Çështje të Sigurisë

Security Issues

Revistë e përtremuajshme

2007

5

Botim i Institutit për Demokraci dhe Ndërmjetësim

NATO OTAN

BOTIMET TOENA TIRANE

IDN

ÇËSHTJE TË SIGURISË

Nr. 5 2007

Financuar nga:

Divizioni i Diplomacisë Publike të NATO-s, Bruksel
Shtëpia Botuese Toena

ÇËSHTJE TË SIGURISË

Security Issues

Revistë e përtremuajshme mbi sigurinë

Instituti për Demokraci dhe Ndërmjetësim

Nr. 5, Tiranë 2007

PËRMBAJTJA

IGLI TASHI*
SOLANGE GHERNAOUTI – HÉLIE**

VENDI I SIGURISË SË INFORMACIONIT NË STRATEGJINË E SIGURISË KOMBËTARE

Në njërin krah siguria kombëtare si koncept, konsiderohet si garante e ushtrimit të të drejtave të njeriut, dhe si e tillë është një nga detyrat më të rëndësishme të një shteti. Kjo garanci, sipas nenit 12 të deklaratës së të drejtave të njeriut, duhet të përmbushet nga një forcë publike, e cila të mbrojë në mënyrë të barabartë interesat e gjera të gjithë popullsisë dhe jo vetëm të atyre të cilëve ajo iu është besuar.

Në krahun tjetër, në këtë fillim të shekullit XXI, informacioni, i trajtuar në të gjitha format e mundshme, elektronike apo tradicionale, përbën një pasuri të vërtetë si për individët ashtu dhe për organizmat privatë apo shtetërorë dhe konsiderohet si një burim strategjik, rreth të cilit zhvillohet ajo që sot quhet shoqëria e informacionit. Nuk është hera e parë që teknologjia dhe inovacionet e lidhura me të, janë në bazën e ndryshimeve të thella për shoqërinë: dje, me

---

*Ekonomist / Master në juridik, për çështjet ligjore dhe të sigurisë në kibernetikë.
Kërkim pasuniversitar dhe asistent-lektor.
Fakulteti i Biznesit dhe Ekonomisë, Universiteti i Luizanës Zvicër.
** Profesor
Fakulteti i Biznesit dhe Ekonomisë Universiteti i Luizanës.
Ekspert ndërkombëtar për krimet kibernetike dhe çështjet kibernetike të sigurisë.
Anëtar i grupit të ekspertëve të nivelit të lartë - Unioni i Telekomunikacionit Ndërkombëtar.

inovacionet në fushat e energjisë dhe sot, me mënyrat e larmishme të komunikimit të njohurive dhe informacioneve nëpërmjet teknologjive të reja të telekomunikacionit. Ky koncept i shoqërisë së informacionit, si një vazhdimësi e shoqërisë industriale të disa viteve më parë, vë në qendër të saj informacionin dhe njohuritë, si dhe mënyrën e përcjelljes së tyre pa limite gjeografikë dhe kohorë. Teknologjitë e telekomunikacionit (dhe ndërmjet tyre më e përdorura është interneti) duke qenë të përdorura gjerësisht, janë një vektor shumë i rëndësishëm dhe i pashmangshëm për shumicën e aktiviteteve. Ky realitet ilustrohet me vendin gjithnjë e më të rëndësishëm që po zë në jetën tonë të përditshme ajo që quhet hapësira virtuale *(cyberspace)*, e cila po ndryshon gjithnjë e më shumë kufijtë tradicionalë kohorë dhe gjeografikë dhe mënyrën e të jetuarit e të menduarit në ditët e sotme.

Në këtë prizëm, informacioni si një motor ekonomik i zhvillimit, është një e mirë jomateriale që kërkon një mbrojtje në lartësinë e vlerave dhe rëndësisë së tij, nga ana e individëve, organizmave dhe mbi të gjitha, të Shtetit.

