UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Dušica Žolger

Informacijski vidik boja proti mednarodnemu terorizmu

Magistrsko delo

Ljubljana, 2012

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Dušica Žolger

Mentor: dr. Bogomil Ferfila
Somentor: doc. dr. Uroš Svete

Informacijski vidik boja proti mednarodnemu terorizmu

Magistrsko delo

Ljubljana, 2012

Zahvala

mentorju dr. Bogomilu Ferfili ter somentorju dr. Urošu Svetetu

za pomoč in strokovne nasvete pri nastajanju magistrske naloge.

Zahvaljujem se staršema in bratu za moralno in finančno pomoč pri študiju, ter prijateljici Jagodi za vzpodbudo.

Nalogo posvečam Bojanu, Sofii in Isabeli.

Univerza
v Ljubljani
Fakulteta
za družbene vede

Kardeljeva ploščad 5
1000 Ljubljana, Slovenija
telefon 01 58 05 122
01 58 05 120

I Z J A V A O A V T O R S T V U
magistrskega dela

Podpisana DUŠICA ŽOLGER, z vpisno številko 18280, sem avtorica magistrskega dela z naslovom: INFORMACIJSKI VIDIK BOJA PROTI MEDNARODNEMU TERORIZMU.

S svojim podpisom zagotavljam, da:

- je predloženo magistrsko delo izključno rezultat mojega lastnega raziskovalnega dela;
- sem poskrbel/-a, da so dela in mnenja drugih avtorjev oz. avtoric, ki jih uporabljam v predloženem delu, navedena oz. citirana v skladu s fakultetnimi navodili;
- sem poskrbel/-a, da so vsa dela in mnenja drugih avtorjev oz. avtoric navedena v seznamu virov, ki je sestavni element predloženega dela in je zapisan v skladu s fakultetnimi navodili;
- sem pridobil/-a vsa dovoljenja za uporabo avtorskih del, ki so v celoti prenesena v predloženo delo in sem to tudi jasno zapisal/-a v predloženem delu;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del, bodisi v obliki citata bodisi v obliki skoraj dobesednega parafraziranja bodisi v grafični obliki, s katerim so tuje misli oz. ideje predstavljene kot moje lastne – kaznivo po zakonu (Zakon o avtorski in sorodnih pravicah (UL RS, št. 16/07-UPB3, 68/08, 85/10 Skl.US: U-I-191/09-7, Up-916/09-16), prekršek pa podleže tudi ukrepom Fakultete za družbene vede v skladu z njenimi pravili;
- se zavedam posledic, ki jih dokazano plagiatorstvo lahko predstavlja za predloženo delo in za moj status na Fakulteti za družbene vede;
- je elektronska oblika identična s tiskano obliko magistrskega dela ter soglašam z objavo magistrskega dela v zbirki »Dela FDV«.

V Ljubljani, 27. septembra 2012 Podpis avtorice:

Informacijski vidik boja proti terorizmu

Povzetek

Ključ učinkovitega boja proti terorizmu so informacije. Zbiranje podatkov, pravilna interpretacija in preglednost zbranih podatkov, oblikovanje informacij in delitev informacij med institucijami oziroma resorji, ki se ukvarjajo z bojem proti mednarodnemu terorizmu, so predpogoj za uspešno preprečevanje terorističnih dejanj. Čimprejšnje oblikovanje učinkovitega koncepta sistemske varnosti, tako na nacionalnih kot na globalnem nivoju, je nujno. Samo uspešno in intenzivno sodelovanje med inštitucijami v ZDA in v Evropi ter zbiranje in preglednost podatkov na enem mestu zagotavlja uspešnost boja proti vse obsežnejšemu pojavu mednarodnega terorizma. Ker teroristične organizacije za svoje delovanje potrebujejo ogromno sredstev, velike finančne pritoke zanje pa predstavlja organizirani kriminal, so podatki s področja organiziranega kriminala nepogrešljivi pri oblikovanju informacij o delovanju terorističnih skupin. Dejstvo je, da so po napadih 11. septembra domala vse varnostne inštitucije pričele razvijati vrsto novih programov, namenjenih boju proti terorizmu na osnovi zbiranja in primerjanja podatkov, ki bi lahko morebitne nove napade preprečili. Kot sredstvo za uspešen boj proti terorizmu se danes z namenom identifikacije ter avtentikacije vse več uporabljajo biometrične metode, zaradi vse naprednejše tehnologije programi beležijo domala vsako izrečeno ali napisno besedo, med preprostim sprehodom do trgovine nas zabeležijo številne kamere. Nekoč le prstni odtisi, danes pa tudi skeniranje očesne mrežnice ali šarenice, prepoznava glasu, prepoznava obraznih oblik, DNA… Metode, ki lahko pogosto zagotovijo uspeh pri odkrivanju načrtovanja terorističnih dejanj, pa so mnogokrat v konfliktu z osnovnimi človekovimi pravicami in svoboščinami. Pomembno je namreč zagotavljanje ravnotežja med varnostjo in demokracijo ter človekovimi pravicami.

Ena ključnih ovir v boju proti terorizmu ostaja neenotna definicija tega pojava. Dogovor na tej ravni bi namreč izboljšal uspešnost delovanja nacionalnovarnostnega sistema v boju proti terorizmu; ključnega pomena je torej poenotenje stališč v mednarodni skupnosti.

Ključne besede: terorizem, zbiranje in izmenjava informacij, nadzor, človekove pravice

Fight against terrorism from the information aspect

Summary

The key of effective counter-terrorism is information. Data collection, transparency and the correct interpretation of collected data, and information sharing between institutions and departments dealing with the fight against international terrorism, is a prerequisite to preventing terrorist acts. Early concept of an effective system of protection, both at national and global levels is essential. Only a successful and intensive cooperation between institutions in the U.S. and in Europe, and the collection and transparency of data in one place, will ensure a successful fight against a growing phenomenon of international terrorism. Since terrorist organizations for their operation require huge funds, large financial inflows come from the organized crime, the information in the field of organized crime are indispensable in developing information on the operation of terrorist groups. The fact is that after the attacks of 11 September nearly all the security agencies began to develop a range of new programs aimed at combating terrorism, based on the collection and collation of data, which could prevent any new attacks. As a means to effectively combat terrorism today is to identify and authenticate increasingly used biometric methods, due to advanced technology programs are recorded almost every word said or inscription, the easy walk to the shops we recorded a number of cameras. Once only fingerprints, but today also retina scans, voice recognition, facial recognition, DNA. Methods, which can often ensure success in identifying the planning of terrorist acts, are often in conflict with basic human rights and freedoms. It is important of course to provide a balance between security and democracy and human rights. Despite the many interpretations, one of the key obstacles in the fight against terrorism remains fragmented definition of this phenomenon. Single, universally accepted definition of terrorism would improve the performance of the national security systems in the fight against terrorism. Therefore it is essential to standardize the views of the international community.

Key words: terrorism, data gathering, information sharing, surveillance, human rights

KAZALO

SEZNAM TABEL, SLIK IN PRILOG

SEZNAM KRATIC:

CECIS – Skupni urgentni in informacijski sistem (Common Emergency Communication and Information System)
CIA – Osrednja obveščevalna agencija, ZDA (Central Intelligence Agency)
DARPA – Agencija za napredne obrambne raziskovalne projekte (Defence Advanced Research Projects Agency)
DHS – Urad za domovinsko varnost (Department of Homeland Security)
EARS – (Effective Affordable Reusable Speach to text)
EELD – (Evidence Extraction and Link Discovery)
EU – Evropska unija (European Union)
FBI – Zvezni preiskovalni urad (Federal Bureau of Investigation)
FADO – (False and Authentic Documents Online)
FATF – (Financial Action Task Force)
GAO – (Government Accountability Office)
HSIN – (Homeland Security Information Network)
IACP – (International Association of Chiefs of Police)
IAO – Oddelek informacijskega zavedanja (Information Awareness Office)
IPTO – (Information Processing Techniques Office)
ISE – Okolje za izmenjavo informacij (Information Sharing Environment)
NATO – (North Atlantic Treaty Organization)
NSA – Nacionalna varnostna agencija (National Security Agency)
MATRIX – (Multi-state Anti-terrorism Information Exchange)
MI5 – britanska obveščevalna služba (Millitary Intelligence)
MONEVAL – (Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism)
NCTC – National Counterterrorism Center
NSA – National Security Agency
OECD – Organizacija za Ekonomsko sodelovanje in razvoj (Organization of Economic Coopeartion and Development)
OZN – Organizacija združenih narodov

SAC HQ – Štab strateških zračnih sil (Strategic Air Command)

SIS – (Schoengen Information System)

SSNA – (Scalable Social Network Analyses)

TIA – Popolno informacijsko zavedanje (Total Information Awareness ali Terrorism Information Awareness)

TIDES – (Translingual Information Detection Extraction and Summarization)

TSC – Terrorist Screeneing Center

UK – Združeno kraljestvo (United kingdom)

UNODC – Urad ZN za droge in kriminal (United Nations Office on Drugs and Crime)

VIS – (Visa Information System)

ZDA – Združene države Amerike

1 UVOD

Izraz terorizem izhaja iz obdobja med francosko revolucijo, poimenovanega »vladavina terorja« (1793/1794). Posluževali so se ga vodje sistematskega odstranjevanja »izdajalcev« v revolucionarnih odborih. Sicer se terorizem dojema kot ekstremno, tj. nasilno politično dejanje, katerega vzrok je konflikt. Čeprav enotne in globalno sprejete definicije terorizma ni, danes z besedo terorizem označujemo vsako organizirano nasilno dejanje, ki je usmerjeno proti civilistom ali civilnim ustanovam v politične ali gospodarske namene. Izvajajo ga nedržavne skupine ali države in je večinoma javno dejanje, saj želijo teroristi z njim zajeti čim več ljudi ter doseči kar se da veliko odmevnost, tudi s pomočjo sodobnih medijev, ki o incidentih poročajo. Lahko bi rekli, da terorizem določa predvsem narava dejanja, ne pa toliko identiteta in razlogi terorista za akcijo (Wilkinson in Stewart 1987, 26).

Napadi na Združene države Amerike 11. septembra 2001 so terorizem silovito postavili v središče pozornosti svetovne javnosti, saj postaja eden izmed virov ogrožanja nacionalne in mednarodne varnosti ter tako globalna grožnja, na katero se mednarodna skupnost mora odzvati. »Nacionalna varnost je politična in osebna dobrina, ki se v razvitih državah uresničuje kot temeljna človekova pravica« (Grizold 1999, 2–3). Država zanjo skrbi ne samo s sprejemanjem ustrezne zakonodaje, temveč tudi z angažiranjem celotne nacionalnovarnostne strukture. Za zaščito svojega pravnega reda in demokratične ureditve se država poslužuje institucij, kot so vojska, policija, obveščevalno-varnostne službe, sodišča. Predvsem obveščevalno-varnostna in policijska koalicija je v boju proti terorizmu vsaj tako, če ne pomembnejša od vojaške (Anžič 2002, 463). Sodobna nacionalna varnost je vpeta v širše mednarodno okolje, v katerem je odgovornost za zagotavljanje varnosti poleg samih držav in njihovih zvez vse bolj domena globalnega mednarodnega sistema (Grizold 1999, 2). Po napadih 11. septembra so se zgodili največji preobrati v delovanju obveščevalnih struktur. Tako v smislu medresorskega sodelovanja, npr. izmenjava informacij med obveščevalnimi in varnostnimi službami, kot tudi mednarodnega sodelovanja. Globalne grožnje in globalni varnostni izzivi potrebujejo sodelovanje in izmenjavo informacij na različnih ravneh znotraj države (intra- in

interresorno) ter zunaj države, dvostransko, znotraj EU in NATA, v OZN, v mednarodnih mirovnih operacijah itn. (Črnčec 2009, 15).

Ključ boja proti terorizmu so namreč informacije. Zbiranje podatkov, pravilna interpretacija in preglednost zbranih podatkov, oblikovanje ustreznih in uporabnih informacij, ter izmenjava informacij med inštitucijami oziroma resorji, so predpogoji za učinkovito spopadanje s terorizmom. Med pomanjkljivosti boja proti terorizmu lahko prištevamo prav in predvsem nezadostno sodelovanje in neučinkovito izmenjavo informacij med številnimi inštitucijami, ki bi morda teroristične napade lahko preprečile. Ameriški Zvezni preiskovalni urad FBI je tako šele maja 2002 v Washingtonu ustanovil eno prvih protiterorističnih skupin, ki naj bi imela pregled nad vsemi ameriškimi preiskavami na področju terorizma po vsem svetu. Tak program centralizira boj proti terorizmu in zagotavlja, da se vsi zbrani podatki natančno in urgentno preverjajo ter primerjajo z drugimi zbranimi podatki. (U. S. Department of State 2012). To pa je le del obširnejše reorganizacije FBI, med drugim tudi zaradi poročil, da naj bi urad prejel številna opozorila o načrtovanih samomorilskih napadih že pred 11. septembrom. Na zaslišanjih pred člani komisije za ugotovitev okoliščin terorističnih napadov na ZDA v Washingtonu so odgovorni poskušali pojasniti, zakaj jim ni uspelo preprečiti najhujših terorističnih napadov v ameriški zgodovini. Najbolj kontroverzni so bili odgovori nekdanjega protiterorističnega koordinatorja Bele hiše Richarda Clarka, ki je med drugim tudi v svoji knjigi " Against All Enemies" izrazil ogorčenje, da si je predsednik George Bush mlajši prizadeval za ponovno izvolitev na podlagi svojih uspehov proti terorizmu, čeprav naj bi pred 11. septembrom[1] to nevarnost zanemarjal.

Zbiranje določenih podatkov na enem mestu in nezmožnost primerjave s podatki, ki se zbirajo drugje, ni produktivno. Še več, tudi neorganizirane informacije niso nič drugega kot le podatki. Informacije so uporabne samo, če so organizirane (Drucker 2001, 124). Dejstvo je, da kdor ima informacijo, ima moč. Sodobna informacijska tehnologija danes omogoča posameznikom, skupinam in organizacijam razpolagati z ogromno količino

[1] Največje preoblikovanje nacionalno varnostnega sistema so ZDA doživele prav po napadih 11. septembra. Ti so sprožili največjo reformo nacionalnovarnostnega sistema po 2. svetovni vojni (Črnčec, 13).

podatkov. »Kdor ima možnost, da poveže različne skupine osebnih podatkov, ki so v različnih bazah podatkov ali so shranjeni na različnih tehničnih sredstvih, ima skoraj neomejene možnosti, da spremlja posameznika na vsakem koraku ter tako posega v njegovo zasebnost brez nadzora oz. njegove vednosti« (Črnčec 2009, 13).

Spremeniti in izboljšati pa se mora tudi sodelovanje ameriških inštitucij, ki se ukvarjajo z bojem proti terorizmu, s tovrstnimi v Evropi in v svetu nasploh. Sodelovanje, usmerjeno v bolj proti terorizmu, ki je po 11. septembru še intenzivnejše, poteka tudi v okviru Evropske unije. Članice Evropske unije razvijajo skupen pristop k preventivi in boju proti organiziranemu kriminalu, prioriteten pa je boj proti terorizmu. Skupen pristop zajema tesnejše sodelovanje med nacionalnimi policijami ter sodnimi in mejnimi organi.

Ker terorizem predstavlja grožnjo varnosti, svobodi in vrednotam Evropske unije ter njenim državljanom, je ukrepanje EU namenjeno zagotavljanju ustreznega, prilagojenega odziva v boju proti temu pojavu. In prav preprečevanje je ob zaščiti, pregonu in odzivu, eden izmed štirih stebrov celovitega pristopa pri ukrepanju proti terorizmu. EU si trdno prizadeva za preprečevanje in zatiranje terorističnih dejavnosti ter zaščito infrastrukture in državljanov. Obravnava tudi vzroke, sredstva in zmogljivosti terorizma. Usklajevanje med organi pregona in pravosodnimi organi v EU ter mednarodno sodelovanje sta prav tako pomembna za zagotovitev učinkovitosti boja proti temu nadnacionalnemu pojavu. Amsterdamska pogodba je oblikovala podlago za ukrepanje EU, a je takrat veljala samo za nekatere države članice. To ukrepanje se je pospešilo po terorističnih napadih – v Združenih državah leta 2001, v Evropi pa po dogodkih v Madridu in Londonu leta 2004 in 2005. (Boj proti terorizmu 2012).

Posebej pomemben v boju proti terorizmu je Europol, ki natančno analizira informacije držav članic in drugih mednarodnih partnerjev. Tudi v okviru Europola je bila ustanovljena posebna skupina protiterorističnih strokovnjakov. Sodelovanje med Europolom in ZDA pa je okronal še dogovor o prenosu osebnih informacij. Združene države Amerike in Evropska unija sta že kmalu po napadih 11. septembra ustanovili kontaktne točke med ameriškimi agencijami in Europolom ter Eurojustom. Amerika je v

Washingtonu že sprejela predstavnike Europola, ameriški agenti so obiskali Evropo. Sodelovanje je kmalu obrodilo prve sadove: identificirali so določene teroriste in teroristične organizacije, ki delujejo v Evropi, ter uspeli zamrzniti sredstva financiranja teh skupin (Europolovo poročilo 2011).

Dejstvo je, da so po napadih 11. septembra domala vse varnostne inštitucije pričele razvijati vrsto programov, namenjenih boju proti terorizmu; delujejo na osnovi zbiranja in primerjanja podatkov, ki bi lahko preprečili morebitne nove napade. Nekateri poskusni programi so celo ugledali luč sveta, kasneje pa zaradi pritiskov civilne družbe zaradi pomislekov o varovanju osebnih podatkov, pa tudi zaradi astronomskih stroškov, ugasnili. Med te spada tudi razvpit program MATRIX – Multi-State Anti-Terrorism Information Exchange. Program je nastal na Floridi in naj bi analiziral vladne in komercialne baze podatkov z namenom pravočasnega odkrivanja osumljencev ali njihovih lokacij. MATRIX so prvič predstavili v Beli hiši leta 2003. Kasneje se je širil, nato pa je, podobno kot program TIA (Total Information Awareness) zaradi pritiskov ACLU (ACLU 2004 – American Civil Liberties Union), da program omogoča podrobno preiskovanje in nadzorovanje posameznikov, leta 2005 ugasnil. Še več negodovanja pa je povzročilo odkritje o zveznem financiranju programa in visokih stroških, ki jih posamezne države, sprva vključene v program, več niso zmogle.

