de acţiune, fotografii ale celor vizaţi pentru a fi lichidaţi, instrucţiuni, coduri şi hărţi.

Pe de altă parte, Internetul este ideal pentru răspândirea unei ideologii sau alteia. În lucrarea lor intitulată „Internetul, criminalitatea şi dreptul", prof. univ. dr. Dan Banciu şi conf. univ. dr. Ion Vlăduţ scriu: „Un exemplu în acest sens îl reprezintă organizaţia teroristă Drumul luminos din Peru, care, dispunând de un site pe Web, îşi promovează propria ideologie extremistă. Interesant este faptul că, aşa după cum constata fostul şef al operaţiunilor F.B.I., Buck Revell, atâta timp cât mesajele acestor grupări fac numai propagandă pentru ideologia lor, fără să treacă la acţiuni criminale, teroriştii pot desfăşura liberi activităţi, astfel încât Internetul a devenit un adevărat «rai» pentru ei."

Simpatizanţii diverselor organizaţii teroriste construiesc site-uri de simpatie. După ce gruparea teroristă „Tupac Amaru" a ocupat reşedinţa ambasadorului Japoniei în Peru, în decembrie 1996, luând ostateci membrii ambasadei şi pe invitaţii acestora, simpatizanţii din S.U.A. şi Canada ai organizaţiei amintite au realizat o serie de site-uri de simpatie.

Dar Internetul este foarte utilizat şi pentru diseminarea mesajelor de ură şi incitare la violenţă. Nu puţine sunt site-urile antisemite şi antioccidentale. Numai că, susţin autorii amintiţi mai înainte, „...în S.U.A. se consideră că informaţiile difuzate pe Internet ţin de dreptul la liberă exprimare, riposta autorităţilor faţă de construirea site-urilor de către grupările teroriste fiind destul de delicată. Astfel, în această ţară, deşi paginile Web ale grupărilor teroriste sunt publice, F.B.I.-ul nu are voie să facă dosare cu fişierele respective decât atunci când investighează un anumit caz care a fost aprobat de procuror." Astfel că, concluzionează aceiaşi autori, „... grupărilor teroriste nu le-a trebuit prea mult timp să înţeleagă 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 şi periclitarea vastelor reţele."

În acest context, se cuvine să amintim faptul că în timpul agresiunii N.A.T.O. asupra Iugoslaviei, au devenit foarte active grupările antisemite şi antisemiţii individuali, vinovaţi pentru atacul N.A.T.O. asupra Iugoslaviei fiind consideraţi evreii americani prezenţi în structurile de conducere ale S.U.A. Pe listele de discuţii sârbeşti şi-a făcut apariţia şi lista conţinând numele şi poziţia 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://AmericanDefense** League.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 discuţii a evreilor de pe Yahoo, respectiv „EEJH" Jewish History, unde Pribich este considerat „...Mr. alias Boris Primich's Organization, should beinvestigated by FBI and State Department, as Terrorist Fascist/Hitlerist Organization", opinia fiind a semnatarului e-mail-ului şi anume un anume dr. Sigmund Mittler, M.D. Professor.

Tot pe unul din site-urile lui Pribich am dat şi peste un text intitulat „Cine controlează media din S.U.A.", unde autorul face o radiografie a mijloacelor de informare şi divertisment din Statele Unite din punctul de vedere al naţionalităţii fondatorilor, proprietarilor sau actualilor conducători, concluzia fiind clară: evreii conduc media în S.U.A. şi pot influenţa şi/sau manipula extrem de uşor opinia publică în favoarea lor sau împotriva persoanelor şi/sau statelor considerate inamice.

Unul dintre principalii vinovaţi 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 şi peste un text dedicat acesteia şi 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 Ilič, un ziarist care a stat de vorbă cu foştii ei prieteni şi colegi de şcoală din Belgrad. Trebuie reţinut că Joseph Korbel, tatăl lui Madeleine Albright, a fost ambasadorul Cehoslovaciei la Belgrad pe timpul preşedinţiei la Praga a lui Benes, iar viitorul secretar de stat al S.U.A. şi-a petrecut aici o bună parte a tinereţii. Cu atât mai ciudată devine din acest punct de vedere aversiunea ei ulterioară faţă de sârbi. Faptul că familia de evrei cehi Korbel a părăsit la un moment dat Cehoslovacia, de teama de a nu fi exterminată de nazişti, şi a ajuns în Iugoslavia pentru a fi ajutată să plece de aici în America, cu ajutorul sârbilor, nu a mai contat în acţiunile din 1999 ale lui Madeleine Albright. Poreclită pe Internet „baba cu coaie de oţel", Albright a fost, este şi va rămâne în memoria sârbilor drept una din maleficele fiinţe 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 esenţial 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 trăieşti...) poate duce şi la ideea unei conspiraţii bine concertate a evreilor împotriva poporului sârb. Câtă dreptate au sau nu antisemiţii declaraţi ori chiar simpli sârbi care cred asemenea lucruri, doar Dumnezeu poate şti.