Krimet që synojnë manipulimin, fshirjen, modifikimin, survejimin, spiunazhin e informacioneve që qarkullojnë në rrjetet e komunikimit mund të prekin direkt interesat e një individi, të një organizmi, apo dhe të një Shteti. Kështu, siguria e informacionit është e lidhur direkt me sovranitetin e një shteti, e cila kalon nga mbrojtja e infrastrukturave kritike, e sistemeve dhe e rrjeteve, e pasurive kulturore të kombit, e të mirave materiale dhe jomateriale, e përmbledhur në një fjalë të vetme: mbrojtja e vlerave.

Në rrethet e specialistëve të sigurisë, marrja në konsideratë e problematikës së sigurisë së informacionit, shpeshherë trajtohet si problem i lidhur tërësisht me një dimension teknik e shpeshherë si një demagogji apo problematikë virtuale. Fatkeqësisht, faktet i kanë dhënë të drejtë vetëm pjesërisht kësaj mënyre të menduari. Në të vërtetë, këto sulme virtualë kanë pasur rezultate më se realë, me një bilanc shumë negativ për organizmat publike apo privatë. Sa për të ilustrim, le të marrim shembullin e Estonisë, një shtet sovran dhe anëtar i organizmave euro-atlantike, siç përmblidhen sot rëndom në

gjuhën e politikës që konsumojmë përditë, organizmat e Komunitetit Evropian dhe të NATO-s. Pas heqjes së statujës së ushtarit sovjetik nga një park i kryeqytetit të Estonisë, një sulm masiv mbi infrastrukturat e informacionit të Estonisë, bëri që këto infrastruktura të ndalonin së funksionuari duke krijuar kështu një kaos total në ekonominë e vendit. Ky sulm përdori një teknikë jo shumë të komplikuar "përmbytjeje" *(flooding)* nëpërmjet kompjuterëve fantazmë *(bootnets)* mbi infrastrukturën estone, gjë e cila mbingarkoi rrjetin në një mënyrë të atillë, saqë ky i fundit nuk mundi ta përballonte ngarkesën dhe pushoi së funksionuari. Ministri i mbrojtjes së Estonisë Jaal Aavisko do të deklaronte për gazetën "The New York Times"[1]: Kemi të bëjmë me një situatë që prek sigurinë kombëtare, të krahasueshme me një situatë ku portet tuaja bombardohen nga deti. Në këtë prizëm rezultatet e një sulmi virtual janë efektivisht më shumë se realë. Dhe me të vërtetë dezinformacioni po përdoret gjithnjë e më shumë si një pjesë integruese e politikave strategjike të organizmave dhe shteteve.

Interneti nga specifika e tij, është një terren ideal për të përhapur e pështëritur dezinformim si dhe për të manipuluar masa të mëdha njerëzish, me qëllimin për të mbjellë pasiguri. Në 2006, rrjeti i Ministrisë së Mbrojtjes së një shteti sovran, u bë objekt i një sulmi nga ana e disa *hacker*-ve, të cilët arritën të fusnin në këtë rrjet disa komunikime zyrtare për shtyp me informacione të pavërteta në lidhje me një skandal korrupsioni të pavërtetë, që gjoja kishte përfshirë ministrinë në fjalë. Specialistët arritën ta zbulonin këtë fakt, por fatkeqësisht shumë vonë, vetëm pasi e panë të botuar lajmin nëpër shumë gazeta kombëtare dhe ndërkombëtare. Dëmi? Jomaterial (i ngjashëm me sulmin) dhe shumë i vështirë për t'u llogaritur, por me rezultate të prekshme mbi imazhin e kësaj ministrie brenda dhe jashtë vendit.