Za uspešen boj proti terorizmu pa ni pomembno le sodelovanje inštitucij, ki se ukvarjajo z bojem proti terorizmu, temveč tudi sodelovanje z inštitucijami, ki se borijo proti kriminalu nasploh. Primarni vir finančnih sredstev terorističnih organizacij namreč neredko predstavlja organizirani kriminal. Omejevanje finančnih virov je torej prav tako pomembna faza v boju proti terorizmu. Teroristične organizacije v primerjavi s preteklostjo danes redkeje financirajo države in se kot njihovi sponzorji pojavljajo v čedalje manjši meri. Ker pa teroristi za svoje delovanje potrebujejo ogromno sredstev, velik finančni vir zanje predstavlja organizirani kriminal, predvsem ilegalna trgovina z mamili. Organizirani kriminal danes ne pozna več meja. Govorimo o mednarodnih razsežnostih tega pojava, ki mu lahko rečemo tudi transnacionalni ali nadnacionalni organizirani kriminal. O tem govorimo, ko kriminalci, ki imajo bazo v eni državi,

prestopijo meje in zagrešijo kaznivo dejanje, nato pa se vrnejo v domovino; o kriminalu te vrste govorimo tudi takrat, ko kriminalna organizacija prenese svoje delovanje v dve ali več držav (Carter 1997, 139). Trgovina z drogo, pranje denarja, ponarejanje in črni trgi spadajo v mednarodni organizirani kriminal. Boj proti tovrstnemu kriminalu torej pomeni omejevanje finančnih virov terorističnih organizacij. Osama Bin Laden je bil npr. tipološko gledano terorist, ki se je za dosego svojih ciljev, predvsem za zagotovitev finančnih sredstev posluževal tudi metod organiziranega kriminala[2]. Svoje prepričanje o lastnem poslanstvu, svojo križarsko vojno proti »nevernikom« je združeval z znatnimi finančnimi sredstvi. Njegova skrajnost in denar sta privedla nazadnje do terorizma – do grozljive enačbe terorističnega globalnega akterja z imperijem financ in terorja, razpredenim po vsem svetu (Pohly 2001, 10).

Čim prejšnje oblikovanje učinkovitega koncepta sistemske zaščite, tako na nacionalnih kot na globalnem nivoju, je torej nujno. Samo uspešno in intenzivno sodelovanje med inštitucijami v ZDA in v Evropi ter zbiranje in preglednost podatkov na enem mestu zagotavlja uspešnost boja tako proti organiziranemu kriminalu kot posredno proti vse obsežnejšemu pojavu mednarodnega terorizma.

2 METODOLOŠKI OKVIR

2.1 Predmet raziskave

Osnovni namen magistrske naloge je opredeliti pomen informacij v boju proti terorizmu. Zbiranje podatkov, selekcija ter pravilna interpretacija podatkov so predpogoji za dobro informacijo.

[2] Podjetja pod krinko, lažne pogodbe in ropanje bank so namreč že na tretjem mestu metod zbiranja sredstev Al Kaide (glej tabelo 5.3).

V nalogi bom poskušala analizirati številne projekte in programe, namenjene zbiranju podatkov, ključnih za uspešno in pravočasno odkrivanje morebitnih načrtovanih terorističnih dejanj.

Kot sredstvo za uspešen boj proti terorizmu se danes z namenom identifikacije ter avtentikacije vse več uporabljajo biometrične metode; zaradi vse naprednejše tehnologije programi beležijo domala vsako izrečeno ali napisno besedo, med preprostim sprehodom do trgovine nas zabeležijo številne kamere. Nekoč so obstajali le prstni odtisi, danes pa tudi skeniranje očesne mrežnice ali šarenice, prepoznava glasu, prepoznava obraznih oblik, DNA … Metode, ki lahko mnogokrat zagotovijo uspeh pri odkrivanju načrtovanja terorističnih dejanj, so večinoma v konfliktu z osnovnimi človekovimi pravicami in svoboščinami. Zato bo del naloge namenjen tudi temu področju. Pomembno je seveda zagotavljane ravnotežja med varnostjo in demokracijo ter človekovimi pravicami (Anžič 2002, 456). »Kdor žrtvuje svoboščine zaradi varnosti, si ne zasluži ne enega ne drugega,« je nekoč dejal Benjamin Franklin (Dnevnik 2005). Dejstvo pa je, da je pri tem treba upoštevati časovno dimenzijo; morda je za dolgoročno varnost sprejemljivo kratkoročno žrtvovati demokracijo.

Ugotoviti bom skušala tudi: v katero smer se razvija sodelovanje mednarodnih inštitucij, ki se ukvarjajo z bojem proti terorizmu, in ali je tovrstno sodelovanje uspešno; kako sta se reorganizirala FBI in Europol, kakšno je njuno medsebojno sodelovanje in sodelovanje z varnostno-obveščevalnimi službami; ali lahko takšne povezave preprečijo morebitne ponovne večje teroristične napade ter koliko se da narediti na področju preventive pred tovrstnimi dejanji. Eden izmed ciljev magistrske naloge je ugotoviti uspešnost identificiranja, odkrivanja ter onemogočanja financiranja terorističnih organizacij.

Magistrska naloga bo temeljila na dejstvu, da je informacijska revolucija, ob vseh ostalih aspektih življenja nasploh, močno spremenila tudi obveščevalno varnostno strukturo in njeno delovanje. Črnčec napade 11. septembra poimenuje kulisa za spremembe, ko je prišel čas nove obveščevalne paradigme. Gre za preoblikovanje nacionalnovarnostnih struktur, širjenje pristojnosti in pooblastil za zbiranje podatkov obveščevalnih služb,

pojavi se potreba po podatkih s skoraj forenzično vrednostjo, poveča se možnost prenosa velike količine le-teh in informacij, čemur obveščevalne službe skoraj ne morejo konkurirati, svetovni splet postaja dostopen skoraj vsem, številni ga zlorabljajo. Na obveščevalnem področju postane sodelovanje med državami pomembnejše kot kdajkoli prej (Črnčec 2009, 83–84).

Nalogo pa začenjam s trditvijo, da ena ključnih ovir v boju proti terorizmu ostaja prav neenotna definicija tega pojava.

2.2 Delovne hipoteze

Glavna hipoteza:

1. Ključ učinkovitega boja proti terorizmu je informacija – zbiranje podatkov, pravilna interpretacija in preglednost zbranih podatkov, oblikovanje informacij in izmenjava informacij med inštitucijami oziroma resorji, ki se ukvarjajo z bojem proti mednarodnemu terorizmu.

Pomožne hipoteze:

1. Enotna definicija terorizma bi izboljšala uspešnost delovanja nacionalnovarnostnega sistema v boju proti terorizmu, zato je ključnega pomena poenotenje stališč mednarodne skupnosti.

2. Teroristične organizacije potrebujejo za svoje delovanje ogromno sredstev, zato je sodoben boj usmerjen k omejevanju teh sredstev. Velike finančne pritoke zanje predstavlja organizirani kriminal.

2.3 Uporabljene metode

Pri svojem delu bom glavno in pomožne hipoteze poskušala potrditi z analizo vsebine ter primerjavo oz. s pomočjo komparativne metode in logičnega odkrivanja vzrokov in posledic.

Z deskriptivno analizo bom opredelila temeljne pojme, kot so: varnostna politika držav, Zvezni preiskovalni urad (FBI), Europol, terorizem, metode in cilji terorističnih skupin, uspešnost inštitucij v boju proti terorizmu, preventiva, biometrija in nacionalna varnost. Z deskriptivno metodo bom pojasnila, kako in ali sploh so zgoraj naštete spremenljivke medsebojno povezane.

Uporabila bom tudi zgodovinsko-primerjalne metode. Terorizem bom opredelila kot pojavno obliko ogrožanja varnosti, ki sicer obstaja že dlje časa, zdaj pa dobiva oznako ključnega vira ogrožanja varnosti.

Pri kvantitativni analizi bom primerjala podatke in nekatere ključne kazalce, ki mi bodo pomagali pri potrditvi osnovne hipoteze. Uporabila bom obstoječe statistike iz podatkov FBI, Europol, Združeni narodi, CIA in drugih. Raziskovanje bo temeljilo predvsem na kvalitativni metodi, le deloma na kvantitativni metodi.

Pri izbiranju literature se predvidoma ne bom srečevala toliko s pomanjkanjem ustrezne literature kot z dejstvom, da mnogo napisanega izgublja aktualnost. Obravnavana tema je namreč v konstantnem razvoju, ustrezna metoda izmenjave varnostno-obveščevalnih podatkov med državami in institucijami, ki se ukvarjajo z bojem proti mednarodnemu terorizmu, prav tako. Samo v času pisanja te naloge so npr. nekatere spletne strani, s katerih sem črpala informacije, ugasnile.

Pri pisanju naloge bom obiskovala spletne strani, namenjene podpornikom različnih terorističnih organizacij, spremljala twite, si prek spleta ogledala nekaj dokumentarcev na temo terorizma ter odkrivanja in preprečevanja morebitnih terorističnih napadov.

Dobršen del magistrske naloge bo temeljil na aktualnih podatkih posameznih institucij ter tiskovnih agencij. Z dejansko situacijo področja proučevanja se bom tako seznanila predvsem s pomočjo primarnih virov, dokumentov in poročil raznih agencij in institucij, objavljenih na spletnih straneh; uporabljala bom tudi sekundarne vire, predvsem članke.

3 OPREDELITEV TEMELJNIH POJMOV

3.1 Informacija

Informacija ima glede na kontekst različne pomene, ki pa so praviloma povezani s pojmi pomen, znanje, navodilo, komunikacija, predstavitev ali miselni stimulus. Informacija na splošno ni nič oprijemljivega, ampak je neposredno uporaben podatek, sporočilo, ki nas poduči o kakem dogodku, količini, stanju – tem, kar je podano za nadaljnjo uporabo. Prejemniku pa mora predstavljati nekaj novega, da mu poveča znanje in vpliva na njegove odločitve in ravnanje. Kakovost informacije se vidi v točnosti, popolnosti, relevantnosti, dosegljivosti, preverljivosti, dostopnosti in varnosti (Šuhel 2011, 5). In prav kakovostna informacija je predpogoj za izdelavo mnenja oziroma ocene o morebitnem tveganju določenega početja posameznika ali skupine.

Kako pomembna je informacija in kaj informacija danes predstavlja, je najbolje strnjeno v 70. opombi knjige »Obveščevalna dejavnost v informacijski dobi« avtorja Damirja Črnčeca, ki piše: »Leta 2002 je podjetje Gartner ocenilo, da je količina informacij, zbranih v svetu v minulih treh letih, enaka vsem podatkom, ki jih je človeštvo na različne načine zbralo in hranilo od kamene dobe do leta 2003.« Ta

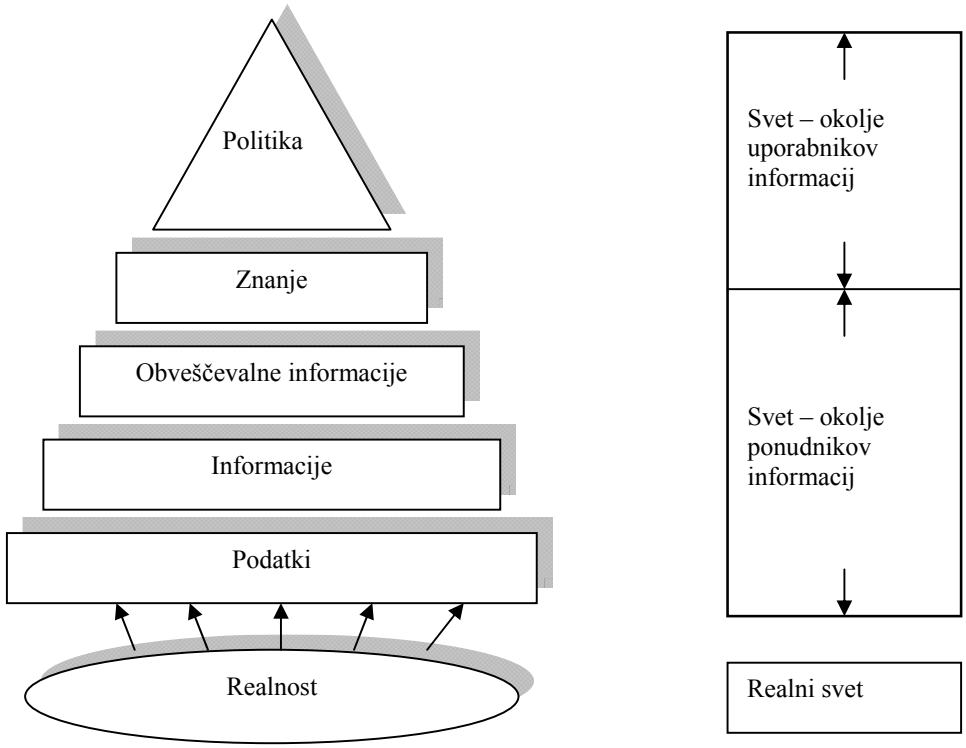
informacija po mojem mnenju strne v enem stavku, kako enormnemu napredku informacijske tehnologije smo priča.

Podatki so prva postaja pri nastajajoči verigi od informacije do znanja. Podatki so ponavadi v obliki besed, črk, številk ali simbolov. »Podatek je nevtralno sporočilo o nekem dejstvu. Pomeni surovino za oblikovanje informacij. Izražen je z znaki, s sliko ali z zvokom. Primeri vrst podatkov so: številka izdelka, številka zaposlenega, datum, naročena količina ipd. Podatek ima določene lastnosti, npr. zanesljivost, točnost, starost, zgoščenost, uporabnost, pogostost uporabe. Izmed podatkov, ki so na voljo v organizaciji ali njenem okolju, so za menedžerja zanimivi samo tisti, ki so uporabni.« (Gričar 2002, 619).

Preobrazba podatkov v informacijo je proces sprejemanja, prepoznavanja in konverzije, ki ga omogoča naša kognitivna zgodovina in sposobnost dešifriranja simbolov znotraj določene kulture, za pravilno in točno konverzijo podatkov pa je pomembno, da smo ji sposobni dati vrednost iz informacij, ki jih poznamo iz preteklosti, in so skladiščene v spominu, knjigah, računalnikih … (Črnčec 2009, 62).

Znanje je naslednja stopnja v informacijski piramidi in je zmožnost dokazovanja. Kot piše Črnčec, vsi avtorji od Aristotela naprej poudarjajo ključno razliko med informacijo in znanjem: za znanje potrebujemo človeka, ki je zmožen nadgraditi informacije, sklepati, dokazovati, vključevati izkušnje – torej nekaj, česar naj tehnologija še ne bi zmogla. Informacijsko piramido pa sestavlja še ena kategorija na poti od informacije do znanja – obveščevalne informacije. Obveščevalne službe imajo namreč le en in edini cilj – zbiranje informacij. Zato je smiselno domnevati, da imajo informacije obveščevalnih služb svojo dodano vrednost in so kot take uvrščene v posebno kategorijo. Informacije in znanje so torej del kompleksne zgodbe, ki se začne s podatki in koča z odločanjem. (Črnčec 2009, 67).

Tabela 3.1: Informacijska piramida



Vir: Strategic Management, (Barabba in Zaltman v Črnčec 2009, 66)

Je pa ta nova oblika sodobne moči – moči znanja uporabe informacij – bolj paradoksalna kot katera koli. Majhni posamezniki ali skupine lahko ogrožajo velike in največje. Tudi teroristične organizacije namreč uporabljajo internet. V obdobju po 11. septembru je mednarodni terorizem pokazal, da lahko za dosego svojih ciljev uporablja dve asimetričnosti. Prva je asimetričnost informacij, kar pomeni, da imajo lahko teroristi boljše informacije za pripravo in izvedbo svojih napadov kot jih imajo na primer države, ki jih teroristi želijo napasti, o tem, kako teroristične mreže delujejo. Druga asimetričnost pa je asimetričnost vrednot, kar pomeni, da je tudi majhen posameznik, ki je pripravljen umreti v samomorilskem napadu, lahko grožnja za veliko državo (Svete 2011).

3.2 Pomen izmenjave informacij

Tako ZDA kot Evropska unija sta po napadih v New Yorku, Londonu in Madridu pričeli razvijati izboljšane sisteme za dostop organov pregona do informacij in delitev informacij.

Evropski državljani menijo, da terorizem in organizirani kriminal predstavljata zanje največjo nevarnost – kar 80 % državljanov je tega mnenja (Sporočilo Komisije Evropskemu parlamentu 2004). Eden izmed načinov, da se učinkovito zajezi ta nevarnost, je seveda kvalitetno sodelovanje organov pregona med državami članicami. V izjavi Evropskega sveta o terorizmu marca 2004 je zaveza, da države najprej preučijo »zakonodajne ukrepe, s katerimi bi poenostavili izmenjavo informacij in podatkov med organi pregona v državah članicah. Komisija je bila pozvana, da svetu predstavi predloge v zvezi z izmenjavo osebnih podatkov in uporabo informacij o potnikih z namenom boja proti terorizmu. Predlogi Komisije morajo vključevati tudi določila, ki omogočajo državnim organom pregona dostop do evropskih informacijskih sistemov.« (Sporočilo Komisije Evropskemu parlamentu 2004.)

Komisija je najprej predstavila elemente, ki so ključnega pomena za realizacijo prostega pretoka informacij med organi pregona in državami članicami na bolj strukturiran način kot doslej. Identificirali so ovire za prosti pretok informacij in obveščevalnih podatkov med Europolom in državami članicami oziroma med samimi državami članicami. Pomanjkljiva izmenjava informacij in odsotnost jasne politike glede informacijskih kanalov sta bili opredeljeni kot oviri pri postopku izmenjave informacij, prav tako pa tudipravne, tehnične in praktične težave, ki ovirajo izmenjavo med državami članicami. Zapisali pa so tudi, da je učinkovitost pregona treba ustvarjati ob upoštevanju človekovih pravic in temeljnih svoboščin, kot jih zagotavljajo mednarodne, evropske in ustavne tradicije, ki so skupne vsem državam članicam.

Komisija je pozvala države članice in ostale sodelujoče stranke, da se lotijo naslednjih drznih ukrepov, pri katerih je potrebno sodelovanje:

- *Prvič: treba je ukrepati in zagotoviti dostop do podatkov in informacij, ki jih organi pregona EU potrebujejo in so zanje pomembni, in sicer s ciljem preprečevanja terorizma in boja proti terorizmu in drugim oblikam resnega in organiziranega kriminala, kakor tudi proti nevarnostim, ki jih predstavljajo. S tem v zvezi se je treba zavedati, da kriminalna dejavnost, ki se na videz ne uvršča v kategorijo "resna in organizirana", pogosto vodi v takšno obliko oziroma je z njo povezana.*
- *Drugič: treba je pridobiti in uporabiti visoko kakovostne kriminalistične obveščevalne podatke EU. Znanje, ki bo v tem postopku na voljo, bo v pomoč na politični ravni pri določanju prednostnih nalog pregona EU na enoten način in v pomoč organom pregona za učinkovito soočanje s kriminalom in z nevarnostmi, ki ogrožajo življenja naših državljanov, njihovo fizično integriteto in varnost.*
- *Tretjič: treba je povečati zaupanje med službami pregona. Uvedba skupnih pogojev, npr. za dostop do podatkovnih sistemov in delitve znanja, bo koristila pri postavitvi skupne platforme informacijske politike predvsem s tem, da se bodo odpravile objektivne ovire za učinkovito delitev informacij in obveščevalnih podatkov (vir: Sporočilo komisije 2004).*

S to politiko bodo organom pregona EU postali dostopni vsi podatki oziroma informacije, potrebni in pomembni za preprečevanje in boj proti terorizmu ter drugim oblikam resnega in organiziranega kriminala. Takšna politika bo pospeševala ustvarjanje in uporabo visoko kakovostnih obveščevalnih kriminalističnih podatkov na ravni EU za pomoč pri sprejemanju političnih odločitev in bo v pomoč organom pregona pri učinkovitem soočanju s tem kriminalom; podpirala bo tudi stopnjevanje zaupanja med pristojnimi službami.

