Elektronska obveščevalna dejavnost - ELINT

Robert Brumnik, Iztok Podbregar, Bernarda Tominc

Povzetek:

Namen prispevka
Države izvajajo razne oblike obveščevalne dejavnosti, da bi identificirale varnostna tveganja in na ta način poskušale najti kriminalce in teroriste. Elektronska obveščevalna dejavnost ali z angleško kratico ELINT (Electronic Intelligence) obsega zbiranje obveščevalnih informacij prek elektronskih sredstev. ELINT vključuje RADINT (Radar Intelligence), COMINT (Communications Intelligence) in TELINT (Telemetry Intelligence)[1]. Pri tem, je nujno potrebno upoštevati možnosti terorističnega delovanja na kritično informacijsko infrastrukturo, katere namen je krmilti vitalne dele, za zagotavljanje temeljnih življenskih procesov v družbi. Osnovni namen elektronskega elektronske obveščevalne dejavnosti je pridobivanje podatkov, ki bi bili preventivno koristni za preprečevanje kriznih situacij ali v primeru spopada.

Metodologija
Prispevek vsebuje pregled sodobnih elektronskih tehnologij v obveščevalni dejavnosti. Hkrati ocenjuje aplikativno vrednost uporabe identifikacijskih tehnologij v funkciji elektronskega obveščanja.

Ugotovitve
Zaradi odvisnosti družbe od informacijsko-komunikacijskih tehnologij in sistemov ter njihov nadzor, lahko v prihodnosti predstavlja najsodobnejšo in tehnološko najbolj sofisticirano obliko, terorističnega delovanja. Kadar govorimo o terorizmu najprej pomislimo na izvedeno fizično nasilje in marsikdo je mnenja, da je informacijski terorizem predvsem pojavna oblika, katere namen je sejati strah s teroristično grožnjo, saj naj bi bilo nemogoče z informacijskimi tehnologijami fizično ogrožati prebivalstvo. To dejstvo postavlja elektronsko obveščevalno dejavnost in vojskovanje v enakovreden položaj ostalim konvencionalnim oblikam vojskovanja.

Praktična uporabnost
ELINT oblika izvidovanja in obveščanja, se je začela z razvojem informacijsko-komunikacijske tehnologije, njen hiter razvoj pa se je pojavil v obdobju hladne vojne. Operacije elektronskega izvidovanja in obveščanja so:

- zbiranje informacij o nasprotnikovi obrambi (vrsta in položaji vojaških enot, radarjev, protiletalskih sistemov, infrastruktura,..),
- zbiranje informacij o pomembnih postavitvah ali objektih (premičnih in nepremičnih) nasprotnika,
- prisluškovanje nasprotnikovim komunikacijam.

Zbiranje informacij se izvaja prek satelitov ali telekomunikacijskih sistemov. Zavedati se je treba, da postaja internet ter telekomunikacijska infrastruktura vedno bolj razširjeno in pomembo sredstvo za pridobivanje informacij, propagandno delovanje, komuniciranje in načrtovanje operacij.

[1] Telemetry Intelligence; Zrakoplovna telemetrija, je telemetrični nadzor zračnih in vesoljskih plovil, uporaba frekvenc predpisana v Ur.l.RS, 10/2006, 17/2006

Izvirnost/pomembnost prispevka
Prispevek obravnava identifikacijsko tehnologijo, kot možen pripomoček elektronske obveščevalne dejavnosti.

Ključne besede: elektronska obveščevalna dejavnost, elektronsko vojskovanje, identifikacijski sistemi

1 UVOD

V obdobju po hladni vojni je terorizem postal najpomembnejša varnostnopolitična tema tudi v državah, ki sicer niso bile neposredno ogrožene. Skozi preteklost si strokovnjaki pri splošni obravnavi in definiranju pojava (Kaj terorizem sploh je?) največkrat niso bili enotni. Ne glede na to, da pojem zgodovinsko izvira že iz časov francoske[2] revolucije, pa večina definicij največkrat izpostavlja uporabo sile ali nasilja z namenom ustrahovati prebivalstvo. Takšen način se kaže v v spremembi odnosa do posameznih (varnostnih, obrambnih in zunanjih) politik neke države. Glede ustrahovanja pa je seveda jasno, da brez medijev in danes pomembnih interaktivnih informacijskih in komunikacijskih tehnologij o terorizmu ni mogoče govoriti. Dandanes imamo tako več splošnih opredelitev terorizma, zato se težave pojavijo, ko je potrebno definicijo praktično uporabiti v sodobnih konfliktih. Medijsko posredovanje in prikaz terorističnih dejanj omogoča pojavitev občutka strahu in zaznavo ogroženosti, ki je mnogo večja od tiste, ki jo kažejo podatki o številu žrtev ali poškodovanih v napadih.