Domosdoshmëria për të përndjekur, mbikëqyrur dhe dënuar krimin kibernetik vjen si rrjedhojë e postulatit "Çfarë është ilegale jashtë rrjetit, mbetet ilegale dhe brenda tij". Lufta kundër

[1] http://www.nytimes.com/2007/05/29/technology/29estonia.html

kriminalitetit të çfarëdo natyre qoftë ai, i përket organizmave të sigurisë, të financuara më së shumti nga taksapaguesit e vendit. Si një krim i njëjtë me atë "tradicional", krimi kibernetik duhet marrë parasysh e trajtuar me të njëjtin seriozitet. Krimi kibernetik duhet konsideruar si një adaptim i mënyrës së të vepruarit të kriminelëve ndaj realitetit të sotëm, të cilin e përshkruam më sipër. Si rrjedhim dhe lufta kundër tij duhet të jetë në përputhje me realitetin. A nuk do të ishte një çështje e sigurisë së brendshme mbrojtja e infrastrukturave dhe kredibilitetit të institucioneve financiare të vendit apo mbrojtja e integritetit të fëmijëve ndaj fenomenit të pedofilisë? Jo pa qëllim zgjodhëm këto dy fenomene, të cilat në botën e interkonjektuar kanë marrë një hov të jashtëzakonshëm. Po cilat janë karakteristikat që e bëjnë internetin dhe botën e ndërlidhur në të cilën jetojmë, një terren fertil për farën e krimit?

Natyra dhe specifikat e krimit

Nga natyra, teknologjitë e reja janë në evolucion të vazhdueshëm dhe për rrjedhojë dhe rreziqet e lidhura me këtë teknologji evoluojnë në të njëjtën mënyrë. Scott Peck, një psikiatër i njohur amerikan dhe autor i suksesshëm librash shkruan: "E vetmja mënyrë për të pasur siguri në jetë është të njohësh pasigurinë". Në fakt, krimi kibernetik duhet distancuar pak nga një nocion i përgjithshëm i asaj që quhet krimi informatik. Ky i fundit lidhet me një aktivitet kriminal që ka si objekt apo si mënyrë të kryerjes së krimit, kompjuterin. Krimi kibernetik, pra, është në këtë prizëm një nënkategori e krimit informatik dhe ka të bëjë me veprimtarinë kriminale të zhvilluar në rrjet *(network)*. Interneti është një nga rrjetet më globale dhe më të përdorur sot. Pas këtij saktësimi, mundemi të evidentojmë që qenia në rrjet na ekspozon ndaj rrezikut të një sulmi të mundshëm. Do të ishte joprofesionale këshilla e një shkëputjeje nga rrjeti, sepse në strukturën ekonomike të sotshme gjithnjë e më shumë globale, shkëputja do të shndërronte organizmin në një njësi jokonkurrente.

Një aspekt tjetër që duhet trajtuar për të kuptuar fenomenin e krimit kibernetik, është dhe teknologjia e përdorur e cila mbetet pak a shumë jotransparente për përdoruesin.

Nga një këndvështrim teknologjik mund të përmendim faktin që Interneti është një teknologji publike e hapur për të tërë. Historikisht, rrjeti komunikues u zhvillua si një mjet i fushës ushtarake për t'u përdorur më pas nga universitarët për të lehtësuar komunikimin ndërmjet tyre. Ky vizion mbi përdorimin bëri që në fillesat e saj, teknologjia e internetit të mos përfshinte aspektin e sigurisë, përderisa komunikimi (si në rastin ushtarak, ashtu dhe në atë universitar) bëhej ndërmjet njerëzve që njiheshin dhe që kishin besim te njëri-tjetri. Teknologjia e internetit është një teknologji *"best effort"*. Kjo do të thotë që në konceptimin e saj "bëmë atë çfarë mundëm" për të arritur në rezultatin e dëshiruar, pa imagjinuar se çfarë devijimi mund t'i bëhej përdorimit të tij.

Nga një këndvështrim i rrjetit dhe i sistemit, në rastin e internetit kemi të bëjmë me një liri të madhe për sa i përket konfigurimit, mënyrës së trajtimit segmentar të sigurisë dhe ç'është më e rëndësishme në rastin tonë, mungesës totale të kontrollit. Jo më kot interneti identifikohet si "rrjeti i rrjeteve" dhe shpesh struktura e tij krahasohet me rrjetën e merimangës.