Temeljni cilj informacijske politike za pregon je oblikovati prost pretok informacij med službami pregona, vključno z EUROPOLOM in EUROJUSTOM. Če bi organi pregona iskali le po podatkovnih zbirkah, ki so dostopne znotraj države, to ne bi bilo produktivno. Vendar pa dostop do informacij, ki jih hranijo službe pregona drugih držav članic, predstavlja tehnično težavo, zaradi katere so te za tuje službe nedostopne. Cilj informacijske politike je zagotoviti, da bi te informacije postale dostopne praktično vsem

organom pregona EU, vključno z EUROPOLOM in EUROJUSTOM. Bile naj bi jim v pomoč pri izvrševanju njihovih nalog, in to v skladu z določili zakona.

Poleg različnih načinov dostopa do podatkov in podatkovnih zbirk na osnovi načela enakega dostopa obstaja še dodatna možnost boljšega dostopa do podatkov in podatkovnih zbirk, in sicer tako, da se le-te vnesejo v omrežje oziroma se oblikujejo centralne zbirke podatkov. Rezultat izboljšav evropske informacijske politike je bilo izboljšanje izmenjave med evropskimi podatkovnimi zbirkami – SISII, VIS in EURODAC.

SIS in SIS II – v okviru Schengenskega sporazuma so se odpravile kontrole na notranjih mejah med državami pogodbenicami – poleg držav članic EU, razen Velike Britanije in Irske, tudi Norveška in Islandija. S tem se je ustvaril skupni prostor za prost pretok oseb in za pospešitev prevoza ter pretoka blaga; uveljavilo se je tudi načelo mejne kontrole ob vstopu v enotno Schengensko območje. Zato je bilo za ohranjanje zadovoljive ravni javnega reda in javne varnosti, vključno z nacionalno varnostjo, potrebno tudi oblikovanje Schengenskega informacijskega sistema (SIS). SIS obsega nacionalne podatkovne zbirke v vsaki državi pogodbenici in tehnični podporni del v Strassbourgu. Skupni sistem omogoča povezavo med državami pogodbenicami in omogoča končnim uporabnikom (policiji, carini, konzulatom …) dostop do informacij, ki jih potrebujejo za opravljanje svojih dolžnosti, v SIS pa so jih vnesle druge države pogodbenice. Zbirka podatkov, ki si jih tako delijo vse države na Schengenskem območju, vsebuje dve široki kategoriji podatkov, najprej o iskanih ali pogrešanih osebah in osebah, ki se jim tajno sledi (prikrito evidentiranje) ter tudi o ukradenih ali drugače odtujenih vozilih in drugih predmetih (osebni dokumenti, orožje, denar). Tehnični podporni del sistema je v Strassbourgu; s prenosom informacij *on-line* zagotavlja, da nacionalne podatkovne zbirke držav podpisnic vsebujejo enake podatke. Temelj SIS je tako posebej varovana linija, ki kot vodnik omogoča pretok informacij, ki so zakodirane. To so močno varovane linije. Podatkovne baze so zaščitene, vsaka država pa ima svojo nacionalno kopijo (Informacijski pooblaščenec 2012).

Druga tehnična verzija oziroma nadgradnja sistema SIS se imenuje SIS II; je še v delu in naj bi začela delovati leta 2013. Sicer pa so v Evropski uniji v okviru Schengenskega sporazuma v uporabi naslednje podatkovne zbirke: EURODAC – baza, ki vključuje podatke o prstnih odtisih in prosilcih azila, VIS (Visa Information System) – baza in informacijski sistem s podatki o potnikih (namenjena je preprečevanju preprodaje viz in izboljšanju sistema vračanja ilegalnih imigrantov), CECIS (The Common Emergency Communication and Information System in FADO, ki je mreža oziroma sistem, namenjen olajšanju izmenjave informacij med državami članicami. Sistem zaznava ponarejene dokumente na področju imigracije in policijske kooperacije (Schengen Information System 2012).

Tovrstni sistemi so učinkoviti le ob dolgotrajni politični podpori izvajanja enotnega prostora pregona v EU na osnovi združljivih državnih sistemov obveščevalnih kriminalističnih podatkov, ki bodo skupaj tvorili konceptualno integrirani evropski model kriminalističnih obveščevalnih podatkov.

Tudi v ZDA vlagajo veliko truda in denarja v oblikovanje okolja za izmenjavo informacij – Information Sharing Environment. Vzpostavljanje okolja za izmenjavo informacij je bilo s strani GAO[3] ocenjeno kot napredno. V preteklih dveh letih je izmenjava informacij, povezanih s terorizmom, napredovala, ampak popolno okolje še ni ustvarjeno (GAO 2011).

Takoj po napadih 11. septembra so ZDA pričele zgodovinsko transformacijo, usmerjeno k preprečevanju terorističnih napadov. Sprejeli so patriotski zakon, ustanovili Urad za domovinsko varnost, reorganizirali obveščevalno skupnost, ustanovili NCTC[4], največ napora pa so usmerili v vzpostavitev tako imenovanega okolja za delitev informacij – Information Sharing Environment. To naj bi izboljšalo delitev informacij med zveznimi, državnimi, lokalnimi in plemenskimi službami ter zasebnim sektorjem. Ustanovljen je bil TSC[5], številni centri združevanja informacij[6], povečalo se je število JTTF[7]. Urad za

[3] GAO – Government Accountability Office
[4] NCTC – National Counterterrorism Center
[5] TSC – Terrorist Screeneing Center.

domovinsko varnost je razširil informacijsko mrežo HSIN[8] v vseh 50 zveznih držav, pet teritorijev, DC in 50 drugih urbanih centrov za zagotovitev dvostranskega pretoka informacij.

Delitev informacij, povezanih s teroristično dejavnostjo, danes poteka med številnimi medsebojno povezanimi okolji, ki služijo petim skupnostim – obveščevalni, varnostni, obrambni, domovinski varnosti ter zunanji politiki. V preteklosti je vsaka od teh slupnosti razvijala svoje politike, pravila, standarde, strukture in sisteme za prenos in zbiranje informacij. Bile so izolirane ena od druge, kar je povzročilo luknje v sistemu delitve informacij. Zato je leta 2004 Kongres sprejel in predsednik podpisal reformo obveščevalne skupnosti[9] . S tem so se ustavrili pogoji za ustanovitev ISE, ki naj bi odslej te luknje v sistemu pretoka informacij odpravljala (National Strategy for Information Sharing 2007).

3.3 Pomanjkljivosti izmenjave informacij

Nacionalna komisija za preiskavo terorističnih napadov na Združene države Amerike je leta 2004 kot ključni faktor neuspeha za preprečitev napada izpostavila prav kolaps pri izmenjavi informacij in neuspešno povezovanje informacij, ki so jih različne inštitucije že posedovale. Prizadevanja po letu 2001 v ZDA za reševanje teh vprašanj so naslednja:

- Kongres je s političnimi smernicami in tehnologijo pooblastil oblikovanje okolja za izmenjavo podatkov, znano kot ISE; to bo zagotovilo in olajšalo izmenjavo informacij med vsemi inštitucijami, zveznimi, lokalnimi, državnimi in tudi zasebnim sektorjem, torej med vsemi, ki se ukvarjajo z bojem proti terorizmu.

[6] Fusion Centers – do septembra 1eta 2007 jih je bilo ustanovljenih ali v ustanavljanu že 58.
[7] JTTF – Joint Terrorism Task Force.
[8] HSIN – Homeland Security Information Center.
[9] Intelligence Reform and Terrorism Prevention Act, 2004.

- V zveznih državah in večjih urbanih naseljih so ustanovili centre zbiranja informacij; ti koordinirajo zbiranje in analizo podatkov, ki jih zberejo zakonodajni organi, domovinska varnost, javna varnost in varnostne službe.
- Številni programi za obdelavo podatkov so pričeli z delovanjem z namenom odkrivanja terorističnih načrtov.

Vendar težave ostajajo. Količina podatkov, ki se od državnih in lokalnih organov pregona stekajo k zveznim, je ogromna. Cilj, da se iz teh podatkov oblikuje kvalitetna informacija, je težko dosegljiv, saj je treba to goro podatkov tudi predelati. V poročilu GAO iz oktobra 2007 so zapisali, da največja težava nastane, ko se podobni ali enaki podatki posredujejo različnim agencijam, nato pa medsebojno še izmenjujejo in tako podvajajo. V Obveščevalnih zbirnih centrih se zaradi preobilice težko loči med pomembnimi in nepomembni podatki. V samo letu in pol pred nastankom tega poročila je npr. FBI zabeležil kar 108.000 potencialnih terorističnih groženj in poročil o sumljivih incidentih; pričakuje se tudi, da bodo te številke še naraščale (FBI 2102).

4 SODOBNO VARNOSTNO OKOLJE

Sodobne varnostne grožnje so sicer podobne grožnjam iz preteklosti, od njih se razlikujejo le v precej povečani možnosti širjenja. Temu je botrovala globalizacija in informatizacija. Na račun sodobne tehnologije ima terorizem globalni doseg (Svete 2011, 156). Zaradi asimetrične soodvisnosti lahko tudi najmočnejšo državo ogrožajo majhne teroristične skupine (Keohane v Svete 2011, 156). Teroristični napad na ZDA 11. septembra ni bil le napad na to državo, temveč napad na temeljne človeške vrednote. Ta ugotovitev je še pridobila na teži leta 2004 in 2005 ob napadih v Madridu in Londonu, ko je postalo jasno, da je tarča mednarodnega terorizma tudi Evropa. Podobno kot oborožene sile so velike spremembe doletele tudi varnostno-obveščevalno dejavnost, ki je najpogosteje ključna komponenta v kontekstu asimetričnega vojskovanja[10] (Svete 2011, 151).

[10] Asimetrija se v obrambnem in varnostnem pojmovanju nanaša na neprimerljivost, neenakost, različnost sodelujočih v konfliktih. Te se kažejo pri uporabi sredstev za doseganje ciljev, metodah uporabe teh

Varnostno okolje po hladni vojni je bolj zapleteno kot tisto pred in njo. Tedaj so ZDA kot sicer veliko, pa vendar skoraj edino grožnjo obravnavale Sovjetsko zvezo[11]; tedanje mednarodno varnostno okolje je bilo mnogo bolj pregledno in predvidljivo od sedanjega (Grizold, Ferfila, 45). Današnji nevojaški viri ogrožanja varnosti, kot so organizirani kriminal, terorizem, množične ilegalne migracije, ekološki terorizem, etnični konflikti itd., spodbujajo konfliktne situacije, v katerih lahko pride do uporabe oboroženega nasilja. (Slovenija in NATO 2004). Sodobno varnostno okolje je zapleteno, polno novih izzivov, razmere se pogosto in hitro spreminjajo in na izzive se je veliko težje odzvati. Zato so tudi varnostno-obveščevalne službe v 21. stoletju morale spremeniti načina operiranja, predvsem pa razpršiti svojo osredotočenost na več posameznih groženj. Evropska varnostna struktura se je najprej morala prilagoditi novi združeni Evropi, nato pa še izzivom, ki jih predstavlja terorizem; ta namreč Evrope ni zaobšel. Postal je mednarodna nevarnost, ki je nobena članica unije ne more reševati sama. EU razvija protiteroristično politiko, s katero se države skupaj borijo proti temu zlu. Sprejeti so bili pomembni zakonski ukrepi in politike za pomoč Evropski uniji pri preprečevanju in boju proti tovrstnemu nasilju. Evropski svet je sprejel akcijski načrt EU za boj proti terorizmu (opravljen je bil tudi medsebojni pregled ukrepov) po vsej EU in v vsaki državi članici). Bistveno za preprečevanje in boj proti terorizmu je, da države članice posredujejo vse ustrezne informacije Europolu. Posredovanje informacij, ki izhajajo iz dejavnosti nacionalnih varnostnih in obveščevalnih služb je pomembna sestavina tega procesa. Države članice morajo tudi zagotoviti vse ustrezne informacije drugim državam članicam, ki jim pomagajo pri preprečevanju in boju proti terorizmu. S tega stališča imajo varnostne in obveščevalne službe vsake članice osrednjo vlogo (Komisija Evropskih skupnosti 2005).

---

sredstev ter dejanskem položaju tako znotraj posamezne družbe kot v širši mednarodni skupnosti. Prava asimetrija se kaže v tehnološki, operativni in taktični inovativnosti (Meigs v Svete 2011, 14). Posebej je asimetrija uporabna za šibke in revne države ter nedržavne entitete, ki lahko tako kljubujejo veliko močnejšemu nasprotniku. Eno od njenih najpomembnejših izhodišč je faktor presenečenja.

[11] Tudi za zrušitev totalitarnih sistemov je imela informacijska revolucija poseben pomen. K zlomu komunizma v Sovjetski zvezi je seveda prispevalo več faktorjev, »če pa se izpostavi en dejavnik, ki je prvi med enakovrednimi, je to informacijska revolucija, ki se je začela sredi osemdesetih let prejšnjega stoletja. Totalitarni sistemi so temeljili na monopolu informacij in sile. S pomočjo širjenja faks naprav, telefonov ter ne nazadnje osebnih računalnikov je začelo preveč informacij uhajati čez železno zaveso.« (Friedman 2005, 54.)

Vsaka država unije ima seveda svojo obveščevalno varnostno službo, ki tako kot slovenska SOVA izvaja vrsto aktivnosti na področju boja proti mednarodnemu terorizmu. Pristojnim inštitucijam – tudi Europolu – te službe, tudi SOVA, zagotavljajo in posredujejo podatke, informacije in ocene, pomembne za ustrezno ukrepanje in zagotavljanje varnosti v lastni državi (SOVA 2009). V širšem kontekstu boja proti mednarodnemu terorizmu pa državne obveščevalno-varnostne službe sodelujejo in izmenjujejo podatke, zbirajo in vrednotijo informacije o mednarodnih terorističnih, ekstremističnih ter ostalih skrajnih skupinah in organizacijah, ki za doseganje svojih ciljev uporabljajo ali zagovarjajo nasilne metode delovanja.

Ameriška varnostno-obveščevalna agencija CIA je po koncu hladne vojne, predvsem pa po napadih 11. septembra prav tako morala prilagoditi delovanje novemu varnostnemu okolju. Po 11. septembru je več kot podvojila število obveščevalcev na področju znanosti, DS&T[12] in tehnologije (USA Today 2008). Urad nacionalnega obveščevalnega direktorja je leta 2008 sprejel Strategijo izmenjave informacij, v kateri je zapisano, »da je potreba po delitvi z drugimi postala imperativ za zavarovanje nacije v obdobju po napadih 11. septembra« (Information Sharing Strategy 2008). Strategija kot ključni vidik izmenjave informacij opredeljuje nov miselni okvir, koncept, odgovornost za zagotovitev varnosti, ki obsega polno implementacijo načela potrebe po delitvi z drugimi (Črnčec 2009, 85).

Strokovnjaki navajajo sedem trendov, ki posegajo v bistvo delovanja obveščevalnih služb (Svete 2011, 157). Prvi trend zaznamuje preoblikovanje nacionalnih obveščevalnih služb in struktur, povezanih z njimi. Najbolj očiten primer tega je preoblikovanje največje obveščevalne skupnosti, tj. obveščevalne skupnosti v ZDA. Gre za spremembe v smislu zagotavljanja boljšega usklajevanja, vrednotenja ter posredovanja podatkov uporabnikom v najkrajšem možnem času. Drugi trend širi pristojnosti in pooblastila za zbiranje

[12] Direstorate of Scinece and Technology deluje v sklopu CIE; je oddelek obveščevalcev, strokovnjakov na področju tehnologije vse od računalniških programerjev do inženirjev in analitikov. Na spletni strani (https://www.cia.gov/offices-of-cia/science-technology/index.html) so med drugim opisani tudi kot znameniti Q v filmih o Jamesu Bondu.

podatkov obveščevalnih služb, vendar z večjimi posegi v človekove pravice in svoboščine. Tretji trend je potreba po podatkih oziroma dokazih, ki imajo skoraj forenzično vrednost (to pomeni, da morajo obveščevalne službe podatke, pridobljene s tehničnimi sredstvi, kakovostno in pravilno obdelati ter posredovati naročnikom). Četrti trend je povezan s povečano zmožnostjo prenosa velike količine podatkov in informacij (obveščevalne službe pri tem niti ne morejo konkurirati drugim prenosnikom podatkov in informacij, kot so televizija, radio, splet ter telefonski klici). Peti trend je v duhu splošnega dostopa in uporabnosti informacijske tehnologije, pa tudi zlorab, ki jih to prinaša. Šesti trend je rezultat in posledica prodiranja tretjega in četrtega trenda v obveščevalno skupnost. Sedmi trend je povezan s prvim, vendar presega njegovo zgolj nacionalno dimenzijo. Mednarodno sodelovanje na obveščevalnem področju in v okviru različnih nadnacionalnih, varnostnih, regionalnih ali gospodarskih organizacij je danes pomembnejše kot kadar koli prej.

Nove tehnologije so povzročile veliko sprememb pri zbiranju podatkov. Še pred dvema desetletjema so se obveščevalne službe pri zbiranju podatkov zanašale predvsem na človeške vire, sedaj pa se skoraj v celoti na tehnična sredstva (Svete 2011, 158–159). Obveščevalna dejavnost se ne usmerja skladno s tem, kar naj bi bilo narejeno, temveč s tem, kar je tehnično možno (Agrell 1987, 34).

Stroga varnostna politika še ne zagotavlja varnosti, če je ne dopolnjuje politična strategija, ki se spopada s koreninami terorizma. Dejstvo je namreč, da danes nobena država ne more svojim državljanom sama zagotavljati optimalne varnosti, zato se tako države kot tudi njihovi varnostni in obveščevalni organi med seboj povezujejo in sodelujejo pri iskanju rešitev za odpravljanje sodobnih groženj.