Internetul ca mijloc de propagandă

Miloš Urošević scria pentru membrii listei de discuţii serbianforum (**http://www.eGroups.com/list/serbianforum**): „Pe CNN au publicat faptul că Pentagonul are probleme cu identificarea ţintelor pe care le-au nimerit sau nu. Pentru aceasta se folosesc de orice izvor de informaţie, oricum şi de acesta de faţă (lista de discuţii, n.n.). Vă rog, fraţilor din Iugoslavia, nu descrieţi detaliat ceea ce a fost nimerit (de bombe, n.n.), ci doar din ce direcţie s-au auzit detonaţiile. Cu cât sunteţi mai nehotărâţi, cu atât mai bine." Nu cumva era vorba de un ordin

prin CNN pentru spionii americani aflaţi în acel timp pe teritoriul Iugoslaviei să-şi facă mai bine treaba şi să trimită detalii despre efectele bombardamentelor? Sau să fi fost însuşi individul cu numele de Miloš Urošević cel care a retransmis acest ordin, spionii americani fiind cuplaţi la lista de discuţii serbianforum? Evident, totul este posibil. Nu există mijloc mai facil pentru transmiterea de informaţii decât Internetul, mai cu seamă că poşta electronică poate transporta de la expeditor către destinatar nu doar un banal text, ci şi imagini statice ori în mişcare şi fişiere audio. Este adevărat că în Timişoara, în zilele fierbinţi ale lui decembrie 1989 şi chiar în ianuarie 1990 era relativ periculos să fii văzut pe stradă fotografiind ori filmând. Însă pe-atunci încă mai persistau prejudecăţile şi ferocea teamă de Securitate. În 1999, însă, când existau aparate digitale de fotografiat şi filmat miniaturale, nu era greu să filmezi un pod distrus la Novi Sad, să fugi în apartament şi să transmiţi imaginea direct din aparat, prin e-mail, către cel care te-a angajat să spionezi. Chiar şi într-o Iugoslavie cum era cea de sub Milošević, aflată în plin război. În acelaşi mesaj, Miloš Urošević îi sfătuia pe membrii listei de discuţii să viziteze site-urile albaneze, citând „Kosova press" care dădea informaţii despre poziţiile exacte ale forţelor iugoslave la Drenica şi în alte localităţi din Kosovo, şi să anunţe cele mai apropiate posturi de miliţie care, la rândul lor, să anunţe armata că se află în pericol. În încheiere, Urošević scria: „Acţiunea: Toţi suntem ţinte!"

Brazilianul Leo Villanova scria la lista de discuţii 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 ofiţer în Bundeswehr. Acesta i-a adus la cunoştinţă că a văzut într-o bază militară aeriană faptul că militarii care încărcau materialele de propagandă (fluturaşi) în avioane erau cu toţii îmbrăcaţi în costume speciale împotriva microorganismelor. Drept urmare, Nenad îi atenţiona pe cei din ţară să nu pună mâna pe fluturaşii aruncaţi pe teritoriul Iugoslaviei, deoarece exista pericolul să fie contaminaţi. Dacă e să ne gândim la faptul că forţele NATO au bombardat Iugoslavia şi cu bombe ce conţineau în componenţa lor şi uraniu, nu este exclus ca necunoscutul din casa lui Joseph să fi fost într-adevăr ofiţer Bundeswehr. Desigur, este o simplă speculaţie, 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 pregăteşte pentru un răspuns rapid şi ferm în cazul unui atac cibernetic. „Provocările noului secol sunt deosebite de acelea ale secolului abia încheiat" – a afirmat el în cadrul unei conferinţe despre apărarea naţională, ţinută la Washington (**www.klik.hr/**). „Am învăţat multe de la primul război al secolului 21, însă nu trebuie să credem că teroriştii sunt unica ameninţare. Viitoarele ameninţări cu care se va confrunta America pot fi teroriştii, un conflict tradiţional 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 aflaţi pe teren şi echipa din S.U.A. vor aduce hotărâri importante, dacă nu cumva vor conduce chiar un război. Toate informaţiile şi conţinuturile comunicaţiilor 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 clickuri de mouse se poate ajunge la orice informaţie importantă. Site-ul este pe deplin sigur vizavi de atacurile hackerilor şi ale celorlalţi răufăcători din domeniul IT.

La rândul său, pentru a ţine pasul cu progresul tehnologic, poliţia britanică a înfiinţat o unitate naţională de luptă împotriva criminalităţii cibernetice. Obiectivul acesteia este vânătoarea a tot mai multor criminali care-şi conduc afacerile prin intermediul Internetului. Pentru dezvoltarea unităţii, spun cei de la **www.becki-informator.at**, s-au cheltuit mai mult de 25 de milioane de lire sterline. În componenţă intră 40 de specialişti care-şi vor desfăşura 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 fărădelegi, de la pedofilie până la hackeri, care ameninţă utilizatorii şi sistemele din întreaga lume. Alarmant este şi faptul că mai mult de 60% din afacerile on-line britanice au fost ţinte ale atacurilor hackerilor.

Nu mult timp după agresiunea NATO asupra Iugoslaviei, dr. Slobodan R. Petrović, poliţistul iugoslav de care am mai pomenit în această carte, îşi exprima temerea că, după readmiterea oficială a poliţiei iugoslave în Interpol, crackerii şi carderii iugoslavi vor fi urmăriţi de societăţile de asigurări străine care au acoperit pagubele produse de aceştia diferitelor companii, îndeosebi din S.U.A. Iar pe lângă problemele cu maşinile furate, lumea va insista pe criminalitatea pe Internet.