Ali se sodobne informacijske tehnologije, ki nam v večini primerov koristijo in skrajšajo operativni izvedbeni čas opravil ter v mnogih primerih celo rešujejo življena, lahko uporabijo tudi v uničevalne namene?

Odgovor je lahko zelo enostaven. "Kot vsako drugo orodje lahko tudi računalnik uporabimo zlonamerno - s posledico oškodovanja". Samo oškodovanje se pri tej obliki kriminala največkrat res ne pokaže neposredno, vendar so posredni učinki delovanja lahko katastrofalni (Nass in Brave, 2005).

2 OPREDELITEV POJMA "INFORMACIJSKI TERORIZEM"

O informacijskem terorizmu govorimo, ko so zaradi terorističnih napadov na kritično informacijsko infrastrukturo fizično ogrožena življenja in premoženje prebivalstva ter moteno normalno delovanje družbe. Pri nas se na srečo to še ni zgodilo. Seveda pa to ne pomeni, da pojav tehnično ni mogoč oziroma izvedljiv.

Mehka verzija definicije informacijskega terorizma izpostavlja predvsem informacijske in komunikacijske tehnologije, ki jih teroristi uporabljajo za izvajanje pritiska in propagando, namenjeno javnosti, in mobiliziranje ter rekrutiranje novih podpornikov (Müller, Wille, Björn, 2004). Za razliko od tradicionalnih komunikacijskih medijev je internet kot najzmogljivejše komunikacijsko sredstvo vse pomembnejši tudi za komuniciranje in načrtovanje operacij prostorsko in organizacijsko dislociranih terorističnih organizacij (Weimann, 2005). Le-te

[2] Francoska revolucija; Izraz »terorizem« izhaja iz francoskega obdobja v letih 1793 in 1794 (med francosko revolucijo). Uporabljali so ga vodje sistematskega odstranjevanja »izdajalcev« med revolucionarnimi odbori, z njim so namreč imenovali najboljšo možnost za obranitev svobode url: http://sl.wikipedia.org/wiki/Terorizem (21.05.2008).

danes niso hierarhično in centralizirano organizirane, ampak povzemajo sodobne mrežne oblike (celice).

Ne glede na različna izhodišča in odprta vprašanja pa ostaja nesporno dejstvo, da so informacijske in komunikacijske tehnologije sredstvo in hkrati cilj terorističnega delovanja v 21. stoletju.

3 "INFORMACIJSKI TERORIZEM" V PRAKSI

Teroristične organizacije in kriminalne združbe pri svojem delovanju vse bolj uporabljajo novo tehnologijo. To dokazujejo vsakdanji primeri, saj se po svetu vrstijo aretacije, pri katerih imajo pripadniki različnih terorističnih celic pri sebi najmodernejšo računalniško opremo. Po terorističnih napadih v New Yorku, 11. septembra 2001 se je med varnostnimi strokovnjaki okrepilo mnenje, da bodo informacijski sistemi ena od naslednjih tarč (Weimann, 2005). Za povečanje učinkovitosti odkrivanja teroristov je bilo potrebno povečati nadzor nad ljudmi ter sprejeti dodatne varnostne ukrepe.

Soočanje z dinamično globalizacijo informacijskih družb v povezavi s tehnološkimi izboljšavami (npr. lokalne brezžične povezave) povečuje možnosti medsebojnega povezovanja. Širjenje storitev in uporabnikov pa povečuje tudi ranljivost in ogroženost, ki se je večina med nami sploh ne zaveda. V poročilu[3] ameriškega sveta za znanost in tehnologijo so tako opredelili naslednje tehnološke trende, ki povzročajo skrbi in povečujejo ranljivost informacijske frastrukture.

- Vse večja kompleksnost informacijskih sistemov predstavlja varnostni izziv za razvijalce in uporabnike.
- Telefomunikacijska infrastruktura se vedno bolj razvija, pri čemer se tradicionalni telefonski sistem in informacijska tehnologija vse bolj združujeta v enotno platformo.
- Vse hitrejša širitev brezžičnih komunikacijskih sistemov zelo povečuje možnosti zlorab. V tem primeru namreč tradicionalni obrambni pristop (securing the perimer) ni učinkovit, saj nimamo fizičnega nadzora nad uporabniki in napravami.
- Vse večja je prepletenost in dostopnost na računalniku temelječih sistemih, ki postajajo kritični oz. ključnega pomena za ekonomijo, logistiko, razširjanje dobrin in storitev.
- Globalnost ITK povečuje število nasprotnikov za uporabnike v domačem in mednarodnem prostoru.