5 TERORIZEM KOT SODOBNI VARNOSTNI FENOMEN

Pojem terorizem je v Slovarju slovenskega knjižnega jezika opredeljen kot »uporaba velikega nasilja, zlasti proti političnim nasprotnikom, s katerim se hoče doseči, da se kdo boji. Uporablja se lahko ekspresivno in pomeni uporabo nasilja, nasilnega ravnanja, s katerim se hoče doseči, da si kdo ne upa ravnati, kot si želi« (SSKJ 1991, 71). V Politični enciklopediji se pojem terorizem opredeljuje kot »doktrina in metoda boja za določene cilje s sistemsko uporabo nasilja« (Politična enciklopedija 1975, 1079). V vojaškem leksikonu je zapisano, da je terorizem »organizirana in sistematična uporaba postopkov nasilja z namenom, da se z izzivanjem strahu in osebne negotovosti državljanov podre avtoriteta države ali pa izpolnijo nekateri politični cilji« (Vojaški leksikon 1981, 622). Na splošno z besedo terorizem sicer označujemo vsako organizirano nasilno dejanje, ki je usmerjeno proti civilistom ali civilnim ustanovam v politične ali gospodarske namene. Izvajajo ga nedržavne skupine ali države in je večinoma javno dejanje, saj hočejo teroristi s tem zajeti kar se da veliko ljudi in doseči čim večjo odmevnost, tudi s pomočjo sodobnih medijev, ki o takih incidentih poročajo, ter tako vplivati na širše javno mnenje.
Obstaja več definicij terorizma, številne imajo veliko skupnega, a kljub vsem naporom mednarodne organizacije še niso uspele strukturirati opredelitve, s katero bi soglašala večina držav. Opredelitev pojma oz. postavitev enotne definicije dodatno zaplete tudi obstoj več vrst terorizma – nacionalistični, verski, levičarski, desničarski, mednarodni/domači, anarhistični terorizem, narkoterorizem – kar skoraj onemogoča oblikovanje definicije, ki bi lahko zaobjela vse njegove oblike. Pri naštevanju vrst terorizma pa velja omeniti, da so ločnice med različnimi vrstami terorizma pogosto zabrisane, saj lahko določena teroristična skupina sodi v več različnih vrst terorizma. Že v uvodu omenjena definicija sestavljena je iz večih definicij, ki jih najdemo v literaturi, ni popolna. Po njej npr. napad na USS Cole 12. oktobra 2000, ko sta se samomorilska napadalca z motornim čolnom zaletela v rušilca, ne bi bil teroristično dejanje, saj napadeni niso bili civilisti, temveč vojaki (17 jih je umrlo, 39 je bilo ranjenih).

Ne samo, da je definicij terorizma več, tudi definiciji v ZDA in Evropi nista enotni. Opredelitev Združenih narodov iz leta 1999 narekuje, da je terorizem sestavljen iz kaznivih dejanj, katerih namen je povzročiti strah med ljudmi, pri čemer gre za

neopravičljiv cilj – ne glede na njegovo politično, filozofsko, ideološko, rasno, etnično, versko ali kakšno drugo naravo (Janželj 2012, 11).

Decembra 2001 je bila na podlagi političnega konsenza glede dokumenta Framework Decision on Combating Terrorism sprejeta skupna evropska tridelna opredelitev terorizma: dejanja morajo biti namerna, s potencialno močjo resnega ogrožanja države ali mednarodne organizacije, njihov cilj mora biti ustrahovanje širše skupnosti oziroma izzivanje vlade ali mednarodne organizacije z namenom destabilizacije temeljnih političnih, ustavnih, ekonomskih ali socialnih struktur; dodanih je osem specifičnih vedenj (med njimi npr.: ugrabitve, jemanje talcev, zasegi letal, ladij ali drugih oblik transporta, izdelava, posest, transport, nabava orožja, eksploziva ali biološkega/kemičnega orožja, onemogočanje ali ogrožanje virov pitne vode itd.). Leta 2008 so dokumentu dodali še amandma, s katerim se med kriminalna dejanja terorizma uvršča tudi napeljevanje, nabor in urjenje prekinterneta. (Libertysecurity 2012.)

Kriminolog Nettler (Explaining Crime 1984) je izluščil šest značilnosti, za katere bi lahko rekli, da predstavljajo stične točke raznovrstnih oblik terorizma, ki jih naštejem v Tabeli 5.1.

Tabela 5.1: Stične točke raznovrstnih oblik terorizma

- odsotnost pravil – moralna pravila glede tipa ali stopnje nasilja, ki ga je še dovoljeno uporabiti, ne obstajajo
- nedolžnih žrtev ni – ni razlikovanja med vojaki in civilnim prebivalstvom; otroci so enako izpostavljeni kot odrasli
- ekonomija – princip: ubij enega, prestraši 10.000 ljudi
- publiciteta – odmevnost v medijih predstavlja teroristom dodatno vzpodbudo
- namen – teroristi na ta način dajo pomen svojemu življenju
- odsotnost jasne vizije – za trenutnimi destruktivnimi dejanji so dolgoročni cilji teroristov zamegljeno opredeljeni, zabrisani

Vir: Stične točke terorizma (Nettler 1984)

Za vsakim terorističnim dejanjem je določena strategija. Ne glede na sredstva napadalcev pa terorizem ni naključno ali spontano dejanje, zmeraj gre za načrtno uporabo sile za politične, gospodarske ali verske cilje.

5.1. Problem definicije terorizma

Terorizem je termin, ki v mednarodnem pravu nima enotne definicije. V svoji knjigi »Politični terorizem« sta Schmidt in in Youngmen naštela 109 različnih definicij terorizma. Čeprav večina ljudi z lahkoto in brez dvoma prepozna teroristično dejanje, pa težave strokovnjakov z natančno definicijo terorizma ostajajo. Vse bolj se v zadnjem času stopnjujejo argumenti za tako definicijo, čeprav nekateri strokovnjaki poudarjajo, da gre v celoti za političen pojem in enotna definicija s pravnega stališča ni potrebna. Zagotovo

pa je odsotnost skupne definicije ena temeljnih pomanjkljivosti boja proti mednarodnemu terorizmu. Težava je predvsem ideološka. Znan je komentar, da je terorist ene države borec za svobodo druge države. Takšno definicijo lahko pripišemo med drugim pripadnikom OVK na Kosovu ali pa čečenskim upornikom.

Poskusi definiranja terorizma so postali takšna polemična in subjektivna naloga, da mejijo bolj na umetnost kot znanost (Burgess 2003). Skoraj noben tekst na temo terorizma ni brez vsaj uvodnega poglavja, namenjenega definiciji . Medijsko pokrivanje fenomena je še dodatno zapletlo konkretno definicijo, saj se v besedilih na mestu terorista pogosto pojavljajo tudi ekstremist, fundamentalist, gverila, komandos in podobno. Ne samo, da je skoraj nemogoče, da bi različne države sprejele enotno definicijo terorizma, celo znotraj države, v tem primeru ZDA, različni resorji različno definirajo terorizem (glej Tabelo 5.2)

Tabela 5. 2: Definicije terorizma različnih resorjev v ZDA

Agencija	Definicija
Obrambno ministrstvo	Nezakonita uporaba ali grožnja z uporabo nasilja, namenjenega prisiljevanju ali zastraševanju vlad ali družb, največkrat z namenom uresničevanja ciljev, ki so v bistvu politični, verski ali ideološki.
FBI	Nezakonita uporaba sile proti ljudem ali premoženju z namenom prestrašiti ali prisiliti vlado, civilno populacijo oziroma njen

	segment v določen politični ali družbeni cilj.
Zunanje ministrstvo	Premišljeno, politično motivirano nasilje, izvršeno proti nebojujočim se tarčam, s strani subnacionalnih skupin ali tajnih agentov, ki ima ponavadi namen vplivati na občinstvo.

Vir: CIA; FBI, State Department (2012)

Vse tri ameriške definicije terorizma imajo elemente treh medsebojno povezanih faktorjev – motiv oseb, ki jih poimenujemo teroristi, njihovo identiteto in metodo.

Sicer pa terorizem kot fenomen nasilja po eni strani od tega ločuje tudi politična motivacija. Vidik terorizma kot političnega nasilja najverjetneje izhaja iz časa francoske revolucije in že prej omenjene vladavine terorja, politična konotacija pa je terorizem spremljala skozi večino nadaljnjega zgodovinskega razvoja. Ni pa politična motivacija edina, ki definira terorizem. Tudi vera ali pa preprosto kriminalno dejanje sta lahko motiv osebe, ki izvaja teroristično dejanje. Tukaj se postavlja vprašanje, ali je bil na primer ostrostrelec, ki je leta 2002 strahoval ljudi na območju Washingtona, terorist. Dejansko je ogrožal (teroriziral) tamkajšnje prebivalce, njegovo početje pa ni bilo politično motivirano, kljub temu pa so ga obtožili po postenajstseptembrskem zakonu o antiterorizmu. Guelke opisuje slikovito rabo besede terorizem v devetdesetih letih prejšnjega stoletja: potrošniški terorizem (zastrupljanje hrane v trgovinah), ekonomski terorizem (agresivne špekulacije z valutami), narkoterorizem, pornografija, nadlegovanje po telefonu, posilstvo, državni terorizem (Guelke 1998, 1). Tako ohlapna raba poimenovanja ima veliko slabih strani – beseda postane preelastična in njen pomen osiromašen (Burgess 2003). Prav tako, še dodaja Burges, psihološki efekt terorističnega

dejanja ni nujno prioriteta terorista. Kot kaže, je namreč njegov končni cilj pogosteje ubiti kot prestrašiti. Vendar pa se za politološko raziskovanje v tej nalogi osredotočam predvsem na tiste tipe terorizma, ki vsebujejo politično komponento.

Čeprav terorizem lahko identificiramo kot politično nasilje, seveda ne velja, da je vsako politično nasilje terorizem. Tudi vojna, na primer, je oblika političnega nasilja. Za vojno veljajo pravila, vsaj naj bi, ki prepovedujejo uporabo nekaterih vrst orožja, prepovedujejo napade na določene skupine, npr. civiliste, in opredeljujejo, kako naj bi se ravnalo z ujetniki. Teroristi ta pravila, zapisana v ženevski konvenciji, večinoma ignorirajo; njihove tarče so civilisti, napadajo v civilnih oblačilih, ugrabljajo ljudi, z ujetniki grdo ravnajo ali jih ubijejo. V enem izmed poročil Združenih narodov je zanimiva preprosta definicija terorizma, ki ga opredeljuje kot "vojni zločin v času miru" (United Nations Office of Drugs and Crime 2003).

Za konec razmišljanja o tem problemu še enkrat izpostavljam, da bi enotna definicija terorizma izboljšala uspešnost delovanja nacionalnovarnostnega sistema v boju proti terorizmu, zato je ključnega pomena poenotenje stališč mednarodne skupnosti.

5.2 Mednarodni terorizem z vidika mednarodnega prava

Terorizem lahko preučujemo z različnih vidikov in v naslednjem poglavju ga bom opredelila v okvirih mednarodnega prava. Že pred napadi 11. septembra, še bolj pa po njih, je bilo sprejetih več pomembnih mednarodnopravnih dokumentov v zvezi s terorizmom. Varnostni svet Organizacije združenih narodov se je že dan po napadih odzval z Resolucijo 1368, ki najostreje obsoja teroristični napad 11. septembra in ga pojmuje kot grožnjo mednarodnemu miru in varnosti. V omenjeni resoluciji izraža sočutje žrtvam in njihovim družinam, ameriškemu ljudstvu in vodstvu, poziva države k sodelovanju pri iskanju vseh, ki so odgovorni za napad, mednarodno skupnost pa nagovarja, naj "podvoji napore" pri prevenciji in pregonu terorističnih dejanj ter izražanju pripravljenost za boj proti vsem oblikam terorizma v skladu s svojimi obveznostmi po Ustanovni listini. (Mednarodni terorizem z vidika mednarodnega prava 2002.)

Maja 2002 je tudi Državni zbor Republike Slovenije sprejel deklaracijo o podpori resoluciji o terorizmu – nevarnosti za demokracijo, človekove pravice in civilno družbo: prispevek parlamentov v boju proti mednarodnemu terorizmu in odpravljanju njegovih vzrokov z namenom ohranjanja mednarodnega miru in varnosti. (Deklaracija o podpori resoluciji o terorizmu 2002.)

28. septembra 2001 je Varnostni svet sprejel še Resolucijo 1373, ki poziva vse države, naj preprečijo in preganjajo financiranje terorističnih dejanj, jim ne nudijo nikakršne podpore, zlasti pa naj ustavijo dobavo orožja terorističnim skupinam ter poskrbijo, da pridejo pred sodišča vsi, ki so kakor koli vpleteni v teroristična dejanja; sodelujejo naj z medsebojno izmenjavo informacij in sprejmejo konvencije s področja boja proti terorizmu.

Sicer pa je bilo že veliko pred napadi 11. septembra sprejetih več pomembnih mednarodnopravnih dokumentov v zvezi s terorizmom. Ko je prišlo do pogostejših ugrabitev letal, je mednarodna skupnost reagirala s sprejemom 4 mednarodnih konvencij proti terorizmu v mednarodnem civilnem zračnem prometu: Tokijske konvencije leta 1963 (o varnosti zračnega prometa), Haaške konvencije leta 1970 (o ugrabitvah letal), Montrealske konvencije leta 1971 (o kaznivih dejanjih, ki lahko ogrozijo varnost poleta oz. življenja potnikov) in Montrealske konvencije leta 1991 (o označevanju plastičnih eksplozivov z namenom njihovega odkrivanja).

Kot posledica številnih napadov na diplomate in diplomatska predstavništva je bila leta 1973 sprejeta konvencija o preprečevanju in kaznovanju kaznivih dejanj, storjenih proti osebam pod mednarodno zaščito, leta 1979 konvencija proti jemanju talcev; konvencijo o fizični zaščiti jedrskega materiala so sprejeli leta 1980, konvencija o zatiranju kaznivih dejanj proti varnosti plovbe, ki obravnava teroristična dejanja na ladjah, je bila sprejeta 1988. leta, leta 1994 pa še konvencija o varnosti osebja Združenih narodov in pridruženega osebja. V okviru OZN sta bili nazadnje sprejeti še dve: Mednarodna konvencija o zatiranju terorističnih bombnih napadov leta 1997 in Mednarodna konvencija o zatiranju financiranja terorizma leta 1999. Na evropski ravni je

najpomembnejša Evropska konvencija o preganjanju zločina terorizma iz leta 1977, ki jo je ratificirala tudi Slovenija.

Ker je tudi mednarodno pravo instrument za mednarodno sodelovanje v boju proti terorizmu, v okviru OZN potekajo pogajanja o osnutku celovite konvencije o terorizmu. Terorističnih napadov je bilo v letu 2011 sicer manj, pa vendar to ni zagotovilo, da bo tako tudi v prihodnje. Nenehne grožnje po smrti Osama bin Ladna v Abottabadu v Pakistanu, zahtevajo, da se mednarodna skupnost odzove

Države članice OZN so okrepile sodelovanje pri vzpostavljanju normativnega okvira, ki obsega konvencije in protokole ter predstavlja korpus mednarodne zakonodaje za olajšavo okrepljenega mednarodnega sodelovanja za učinkovit boj proti različnim oblikam terorizma v praksi. Te pobude segajo v leto 1960, ko so ugrabitve letal postale zelo razširjen pojav. (CNVOS, 2011).

V novejšem času je vloga Varnostnega sveta OZN postala pomemben dejavnik pri obravnavi specifičnih terorističnih napadov. Tako so uvedene sankcije proti Libiji po nesreči letala nad Lockerbijem, proti talibanom po napadih na ameriški veleposlaništvi v Keniji in v Tanzaniji; sprejete so številne resolucije, posledično tudi resolucija VS OZN 1373 iz leta 2001 za napad 11. septembra v ZDA (Mednarodni inštitut za bližnjevzhodne in balkanske študije 2011).

5.3 Najpomembnejše teroristične organizacije

Danes na svetu deluje več kot 50 terorističnih skupin. Napade izvajajo tudi posamezniki, ki se ne povezujejo v skupine, značilno zanje pa je, da so to praviloma t. i. domači teroristi. Skoraj zagotovo edini pravi mednarodni terorizem izvajajo islamski skrajneži, saj ostale znane teroristične skupine delujejo lokalno. Sledi opis nekaterih najbolj znanih terorističnih skupin. Mnoge imajo veliko skupnega, druge so povsem specifične. Kratek opis pomembnejših terorističnih skupin je relevanten, saj prav specifike skupin

opozarjajo na to, da mora vsak program, namenjen predčasnemu odkrivanju morebitnih načrtovanih terorističnih dejanj, zaobjemati številne parametre.

Al Kaida, v arabščini poimenovanje pomeni "baza", savdskega disidenta Osame bin Ladna je danes brez dvoma najbolj znana teroristična skupina, ki ima svoje člane, simpatizerje in finančne podpornike v številnih državah. Po napadih 11. septembra 2001 za mnoge predstavlja poosebljeni mednarodni terorizem. Al Kaida se je iz organizacije, ki je združevala mudžahide afganistanske vojne, razvila v mednarodno mrežo in krovno organizacijo islamskih skrajnežev. V terorističnem napadu 11. septembra, v katerem sta se dve letali zaleteli v dvojčka Svetovnega trgovinskega centra v New Yorku, tretje je treščilo v Pentagon, četrto pa strmoglavilo na polje v Pennsylvaniji, je izgubilo življenje več kot 3000 ljudi. ZDA so kot glavnega osumljenca za napade takoj označile Bin Ladna. Skoraj 10 let po terorističnih napadih, v začetku maja 2011, so ga ameriške sile ubile v Pakistanu, kjer se je skrival. To se je zgodilo v vojaški operaciji nedaleč od Islamabada; ZDA so akcijo načrtovale na podlagi podatkov obveščevalne službe (Guardian 2011).

Organizaciji **Džamaja Islamija in Islamski džihad** veljata za nekakšni podružnici Al Kaide v Egiptu, saj je vodja Džamaje Islamije Ajman al Zavahiri bil hkrati tudi desna roka Osame bin Ladna. Eden najbolj znanih napadov, ki jih je izvedla Džamaja Islamija, je bil poboj 58 tujih turistov v Luksorju, Islamski džihad pa je odgovoren za umor predsednika Anvarja Sadata leta 1981, potem ko je ta sklenil mirovni sporazum z Izraelom.

Militantna islamistična skupina **Džamaja Islamija** ima sedež v Indoneziji, sicer pa deluje na širšem območju jugovzhodne Azije (Indonezija, Malezija, Singapur, Filipini in Tajska). Skupina je zelo aktivna in prav tako tesno povezana z Al Kaido. Odgovorna je za vse večje napade v Indoneziji v zadnjih letih, med njimi tudi za bombni napad na Baliju oktobra 2002, v katerem sta umrli 202 osebi; njeni cilji so predvsem predstavništva zahodnih družb. Indonezijske oblasti so skupini v zadnjem času zadale precej udarcev, saj

so prijele njenega spiritualnega vodjo Abu Bakar Baširja in vodjo operacij Hambalija, ki naj bi bil tudi vodja operacij Al Kaide za vzhodno Azijo (24ur.com 2002).

Skupina **Abu Sajaf** s sedežem na južnih Filipinih je radikalna islamska skupina, katere prvotni cilj je ustanovitev islamske države za manjšinsko muslimansko prebivalstvo na Filipinih. Njeno ime v arabščini pomeni "tisti, ki nosi meč", znana pa je predvsem po ugrabitvah in bombnih napadih. Njene žrtve so predvsem Filipinci, največjo publiciteto pa je doživela z ugrabitvami in napadi na ameriške državljane (Dnevnik 2010).