Nga një këndvështrim legal, Interneti është i konceptuar dhe funksionon në një mënyrë të tillë, që për të, nocioni i kufijve nuk ekziston. Në fushën juridike një krim në radhë të parë sanksionohet nga një ligj. Ky ligj i përket një shteti të caktuar dhe zbatohet nga një gjykatë kompetente e një shteti të caktuar. Nocioni i shtetit është i lidhur ngushtë me nocionin e territorit, pra me kufijtë shtetërorë. Kjo ndikon shumë në fazën e përndjekjes së krimit.

Me të tilla karakteristika, rrjeti nuk mund të mos jetë një terren pjellor për krimin. Së pari, krimineli do të shkojë atje ku gjenden vlerat më të çmueshme. Të mbështetur mbi këtë logjikë besoj se të gjithë biem dakord mbi faktin që vlera më e çmuar, si për organizmat privatë, ashtu dhe për ata shtetërorë, gjendet tek informacionet e përcjella gjithnjë e më shumë nga teknologjitë e informacionit. Së dyti, organizmat kriminalë duke vepruar në një mënyrë racionale do të veprojnë në

terrenin më të favorshëm, me një raport përfitimi më të madh dhe më pak të rrezikshëm, duke goditur shënjestrën më të lehtë. Kush më shumë se një terren opak dhe anonim, si ai i internetit mund të ofrojë të tilla mundësi? Pyetje shumë normale e të lidhura shumë ngushtë me luftën kundër krimit janë shumë të vështira për të gjetur përgjigje në botën virtuale. Si të tillë mund të përmendim problematikën e shenjave dhe provave në botën numerike. Cila do të ishte vlera e një prove numerike në një sistem gjyqësor të caktuar, në raport me provat materiale "tradicionale"?

Çështje teknike apo çështje sigurie?

Krimi tradicional mund të cenojë sigurinë e brendshme të një vendi, po ashtu edhe krimi kibernetik mund të këtë pasoja të rënda në këtë aspekt. Përmendëm më sipër një fenomen shumë shqetësues dhe objekt të rëndësishëm të sigurisë së brendshme, si pedofilia, e cila është amplifikuar me përdorimin në masë të teknologjive të reja. Po sa të përgatitur janë fëmijët tanë në lidhje me këtë fenomen? Çfarë mjetesh apo strategjish u ofrojmë ne atyre për të mos rënë pré e këtij akti katastrofik për jetën dhe integritetin e tyre? E pra, është fakt që më shumë se 70% e kontakteve të para ndërmjet kriminelit dhe fëmijës, bëhen nëpërmjet teknologjive të *chat*-it dhe të *forum*-eve. Sa internet kafe' ekzistojnë në territorin tonë dhe cila është pjesa më e madhe e klientelës? Cila është përgjegjësia e këtyre bizneseve në këtë kontekst? A janë të ndërgjegjshëm këta biznese për rrezikun që mund të vijë nga aktiviteti i tyre? A kanë këta të fundit një obligim monitorimi mbi aktivitetin që zhvillohet në kompjuterët e tyre? Këto pyetje të shumta mund të gjejnë apo jo një përgjigje nga ana e të interesuarve. Por një gjë është e sigurt, shteti ka për detyrë të mbrojë fëmijët dhe për këtë duhet të vërë në lëvizje gjithë mekanizmat e tij që të ketë sa më pak krime të kësaj natyre.