Znano je, da je treba delovati na več področjih, uskladiti ukrepe različnih družb in akterjev kriminalne prevencije, v nasprotnem primeru se pokaže, da levica ne ve, kaj desnica dela. Zavedanje o tem bi moralo biti prisotno pri vseh snovalcih kriminalitetne politike (Meško, 2000).

4 ELEKTRONSKA OBVEŠČEVALNA DEJAVNOST (ELINT)

V izogib sodobnim pojavnim oblikam terorizma je torej potrebno zagotoviti sofisticiran koncept identifikacije deviantnega obnašanja, ki zahteva prožnost in hitrost izvajanja.

[3] Poročilo ameriškega sveta za znanost in tehnologijo (Federal Plan for Cyber Security and Information Assurance Research and Development); url: http://www.nitrd.gov/pubs/csia/FederalPlan_CSIA_RnD.pdf (21.05.2008)

S hitrim razvojem informacijske in telekomunikacijske tehnologije se je temu primerno razvila in posodobila tudi obveščevalna dejavnost. Segment obveščevalne dejavnosti, ki za zbiranje obveščevalnih informacij uporablja elektronska sredstva, imenujemo elektronska obveščevalna dejavnost ali z angleško kratico ELINT[4] (Electronical Intelligence).

Osnovni namen elektronskega izvidovanja je pridobivanje podatkov, ki bi bili koristni v primeru zagotavljanja nacionalne varnosti. Operacije elektronskega izvidovanja so:

- zbiranje podatkov o nasprotnikovi obrambi (vrsta in položaji vojaških enot, radarjev, protiletalskih sistemov, itd.),
- zbiranje podatkov o pomembnih postavitvah ali objektih nasprotnika in
- prisluškovanje nasprotnikovim komunikacijam.

Ta vrsta izvidovanja je doživela posebno hiter razvoj v obdobju hladne vojne in je danes v sodobnih nacionalno varnostnih sistemih nepogrešljiv element zagotavljanja kakovostnih informacij. Za izvajanje operacij, ki spadajo v okvir ELINT-a, je nujno potrebno zagotoviti usposobljen kader z visokim nivojem praktičnega poznavanja delovanja informacijsko telekomunikacijskih tehnologij. Ob tem pa obveščevalno dejavnost opredeljujejo legalna, strokovna in etična načela, kar je še zlasti pomembno zaradi njene posebne občutljivosti – le-ta namreč vključuje posege v človekovo zasebnost, kar predstavlja določena varnostna tveganja. Delo posega na področje tajnosti podatkov, kar ob zagotovitvi visoko strokovno usposobljenega kadra zahteva ljudi s prav tako visokimi moralnimi kriteriji. Zahtevana kriterija pa sta si lahko tudi izključujoča, saj je znano, da so lahko prav ljudje[5] z največ računalniškega znanja motivirani z interesi združb, ki ne delujejo v korist nacionalne varnosti neke države.

4.1 Echelon[6]

Echalon je sistem, ki so ga Američani skupaj z zavezniki razvijali več kot 20 let. Sistem elektronskega nadzorovanja je bil vzpostavljen že med hladno vojno. Ideja tega sistema je, da bi ob pomoči zmogljivih računalnikov vzpostavili sistem globalnega nadzora telekomunikacij. Sistem ima seveda svoje omejitve. Dejstvo, da sistem Eshalon obstaja, še ne pomeni[7], da je mogoče prestreči prav vsako informacijo, ki potuje po telekomunikacijskem omrežju.

Je Echelon uporaben tudi za prisluškovanje mobilnih telefonov?

Mobilna telefonija ima relativno kratek domet. V kolikor bi imeli postavljene posebne prisluškovalne postaje na terenu, pa bi bilo to bilo možno. Potrebno je namreč reproducirati mikrovalovno dogajanje na posameznem mestu in potem izolirati posamezne signale. Vendar ideja sistema Eshalon ni osredotočenost na posameznika. Področje obdelave (Slika 1.) je celoten telekomunikacijski sistem.