Aum Šinrikjo pravzaprav ni teroristična skupina v klasičnem pomenu besede, ampak apokaliptični kult. Zaslovela je leta 1995, ko je s strupom sarin napadla civiliste v tokijski podzemni železnici. V tem največjem terorističnem napadu v zgodovini Japonske je umrlo 12 ljudi, več kot 5.000 so jih prepeljali v bolnišnice. Čeprav je vodja skupine Šoko Asahara v zaporu, skupina še vedno obstaja, po podatkih policije naj bi bilo v njenih vrstah vsaj 2.100 ljudi. Je pod stalnim nadzorom policije in od leta 1995 ni pripravila novega napada. Junija letos so aretirali zadnjega člana sekte, odgovornega za napad s sarinom (SIOL 2012b).

Med dolgo in kruto vojno za osamosvojitev Čečenije so nekatere skupine **čečenskih borcev** posegle tudi po terorističnih metodah in v svoje vrste pritegnile manjše število islamskih skrajnežev, večinoma iz arabskih držav. Čečenski skrajneži so odgovorni za številne teroristične napade na ruske cilje, med bolj znanimi je bila ugrabitev 700 talcev v moskovskem gledališču Dubrovka. V akciji ruskih specialcev, ki je sledila ugrabitvi, je bilo ubitih okoli 120 talcev in vsi teroristi (24ur.com 2011).

Baskovska separatistična organizacija **ETA** (Euskadi ta Askatasuna – Baskovska domovina in svoboda) izhaja iz severne Španije in jugozahodne Francije. Ima že dolgo zgodovino boja za neodvisno Baskijo, saj je nastala leta 1959 kot odgovor na represijo frankističnega režima nad baskovsko kulturo in jezikom. Njene akcije niso omejene samo na Baskijo, ampak deluje v celotni Španiji. Strokovnjaki domnevajo, da se financira pretežno z ugrabitvami, bančnimi ropi, preprodajo mamil in t. i. pobiranjem zaščite. V

času po 11. septembru 2001 je skupina precej zmanjšala število napadov, ni pa z njimi v celoti prenehala.

Levičarski **FARC** (Revolucionarne oborožene sile Kolumbije), ustanovljen leta 1964, velja za najbolje organizirano, vodeno in opremljeno uporniško gibanje v Kolumbiji. Po nekaterih ocenah je v njegovih vrstah do 18.000 vojakov. Skupina ima tesne stike s preprodajalci kokaina; prepovedana droga je namreč eden glavnih finančnih virov skupine. FARC je odgovoren za številne napade na predstavnike sodstva, policije, vojske in gospodarstva. Protiutež skupini FARC predstavlja **AUC** (Samozaščitne sile Kolumbije), desničarska paravojška skupina, ki jo podpirajo nekateri bogati posestniki, trgovci z mamili in celo nekateri visoki vojaški častniki. Čeprav je skupina precej manjša, šteje okoli 8.000 pripadnikov, pa strokovnjaki menijo, da je odgovorna za kar 75 % vseh civilnih žrtev v kolumbijski državljanski vojni.

Hamas, islamsko odporniško gibanje je leta 1987 ustanovil šejk Ahmed Jasin. Vojaško krilo Hamasa je v preteklosti izvedlo številne teroristične napade na Izrael. Leta 1993 pripravilo tudi številne samomorilske bombne napade v Izraelu. S tem je želelo preprečiti izvajanje sporazuma ter nadaljnje dogovarjanje med Izraelom in Palestinsko osvobodilno organizacijo o zagotavljanju omejene avtonomije Palestincev v Gazi in na Zahodnem bregu. Hamas predstavlja verjetno najradikalnejšo palestinsko organizacijo, deluje pa na palestinskih zasedenih ozemljih in v Izraelu.

Hezbolah je radikalna šiitska skupina, ki deluje v južnem Libanonu, v Bejrutu in v dolini Beka. Prizadeva si za ustanovitev države po vzoru Irana, ki je sicer tudi glavni podpornik skupine. Šteje več tisoč članov, njeni pripadniki pa so odgovorni za nekatere najbolj odmevne akcije proti zahodnim interesom, kot je bil napad na ameriške vojake v Libanonu leta 1983 (Council on Foreign Relations 2012).

Irska republikanska armada, verjetno najbolj znana evropska teroristična skupina, je bila ustanovljena leta 1969 z namenom pregnati britanske sile iz Severne Irske in združiti se z matično državo. Ker je politično krilo IRE Sinn Fein začelo politična pogajanja o

rešitvi severnoirskega vprašanja, je ZDA od leta 2000 ne prištevajo več med teroristične organizacije. So pa nekateri radikalni člani IRE ustanovili novo organizacijo, poimenovano Prava IRA, ki občasno nadaljuje s terorističnimi akcijami. V preteklosti je IRA veliko sodelovala z baskovsko separatistično organizacijo ETA.

Tamilski tigri so bili poleg radikalnih islamskih organizacij edina teroristična skupina, ki je uporabljala tudi samomorilske napadalce. Od leta 1976 so se borili za ustanovitev samostojne tamilske države na severu Šrilanke, leta 2009 pa so bili uničeni v spopadih s šrilanskimi oboroženimi silami. Njihov najbolj znani napad je bil umor nekdanjega indijskega premierja Radživa Gandija leta 1991 (ubit je bil v samomorilskem bombnem napadu; Reuters, 2009).

Do 11. septembra 2001 so za ZDA predstavljale največjo teroristično grožnjo **domače radikalne skupine.** Njihove idelologije in politični cilji so zelo različni, saj med njimi najdemo bele supremaciste, portoriške separatiste, nasprotnike umetne prekinitve nosečnosti in radikalne okoljevarstvenike (ekoteroriste). Najbolj znan ameriški terorist je brez dvoma Timothy McVeigh, beli rasist, ki je z improvizirano bombo leta 1995 v Oklahoma Cityju porušil zvezno upravno stavbo in ubil 168 ljudi (CNN 2001).

5.4 Komuniciranje terorističnih organizacij

V zadnjem desetletju je na področju informacijske tehnologije prišlo do izjemno hitrega razvoja in do še pred nekaj leti neslutenih sprememb. To je močno vplivalo tudi na delovanje terorističnih skupin oziroma na njihov način sporazumevanja. Komunikacijskim kanalom, ki so jih teroristične skupine uporabljale že v preteklosti (tisk, radio, televizija, stacionarna telefonija), so se pridružili številni novi načini komuniciranja. Med njimi najbolj izstopa internet ter brezžična telefonija. Pojav interneta je znatno povečal propagandne sposobnosti terorističnih skupin, saj lahko s pomočjo tega medija v zelo kratkem času na enostaven način dosegajo vsakogar na svetu. Zanimivo je, da je DARPA, ki je v šestdesetih letih prejšnjega stoletja zaslužna za nastanek interneta,

danes agencija, ki razvija največ programov za nadzor komunikacij in zbiranje ter izmenjavo informacij z namenom preprečevanja terorističnih dejanj.[13] Nadzira tudi GSM-telefonijo, ki jo danes teroristi kljub izsledljivosti največ uporabljajo. Za razliko od stacionarnih, brezžični telefoni omogočajo, da uporabnik ni vezan na specifično lokacijo. Kar še govori v prid GSM-telefoniji z vidika terorista, je vse večji obseg prometa, zaradi česar je nekoliko težje prisluškovanje. Za prenašanje sporočil prek interneta teroristi uporabljajo različne kanale. Najbolj običajni so elektronska pošta, različni načini komuniciranja v realnem času, ter spletne strani. Za zakrivanje vsebine sporočila uporabljajo tudi številne enkripcijske in steganografske računalniške programe, ki so na voljo v prosti prodaji.[14] Na spletnih straneh so povezave do klepetalnic, ki omogočajo medsebojno komuniciranje v realnem času. Kot sem že omenila, teroristične skupine za komuniciranje pogosto uporabljajo enkripcijo, vendar pa lahko tako zakrito sporočilo zaradi anomalij v zapisu še prej pritegne pozornost varnostnih organov. Zato so najbolj v uporabi odprte kode, kar pomeni, da teroristi besede, ki bi sicer lahko pritegnile pozornost, preprosto zamenjajo z drugimi. To potrjujejo tudi ugotovitve preiskovalcev napadov na WTC in Pentagon 11. septembra 2001, ki pri pregledu elektronske pošte niso zaznali enkripcije.[15]

Teroristične organizacije danes uporabljajo tudi socialna omrežja – Facbook, Twitter in drugo (Teroristične organizacije na Twitterju 2012). Organizacija Hezbolah je na twitterju aktivna pod imenom al Manar News (@almanarnews). Ima 8000 sledilcev in redno objavlja tvite, ki vsebujejo povezave na arabski spletni medij. Objavila je že več

---

[13] Predsednik Dwight Eisenhower je leta 1958 imenoval predsednika MIT Jamesa Killiana za predsedniškega svetovalca za znanost in ustanovil agencijo ARPA z namenom pospešitve ameriške tehnologije na področju zaščite pred napadi z izstrelki iz vesolja. Ameriška vojska je bila še posebej zaskrbljena zaradi možnosti uničenja telekomunikacijske infrastrukture. Brez komunikacije se namreč ne bi mogli ustrezno odzvati. ARPA je zato leta 1962 ustanovila IPTO (Information Processing Techniques Office), da bi ustvarila računalniško mrežo, ki bi povezala glavne računalnike v Pentagonu, v jedrskem bunkerju na Cheyenne Mountainu in na štabu strateških zračnih sil – SAS Headquarters. Ta pobuda je vodila k razvoju ARPANET-a sedem let kasneje, nato NSFNET-a in nato Ineterneta, kot ga poznamo danes (Internet Story 2012).

[14] Steganografija je tehnika, s katero je mogoče sporočilo v tekstovni obliki skriti v datoteke s slikovnim in zvočnim zapisom (.jpeg, .gif, .mp3,..).

[15] Al Kaida je na primer izraz za bombo nadomestila z arabsko besedo za otroško hrano (Campbell, Duncan – how the terror trail went unseen).

kot 16 tisoč tvitov, mešanice novinarskih zgodb in propagande v angleškem, arabskem in perzijskem jeziku.

Organizacija Hamas ima na twitterju račun pod imenom @AlqassamBrigade. Sledi ji skromnih 2840 ljudi, vendar pa so objave redne, vsebujejo povezave na spletno stran Al Qassam. Pred kratkim so objavili tvit o zračnem napadu na Gazo, ki so ga izvedle "izraelske okupacijske sile". Ostali tviti omenjajo "tretjo obletnico zionistične vojne na območju Gaze" ter zgodbe o Izraelcih, ki so napadli mošejo in pustili "rasistične grafite". Zaradi talibanov je Twitter kritiziral že ameriški senator Joe Lieberman, izraelski center pa se zaradi uporabe njihove platforme ni pritoževal. Kot je decembra poročal britanski Daily Telegraph, je Twitter Liebermanove kritike zavrnil z utemeljitvijo, da State Department talibanov ni uradno določil kot tujo teroristično organizacijo.

Stališče Twitterja je, da so zavezani k svobodi govora in da zapirajo le račune tistih, ki kršijo pogoje uporabe, denimo se predstavljajo kot nekdo drug ali nadlegujejo ostale uporabnike. Daily Telegraph je pred časom poročal, da so objave talibanov na Twitterju včasih izjemno natančne, iz minute v minuto opisujejo odvijanje napadov, pogosto pa so tudi popolnoma izmišljene ali močno pretirane navedbe o ameriških in britanskih žrtvah. Računi so pogosto polni pisanja o smrtih "strahopetnih okupatorjev" in "lutk" – afganistanskih vladnih sil. Organizacija Al Šabab je račun na twitterju odprla v Somaliji, imenuje se @HSMPress, ima pa okoli 8000 sledilcev. Pišejo večinoma v angleščini. Veliko njihovih tvitov vsebuje zapise o boju skupine proti kenijski vojski, ki je v Somalijo vstopila oktobra, da bi se borila s Šababom. Obamovo administracijo pa skrbi, da bi prek twitterja skupina iskala nove militante.

Slika 5.1: Teroristične organizacije na Twitterju

Vir: Teroristične organizacije na Twitterju (2012)

Teroristične organizacije uporabljajo tudi lastne internetne strani. Terorizem in internet sta povezana na dva načina: internet je postal forum za teroristične skupine in posameznike za širjenje njihove ideje ter medsebojno komuniciranje; posamezniki in skupine napadajo medmrežje, kar je postalo znano pod imenom kiberterorizem.

Ena izmed organizacij, ki sledi ineternetnim aktivnostim terorističnih organizacij, se imenuje SITE – Search for International Terrorist Entities (SITE) Intelligence Group. Inštitut SITE je bil ustanovljen leta 2002, leta 2008 se je preimenoval v SITE Intelligence Group. Je zasebna profitna organizacija in opozarja na izstopajoče grožnje in sumljive zapise na inernetu.[16]

Protiteroristična skupnost se lahko na spletne strani teroristov odzove na različne načine.

[16] SITE je dvignila veliko prahu, ko je avgusta 2011 opozorila na grožjo na eni izmed popularnih radikalnih islamistični inertentnih straneh. Tam je namreč ekstremist z imenom Umar Al-Basravi zagrozil znanemu ameriškemu TV-voditelju Davidu Lettermanu, da mu je treba, ker se je norčeval iz Bin Ladnove smrti, odrezati jezik in ga utišati za vedno. Objavil je kar 1200 sporočil z grozilno vsebino.

Najbolj enostavno je zapreti sporno spletno stran, vendar se s tem zapre možnost pridobivanja pomembnih informacij.[17] Poleg tega je zapiranje spletne strani le začasna motnja. Za prekinitev delovanja spletne strani je treba ustaviti njenega skrbnika. Možnost ameriške NSA, da nadzira te posameznike, pa je v ZDA kamen spotike tudi zaradi zagovornikov svobode govora. Obstaja tudi možnost kreiranja lažnih terorističnih spletnih strani, s katerimi se lahko širi napačne informacije o na primer izdelavi eksplozivnih sredstev ali o strateških lokacijah, ki posredno vodijo teroriste v zasedo.

6 POVEZAVA MED ORGANIZIRANIM KRIMINALOM IN TERORISTIČNIMI ORGANIZACIJAMI

Stockholmski program opredeljuje dve grožnji notranji varnosti v Evropski uniji – mednarodni terorizem in organizirani kriminal. V mnogih primerih sta prisotni na istih področjih, na primer v trgovini z orožjem in trgovini z mamili. (Sprejeto besedilo, 14. dec. 2011). Ker se organizirani kriminal in teroristične skupine pogosto, v zadnjih letih celo še pogosteje prekrivajo, skoraj ne moremo več govoriti o različnih oziroma ločenih skupinah. Zaskrbljujoč izziv predstavlja, kako zagotoviti, da bo boj proti tem skupinam ravno tako povezan, kot je njihovo delovanje. Ne nazadnje je kriminal v veliki meri stvar policije, medtem ko gre pri terorizmu za širšo varnostno grožnjo. Dopuščanje še tako majhnih vrzeli med obema bi pomenilo samo lažje delo za kriminalce. V končni fazi gre pri vseh kriminalnih dejavnostih za denar. Ta je bodisi cilj ali pa sredstvo za doseganje cilja (King 2009).

[17] Spremlja se namreč lahko, kdo pri spletni strani sodeluje in kdo jo financira. Nemški varnostni organi so na primer zaradi spremljanja pogovorov na internetu lahko izdali zgodnje opozorilo pred bombnimi napadi v Madridu leta 2004 (Council on Foreign Relations 2009).

6.1 Organizirani kriminal kot finančni vir terorističnih organizacij

Ko sta novinarja Carl Bernstein in Bob Woodward preiskovala afero Watergate, je bil nasvet njunega zloglasnega informatorja, znanega kot 'globoko grlo', enostaven: sledita denarju. Za delovanje vsake teroristične organizacije, še posebej mednarodne, so potrebna velika denarna sredstva. Zagotavljanje finančnih sredstev je bistvenega pomena za delovanje terorističnih skupin, saj s tem izpolnjujejo enega izmed predpogojev za izvajanje drugih aktivnosti. Obseg stroškov je seveda odvisen od velikosti posamezne teroristične skupine, njihovih ciljev ter stopnje sofisticiranosti napadov. Finančna sredstva za svojo dejavnost teroristične skupine črpajo iz legalnih in nelegalnih virov, ki med drugim vključujejo državno podporo, legitimno poslovanje (onesnaževanje denarja), donacije posameznikov, dobrodelno dejavnost, kriminal. Predvsem državna podpora v zadnjih dveh desetletjih močno upada, narašča pa financiranje s pomočjo organiziranega kriminala. S tem pa teroristične skupine postajajo bolj finančno samostojne. Italijanska policija je leta 2007 potrdila trend, ki potrjuje vse večjo povezavo med organiziranim kriminalom in terorizmom. Potrdili so, da Al Kajda za preseljevanje teroristov skozi Evropo do varnih hiš v Parizu, Berlinu in Madridu uporablja neapeljsko Comorra mafijo z njeno obširno mrežo in izkušnjami pri ponarejanju dokumentov. DIGOS, zveza italijanskih političnih kriminalistov, ocenjuje, da število teroristov, ki so na takšen način prišli skozi Neapelj, presega 1000 (Perri 2009). Povezava med Al Kajdo in Comorro je le en primer vse naraščajočega varnostnega izziva. Nekoč močna razmejitvena linija med organiziranim kriminalom in terorizmom postaja vse bolj zabrisana in predstavlja velik izziv v vojni proti terorizmu. Omenjeni združbi imata namreč vzajemne koristi. Teroristi izkoriščajo dobro vzpostavljene sisteme ponarejanja dokumentov, tihotapljenja ljudi in podobno, kriminalne združbe pa med drugim od teroristov kupujejo orožje ali pa jih uporabljajo za zaščito.

Doba globalizacije je ustvarila pogoje, ki omogočajo skupinam, ki se ukvarjajo z organiziranim kriminalom, in teroristom, da združijo moči. S koncem hladne vojne so morale nekatere teroristične skupine, ki jih je financirala Sovjetska zveza, postati neodvisne in preživeti. FARC (Revolutionary Armed Forces of Columbia), največja

kolumbijska gverila je takšen primer (In Sight 2012). Od leta 1990 je postala vse bolj vpletena v kolumbijsko trgovino z drogami, predvsem v smislu varovanja pridelka, laboratorijev in lokalnih letališč, pa tudi obdavčevanja kmetovalcev na njihovem ozemlju. Ameriške oblasti ocenjujejo, da od leta 2000 FARC od nezakonite trgovine z mamili prejme do 400 milijonov dolarjev letno.

Kot še pišejo na spletni strani In Sight[18], so kolumbijski gverilci osumljeni tudi izmenjave droge za orožje s skupinami, kot je na primer IRA. Medtem pa varnostno obveščevalne službe Južne Amerike poročajo, da čečenska mafija uporablja Argentino za tranzitno deželo pri pošiljkah kolumbijskega kokaina v Evropo. V zameno pa Čečenci prodajajo orožje kriminalnim organizacijam v Braziliji in Kolumbiji.