Po krimi ekonomik nuk përbën një fushë që do të cenonte rëndë sigurinë kombëtare të një shteti sovran? Çfarë vendi zë fenomeni i korrupsionit dhe lufta kundër tij në strategjinë e

sigurisë së brendshme? Një gjë është e sigurt dhe për këtë shifrat na japin të drejtë - krimi ekonomik po e zhvendos gjithnjë e më shume fushën e tij të veprimit në aktivitete *on-line*, si mënyra më e lehtë dhe më fitimprurëse. Le të përmendim këtu rastin e Bankës së Sicilisë në vitin 2000, ku një grup prej 20 personash, natyrisht me njohuri specifike në fushën e informatikës dhe të lidhur me disa familje mafioze, arritën të krijonin një klon të servisit "e-banking" të bankës. Kështu, arritën në këtë mënyrë të përvetësonin shumën prej 400 milionë$, të vëna në dispozicion nga Komuniteti Europian për zhvillimin rajonal. Le të mos shkojmë më larg se 2 javë më përpara, ku 420 shtetas shqiptarë u mashtruan me një skemë vjedhjeje, tashmë të njohur si ajo e lotarisë, dhe falën kursimet e tyre kush e di se ku e kujt? Kush janë përgjegjësitë në këtë ngjarje?

Para disa ditësh nga ana e qeverisë u komunikua lajmi i mirë që tani aplikimet për tenderë do të bëhen nëpërmjet internetit. Kjo natyrisht do të thotë shërbim më cilësor e më i shpejtë. Po cilat janë rreziqet që një ndërmarrje e këtillë të bjerë pré e sulmeve të personave të interesuar për destabilizim e përfitim? Sa jemi të përgatitur për të përballuar këto sulme dhe mbi të gjitha n.q.s. sulmi fatkeqësisht del me sukses, çfarë jemi gati të humbim dhe çfarë ka vlerë më të madhe? Pa u përgjigjur këtyre pyetjeve, nuk mund të imagjinojmë masat teknike që duhen marrë.

Le t'i kthehemi pak çështjeve më tradicionale të sigurisë kombëtare si p. sh. mbrojtja e kufirit, parandalimi i kriminalitetit transfrontalier, apo dhe mbrojtja e infrastrukturave kritike (siç janë burimet e energjisë, të ujit të pijshëm, kontrollit të mallrave ushqimorë apo mjekësorë etj.). Pavarësisht që këto që përmendëm mund të jenë shumë të ndryshme në natyrën e tyre, një gjë i bashkon në epokën ku jetojmë - menaxhimi nëpërmjet teknologjive kompjuterike. Dëmi do të ishte i njëjtë si ai i një eksplozivi në një nga infrastrukturat, ashtu dhe dhënia e një komande të gabuar në sistemin e drejtimit. Dëmi do të ishte i njëjtë si kalimi natën i një krimineli dhe futja e tij në territorin tonë, ashtu dhe fshirja e të dhënave të tij kompromet uese në kompjuterët apo serverët

e policisë. Dëmi do të ishte po i njëjtë si futja e mallrave të skaduar apo të rrezikshme në territorin tonë, ashtu dhe falsifikimi i të dhënave në lidhje me këto mallra.

Një nocion shumë i përfolur këto kohët e fundit është dhe ai terrorizmit kibernetik *(cyberterrorism)*. Dhe këtu spekulimet janë të shumta: disa e quajnë demagogji, disa e quajnë realitet. Në fakt është e vërtetë, me internetin nuk mundesh të vrasësh njerëz direkt. Po indirekt? A nuk ekzistojnë vallë me miliona website të financuara kush e di nga kush që bëjnë një propagandë aktive në favor të kësaj apo asaj organizate? Më keq akoma a nuk ekzistojnë me qindra website që të mësojnë se si të fabrikosh bomba artizanale? Kundër kujt do të përdoren? Komenti mbi këtë realitet do të ishte tepri, ajo çfarë nevojitet është kundërpërgjigjja e organeve të specializuara.

Po interneti a mund të konsiderohet si infrastrukturë kritike e denjë pra për t'u mbrojtur? Ndoshta një përgjigje më realiste mund t'ua japë qeveria e Estonisë apo ministri i tyre i brendshëm, apo i mbrojtjes.