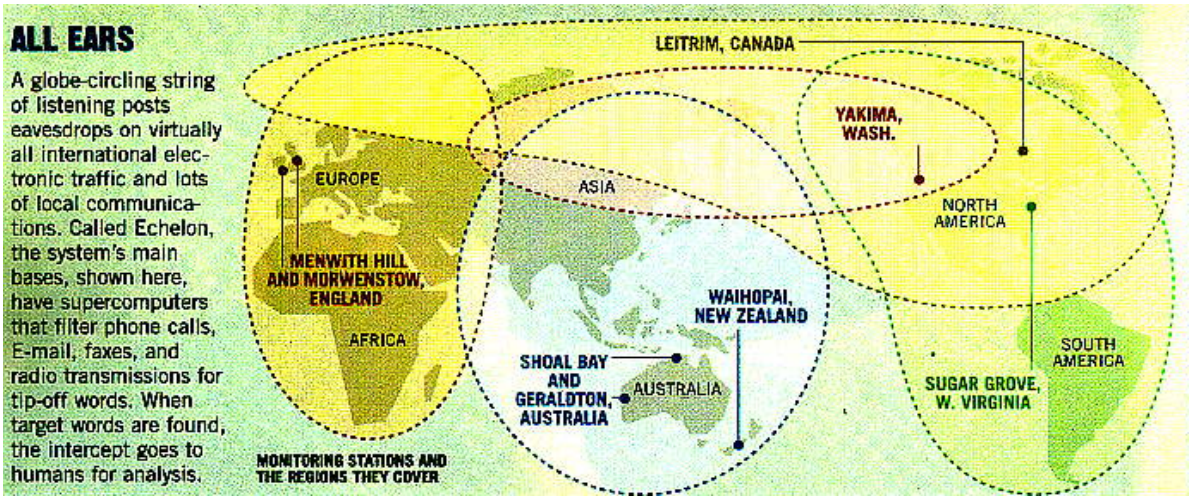
---

[4] ELINT(Electronic Intelligence); Elektronsko izvidovanje(ELINT) zajema več metod in sicer; SIGINT(Signals Intelligence), TELINT (Telemetry Intelligence), COMINT(Communications Intelligence) , MASINT(Measurement and Signature Intelligence), RADINT (Radar Intelligence) url: http://www.milnet.com/inttop.htm (20.05.2008)..

[5] Tipi kiberkriminalcev; M. Rogers je identificiral osem tipov kiberkriminalcev, ki se med seboj razlikujejo po sposobnostih in motivaciji. V sedmo skupino je razvrstil profesionalne kriminalce, ki so specializirani v industrijsko vohunjenje, delujejo po naročilu-proti plačilu, so visoko izobraženi in motivirani, imajo dostop do najnovejše tehnologije in v osmo skupino(najvišjo po stopnji/teži kriminalnih dejanj) je razvrstil informacijske bojevnike(kiberteroriste) so dobro finančno podprti, pogosto politično motivirani, vendar z omejenim znanjem. url: http://www.networkworld.com/supp/2004/cybercrime/112904profile.html (19.05.2008).

[6] Echelon; je ime, ki označuje varovano svetovno razširjeno signalno-obveščevalno in analitično mrežo, ki jo upravlja skupnost imenovana UKUSA. UKUSA je združenje petih angleško govorečih držav in sicer Velike Britanije, Združenih držav Amerike, Kanade, Avstralije in Nove Zelandije. Obstoj Echelona je prvič omenil Duncan Campbell leta 1988.

[7] Pri uporabnosti Echelona prihaja do omejitev, zlasti pri optičnih povezavah. V preteklosti se je večino mednarodnih komunikacij (point-to-point) izvajalo preko radijskih valov, kasneje preko satelitov, sedaj pa 99% (statistika za leto 2006) vseh pogovorov teče preko optičnih kablov, za kar so ogromni prisluškovalni sistemi neuporabni Za prestrezanje informacij preko optičnih kablov pa se je potrebno dejansko fizično priključiti na optične vode (lep primer je ravno afera SOVA, ko so Nemški agentje prisluškovali preko optičnih kablov Telekoma), kar pomeni, da ima Echelona omejene kapacitete in lahko prestreza samo del komunikacij url: http://www2.blog.siol.net/2007/08/19/echelon-usesa-zahodnega-sveta/ (19.05.2008).



Slika 1: Področja, ki jih pokrivajo postaje sistema Echelon

Vse telekomunikacije, ki potekajo prek satelitov, mikrovalovnih zvez ali prek kablov,[8] položenih na dnu morja, je mogoče nadzorovati. Ogromne količine podatkov, ki vsak trenutek potujejo preko telekomunikacijskih sistemov, so lahko nadzorovane. V trenutku, ko obveščevalne agencije prestrežejo tok podatkov, jih obdelajo z računalniki. Vsa elektronska pošta, telefaksi, vedno pogosteje pa tudi telefonski klici, so tako rekoč obdelani v trenutku, ko so poslani. Računalnik lahko podatke obdela glede na to, kdo jih pošilja, išče lahko specifične telefonske številke ali naslove elektronske pošte, išče lahko ključne besede v sporočilih, kombinacije besed. Obveščevalci, ki krmilijo računalnike, določajo ključne besede, kombinacije besed, telefonske številke in naslove, ki jih velja nadzorovati.