Povezave med organiziranim kriminalom in terorizmom lahko opazimo tudi v drugih Južnoameriških državah. V Ekvadorju je policija razkrila mednarodno trgovino z drogami, ki jo je vodil Rady Zaiter, sicer lastnik libanonske restavracije, ki je kar 70 % nelegalno prisluženega denarja namenjal Hezbolahu. V Braziliji so aretirali 19 članov njegove tolpe in zasegli kokain v vrednosti 65 milijonov dolarjev. Po poročilih ameriškega urada za domovinsko varnost Al Kada sodeluje z mehiškimi mafijskimi družbami pri ilegalnih prehodih meje (Chepesiuk 2002).

Seveda pa trgovina z drogo ni edina kriminalna aktivnost, ki se je poslužujejo teroristi. Ugrabitve, tihotapljenje blaga in ljudi, kraja identitete in celo oboroženi ropi so zelo donosni načini zaslužka. Do leta 2002 je na primer celica Hezbolaha, ki je delovala v kraju Charlotte v Severni Karolini, za potrebe teroristične skupine v Libanonu zbirala denar z zlorabo kreditnih kartic in tihotapljenjem cigaret.

Indijski kriminalec Dawood Ibrahim naj bi skoval posel z Al Kajdo in drugimi terorističnimi skupinami, ki delijo njegove tihotapske poti od Indije do Evrope. Ibrahim je kriv za bombni teroristični napad leta 1993 v Mumbaju v Indiji, v katerem je umrlo 257 ljudi.

[18] Spletna stran In Sight (The Organized Crime in Americas) je bila ustanovljena z namenom povečati stopnjo analize, preučevanja in raziskovanja organiziranega kriminala v Latinski Ameriki in Karibih. Sedež organizacije In Sight je v Columbiji in na Ameriški Univerzi v Washingtonu, ZDA.

Od ekonomskega trenda globalizacije imajo tudi teroristi vse večje koristi. Tudi njim namreč omogoča prost pretok blaga in ljudi ekonomsko integracijo ter izkoriščanje razvoja napredne tehnologije. Kimberly L. Thachuk, pomočnica direktorja Projekta Globalizacije pri Inštitutu za nacionalne Strateške Študije, je dejala: »Kriminalne združbe in teroristične skupine so v razcvetu zaradi pogojev, ki jih nudi globalna soodvisnost, povečana svetovna trgovina in razvoj komunikacij ter vse hitrejši transport.«

Naraščajoča povezanost med kriminalom in terorizmom spreminja naravo boja proti terorizmu in zahteva nove strategije. Omejevanje finančnih virov je pomembna faza v boju proti terorizmu, zahteva pa tesno sodelovanje tako inštitucij za preprečevanje kriminala kot inštitucij, ki se borijo proti terorizmu. Trgovina z drogo, pranje denarja, ponarejanje in črni trgi spadajo v mednarodni organizirani kriminal in tako preprečevanje in boj proti tovrstnemu kriminalu pomeni omejevanje finančnih virov terorističnih organizacij. Osama Bin Laden pa je bil tipološko gledano nov tip terorista. Svoje prepričanje o lastnem poslanstvu, svojo križarsko vojno proti »nevernikom« je združeval z znatnimi finančnimi sredstvi. Njegova skrajnost in denar sta privedla nazadnje do terorizma – grozljive enačbe terorističnega globalnega akterja z imperijem financ in terorja, razpredenim po vsem svetu (Pohly 2001, 10).

6.1.1 PRANJE DENARJA IN ONESNAŽEVANJE DENARJA

Pranje denarja je proces, s pomočjo katerega poskušajo teroristične skupine z uporabo različnih mehanizmov zakriti izvor pridobljenih sredstev. Najpogosteje ga uporabljajo teroristične skupine, ki večji del finančnih sredstev za svoje delovanje pridobijo s pomočjo nelegalnih dejavnosti. Proces pranja denarja v večini primerov poteka prek bančnega poslovanja s pomočjo številnih hitrih transakcij med različnimi računi. S tem se izgubi sled za izvorom denarja. Dejstvo pa je, da teroristične skupine predstavljajo relativno majhen delež v globalnem procesu pranja denarja. (Miholič 2004, 49)

Drugi način financiranja terorističnih skupin je t. i. onesnaževanje denarja. To pomeni financiranje nelegalnega delovanja z denarjem, zbranim po legalnih poteh. Sledenje finančnim transakcijam teroristov, ki se financirajo iz legitimnih virov, je namreč dosti težje kot sledenje izvoru finančnih virov v procesu pranja denarja.

6.1.2 TRGOVINA Z DROGO

Za financiranje svojih dejavnosti se teroristične organizacije poslužujejo tudi trgovine z mamili. Trgovina z mamili je za teroristične organizacije vsekakor najbolj dobičkonosna nelegalna dejavnost. Za svoje delovanje potrebujejo na milijone dolarjev, in sicer za orožje, letalske karte, varna stanovanja, vozila, podkupnine in podobno. Politični cilj sicer ostaja primaren, kriminal in trgovina z drogo pa sta sredstvo za doseganje tega cilja. Tako lahko borba proti trgovini z drogo pripomore k zmagi nad terorizmom. Teroristične organizacije največ služijo s trgovino z mamili predvsem na področjih Jugovzhodne in Srednje Azije, na Bližnjem vzhodu in v Latinski Ameriki. Tipičen primer sodelovanja med terorističnimi organizacijami in kriminalnimi združbami, ki se ukvarjajo s trgovino z mamili, je kolumbijska teroristična skupina FARC.

Izraz narkoterorizem izhaja iz 80. in 90. let, ko so kriminalci v Kolumbiji sklenili pakt s teroristi, ki so jim nudili zaščito pri gojenju, predelavi in transportu mamil. Nato so skupaj nastopili proti državi. Kasneje se je ta praksa prenesla tudi drugam, na primer v Afganistan. Odkar so talibani v Afganistanu leta 1995 prevzeli oblast, v tej državi pridelajo 70 % svetovnega pridelka opija (Lazanski 2001, 307). Talibanski režim je s pobiranjem davkov od pridelovanja opija, proizvodnje morfina in transporta financiral Al Kaido.

Na konferenci v Instanbulu novembra 2011, skupaj so jo organizirale Turčija, ZDA in Kolumbija z naslovom Vloga trgovine z mamili pri promociji in financiranju globalnega terorizma, je visoki predstavnik Urada ZN za droge in kriminal, UNODC, Irka

Kuleshnyk dejal, da je težko oceniti razsežnosti medsebojne povezanosti terorističnih skupin in trgovine z mamili ter naravo sodelovanja teh dveh kriminalnih skupin, vsekakor pa so s tem sodelovanjem povezane ogromne številke, kar je zagotovo zaskrbljujoče. Po UNODC približna ocena prometa z afganistanskim opijem leta 2006 znaša 3.1 milijarde dolarjev. Ob tem obstajajo poročila, da so leta 2004 iz ene izmed držav Latinske Amerike izvozili približno 400 ton kokaina v vrednosti 2 milijardi ameriških dolarjev. Ocene, koliko tega denarja je bilo namenjenega za teroristične aktivnosti, so različne, vendar tudi majhen odstotek bi bil zadosten za za načrtovanje, financiranje in izvedbo terorističnih dejanj. V nekaterih primerih pa so sama mamila valuta za plačilo terorističnih dejanj – to se je zgodilo pri bombardiranju v Madridu.

Obstajajo pa načini, ki krhajo te povezave. Na mednarodnem nivoju je pravni okvir sestavljen iz 16 splošnih antiterorističnih instrumentov in tudi resolucij Združenih narodov. Med slednje spadajo sankcije – zamrznitev sredstev, prepoved potovanj, prepoved trgovanja z orožjem. Preprodajalci mamil in teroristi namreč niso neka skrivnostna entiteta, dodaja Kuleshnyk, temveč le skupina ljudi ali mreža, ki operira na načine, ki se jih da razumeti, identificirati in končno onesposobiti. Potrebno je le vzpostaviti bolj produktivne mreže, ki bodo lahko razbile tovrstna delovanja po svetu (UNODC 2012).

6.1.3 DRUGE KRIMINALNE DEJAVNOSTI

Pri zagotavljanju finančnih sredstev se teroristične skupine ob trgovini z mamili zatekajo tudi k drugim kriminalnim dejanjem. Financiranje prek kriminala lahko teroristične skupine izvajajo samostojno ali v sodelovanju s kriminalnimi združbami. Predvsem v sodelovanju s kriminalnimi združbami si teroristične skupine zagotavljajo največje finančne pritoke, res pa je, da takšna dejavnost povečuje tveganje odkritja s strani varnostnih organov. V 70. in 80. letih prejšnjega stoletja so se teroristične skupine financirale predvsem z bančnimi ropi in ugrabitvami. Takšne kriminalne

metode so uporabljale levičarske skupine v Evropi in Latinski Ameriki,[19] desničarske skupine v ZDA[20] in tudi nekatere nacionalno usmerjene skupine.[21]

Ugrabitve še vedno predstavljajo donosen vir zaslužka predvsem v Kolumbiji, kjer naj bi bili glavni levičarski skupini FARC in ELN v letu 1997 odgovorni za približno 1800 ugrabitev, z odkupninami pa naj bi pridobili med 75 in 120 milijoni dolarjev (Leader v Miholič 2004, 42). Po aktualnih podatkih kolumbijskega Ministrstva za obrambo je število ugrabitev ponovno v porastu. Potem, ko je po letu 2000 počasi, a konstantno upadalo, se je leta 2010 število ugrabitev povečalo za kar 22 %, za kar 23 % le-teh pa je odgovorna FARC.[22] Islamistične skupine, razen nekaterih manjših, se iz verskih razlogov le redko poslužujejo tovrstnih kriminalnih metod pri zbiranju finančnih sredstev.

6.2 Trendi boja proti financiranju terorizma

Teroristične organizacije nekoč za delovanje niso potrebovale veliko denarja. V sedemdesetih in osemdesetih letih prejšnjega stoletja so bile to preprosto organizirane skupine. Danes je zgodba drugačna. Kompletna mreža teroristične organizacije, kot je Al Kaida, za svoje operacije potrebuje enormna sredstva. Za napad na rušilec USS Cole leta 2000 se predvideva, da je samo za izvedbo potrebovala med 5.000 in 10.000 dolarjev, napad 11. septembra pa naj bi stal tudi do pol milijona dolarjev (Brisard, Terrorism Financing, 2002). Iz spodnje tabele so razvidne ocene stroškov posameznih terorističnih napadov.

[19] RAF, Rdeče brigade
[20] The Order
[21] PIRA, ETA
[22] FARC se osredotoča predvsem na visokoprofilne ugrabitve delavcev v naftni industriji. Marca 2012 so v samo enem primeru ugrabili 23 zaposlenih, junija pa 3 kitajske državljane in njihovega prevajalca, ki jih še niso izpustili.

Tabela 6.1: Stroški terorističnih napadov

Teroristični napad	Datum	Stroški operacije
Napad na USS Cole	2000	5–10.000 USD
11. september, 2011	2001	500.000 USD
Napad na Baliju	2002	74.000 USD
Napad na tanker Limburg	2002	127.000 USD
Napad na mošejo na Djerbi	2002	20.000 USD

Vir: Terrorism Financing, poročilo Varnostnemu svetu ZN (2002)

To so seveda le stroški posamezne operacije, za vse ostalo so vsote denarja mnogo večje.

Tabela 6.2: Finančne potrebe Al Kaide

FINANČNE POTREBE AL KAIDE
Infrastruktura Komunikacije, mreženje, vadbišča, varovanje 90 %
Operacije Sprotni denar, načrtovanje in izvedba terorističnih napadov <10 %

(Vir: Terrorism Financing, poročilo Varnostnemu svetu ZN 2002)

Al Kajda se financira iz raznolikih virov. V naslednji tabeli je naštetih nekaj najpomembnejših:

Tabela 6.3: Metode financiranja operacijskih celic Al Kaide

Metode financiranja operacijskih celic Al Kaide
- članarine in verski davki - investicijski projekti - podjetja pod krinko - lažne pogodbe - kraje in ropi - poneverbe - ugrabitve - izsiljevanja - tihotapljenje orožja - tihotapljenje droge

Vir: Terrorism Financing, poročilo Varnostnemu svetu ZN (2002)

Dogodki 11. septembra 2001 v ZDA, marca 2004 v Španiji in julija 2005 v Angliji kličejo po implementaciji zakonodajnih in tehničnih posegov proti financiranju terorizma ter zlorabi nacionalnih in internacionalnih finančnih sistemov s strani islamskih terorističnih mrež. Teroristi zbirajo sredstva v državah, ki jih ne nameravajo napasti, to pa je le še dodaten dokaz, da teroristične mreže pametno izkoriščajo obstoječe finančne kanale za prenos denarja iz ene države v drugo. Ko poznamo proces onesnaževanja denarja, postane jasno, da je za uspešen boj proti temu fenomenu potrebno odločno sodelovanje finančnih in bančnih sektorjev, saj je treba proces sumljivih transakcij identificirati in registrirati. Tudi v tem primeru je informacija o sumljivih transakcijah, ki jo bo najverjetneje zasledila finančna inšpekcija, ključna in pomembna ter uporabna samo, če jo inštitucije delijo.

Finančna industrija je zelo privlačna za namene onesnaževanja denarja, saj vsebuje visoko stopnjo informacijske asimetrije. Izmenjavo informacij o pretoku denarja namreč nadzorujejo in upravljajo sposobni kadri, ki imajo na podlagi privilegiranih pozicij dostop do občutljivih informacij in možnost, da jih ohranjajo skrite (Ghioni 2006). Zaradi asimetrične distribucije informacij, tipične za finančne trge, so Off-shore države in države s sproščenimi finančnimi regulacijami zelo atraktivne za skupine, povezane s terorističnimi organizacijami. Off-shore finančni sistemi namreč otežujejo tujim regulatorjem, da pridejo do informacij. Preiskovalci sumljivih finančnih transferjev se osredotočajo predvsem na investitorje s sedežem v državah, ki sta jih OCDE in FATF (Financial Action Task Force) označila za nekoopeartivne, na ameriške in evropske družbe, ki poslujejo z državami, znanimi po terorističnih aktivnostih, ter na sklade z netransparentnimi podatki o vlagateljih.

Osrednjo vlogo v boju proti financiranju terorizma igra FATF.[23] Jasno je, da je za to, da bi onemogočili delovanje terorističnih skupin ali pa ga vsaj otežili, treba onemogočiti dotok finančnih sredstev. Namen FATF pa je razviti ustrezno politiko boja proti pranju denarja in financiranju terorizma.

FATF ima osrednjo pisarno v centrali OECD v Parizu (FATF 2012). V njenem okviru deluje tudi Odbor strokovnjakov Sveta Evrope za ocenjevanje ukrepov odkrivanja in preprečevanja pranja denarja ter financiranja terorizma (MONEYVAL). Poslanstvo MONEVAL-a je zagotoviti, da imajo vse države članice vzpostavljen ustrezen sistem za boj proti pranju denarja in financiranju terorizma ter da ustrezajo primernim mednarodnim standardom na tem področju, ki jih je vzpostavil FATF. MONEVAL ocenjuje sodelovanje članic po priporočenih mednarodnih standardih na pravnem in finančnem področju. Te ocene nudijo natančna priporočila za izboljšanje uspešnosti sistemov posameznih članic in nudijo smernice za uspešnejše sodelovanje na

[23] FATF je bila ustanovljena na pobudo skupine sedmih gospodarsko najrazvitejših držav G-7 na srečanju v Parizu. Članice G-7, Evropska komisija in osem drugih članic so FATF dodelile predvsem pregled tehnik, metod in trendov pranja denarja, pregled vseh dotedanjih aktivnosti na tem področju, tako na nacionalni kot mednarodni ravni, ter izdelati oceno in postaviti merila, standarde in ukrepe, potrebne za boj proti pranju denarja (Veselko 2004, 18).

mednarodnem področju. MONEVAL izvaja tudi tipološke študije na področju pranja denarja in financiranja terorizma.

Na srečanju oktobra 2010, je Svet ministrov sprejel resolucijo, s katero je MONEVAL od januarja 2011 neodvisen nadzorni mehanizem v okviru Sveta Evrope.[24]

7 PROGRAMI ZA ZBIRANJE IN IZMENJAVO INFORMACIJ Z NAMENOM PREPREČEVANJA TERORISTIČNIH DEJANJ

Teroristične skupine se za svoje delovanje poslužujejo vse bolj naprednih sistemov komuniciranja. Države pa že od nekdaj izvajajo nadzor, saj je to edini način, da so v koraku z njimi. Prestrezanje komunikacij je eden glavnih aspektov nadzora. Tako kot postajajo komunikacijski sistemi vse bolj napredni, napredujejo tudi sistemi za nadzor in metode prestrezanja informacij. Vlade sveta za razvoj tovrstnih sistemov porabljajo ogromne vsote denarja. Globalno naj bi po nekaterih ocenah temu bilo letno namenjeno celo med 15 in 20 milijardami dolarjev (Campbell v Bailey 2005).

Sicer pa sistemi tovrstnega nadziranja segajo daleč v zgodovino. Klasične prisluškovalne metode za nadzor pogovorov, ki so nekoč potekali predvsem osebno ali pa prek stacionarne telefonije, so v zadnjih letih domala povsem zamenjali sofisticirani sistemi elektronskega nadziranja. Tudi sistema, kot sta Echelon in Carnivore, nekoč zelo napredna, sta danes domala zastarela. Začetki sistema za nadzor Echelon, ki je v domeni ameriške Nacionalne varnostne agencije, segajo v čas po drugi svetovni vojni. V njem so poleg ZDA sodelovale še Kanada, Velika Britanija, Avstralija in Nova Zelandija. Namenjen je nadzoru civilnih komunikacij. Nekoč je bil uporabljan predvsem za nadzorovanje stacionarne telefonije in radijskih valov, kasneje pa tudi za pregledovanje vsebine po internetu. Gre za sistem zmogljivih računalnikov, ki procesirajo podatke ter izločijo tiste, ki ne ustrezajo iskalnim kriterijem. Največjo težavo sistemu povzroča to, da preiskovanje pisanega gradiva poteka prek ključnih besed, pri prenosu zvoka pa sistem

[24] Resolution CM/Res(2010)12.

prepoznava izrečene besede ali pa t. i. 'odtis glasu'. To pomeni, da se lahko teroristi nadzoru izognejo z uporabo šifer oz. t. i. odprte kode. Al Kaida je na primer izraz za bombo nadomestila z arabsko besedo za otroško hrano (Campbell 2001). V imenu osebe, katere odtis glasu varnostni organi že imajo, lahko govori kdo drug.