În cyberspaţiu totul e posibil

Nu, nu este o afirmaţie atât de gratuită precum pare dacă avem în vedere faptul că Internetul îşi are deja şi 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". Ştirea, apărută pe site-ul televiziunii italiene RAI, cu toate că era falsă, a fost preluată şi de alte site-uri, care au adăugat şi un necrolog dedicat Papei Wojtyla.

Ion Iliescu, preşedintele României, vizitând în 2001 compania românească „Romsys", unul dintre cei mai importanţi furnizori de servicii informatice din România folosite în domeniile financiar-bancar, medical, învăţământ şi guvernamental, afirma că hackerii „pot deveni factori constructivi" şi că „Acum ei îşi folosesc inteligenţa pentru şmecherii, dar pot fi folosiţi". 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 şi 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-caffé-uri din Grecia. Supăraţi că Executivul elen plănuia să interzică distracţia electronică în locurile publice, membrii Asociaţei Naţionale a Proprietarilor de Internet-caffé-uri din Grecia a organizat un Internet-caffé în piaţa centrală din oraşul 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.

Aceeaşi agenţie de presă se referea, în aceeaşi zi, şi 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 nemulţumiţi că li se interzice accesul. În capitala chineză au fost închise, din aceeaşi cauză, toate Internet-caffé-urile (din cele 2 400 existente aproximativ 2 200 nu aveau autorizaţii de funcţionare).

Politicienii îşi 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 greşit. 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 câştiga 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. Activiştii împotriva spam-urilor şi utilizatorii care au primit asemenea e-mail-uri au fost deosebit de furioşi, ceea ce, cu siguranţă, a avut un efect deosebit de negativ asupra campaniei politicianului în cauză.

Cu atacuri DoS împotriva naziştilor. Aceasta era, la un moment dat, în 2001, esenţa unei informaţii publicate în publicaţia germană „Der Spiegel" şi preluată de mass-media internaţională. Otto Schily, ministrul german al afacerilor interne, a găsit o soluţie viabilă pentru a opri atacurile din partea site-urilor naziste: atacurile DoS (Denial of Service). Pentru a apăra infrastructura germană de Internet, acelaşi Otto Schilly a înfiinţat în cadrul ministerului condus de el o secţie specială care se ocupă cu apărarea părţii germane a cyber-spaţiului.

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

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

Din aprilie 2001, austriecii au o întreprindere de stat care regularizează şi plăteşte expedierea de e-mail-uri. „Austria Email", scria „BOL", înregistrează fiecare e-mail trimis şi, prin ISP-urile locale, plăteşte utilizatorilor finali câte un şiling/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 internauţilor. Reprezentantul guvernului a afirmat că, citäm: „Comunicaţia prin e-mail este acelaşi lucru cu distribuţia apei ori a energiei electrice şi 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-şi îmbunătăţească sistemele de securitate informaţională şi anume prin atragerea de partea sa a hackerilor care doresc burse de studiu. Prin colaborarea dintre Guvern şi National Science Foundation – NSF, câte 200 de studenţi 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 alocaţi 8,6 de milioane de dolari.

În mai 2001, **www.active-security.org** anunţa, preluând o informaţie 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, îşi va întrerupe rubrica unde apăreau deja de doi ani de zile adresele paginilor şi 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 ştearsă. Am căutat apoi adresa **http://aldas.de**. Nici vorbă de ceea ce mă aşteptam, 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 veşnic şi nici sigur.

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

Statele nu stau cu mâinile încrucişate în lupta cu hackerii, ele adoptând tot felul de legi, unele mai eficiente, altele total ineficiente. La rândul lor, anunţau 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 dezvolta P2P (peer to peer), un soft de reţea care trebuia să învingă cenzura corporaţiilor şi a guvernelor. Marea problemă consta însă în faptul că un asemenea browser putea fi utilizat de către criminali şi pedofili pentru a-şi ascunde fărădelegile.

În iunie 2002, **www.suonline.net** anunţa faptul că tehnicianul însărcinat cu întreţinerea arhivei electronice conţinând cele mai importante documente istorice ale Norvegiei a murit fără a încredinţa cuiva parola de acces. De la moartea acestuia au trecut deja mai mulţi ani şi angajaţii „Centrului Naţional Norvegian pentru Limbă şi Cultură" tot nu au acces la arhivă, astfel că directorul Centrului a făcut apel prin radio la toţi hackerii care ar putea ajuta la spargerea parolei de acces. Evident că s-au anunţat mult mai mulţi hackeri decât s-ar fi aşteptat. Această întâmplare a readus în centrul atenţiei 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 şi la securizarea bazelor de date prin cifrare ori chiar la ştergerea lor.