5 INFORMACIJSKA ORODJA[9] ZA BOJ PROTI TERORIZMU

5.1 Računalniška forenzika

Kadar želimo v dokaz osumljenemu uporabiti dokaze, ki jih je ta že zbrisal iz računalniškega diska, se poslužimo računalniške forenzike. S posebnimi orodji[10] lahko restavriramo in izluščimo računalniške dokaze ali poskrbimo za njihovo ohranitev in predstavitev.

Zbrisanih podatkov namreč operacijski sistem fizično ne odstrani z diska, temveč odstrani le povezave do njih. Dokler le-ti niso prepisani z novimi podatki (metoda očiščenja[11]) ali nepreklicno brisani s posebnimi orodji[12], jih je mogoče z ustrezno programsko opremo obnoviti.

---

[8] Obstajata dva načina prestrezanja informacij, ki potujejo preko podmorskih kablov; če pogledamo, kako potekajo podmorski kabli, vidimo, da znaten del teh kablov pride do ameriškega ozemlja, ali pa gredo v Kanado, Avstralijo ter Veliko Britanijo. Ko torej kabli pridejo iz morja, lahko agencije, ki se ukvarjajo z ELINT, prestrežejo podatkovne tokove. V Angliji, je tako postavljena orjaška zemeljska ELINT postaja, nedaleč od vozlišča britanskega telekoma. Manj zanesljiva pa je varianta, ko podmornica v bližini kabla postavi prisluškovalno napravo.

[9] Informacijska orodja; url: http://news.netcraft.com/archives/2004/01/30/wwwscocom_is_a_weapon_of_mass_destruction.html (10.04.2008).

[10] Orodja (za restavriranje); Npr. PC Inspector Smart Recovery Program je namenjen reševanju podatkov na pomnilniških karticah različnih tipov. Med drugim je sposoben rešiti datoteke na kartici, ki smo jo formatirali ali iztaknili iz naprave med procesom pisanja nanjo.
BinaryBiz je še en program za okolje Windows, med najzmogljivejši in tudi najdražji. Reševanje je mogoče v različnih primerih, med drugim po formatiranju diska ali preoblikovanju njegovih particij. Program je zmožen rešiti izbrisana sporočila elektronske pošte.

[11] Očiščenje; Tehnika očiščenja (purging) zagotavlja uničenje podatkov do te mere, da jih sorazmerno z njihovo pomembnostjo ni mogoče obnoviti niti z laboratorijskimi tehnikami. Ta tehnika je uporabna, ko pomnilniškega medija ne bomo ohranili v varnem okolju.

[12] Orodja (za brisanje); Npr. AbsoluteShield File Shredder omogoča uničevanje datotek in map na preprost način, saj se program poveže v operacijski sistem. To pomeni, da datoteko ali mapo izbrišemo s klikom na desno tipko miške. Ta program ponuja dve metodi, in sicer hitro dvakratno ali zanesljivejše sedemkratno prepisovanje.

Pri preiskovanju podatkov, ki so predmet preiskave, ne smemo preiskovati v računalniku, kjer smo jih našli, temveč moramo najprej narediti kopijo diska, pomnilniške kartice ali katerega drugega pomnilniškega medija. Original tako ostane nedotaknjen, kar je bistveno za poznejšo sodno obravnavo.

5.2 Biometrija

Zaradi povečevanja mobilnosti populacije ter posledično globalizacije terorizma, je nujnost po razpoložljivosti globalnih informacij, s katerimi lahko identificiramo človeka na lokalnem nivoju, vedno večja. Zagotoviti moramo verodostojne in hitro dosegljive informacije ter upoštevati njihovo morebitno zaupnost.

"Teroristu je mogoče slediti edino s pomočjo biometrije[13]" (Michael Kirkpatrick[14], 2002). O uporabnosti biometričnih sistemov v boju proti terorizmu je dosti napisanega tako v strokovni literaturi kot znanstvenih člankih (Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism). V Sloveniji smo v fazi implementacije SIS_II (Schengenskega Informacijskega Sistema), ki omogoča vpogled v skupno evropsko bazo ter na osnovi tega lažjo identifikacijo terorista.

5.3 Kriptoanaliza[15] (primer GSM omrežje)

Digitalno telefonsko omrežje GSM uporablja vrsto kriptografskih protokolov kot so A3, A5 in A8, s katerimi poskuša zagotoviti določen nivo varnosti. Velika večina GSM operaterjev uporablja pri protokolu A3 in A8 algoritem COMP12814. Protokol A3 se uporablja za avtenticiranje uporabnikov v GSM omrežje, A8 pa za generiranje ključa seje, s katerim operira kriptografski protokol A5[16]. Ta je na voljo v več različicah: A5/0 (ne uporablja kodirnega mehanizma), A5/1 (osnoven kodirni algoritem), A5/2 (oslabljen kodirni algoritem) in A5/3 (imenovan tudi KASUMI, močnejši kodirni algoritem).