Sistem Carnivore pa je pod pristojnostjo ameriškega FBI in je namenjen izvajanju nadzora nad sistemom elektronske pošte. S sistemom Carnivore je mogoče ugotoviti, kdo so prejemniki in pošiljatelji sporočil. Kljub veliki zmogljivosti teh dveh sistemov vse večji promet tovrstnih komunikacij danes že presega njune zmožnosti. Carnivore je leta 2005 zamenjal izboljšani sistem NarusInsight (Fox News 2005). Dejstvo je, da so po napadih 11. septembra domala vse varnostne inštitucije pričele razvijati vrsto novih programov, namenjenih boju proti terorizmu na osnovi zbiranja in primerjav podatkov, ki bi lahko morebitne nove napade preprečili. Nekateri poskusni programi so, ko napadi leta 2011 v ZDA ter v letih 2004 in 2005 v Evropi še niso bili časovno oddaljeni, ugledali luč sveta. Mnogi so zaradi pritiskov civilne družbe zaradi pomislekov o varovanju osebnih podatkov in tudi zaradi astronomskih stroškov ugasnili. Med te spada tudi razvpiti program MATRIX – Multi-State Anti-Terrorism Information Exchange. Program je nastal na Floridi; analiziral naj bi vladne in komercialne baze podatkov z namenom pravočasnega odkrivanja osumljencev ali njihovih lokacij. MATRIX so prvič predstavili v Beli hiši leta 2003 ter takrat prejeli 4 milijone dolarjev od Pravosodnega ministrstva in kasneje še 8 milijonov dolarjev od Urada za domovinsko varnost. Program se je širil, nato pa kot TIA (Total Information Awareness), ki je prav zaradi očitkov ACLU (American Civil Liberties Union), da omogoča podrobno preiskovanje in nadzorovanje posameznikov, leta 2005 ugasnil. Še več negodovanja je povzročilo odkritje o zveznem financiranju programa in visokih stroških, ki jih posamezne države, sprva vključene v program, niso več zmogle. Številni drugi spodaj opisani programi pa so v uporabi, vendar ostaja vprašanje, v kakšnem obsegu delujejo. Njihovo delovanje je v številnih primerih v konfliktu s splošno sprejetimi normami človeških svoboščin, tovrstni programi pa so ne nazadnje tudi v domeni varnostno-obveščevalnih služb in tako že po sami naravi niso javni. Ne samo ZDA, tudi države Evropske unije že od nekdaj, še posebej intenzivno pa

po napadih v Madridu in Londonu, uporabljajo in razvijajo tovrstne programe. Eden izmed njih je projekt Check the Web.

7.1 Programi za zbiranje in izmenjavo informacij v ZDA

7.1.1 PROGRAMI ZA ZBIRANJE IN IZMENJAVO INFORMACIJ IAO

Information Awareness Office (IAO)[25] ali Urad informacijskega zavedanja je ustanovila Agencija za napredne obrambne raziskovalne projekte (Defense Advanced Research Projects Agency – DARPA) januarja 2002. S tem so želeli združiti več DARPA projektov, osredotočenih na izvajanje nadzora in uporabo informacijskih tehnologij za odkrivanje in spremljanje teroristov in drugih asimetričnih groženj nacionalni varnosti, in sicer z namenom, da dosežejo Total Information Awareness (TIA) ali popolno informacijsko zavedanje (Wikipedia 2012).

To bi dosegli z ustvarjenjem ogromne računalniške baze za zbiranje in shranjevanje osebnih podatkov vseh ljudi v Združenih državah Amerike, vključno z osebno e-pošto, socialnimi omrežji, evidenco kreditnih kartic, telefonskih klicev, zdravstvenih kartotek in številnih drugih virov, in to brez zahteve za nalog za preiskavo (Markoff, 2002). Te podatke bi nato analizirali z namenom odkrivanja sumljive dejavnosti, povezav med posamezniki in morebitnih grožnenj ali nevarnosti. Program je vključeval tudi sredstva za tehnologijo biometričnega nadzora, ki bi lahko identificirala in sledila posameznikom, med drugim tudi s pomočjo nadzornih kamer. Zaradi vse glasnejših javnih kritik, da bi razvoj in uvajanje te tehnologije lahko privedel do sistema množičnega nadzora, je ameriški kongres IAO leta 2003 sredstva ukinil. Več projektov IAO pa naj bi kljub temu še naprej prejemalo denar, delovali pa naj bi pod različnimi imeni (Harris 2006).

[25] V tem deli naloge povzemam programe, ki so jih vzpostavljali v okviru IAO. Podatke sem črpala z njihove uradne spletne strani www.IAO.com, ki pa je med tem že ugasnila, saj je ameriška vlada ukinila sredstva namenjena temu projektu.

IAO je začel s programom TIA februarja 2003, vendar ga je iz Total Information Awareness meseca maja preimenoval v Terrorist Information Awareness. Namenjen je bil integraciji informacijskih tehnologij v prototipski sistem, ki bi zagotovil lažje odkrivanje, klasificiranje in identificiranje potencialnih tujih teroristov s ciljem povečati možnosti pravočasne reakcije organov pregona in varnostnih služb.

Cilj programa TIA je bil oblikovanje protiteroristične informacijske arhitekture, ki bi združevala tehnologijo drugih programov IAO. Raziskoval, razvijal in inegriral naj bi tehnologije za virtualno agregacijo podatkov, da bi razvili modele, ki bi napovedali in opisovali s pomočjo obdelave podatkov, ti modeli pa bi skupaj z drugimi bazami podatkov lahko identificirali teroriste ali teroristične skup ine.

Ko so se pojavili prvi pomisleki v zvezi z nadzorom navadnih državljanov, je DARPA v govoru pred Kongresom maja 2003 še enkrat poudarila, da namen programa ni kopičenje dosjejev ameriških državljanov, temveč raziskati in razviti orodje, ki bi pooblaščenim agencijam dopuščalo zbiranje informacij o terorističnih skupinah. Kljub spremembi imena in tem zagotovilom so se kritike programa in pomisleki o njegovih možnih zlorabah kopičile.

Kot rezultat teh pritiskov je bilo to, da sta Kongres in Senat preklicala nadaljnje financiranje TIA. Vendar pa je, kot sem že omenila, jedro programa preživelo. Po nekaterih podatkih so TIA-projekti še naprej finančno podprti v okviru zaupnih aneksov k zakonom Obrambnega ministrstva in obveščevalnih agencij.

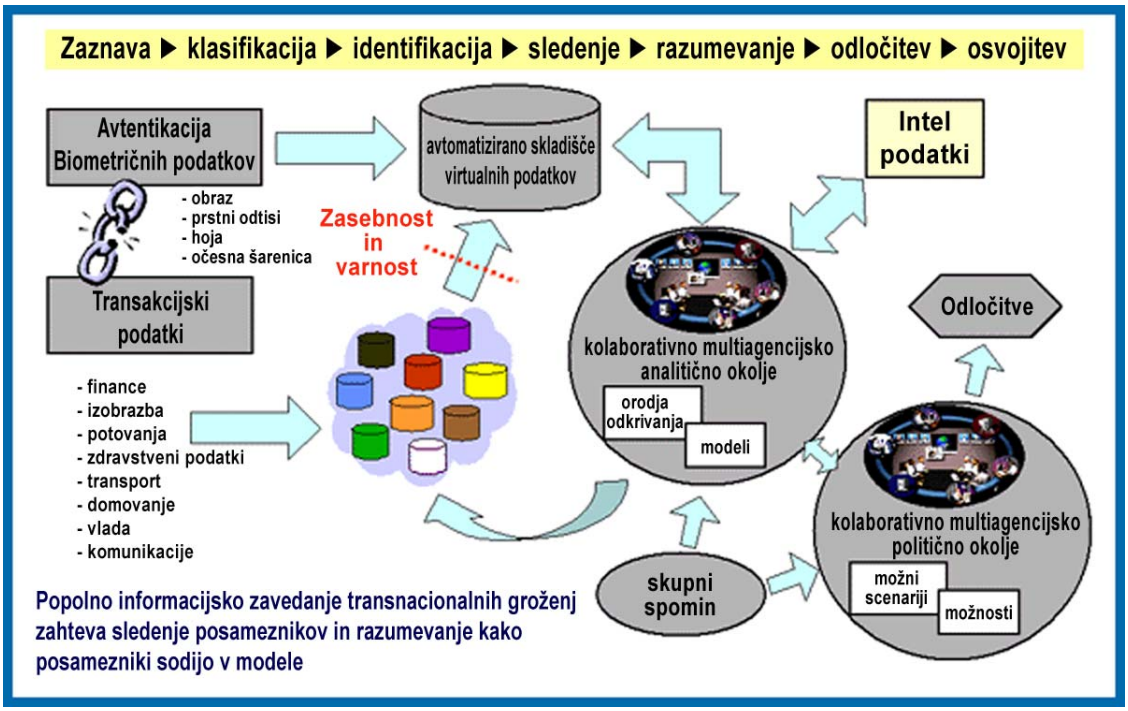
Ena izmed tehnologij, ki so jo poimenovali Basketball,[26] je prototip IAO; drugi projekt se imenuje TopSail,[27] prej Genoa II, in zagotavlja IT orodja za možnost napovedovanja in predvidevanja terorističnih napadov.

---

[26] Čeprav ni jasno, ali Basektball še deluje, naj bi bil ta program po javnosti dostopnih dokumentih prototip sistema za predčasno opozarjanje in odločanje na podlagi navzkrižne primerjave informacij in analize (Harris 2006).

[27] Še en projekt, ki je prišel pod okrilje ARDA, je Top Sail. Cilj projekta Top Sail je »razviti orodja, ki bodo v pomoč obveščevalnim analitikom pri predčasnemu napovedovanju terorističnih groženj ameriškim

Slika 7.1: Diagram sistema popolnega informacijskega zavedanja



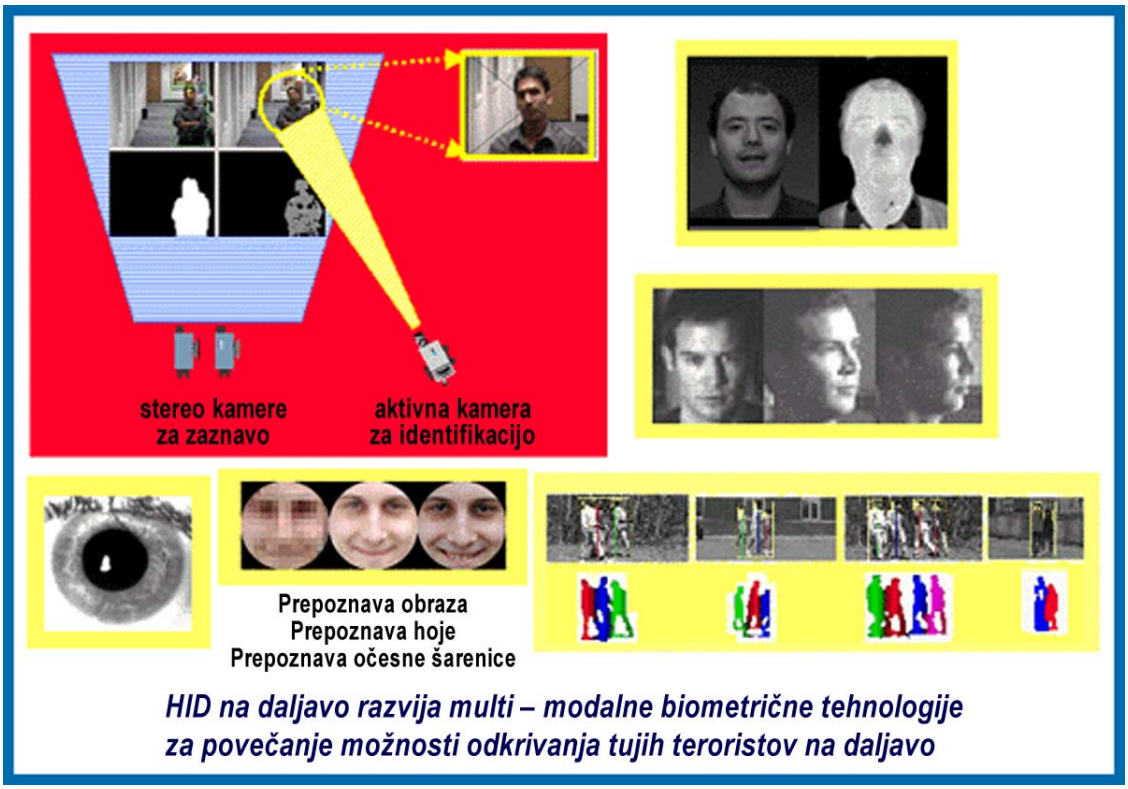
Vir: Uradna spletna stran IAO (2003)

IAO je bila ustanovljena, ko sta admiral John Poindexter, nekdanji svetovalec ameriškega predsednika Ronalda Reagana, in vodilni v SAIC, Brian Hicks, ministrstvu za obrambo predstavila idejo za program informacijske zavesti po napadih 11. septembra 2001. Poindexter in Hicks sta že prej sodelovala pri podobnih programih za DARPA. Ta je program sprejela in leta 2002 imenovala Poindexterja za vodjo. IAO je pričela s financiranjem raziskav in razvoja programa TIA. Med najbolj odmevnimi programi, ki danes naj ne bi več delovali, po mnenju mnogih pa so le preoblikovani, so naslednji:

interesom«. To je skoraj enak opis, kot ga je pred leti imel program Genoa II. Prav tako ime programa izhaja iz navtične nomenklature – "genoa" je namreč sinonim za glavno jadro (headsail) ladje (Harris 2006).

HumanID – omogočanje identifilkacije na daljavo.

Slika 7.2: Človeška identifikacija na daljavo – HumanID



Vir: Uradna spletna stran IAO (2003)

To je postopek, ki s pomočjo avtomatiziranih biometričnih tehnologij odkriva, prepozna in identificira ljudi z velike razdalje. Na uradni strani IAO so navedeni naslednji cilji programa HumanID:

• Razvoj algoritmov za iskanje in lociranje v območju 150 metrov.

• Združiti prepoznavo obraza in hoje v sistemu, ki deluje neprekinjeno.

• Razviti in demonstrirati sistem človeške identifikacije, ki deluje na območju 150 metrov z uporabo vidne podobe.

• Razviti radarski sistem z malo porabo energije za široko področje odkrivanja in ozek pogled za klasifikacijo hoje.

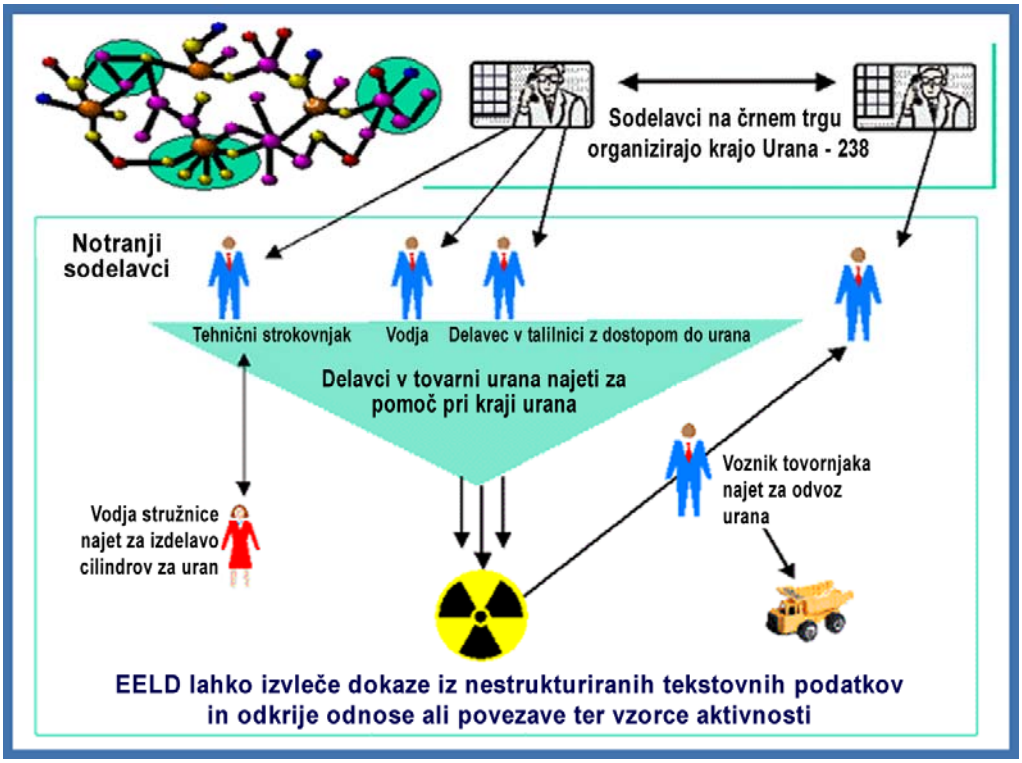
• Karakterizirati hojo s posnetka iz daljave.

• Razviti multispektralen infrardeč vizualni sistem za prepoznavanje obraza.

EELD – Izločevanje dokazov in odkrivanje povezav

Evidence Extraction and Link Discovery (EELD) je program, namenjen razvoju tehnologij in orodij za samodejno odkrivanje, pridobivanje in povezovanje na videz nepovezanih dokazov iz velike količine tajnih podatkov. To so npr. zapisi telefonskih klicev iz baze podatkov NSA, zgodovina interneta, bančni podatki.

Slika 7.3: Diagram, ki pojasnjuje delovanje EELD



Vir: Uradna spletna stran IAO (2003)

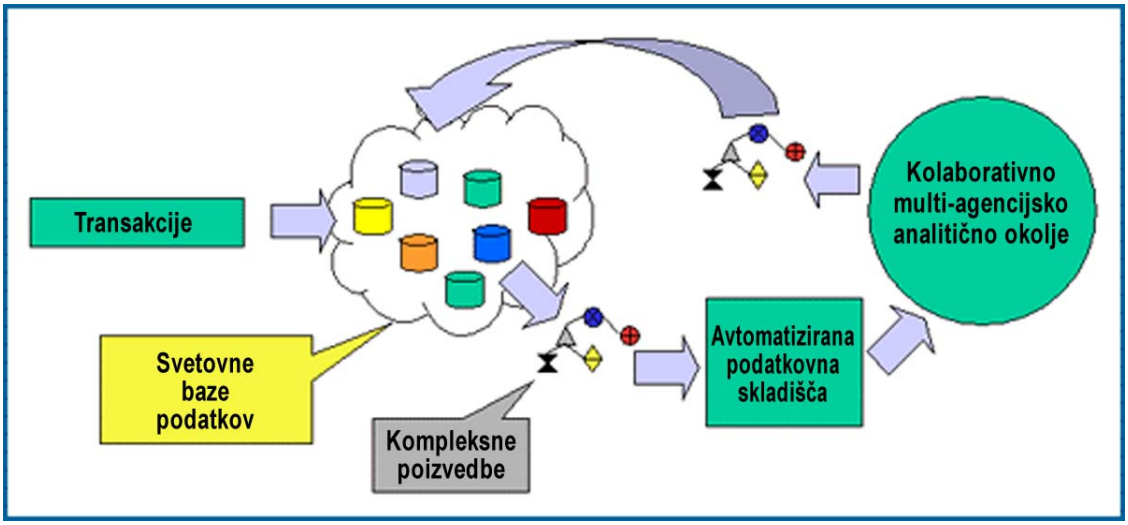
EELD je bil zasnovan za oblikovanje sistemov z možnostjo izpisa podatkov iz različnih virov (npr. besedilna sporočila, socialna mreženja, finančne evidence, spletne strani). Namenjen je odkrivanju vzorcev, ki zajemajo več vrst povezav med podatki in komunikacijo (npr. finančne transakcije, komunikacije, potovanja itd).