O interesantă situaţie, amintită de acelaşi **www.suonline.net**, s-a petrecut în Coreea de Sud, după ce compania de software de securitate „KDWorks" a organizat o competiţie prin care hackerii erau invitaţi să spargă un anumit server, pe învingători aşteptându-i premii băneşti importante. Numai că doi hackeri au pătruns în chiar serverul lui „KDWorks" şi şi-au inserat datele de identificare în locul datelor fiecărui potenţial câştigător 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 aplicaţii şi nu reprezenta o situaţie reală, astfel că s-au hotărât să „aranjeze" serverul principal. Pe de altă parte, „KDWorks" a susţinut că serverul pentru concurs, care rula pe Smoothwall Linux, a fost o momeală pentru hackeri şi a constat dintr-un server fals şi din software pentru urmărirea şi 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 pridideşc să condamne hacking-ul şi inclusiv pe hackeri, undeva în deşert se organizează DefCon, un concurs în cadrul căruia sunt testate abilităţile de a sparge, dar şi de a proteja o reţea. Ca dovadă că asocierea termenului de «hacker» cu cel de «răufăcător» este greşită, printre participanţi se numără şi angajaţi ai unor agenţii federale. [...] Concursul întăreşte regula conform căreia cea mai bună cale de a apăra un server este de a şti cum să îl ataci. «Uneltele 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

şi căpitan al echipei din concursul DefCon cu acelaşi nume, n.n.), subliniind încă o dată diferenţa dintre hackeri şi crackeri."

Căutând cu **www.google.com**, un puternic motor de căutare pe Internet, adrese de pagini web care să conţină cuvintele-cheie „hacker" (haker, potrivit ortografiei sârbo-croate), am ajuns şi la domeniul **www.elitesecurity.org**, întreţinut de bosniaci şi care conţine o serie de forumuri de discuţii. Atenţia ne-a fost atrasă de mesajul membrului cu numărul 12119, de loc din Sarajevo, însă care nu şi-a dat şi numele real. El făcea cunoscut celorlalţi membri din forumul despre hackeri şi hacking faptul că EC-Council (**www.eccouncil.org/index.htm**) permite certifierea hackerilor în domeniile metodologiei şi eticii hackingului. „Oamenii care au cunoştinţe în hacking pot primi pentru cunoştinţele lor un certificat şi, evident, pot accesa un loc de muncă în calitate de consultanţi" - scria bosniacul. Credeam că este vorba despre o banală glumă a unui adolescent pus pe şotii, însă accesând, la rândul nostru, **www.eccouncil.org**, ne-am convins că acesta nu minţea. Cel care doreşte să intre în posesia unui certificat din partea lui EC-Council, deci să devină un „Certified Ethical Hacker", trebuie să treacă 21 de teste şi 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 „curiozităţi" poate fi trecut, în mod evident, şi „Muzeul fraudei pe Internet" înfiinţat de către compania „Ad Cops", care conţine deocamdată o colecţie de exponate pentru ajutor împotriva fraudei prin e-commerce.

Mass-media şi agresiunea asupra Iugoslaviei

Războiul mediatic, îndeosebi cel de la televiziune şi de pe Internet, i-a prins şi pe români. Majoritatea populaţiei nu era neapărat împotriva alianţei nord-atlantice şi a americanilor, însă simpatiza cu sârbii. Doar puterea politică a momentului, din dorinţa de a fi pe placul S.U.A. şi N.A.T.O., de-a dreptul a excelat în a susţine acţiunile militare împotriva ţării vecine (şi "prietene", ar completa, zeflemitor, un cunoscut "analist politic"). A rămas proverbială afirmaţia preşedintelui de atunci al României, Emil Constantinescu, cum că bombardarea Iugoslaviei este necesară şi legitimă, afirmaţie criticată de mass-media românească. "Avea România interesul ca preşedintele ţării să declare că un război împotriva Iugoslaviei este "necesar şi legitim" chiar înainte de a începe bombardamentele? Şi de ce legitim, dacă ONU nici după sistarea bombardamentelor nu a legitimat intervenţia militară a NATO?" - scria Corneliu Vlad (**www.lumeam.ro**, site-ul "Lumea magazin"). "Nu am fost capabili să înţelegem că, în numele democraţiei şi al drepturilor omului, era necesar şi legitim să moară copii şi bătrâni, să fie bombardate spitale, case, trenuri, poduri. Ei, politicienii, sunt singurii care ştiu ce e bine pentru noi şi pentru ţară" - scria, la rândul său, şi 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 şi călău decât la modul sârbesc: când el persecută, violentează, jefuieşte, 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 şi-a început cariera de cetnik gâtuind mâţa (vecinului), şi

a sfârşit prin a tortura, a arde de vii femei şi copii (dar ne-uitând ca, în elanu-i patriotic - şi 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, brăţările, lănţişoarele 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 şi fără interese de-o parte ori de alta nu poate lua în serios asemenea aberaţii. Iar de Paul Goma, pe care, cândva, în timpul lui Ceauşescu, îl admiram, ţi se face de-a dreptul milă pentru cât de mult s-a lasat prins în mrejele propagandistice ţesute cu atâta abilitate de către N.A.T.O. Dar acesta a fost primul e-razboi mondial şi 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. Maşina propagandistică a lucrat excelent. Din păcate, în joc s-au prins destui intelectuali români cărora, acum, când Kosovo se află sub protecţia N.A.T.O. (care se pare că mai mult protejează mafia albaneză şi traficul de droguri şi nicidecum enclavele cu sârbii care au mai rămas), când copiii sârbilor merg la şcoală sub escortă, iar obiective culturale şi religioase sârbeşti, destule aflate pe lista UNESCO, sunt aruncate în aer, distruse şi scârnăvite de albanezi, nu mai dau dovadă de acelaşi zel în apărarea drepturilor omului.