Napad na A5 je potreben, če želi napadalec prisluškovati pogovorom v GSM omrežju, na A3 in A8 pa, če želi opraviti kloniranje SIM kartice. Če povzamem: napadi na GSM omrežja so možni in so prav verjetno tudi dejansko prisotni. Seveda pa je dandanes moderna kriptografija visoko presegla kriptoanalizo, saj obstaja kar nekaj kriptosistemov[17], ki jih ni mogoče zlomiti. Po drugi strani pa ne smemo pozabiti na druge učinkovite metode, kot so prestrezanje, uporaba fizične sile, bočni napadi, mobilni virusi[18], kvantni računalniki[19] itd.

---

[13] Biometrija; je proces zbiranja, proučevanja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije in avtentikacije. url: http://whitepapers.zdnet.co.uk/0,1000000650,39000644q,00.htm (28.08.2008).

[14] Michael Kirkpatrick; direktor FBI 2002 url: http://www.fbi.gov/congress/congress04/033004kirkpatrick.htm (28.08.2008).

[15] Kriptoanaliza; izvor besede gre verjetno iskati v grščini. Grška beseda kryptós pomeni skrito, beseda analýein pa sprostiti ali odvezati. Kriptoanaliza je študija metod za pridobivanje pomena kodiranih informacij brez dostopa do skrivne informacije, ki bi jo v normalnem primeru potrebovali. To navadno pomeni iskanje skrivnega ključa. Kriptoanaliza označuje tudi poskuse zaobiti varnosti drugih tipov šifrirnih algoritmov in protokolov na splošno (Stergaršek, 2006) in url: http://lkrv.fri.uni-lj.si/ (09.05.2008).

[16] Algoritma A5/1 in A5/2, ki sta bila razvita leta 1989, nista bila javno objavljena. Leta 1999 ju je s pomočjo vzvratnega inženirstva razbil Marc Briceno. Danes velja, da je možno oba algoritma razbiti v manj kot sekundi prestrežene komunikacije (Žagar, 2006).

[17] Kriptosistem RSA, kvantna kriptografija. Podani so predlogi za minimalne dolžine ključev, ki so potrebne za varen simetrični sistem (Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson, Wiener, 1996). Prisotna sta dva tipa kvantnih kriptografskih protokolov. Prvi tip uporablja polarizirane fotone v katere vkodira bite informacije in se zanaša na kvantno naključnost, kar preprečuje napadalcu, da bi prestregel podatke. Drugi tip uporablja soodvisne fotone, kjer naj bi se ti pravilno polarizirali (t.j. zasegli predvideno informacijo) šele, ko so opazovani (prebrani) od prejemnika. Vsako prestreganje oz. opazovanje kvantnih bitov spremeni njihovo vrednost. Napadalec lahko podatke prestreže, s tem dejanjem pa bo povzročil, da bodo podatki ob naslednjem opazovanju drugačni, kar bo prejemnik zaznal.

[18] Mobilnih virusov obstaja trenutno okrog 30 različic, ki si jih lahko ogledate na spletnih straneh url: http://www.symantec.com/search/ tako, da vnesete iskalni parameter: symbos (24.04.2004). Prvi dokaz koncepta med mobilnimi virusi je bil znan junija 2004 pod imenom Cabir in je napadal operacijski sistem Symbian.

[19] Kvantni računalnik je naprava, ki računa s superpozicijami kvantnih stanj. Pri kvantnih računalnikih se operira z valovnimi funkcijami, ki so edine primerne za opis stanj. Kvantni računalnik lahko v kratkem času izvede milijarde računskih operacij. S temi poskusi skuša razvozlati kriptirana sporočila. Računalniki, potrebni za prebiranje sporočil, ki potujejo prek telekomunikacijskih sistemov, se ne razlikujejo bistveno od običajnih računalnikov. Številne vladne in vojaške organizacije (npr. NATO) po svetu vlagajo velika sredstva v razvoj kvantnega računalništva za potrebe kritpografije in podobnih potreb vojaških obveščevalnih služb.

6 PROTIOBVEŠČEVALNA ZAŠČITA IN "INFORMACIJSKI TERORIZEM"

Obveščevalno varnostne agencije se v protiterorističnem in protiobveščevalnem segmentu dela soočajo z dejavnostjo, ki jo posameznik izvaja v daljših časovnih obdobjih, pri čemer znaten delež časa porabi za prikrivanje dejavnosti oziroma vključevanje v okolje, navezavo stikov z okolico ter pridobivanje zaupanja posameznikov, ki bi jih bilo možno izkoristiti za pridobivanje podatkov ali vključiti v sodelavsko mrežo. Za varovanje nacionalnih interesov je vitalnega pomena, da agencija takšne poskuse čim prej identificira ter pripravi primerne protiukrepe. V skladu s sprejetimi protiukrepi se izvajajo tehnične operacije z namensko informacijsko-telekomunikacijsko opremo[20].