Integrimi i strategjisë së sigurisë së informacionit

Shpeshherë siguria trajtohet në një mënyrë segmentare, duke implementuar zgjidhje të veçanta për probleme të shkëputura. Specialistët e sigurisë bien të gjithë dakord mbi faktin që, elementi siguri, qoftë ky në kuptimin tradicional të fjalës apo në atë kibernetik ose virtual, duhet vendosur e ideuar në themelin e strukturës të cilën duam të mbrojmë. Për të realizuar sa më mirë këtë objektiv, një strategji gjithëpërfshirëse nevojitet. Pa këtë strategji nuk do të mundemi të implementojmë zgjidhjet më efikase dhe të kemi rezultat. Nga mungesa e një strategjie, turizmi ynë përfaqësohet nga një natyrë e mrekullueshme, të cilën dalëngadalë po e betonojmë e po e prishim me ndërtime vend e pa vend e mbi të gjitha, pa harmoni. Le të mos bëjmë të njëjtin gabim.

Reflektimi i një strategjie të sigurisë kombëtare që të përmbledhë brenda saj dhe një strategji mbi sigurinë e informacionit është e domosdoshme. Kjo strategji do na

detyrojë të reflektojmë mbi natyrën e vlerave që ne dëshirojmë dhe gjykojmë që duhen mbrojtur.

Në kuadrin e një strategjie gjithëpërfshirëse mund të përcaktojmë se cilat janë rreziqet që na kanosen, cili është realiteti që ne duhet të përballojmë, cili është probabiliteti që këto rreziqe të realizohen dhe cili do të jetë impakti i tyre mbi vlerat apo asetet që duam të mbrojmë. Vetëm në këtë mënyre do të mundemi të vëmë në vend, mjetet më efikase për parandalimin e rreziqeve. Vetëm ndërtimi i një strategjie koherente do të na mundësojë të kuptojmë në cilin segment gjendet ajo hallka e dobët që rrezikon gjithë sistemin. Dhe e gjitha kjo nuk mund të zgjidhet vetëm me një implementim të masave teknike, por duke kuptuar dhe integruar funksionimin e teknologjisë, proceseve dhe faktorit human.

Të luash me frikën e njerëzve është një metodë jo pak e përdorur nga organet e sigurisë të prirura shpeshherë nga një rritje e buxhetit apo përfitime të natyrave të ndryshme. Megjithatë logjika e këtij refleksioni u motivua nga diçka diametralisht e kundërt. Thonë që po të mos e dish e të mos veprosh është gabim, por po të dish e të vazhdosh të mos veprosh, është faj.

Objektivat e revistës "Çështje të Sigurisë" janë: (1) informimi i një publiku të specializuar mbi çështje të sigurisë kombëtare; (2) informimi i publikut mbi NATO-n dhe procesin e integrimit të Shqipërisë; (3) krijimi i një forumi diskutimi mbi sfidat kombëtare dhe globale ndaj sigurisë njerëzore. Këta objektiva revista do t'i realizojë nëpërmjet botimit në faqet e saj të informacionit mbi zhvillimet në NATO dhe misionet e saj nëpër botë, artikujve analitikë nga specialistë dhe analistë vendas dhe të huaj mbi sigurinë, procesin e integrimit në NATO, bashkëpunimet rajonale për sigurinë dhe sfidat ndaj sigurisë në rrethanat e tanishme globale. Revista do të afrojë autorë të mirënjohur nga Shqipëria dhe të huaj.

The objectives of the Security Issues are: (1) informing a specialized public on isues of national security; (2) informing the public at large on NATO; (3) creating a discussion forum on national and global challenges to human security in Albania and developing efficient strategy to meet them. These objectives will be fulfilled through the publication of information about developments in NATO and its missions throughout the world, analytic papers by native and international experts and analysts on security, processes of integration to NATO, regional cooperations on security and on challenges to security in contemporary global setting. The journal will engage well-known Albanian and foreign authors.