Evident, războiul propagandistic prin mass-media a fost folosit din plin şi de către R.T.S., televiziunea naţională sârbă, şi de alte televiziuni iugoslave din acea perioadă. Cât despre epitetele cu care gratulau aceste posturi atât Alianţa Nord-Atlantică, cât şi diverse personalităţi occidentale, ele au fost tema colecţiei lui Predrag Timotić, care le-a făcut cunoscute pe lista de discuţii nato-agresija-na-srj.

Pentru N.A.T.O.: hoarde de gangsteri, piraţi ai văzduhului, haimanale fasciste, forţă mecanică brutală, hoarde bestiale, sălbăticiunile N.A.T.O., monştri N.A.T.O., agresori însetaţi de sânge, falăngi fasciste N.A.T.O., N.A.T.O. - alianţa răului, armada răului, seniorii războiului în imperiul ucigaşilor, democratia tomahawk într-o aventură războinică, ceată de sălbatici, canibali gigantici, tirani cu creier liliputan, monştri mongoloizi, conglomerat mongoloid, autoproclamaţi apostoli ai democraţiei în rolul celor mai periculoşi ucigaşi, businessmani cu puşcă, o urâtă amintire istorică, galeria de tipi ai lui Freud, vrăjitoarele N.A.T.O.-ului, maniaci îmbătaţi cu forţa, monştri ucigaşi însetaţi de sânge şi maşina lor de propagandă a minciunii, puternică maşină media prevăzută cu turbo-manipulatoarele CNN-ului, răufăcători impotenţi, semănătorii morţii, călăreţii apocalipsei, mutanţi, camarila militară regională, corporaţie internaţională monstruoasă, bandă războinică de fascişti, răufăcătorii încăpăţânaţi ai lui Goebbels, cei mai mari vandali ai secolului al XX-lea, sălbăticiunile lui Clinton, semănătoarele de fier ale morţii, proiectile răufăcătoare, satrapii întregii lumi, atacurile brutale şi răufăcătoare ale laşilor din America, gealaţii văzduhului, crimă a bestialilor piloţi N.A.T.O., dinaintea a cândva casei albe, iar acum a casei negre din Washington, hoardele aeriene ale răufăcătoarei alianţe N.A.T.O., nocturni ucigaşi cu sânge rece, nu ştim cum să le mai spunem.

Pentru Bill Clinton: bolnavul războiului, pedofilul bolnav, nestăpânitul barbar, amorezul mincinos, Adolf Goebbels Hitler Clinton, creatura Washingtonului, greşeală biologică, şeriful legii junglei, sălbaticul cu zâmbet ruşinos, preşedintele al cărui centru este în şliţ, răufăcătorul nervos.

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

Pentru Koffi Anan: cel nu îndeajuns de informat, cel care nu citeşte ştirile.

Pentru Madeleine Albright: uliul american, pocitania cu chip de femeie, şarpele 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 vreţi, un fel de… întoarcere, după palma primită, a celuilalt obraz. Un fel de rezistenţă sub teroarea Satanei. Românii ştiu perfect ce rol au jucat bancurile politice în timpul dictaturii comuniste. Sârbii şi-au întors şi ei obrazul. Şi ce anume a rezultat? Acum, când totul pare a se fi terminat, putem spune cu mâna pe inimă: mai multe şi splendide colecţii de bancuri, caricaturi, montaje fotografice şi graffiti. Cu autori mai mult sau mai puţin cunoscuţi. Dar care, datorită Internetului, şi-au îndeplinit pe deplin rolul de supapă psihică.

Aforisme:

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

o Când ataci spitalele cu bombe, ori eşti un criminal conştient, ori un ucigaş nebun, ori un … "american umanitar".

o Ai grijă, acum, Bill (Clinton), că l-ai supărat şi 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 piloţi americani cu o bicicletă!

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

o Fraţilor ruşi, nu mai filosofaţi atât, treceţi la răfuiala fizică!

o Avem şi noi minte şi putere, numai că ne lipsesc 300 de dolari.

o N.A.T.O. se comportă ca un huligan. Noi îi azvârlim pe-alde ăştia afară din cafenea!

o Aceasta este o lovitură dată umanităţii cu democraţia americană.

o Amerii vor să preia mass-media noastră… probabil cred că tuturor le plac desenele animate!

o Ei îşi au creaturile, noi, caricaturile!

o Nu putem primi trupele N.A.T.O., nu avem destule forţe să le asigurăm securitatea!

o Billy, te aşteptăm la ora 20, pe Podul Brankovo.

o Daţi poporului comici, nu politicieni!

o Vino repede, Bill… s-a sculat!

o Clinton, te iubesc… mort!

o Billy, te aştept pe tine şi compania ta la un pahar de vorbă…

o Hillary, nu-l lăsa să se înmulţească!

o Bill, tu eşti cea mai mare catastrofă umanitară!

o Dintre toate limbile, Clinton o cunoaşte cel mai bine pe-a Monicăi!

o Bill, azi-noapte am visat că nu mai exişti!

o Chelsea, aruncă-l pe tata din tren!

o Billy, de ce nu ţi se mai întorc avioanele! Dresează-le!