7 ZAKLJUČEK ("NETWAR[21]" ALI SODOBNO VOJSKOVANJE PRIHODNOSTI)

Večplastni in večdimenzionalni varnostni izzivi, tveganja in grožnje v regiji, Evropi in svetu povzročajo številne negotovosti pri zagotavljanju nacionalne in mednarodne varnosti. Za pravočasno načrtovanje in izvajanje ukrepov za ohranjanje in krepitev tako nacionalne kot tudi mednarodne varnosti je potrebno vzpostaviti učinkovit sistem zgodnjega odkrivanja in opozarjanja na potencialna tveganja in grožnje. V skladu z navedenim morajo biti vzpostavljeni organizacijski, kadrovski in materialni temelji za sodelovanje in izmenjavo obveščevalnih in varnostnih podatkov na nacionalni ravni (po potrebi tudi institucionalizirani) v okviru dvostranskega sodelovanja ter v okviru zavezništev.

V tehničnem smislu nas seveda zanima, ali je komunikacija preko računalnika in spleta varnejša od tiste z mobilnimi ali navadnimi telefoni? Seveda je z nekaterimi razumnimi ukrepi mogoče povečati varnost, toda če povprečni uporabnik naleti na kakšnega 'hudega' hekerja ali motivirano kriminalno združbo, najbrž nima veliko možnosti. Lahko zaščitimo računalnike s požarnimi zidovi, s protivirusnimi programi, lahko pošiljamo sporočila, kodirana s šifrirnimi programi, kot je program PGP[22], lahko anonimno brskamo po spletu s programom Tor[23], toda nikoli ni izključena možnost, da bo kakšen poznavalec, kiberkriminalec ali tajna služba s sofisticirano opremo našla varnostno luknjo ali dekodirala sporočila. Sodobne obveščevalne službe in policija uporabljajo učinkovitejše in še bolj sofisticirane načine nadzora, kot smo jih navedli v prispevku. Ob tem pa je potrebno izpostaviti, da je pravna in zakonodajna podlaga v večini držav še na trhlih in nedorečenih temeljih.

Veljavni zakon ZSOVA v tretjem odstavku 24. člena določa kot rok za izvedbo kontrole pisem in drugih pošiljk ter nadzorovanja in snemanja telekomunikacij tri mesece, s podaljševanji po en mesec, vendar skupno čas izvajanja nadzora ne sme preseči šest mesecev. Zlasti zadnja

[20] Oprema za elektronsko protiprotiukrepanje (tj. oprema, zasnovana za oddajanje motečih ali napačnih signalov v radarske in radiokomunikacijske sprejemnike ali, ki kako drugače otežuje sprejem, delovanje ali učinkovitost nasprotnikovih elektronskih sprejemnikov, vključno z njegovo opremo za protiukrepanje) vključuje opremo za motenje in proti motenju ter opremo za motenje sistemov globalne satelitske navigacije ("Global Navigation Satellite Systems – GNSS") url: http://www.ignss.org/ (09.05.2008).
V podskupino te zvrsti opreme (naprav) bi lahko uvrstili še letala za elektronsko bojevanje, ki pa danes kot samostojna praktično izginjajo in izgubljajo svoj pomen zaradi dejstva, da so danes ustrezno opremo za elektronske protiukrepe in motenje že tako zmanjšali (ob enaki ali nekajkrat večji zčinkovitosti), da jo lahko v zabojniku nosi praktično vsak lovec ali lovski bombnik url: http://sierra5.net/index.php?option=com_content&task=view&id=349&Itemid=1 (09.05.2008).

[21] NetWAR spopad v informacijski sferi ali mrežna vojna pri čemer se "netwar" nanaša na konflikte in ambicije po nadzoru interneta in zajema "Information Warfare" in "Cyber Intelligence".

[22] Program PGP (Pretty Good Privacy), se uporablja za zaščito elektronske pošte in podatkovnih datotek. Omogoča komuniciranje, ne da bi potrebovali varen kanal. url: http://www1.fov.uni-mb.si/Studentske_strani/seminarske/pgp/default.html (24.04.2008).