o Pentru războiul împotriva sârbilor, Pentagonul solicită Congresului alte cinci-şase miliarde. De ar fi avut sârbii aceşti bani ar fi ajuns deja la Washington!

o Cum se simt Clinton şi restul politicienilor care deja de o lună de zile nu au mai fost la WC din cauza situaţiei din Kosovo? Plini de sine!

o De-ar avea tomahawk-ul capul lui Madeleine Albright ar fi fost şi mai oribil!

o Dostoievski a fost un clarvăzător. A scris cartea "Idiotul" înainte de naşterea lui Clinton.

o Proletari din toate ţările, unde sunteţi?

o Criza kosovară este o criză de domeniul trecutului, N.A.T.O. este criza viitorului!

o CNN. Cinic. Neargumentat. Noutăţi.

o Am demonstrat că Pământul e rotund: ne-am căcat prin Orient, iar rahatul a ajuns până-n Occident!

o Boris, păi nu ţi-am spus să trimiţi popi, ci tunuri! Sloba.

o Iată rezolvarea: Milošević - secretar general al O.N.U.

o Noi suntem în realitate ceea ce doriţi voi să fiţi în filme.

o Doamne, să nu-i ierţi, au ştiut ce fac!

o Dacă avionul a fost invizibil, iar noi nu l-am văzut, cine a cheltuit muniţie pe degeaba?

o Doar hoţii, curvele şi N.A.T.O. lucrează noaptea!

o Fraţi sârbi, rezistaţi! Sârbii sunt alături de voi!

o Pacifişti din toată lumea, uniţi-vă… bombardaţi Serbia!

o Două luni mai târziu: Pace, pace, pace, nu e nimeni vinovat.

o Trimiteţi-ne trupe. Să umplem gropile.

o După război, Clinton şi 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., ţinteşte vaca vecinului, în zona 44,12 pe 38,13. Nu are importanţă cât costă.

o Garantăm ieşirea soldaţilor N.A.T.O. din Serbia pe orizontală.

o Albright, nu te-aş ciocăni nici măcar cu o piatră-n cap.

o America mai trimite trei sute de avioane. Înseamnă că atâtea au fost doborâte.

o Nu bombele inteligente sunt proaste, ci proşti sunt piloţii 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 iubeşte şi ne respectă atât de mult încât ne-a anunţat în limba sârbă că o să ne bombardeze

o Vorbeşte sârbeşte, 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 şi pe bucăţi.

o Clinton, tu eşti 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, puţin 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 comandoşi. 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 infracţiune: 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 aveţi avionul invizibil, noi avem dioptrii.
o Azi au decolat de la Aviano mai multe avioane. S-au întors şi mai multe.
o Moarte lui Clinton, Monica - poporului!
o Clinton, F-117 nu e bun. Încearcă un MIG!
o Clinton, să dea Dumnezeu să-ţi nască Chelsea un sârb.
o Aţi avut avioane invizibile, acum aveţi piloţi miopi.
o Intrarea în Serbia e liberă - ieşirea se plăteşte cu capul.
o Monica, a lui Sloba e mai tare.
o Hei... arde aripa avionului dumneavoatră!
o Dacă pentru dumneavoastră a fost invizibil, vă vom trimite o fotografie.
o Fraţi ruşi, în numele lui Hristos, trimiteţi rachete S-300.
o Iartă-i, Doamne, au mâncat vaci nebune.
o N-aveţi nici o şansă, Serbia e-n transă.
o Cine nu are nimic în cap, are în bombe.
o Bill, şi eu am păţit la fel. Murat.
o Serbia, cel mai mare consumator de avioane americane.
o Victor Cernomârdin + Bill Clinton = Cernobâl sârbesc.
o Europa, dormi liniştită! Serbia veghează.
o Monica, strânge din dinţi!
o Nu e bine să zbori până nu cresc aripile.
o Monica e bună, dar Tony e şi mai bun.
o Diferenţa dintre Hitler şi Clinton e că Hitler i-a fost credincios Evei Braun.
o Tony Bleeeeeer, oaie neagră!
o Scuzaţi, nu am ştiut 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 şi mâine avioane.
o Clinton, cel mai bun lucru care ţi se poate întâmpla în viaţă este să rămână Hilary văduvă.
o Americanii au primit două milioane de albanezi. Noi, un singur Kosovo. Nu înţeleg 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 şi basci!
o De ce nu reuşeşte N.A.T.O. să nimerească rezervoarele de benzină din Serbia Centrală, ci în principal case ţărăneşti? Tacticienii au priceput că rezervoarele de ţuică sunt un factor mult mai important al apărării şi o ţintă potenţial mai mare.
o Sloba: îţi mulţumesc, Clinton, pentru că în 20 de zile ai făcut ceea ce eu încerc de zece ani!
o Cum reacţionează "verzii" în Germania vizavi de participarea ţării lor în agresiunea asupra Iugoslaviei? Îşi schimbă denumirea în "verzi-măslină".
o Nu arunca gunoi, nu hrăni animalele sălbatice şi piloţi pierduţi!
o Poate că americanii ştiu să facă bombe inteligente, dar nu şi politicieni deştepţi.
o Departe ideea că sârbii sunt un popor celest. Ei caută salvarea îndeosebi sub pământ.

o Cum te poţi răzbuna cel mai bine pe ţările N.A.T.O.? Bucurându-te sincer să primească refugiaţi din Kosovo cât mai mulţi.

o Raportul institutului meteorologic: deasupra Iugoslaviei este în continuare vreme frumoasă; plouă cu găleata.

o Monica, acum lasă-mă şi pe mine puţin! Tony Blair.

o Dacă începe aici cel de-al treilea război mondial, poate ne vor recunoaşte drepturile de autor.

o "Titanic", mândria Flotei a VI-a.

o Cel mai nou blestem: Dar-ar Dumnezeu să-ţi 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 şi două locatoare.

o Poate ar trebui să se strângă bani pentru a le da piloţilor posibilitatea să vadă pe cine şi pe ce aruncă bombe: cumpăraţi-le ochelari, iar testul la alcool să fie obligatoriu!

o Fratele meu îi ajută pe albanezi: le trimite regulat muniţie prin ţeavă!

o Tot mi se pare că Bill are deficit de minte şi suficit de piloţi.

o Lui Clinton îi lipseşte Princip (Gavrilo).

o F-117 suferă de epilepsie. Dr. Freud.

o Ei nu înţeleg 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 şi pirateria

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

Tot „Mediafax“ precizează că „Organismul (B.S.A., n.n.) a semnalat că regiunea Asia-Pacific, Europa de Est şi America Latină continuă să fie «punctele fierbinţi 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 şi în România? Directorul general al B.S.A. EMEA (Europa, Orientul Mijlociu şi Africa), Steven Frantzen, spunea în iunie 2004: „Regiunea Europei Centrale şi de Est se confruntă cu provocarea creşterii economice şi cu tradiţionalul respect redus pentru drepturile de proprietate

intelectuală. De aceea, nu este surprinzător că această regiune înregistrează cea mai ridicată rată a pirateriei software. Totuşi, trebuie luaţi în consideraţie unii factori care vor ameliora această situaţie, cel mai important fiind aderarea la Uniunea Europeană a unor state din regiune, fapt care va determina aplicarea mai eficientă a legislaţiei 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 şi în România şi se înscrie în linia generală a activităţilor derulate până în prezent. Planul în cinci puncte poate reuşi numai cu sprijinul Guvernului, al administraţiei locale, al asociaţiilor profesionale şi al altor instituţi şi autorităţi. Îmbunătăţiri reale pot să apară numai printr-un cadru legal modern şi aplicarea legislaţiei, cu ajutorul sprijinului public, la toate nivelurile, pentru proprietatea intelectuală şi industriile din domeniile de creaţie a proprietăţii 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 autorităţile româneşti.

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

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

„România liberă“ scria despre un „Hacker albaiulian, maestru în «ţepe virtuale»“ care, abia ieşit din liceu, a scos aproape 30 000 USD de la „fraieri americani“. „Fost elev al unui liceu cu profil informatic din judeţul 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 licitaţi on-line «e-Bay», sub identitatea cărora ar fi indus în eroare mai mulţi cetăţeni americani. [...] Păgubiţii plăteau între 200 şi 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 bucureştean „România liberă“ titra: „Piraţii informatici reuşesc să scape cu pedepse derizorii sau chiar basma curată“. De unde şi până unde o asemenea concluzie la autorul articolului, respectiv o cunoscută ziaristă din Timişoara pe nume Laura M. Forţiu. Ne permitem să preluăm un fragment din acest material: „Instanţele timişorene s-au confrunat în ultima vreme cu o adevărată «explozie» de cauze având ca obiect fraude prin Internet. Startul, să spunem aşa, a fost dat de celebrul deja Mircea Harapu, un tânăr de 24 de ani, care a reuşit 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 informaţii confidenţiale, în care apăreau inclusiv seriile cărţilor de credit ale persoanelor care au avut relaţii de afaceri cu firma. Aşadar, după ce a extras 15 fişiere ce conţineau date confidenţiale despre clienţii companiei, timişoreanul a contactat conducerea firmei şi i-a

solicitat suma de 5 000 de dolari pentru a nu face cunoscute informaţiile obţinute. Reprezentanţii companiei au anunţat însă imediat FBI, care a luat legătura cu specialiştii Centrului Zonal pentru Combaterea Crimei Organizate şi Antidrog Timişoara. Harapu a fost prins în flagrant tocmai când s-a prezentat la bancă pentru a ridica o parte din banii pretinşi. Deferit justiţiei sub acuzaţia comiterii infracţiunilor de şantaj şi violarea secretului corespondenţei, Mircea Harapu a fost condamnat de Judecătoria Timişoara la trei ani închisoare. Surpriză însă! Tribunalul Timiş, o instanţă-campion la achitări cu cântec, a admis recent apelul aşa-zisului hacker şi l-a scos în final nevinovat."

Nici Iaşul nu se lasă mai prejos. „România liberă scria, sub semnătura Deliei Ştefănoaie: „Cyber-spărgătorii de maşini au îngenuncheat Poliţia Iaşi", cu subtitlul: „O bandă de informaticieni sparge cele mai sofisticate sisteme de alarmă cu ajutorul laptopurilor şi al dispozitivelor de ultimă generaţie, lăsând limuzinele încuiate". În context, un poliţist de la Secţia 3 Poliţie din Iaşi declara: „Vin cu laptopurile şi un dispozitiv special de spargere a codurilor de acces, care substituie comenzile. Uşile se deschid şi infractorii pătrund în interior. Poartă mănuşi chirurgicale şi nu lasă nici o urmă. Taie cu cleşti speciali cablurile casetofoanelor şi ale CD-playerelor sofisticate şi le scot din locaşurile lor. Golesc torpedourile şi apoi încuie la loc maşinile. Lucrează extrem de curat. Suntem depăşiţi de tehnica lor."