[23] Tor je sistem (projekt), ki nastaja pod pokroviteljstvom organizacije Electronic Frontier Foundation. Trenutno gre za razvojno različico zbirke orodij, ki omogočajo anonimno brskanje po spletnih straneh, objavljanje vsebin, anonimno uporabo programov za neposredno sporočanje IM, IRC in SSH in drugih programov, ki slonijo na protokolu TCP. Sistem Tor zmanjša možnost, da bi vas našli, saj preusmeri promet prek večjega števila naključno izbranih strežnikov v omrežju, kar metodo analize prometa močno oteži, če ne celo prepreči. url: www.eff.org (23.04.2008)

omejitev predstavlja veliko pomanjkljivost pri delu agencije na protiobveščevalnem in protiterorističnem področju. Nadzor v sedaj dovoljenem časovnem obsegu omogoča samo osnovni vpogled v komunikacijo nadzorovanih oseb. Za kakovostna spoznanja in možnost sprejetja nekaterih zaključkov pa je s strokovnega vidika čas nadzora odločno prekratek za učinkovito preprečevanje kriminalnih ali terorističnih aktivnosti. Agenciji so tako onemogočena globlja spoznanja o metodologiji delovanja posameznikov oziroma celovita spoznanja o povezavah ter mreži oseb, s katerimi posameznik sodeluje. Za povečanje učinkovitosti posebnih oblik zbiranja podatkov v smislu kontrole pisem in drugih pošiljk ter nadzorovanja in snemanja telekomunikacij v Republiki Sloveniji (tretji odstavek 24. člena ZSOVA) je v pripravi zakon[24], ki predvideva podaljšanje časa trajanja uporabe posebnih oblik pridobivanja podatkov ter pristojnosti glede odrejanja in podaljšanja ukrepa uporabe posebnih oblik pridobivanja podatkov.

8 VIRI

1. Council of Europe, (2003) Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed
2. Europol, (2003) Computer-related crime within the EU: Old crimes new tools; new crimes new tools. Luxembourg: Office for Official Publications of the European Communities.
3. Deleuze, G., (2002) "Družba nadzora". V Filozofski vestnik, št. 3, letnik XXIII, Ljubljana: Filozofski inštitut ZRC SAZU.
4. Hager, N., (2001) Secret Power - New Zealand's Role in the International Spy Network, Craig Potton Publishing
5. Huey, L ., Rosenberg, R. S., (2004) Thoughts on Expanding Police Surveillance Opportunities under the Cyber - Crime Convention. V: Canadian Journal of Criminology and Criminal Justice, Volume 46, no. 5. 597–606.
6. Hutter, R., (2002) Cyber Terror-eine realistische Gefahr? url: http://www.aksis.de/Cyber-Terror.pdf (09. 05. 2008).
7. IFCC, International fraud compliant center, IFFC Annual Internet Fraud Report 2006. url:http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf (09.05.2008)
8. Kovačič, M., (2006) Nadzor in zasebnost v informacijski družbi, Filozofski, sociološki, pravni in tehnični vidiki nadzora in zasebnosti na internetu, Ljubljana, 2006.
9. Kučič L. J., Intervju z Jurijem Kebetom (MNZ): Prestopniška domišljija ne pozna računalniških meja. Delo, 2002.
10. Lyon, D., (1994) The Electronic Eye. Cambridge: Polity Press.
11. Müller, Wille, Björn, (2004) For our eyes only? Shaping an intelligence community within EU. Occacional paper No.50. Paris. Institute for security Study.
12. Podbregar, I., Slapar, M., (2006) Razsežnosti gospodarskega vohunstva v 21. Stoletju-primer gospodarskega vohunstva s pomočjo trojanskega konja, Bled, Dnevi varstvoslovja.
13. Potter Evan, H., (1998) Economic Intelligenc and national security. Ottawa: Carleton Uiversity press.
14. Singel, R., (2003) "Congress Expands FBI Spying Power". Wired News, 24. november, 2003. url: http://www.wired.com/news/politics/0,1283,61341,00.html. (09. 5. 2008).
15. Trampuž, M., (2002) "Izguba skrivnosti z nadzorovanjem": Bentham in nove tehnologije nadzorovanja. Magisterska naloga, Ljubljana.

[24] Predlog novega zakona ZSOVA, url: http://193.2.236.95/dato3.nsf/OC/0603140949103/$file/116v1.doc (19.05.2008)

16. Uredba Sveta (ES) št. 2252/2004 (2004) Standardi za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajajo države članice (Uradni list L 385, 29.12.2004, str. 1–6)
17. Whitaker, Reg. (1999) The End of Privacy. New York: The New Press.
18. Weimann, G., 2005. Cyberterrorismus ist einegroße, schwarze Wolke am Horizont. url:http://www.sicherheitheute.de/index.php?cccpage=readtechnik&set_z_artikel=200 (09.05.2008)
19. Žerdin, A., (2001) Tajni echelon, intervju z Nicky Hager url: http://www.mladina.si/tednik/200119/clanek/hager-intervju/ (09.05.2008)