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

Luni, 12 mai 2003, cotidianul bucureştean „Adevărul" titra: „Pentru a pune capăt valului de fraude comise prin Internet, IGP a înfiinţat un serviciu de luptă împotriva infracţionalităţii cibernetice". Oricare dintre metodele de luptă utilizate pe Internet în 1999, în timpul agresiunii NATO asupra Iugoslaviei, poate fi considerată infracţionalitate cibernetică. După ce dă drept exemple negative faptele comise la Bucureşti, Braşov, Cluj-Napoca, Craiova, Argeş şi Timişoara, „Adevărul" spune că „Valul de fraude prin Internet, puse la cale în special de tinerii pasionaţi de calculatoare, au pus pe jar conducerea IGP (Inspectoratul General al Poliţiei, n.n.), care a decis să înfiinţeze un serviciu specializat în combaterea infracţionalităţii cibernetice. Noua structură va funcţiona în cadrul Direcţiei Generale de Combatere a Crimei Organizate şi Antidrog (DGCCOA) şi va avea poliţişti în fiecare centru zonal al Direcţiei." Referindu-se la victimele predilecte ale fraudelor cibernetice înfăptuite de români, autorul articolului spune că e vorba de cetăţeni din S.U.A. şi Europa Occidentală.

În cotidianul timişorean „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 neindentificat, a atacat site-ul IPJ Timiş şi a distrus întreaga bază de date. „Moise, care a folosit porecla DarkHate, a lăsat şi un mesaj: «Lăsaţi lumea să bea în scara blocului! Că asha-i frumos! Promitem să ne cuminţim şi ne lăsăm de hacking şi vă lăsăm site-ul în pace.»" Este vorba despre bucureşteanul Valentin Moise, care a fost acuzat de acces fără drept la un sistem informatic, prin încălcarea măsurilor de securitate şi perturbare gravă, inacceptabilă, a funcţionării unui sistem informatic, prin ştergerea datelor informatice. El a fost condamnat la doi ani de închisoare cu suspendare condiţionată a executării pedepsei. Totodată, el a fost obligat să plătească IPJ Timiş 10 000 USD cu titlu de despăgubiri. Tot Daniela A. Budici scria în cotidianul timişorean „Agenda zilei": „Cinci tineri timişoreni care au tras pe sfoară peste 60 de cetăţeni americani cu câteva zeci de mii de dolari au fost condamnaţi de către Judecătoria Timişoara."

Şi dacă tot suntem la Timişoara... Laura M. Forţiu titra în „România liberă“ din 16 februarie 2004: „Costel Balint, acuzat de complicitate la o înşelăciune de proporţii“. Iar în subtitlu: „51 de americani au fost traşi pe sfoară, plătind sume grele în dolari pentru produse electronice... inexistente; misiunea revoluţionarului era aceea de a ridica valuta din bancă şi 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 şi cele în apărare nu au fost (cel puţin pe moment) suficiente pentru a convinge instanţa de judecată de vinovăţia sau nevinovăţia revoluţionarului acuzat de complicitate la înşelăciune astfel încât magistraţii să poată da un verdict.“

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

Se pare că, totuşi, ceva începe să se mişte şi în România. În aprilie 2004, a fost lansat la Iaşi primul comitet local de iniţiativă al Coaliţiei „proIntelect“ (**www.prointelect.ro**). Acesta reuneşte personalităţi din diferite medii (universitar, de afaceri, administraţie, procuratură, poliţie) interesate să facă ceva pentru a pune capăt furtului uriaş şi generalizat din domeniul proprietăţii intelectuale, care afectează economia, dar şi statul în acelaşi timp. Printre scopurile sale se numără şi informarea asupra riscurilor pirateriei şi a gravităţii fenomenului de furt din domeniul proprietăţii intelectuale din România. Coaliţia îşi propune să atragă atenţia tuturor românilor că furtul de proprietate intelectuală este o infracţiune la fel de gravă ca şi furtul de bunuri, care poate fi pedepsit atât civil, cât şi penal, iar cei care continuă să pirateze se expun unor pedepse grave, dar şi faptul că rata pirateriei este unul dintre elementele care dau măsura societăţii româneşti. Iniţiativa ieşenilor a avut ecou la Cluj-Napoca, iar apoi, la 30 iunie 2004, şi la Timişoara. Fiecare comitet local al Coaliţiei „proIntelect“ va edita un buletin lunar. Din păcate, dacă membrii coaliţiei nu vor da dovadă de maximă agresivitate în lupta lor împotriva pirateriei IT, dacă nu-i vor „urechea“ cu fermitate pe cei puşi şi plătiţi să aplice o legislaţie deja existentă pentru apărarea dreptului de autor, nu vor fi altceva decât încă o mişcare/grupare ai cărei membri îşi plâng unul altuia pe umăr fără a fi în stare să dea jos drobul de sare.