Njegov namen je povezati elemente, ki se nanašajo na potencialne "teroristične skupine" in scenarije, ter prepoznavanje vzorcev različnih skupin ali scenarijev za določitev novih organizacij in nastajajoče nevarnosti.

GENISYS

Genisys je namenjen razvoju tehnologij, ki bi omogočile "izjemno veliko skladiščenje informacij vseh virov.

Slika 7.4: Prikaz skladiščenja podatkov



Vir: Uradna spletna stran IAO(2003)

Za zbiranje, organizacijo in analizo ogromnih količin podatkov je bila takrat obstoječa tehnologija nezadostna. Zato so razvili tehnologijo za virtualno agregacijo podatkov, s katero bi lahko uspešno analizirali heterogene baze podatkov, kot tudi nestrukturirane javne baze podatkov, kot je npr. internet. Efektivna analiza med heterogenimi bazami podatkov pomeni sposobnost zbrati informacije iz baz podatkov, ki so namenjene shranjevanju različnih zvrsti informacij. Na primer baz s podatki o kriminalni preteklosti, baze podatkov s telefonskimi klici z bazami podatkov tujih obveščevalnih agencij. Splet

je na primer nestrukturirana baza javnih podatkov, ker je javno dostopen in vsebuje mnogo različnih tipov informacij ali podatkov (blogi, elektronska pošta, zgodovina ogledov …), vse pa je treba analizirati in učinkovito skladiščiti. Drugi cilj je bil razviti veliko, porazdeljeno arhitekturo sistema za upravljanje velike količine surovih podatkov, rezultatatov analiz in povratnih informacij z namenom pridobiti preprostejši rezultat, bolj prilagodljivo shranjevanje podatkov, ki dobro deluje ter nam omogoča zadržati in skladiščiti pomembne podatke za nedoločen čas.

SSNA – Analiza socialnih omrežij

Opis SSNA na uradni spletni strani IAO[28] je strnjen s citatom Seana McGahana z Univerze Northeastern, ki je v študiji SSNA povedal naslednje: »Namen programa SSNA je razširiti tehnike socialnih omrežij za pomoč pri razlikovanju med morebitnimi terorističnimi celicami in legitimnimi skupinami ljudi. Da bi bili uspešni, bi moral SSNA zahtevati podatke o socialnih interakcijah večine ljudi po vsem svetu, saj ni mogoče zlahka razlikovati med miroljubnimi državljani in teroristi«.

TIDES – Translingual Information Detection, Extraction and Summarization

TIDES (čezjezikovno zaznavanje, ekstracija in povzetje informacij) bi s pomočjo napredne tehnologije procesiranja jezika omogočal angleško govorečim ugotoviti in interpretirati ključne informacije v številnih tujih jezikih, ne da bi za to morali ta jezik tudi obvladati.

Genoa in Genoa II

Program se osredotoča na zagotavljanje naprednih orodij za odločanje za hitro obravnavo in prilagajanje dinamiki kriznega upravljanja ter omogoča sodelovanje med agencijami v realnem času. Imel naj bi še drugo funkcijo: omogočal naj bi pripravo ocene in možnih bodočih scenarijev, s tem pa bi pomagal pri odločitvah obveščevalcev. Na podoben način deluje program Deep Green, ki asistira vojaškim poveljnikom pri sprejemanju odločitev na bojišču.

[28] Uradna spletna stran IAO je kmalu po letu 2004, ko je IAO uradno prenehala delovati, ugasnila.

EARS – Effective Affordable Reusable Speach to text

Cilj tega programa je razviti hitrejšo tehnologijo pretvorbe govora v besedilo v več jezikih.

7.1.2 PROGRAM ZA ZBIRANJE IN IZMENJAVO INFORMACIJ MATRIX

MATRIX, večdržavni protiteroristični program za izmenjavo informacij, je bil ameriški zvezno financirani program za obdelavo podatkov, sprva razvit za zvezno državo Florido in opisan kot orodje za identifikacijo teroristov. Sistem naj bi analiziral vladne in komercialne baze podatkov in odkrival povezave med osumljenci oziroma jih odkrival . Baza podatkov in tehnologija, ki jo je MATRIX uporabljal, je bila last floridskega podjetja Seisint, ki ga je nedavno prevzel Lexis Nexis. Program so prenehali uporabljati junija 2005, ko so mu ukinili zvezno financiranje zaradi vse glasnejših kritik v zvezi z zasebnostjo in državnim nadzorom. Idejno ga je zasnoval Hank Asher, ki je kmalu po napadih 11. septembra floridskim organom pregona zatrdil, da pozna način, kako ujeti ugrabitelje oziroma potencialne teroriste. Ko so sistema leta 2003 predstavili v Beli Hiši, je od ameriškega pravosodnega ministrstva prejel 4 milijone USD nepovratnih sredstev ter 8 milijonov USD od Urada za domovinsko varnost. Kmalu so program prevzele številne druge zvezne države.

Kot verjetna bodoča uporabnika sta se omenjala tudi zvezna vlada in CIA. Podobnost med MATRIX-om in programom TIA, ki je bil ukinjen zaradi spornih posegov v zasebnost državljanov, je verjetno pripomogla k ukinitvi tudi tega programa.

Na uradni spletni strani MATRIX je zapisano, da bi zbrani podatki zaobjemali kriminalno preteklost posameznikov, podatke iz vozniških dovoljenj[29] in o registraciji vozil, fotografije iz vozniških izpitov, poročne in ločitvene dokumente, številke

[29] V ZDA ima vozniško dovoljenje podobno vlogo kot v Sloveniji osebna izkaznica; najpogosteje predstavlja edini vir identifikacije državljana. Potni list, ki bi prav tako lahko veljal za uradni osebni dokument, ima namreč po podatkih iz leta 2010 le 38 % Američanov (The Expeditioner 2012).

socialnega zavarovanja, datume rojstva ter imena družinskih članov, sosedov in sodelavcev. Vsi ti podatki so vladi na voljo brez potrebnega naloga. Pri ACLU[30] pa so bili prepričani, da bi se tem kmalu pridružili še podatki iz komercialnih baz , kot na primer nakupovalne navade, naročnine, dohodki in zgodovina zaposlitve. MATRIX bi nato kombiniral obe bazi podatkov. Kot TIA bi tudi sam uporabil »data mining« ali obdelavo podatkov, pri čemer bi iskal vzorce, ki bi obremenjevali potencialne osumljence.

7.1.3 PROGRAMI V OKVIRU FBI

V skladu z napredkom tehnologije in trendi komuniciranja tudi FBI intenzivno razvija in izboljšuje sistem, ki bi dovolj zgodaj opozoril na možne grožnje doma in po svetu. Federal Bureau of Investigation ali Zvezni preiskovalni urad je najbolj prepoznaven s kratico FBI. Poznamo jo v strokovnih krogih, v katerih velja za elitno policijsko organizacijo, zaradi velike medijske izpostavljenosti predvsem v filmih in na televiziji pa jo pozna tudi velik del javnosti. Od začetkov v začetku 20 stoletja, ko je FBI štel le 34 posebnih agentov, pa do danes, ko je to ena največjih policijskih agencij na svetu, se je spremenilo veliko. V prvih vrstah boja proti terorizmu v okviru FBI so majhne celice visoko usposobljenih predanih preiskovalcev, analitikov, jezikoslovcev, SWAT strokovnjakov in drugih ekspertov, zbranih iz številnih ameriških zakonodajnih organov in obveščevalnih agencij. Sledijo namigom, zbirajo podatke, varujejo, aretirajo, usposabljajo, izmenjujejo podatke in reagirajo, ko je to potrebno. To so skupne delovne skupine v boju proti terorizmu ali Joint Terrorism Task Forces – JTTF (FBI 2012). Projektne skupine so locirane v 103 mestih po vsej državi, vključno z vsaj eno v vsakem od 56 področnih uradov. Danes imajo JTTF po ZDA prek 4400 članov, tj. več kot štirikrat toliko kot pred napadi 11. septembra. Na spletni strani JTTF je zapisano, da »so, kar zadeva teroristično dejavnost, prostor z informacijami na enem mestu. Tukaj je vzpostavljena enotna informacijska baza za vse agencije. Tukaj se združujejo znanje,

[30] ACLU – American Civil Liberties Union je nevladna, neprofitna organizacija za zaščito človekovih pravic in svoboščin. Ustanovljena le bila leta 1920 v prvi vrsti za zaščito svobode govora. Danes ima več kot 500.000 članov ter 100 milijonov USD letnega proračuna.

sposobnosti in talent različnih zakonodajnih in obveščevalnih agencij v eni sami enoti, ki se odziva skupno.«

V skladu z napredkom tehnologije in trendov komunikacij je FBI pričel še z razvojem aplikacije, ki bi obveščala o grožnjah s spletnih socialnih omrežij (Dnevnik, 3. 2. 2012). Kot so zapisali, mora biti aplikacija fleksibilna in se mora prilagajati spreminjajočim se grožnjam ter nuditi strateško in taktično prednost uporabnikom. FBI jo bo uporabljal tudi v boju proti spletnemu kriminalu, vgrajeno pa bo imela tudi možnost avtomatskega preiskovanja ključnih besed in prepoznavanja groženj.
Poleg tega bo morala ob zaznani grožnji prikazati tudi točen geografski položaj, da bi lahko organi pregona čim hitreje reagirali. V dokumentu, ki opisuje FBI-jeve zahteve glede nove aplikacije, je zapisano: "Družbeni mediji so primaren vir informacij, saj so na njih objavljeni prvi odzivi na ključne dogodke, iz njih pa lahko dobimo tudi prva opozorila pred prihajajočimi grožnjami." (TG Daily 2012.) FBI na svoji spletni strani trdi, da gre pri programski opremi, ki jo zdaj raziskujejo, za "aplikacijo ki jo uporabljajo druge vladne agencije," in da se "aplikacija ne bo osredotočala na specifične osebe ali pa varovala skupin, temveč bo pazila na besede in aktivnosti, ki sodijo pod kršitve zveznega kazenskega prava oz. grožnje nacionalni varnosti." (FBI 2012.) Sodeč po pisanju News.com je ameriški FBI predlagal tudi zakon, s katerim bi ponudniki programske opreme za VoIP komunikacijo v svoje programe morali vgraditi določeno opcijo (wiretap-friendly), ki bi uradnim oblastem omogočila nemoteno spajanje na omrežje in s tem posledično prisluškovanje in nadzor komunikacij med uporabniki. Isti zakon bi veljal tudi za družbena omrežja, kot sta Facebook in Google+, ter tudi za storitve spletne pošte. Pri FBI-ju namreč menijo, da je to normalna evolucija policijskih aktivnost, ki morajo slediti razvoju informacijskih tehnologij. Organi pregona po vsem svetu imajo namreč po večini zakonsko pravico do prisluškovanja telefonskim pogovorom določenih osumljencev, pri čemer so jim telekomunikacijski ponudniki dolžni ponuditi »infrastrukturo« za prestrezanje klicev, medtem ko takšni zakoni za spletno komunikacijo ne obstajajo. Tega se zavedajo tudi številni kriminalci, ki za medsebojno komunikacijo vse bolj uporabljajo prav internet. FBI je že začel kontaktirati s podjetji, kot so Microsoft, Facebook in ostalimi, ki bi mu ob sprejetju zakona lahko olajšali prisluškovanje. Pri

Microsoftu so komentirali, da je FBI-jev predlog »področje, na katerem ima Microsoft stalni interes«, temu pa niso dodali nadaljnjih pojasnil, medtem ko pri Facebooku, Googlu in Yahoojo novega predloga zakona niso želeli komentirati (Računalniške novice 2012).

7.1.4 PROGRAMI V OKVIRU PENTAGONA

Tudi Pentagon želi razviti posebne programe, s katerimi bi lahko predvideval delovanje kriminalnih združb in hekerjev, ki se med seboj povezujejo prek interneta. S kontrolo družbenih omrežij bi lahko namreč bolje nadzirali tudi terorizem. S posebnimi orodji tako želijo "prečesati" spletne strani in družbena omrežja, kot sta Facebook in Twitter, da bi lahko analizirali dinamiko kriminalnih skupin. Želijo ugotoviti tudi, kako skupine rekrutirajo nove člane in kdo so njihove tarče. Prav tako jih zanimajo programi, s katerimi bi razbrali konflikte med skupinami in šibke člene, kar bi oblasti lahko izkoristile v svoj prid ter razbile takšne skupine. V Pentagonu tako upajo, da se bodo uspeli v bližnji prihodnosti bolje soočali z grožnjami kriminalnih združb, ki svoje delovanje organizirajo s pomočjo interneta (24 ur.com 2012).

7.2 Programi za zbiranje in in izmenjavo informacij v Evropski uniji

Ker terorizem predstavlja grožnjo varnosti, svobodi in vrednotam Evropske unije ter njenim državljanom, je ukrepanje EU namenjeno zagotavljanju ustreznega, prilagojenega odziva v boju proti temu pojavu. In prav preprečevanje je ob zaščiti, pregonu in odzivu eden izmed štirih stebrov celovitega pristopa pri tem ukrepanju . Usklajevanje med organi pregona in pravosodnimi organi v EU ter mednarodno sodelovanje sta prav tako pomembna za zagotovitev učinkovitosti boja proti temu nadnacionalnemu pojavu. Osrednjo vlogo v okviru EU pri tem igra Europol. Od držav članic mora prejeti potrebne informacije, da lahko opravlja svoje naloge, zlasti lahko razvije delovne datoteke za analizo terorizma in projekte delovne skupine za boj proti njemu. S posredovanjem

ustreznih informacij Europolu oziroma z njihovim nalaganjem v Europolov informacijski sistem vsaka država članica prispeva h krepitvi varnosti EU kot celote. Europol lahko nato analizira informacije držav članic in drugih mednarodnih partnerjev.

V Evropolovem poročilu iz leta 2011 je zapisano, da se je v tem letu zgodilo 174 terorističnih napadov, kar je sicer manj od 249, ki so se zgodili leta 2010. Res pa je, da so prijeli tudi manj teroristov. Leta 2010 so jih ujeli 611, lani pa 484.

Tabela 7.1: Število terorističnih napadov se je zmanjšalo

Leto	**Število napadov**	**Število prijetih teroristov**
2010	249	611
2011	175	484

Vir: Europolovo poročilo (2011)

V raziskavi pa so še posebej opozorili na "volkove samotarje"; taka sta bila lani in letos norveški množični morilec Anders Behring Breivik in francoski morilec na skuterju Mohamed Merah.[31]

7.2.1 PROGRAM CHECK THE WEB

Ker igra internet pomembno vlogo pri logistiki, operativi in komunikacijah terorističnih organizacij, ga je pod lupo vzela tudi Evropska unija. Osnovni namen in cilj njenega spopada s tem pojavom sta predvsem uporaba interneta z namenom radikalizacije in

[31] Podobno kot v lanski raziskavi je Europol tudi letos še posebej opozoril na splet in dejstvo, da teroristične in ekstremistične organizacije veliko večino komunikacije danes opravijo prek interneta. Uporabljajo ga tako za propagando kot za iskanje novih članov in zbiranje denarja; največkrat to počnejo prek družbenih mrež. Internet jim daje možnost za spletni terorizem, omogoča jim tudi napade na glavne operativne sisteme držav Evropske unije, še dodaja Europol (Dnevnik 2012).

novačenja teroristov. Svet Evrope je tako podprl pobudo Nemčije za ustanovitev programa Check the Web. V pobudi je poudarjen pomen medsebojnega sodelovanja držav članic v boju proti uporabi interneta v teroristične namene. Teroristi ga uporabljajo za komuniciranje in propagando ter tudi za pridobivanje novih članov, njihovo urjenje, posredovanje navodil o tem, kako storiti določeno kaznivo dejanje, prenos informacij in tudi za financiranje svojih dejavnosti. Cilj pobude Check the Web je okrepiti sodelovanje in delitev nalog spremljanja ter ocenjevanja internetnih virov na prostovoljni bazi. Na področju usklajenega spremljanja in ocene islamskih terorističnih spletnih strani v okviru projekta so izvedli že vrsto uspešnih preiskav. Informacijski portal Europola je ključnega pomena za medsebojno sodelovanje držav članic (Poročilo Sveta Evrope 2007). Drugi način boja proti terorizmu na področju informacij so že prej omenjene tehnično posodobljene baze podatkov, ki so dostopne organom pregona v vseh državah članicah Evropske unije.

7.3 Protiteroristične telefonske linije

Eden izmed načinov zbiranja informacij, ki je še najmanj tehnološko napreden in preprost, pa vendarle v nekaterih primerih zelo učinkovit, so protiteroristične telefonske linije. Takšno telefonsko linijo[32] je uvedel na primer Scotland Yard, nanjo pa se lahko obrnejo posamezniki, ki bi radi prijavili primere morebitnega sumljivega vedenja. S preprostim nagovorom se pri tem poziva ljudi, da so na preži za nenavadnim. Spodbuja se jih, naj upoštevajo svoje instinkte in po prijavi pustijo strokovnjakom, da presodijo, ali se morda motijo. Kot sumljiva se pri tem opredeli oseba:

- ki kupi ali hrani veliko količino kemikalij oz. gnojil brez razvidnega razloga;
- ki kupi ali najame vozilo v sumljivih okoliščinah;
- ki brez posebnega razloga poseduje potne liste in druge osebne dokumente z različnimi imeni;
- ki veliko potuje in je dlje časa odsotna ter o tem ne govori oz. se izmika odgovorom.

[32] Protiteroristična telefonska linija, ki jo je uvedel Scotland Yard, se imenuje »It's probably nothing, but …« oziroma »Najverjetneje ni nič, pa vseeno …«. S tem so želeli spodbuditi morebitne očividce sumljivih dejanj, naj kljub temu, da se opaženo zdi nepomembno, to sporočijo pristojnim organom, saj obstaja možnost, da gre dejansko za teroristično dejavnost.

Podobno proteroristično linijo ima tudi Avstralska vlada.[33] To je skupna kontaktna točka za javnost, da poroča o morebitnih sumljivih dejanih, povezanih s terorizmom. Klicatelju nudi še povratne informacije, ki zadevajo področje nacionalne varnosti. (National Security Hotline 2012).

V nekoliko slabo luč pa je tovrstne telefonske linije postavila skupina hekerjev, ki so vdrli v britansko protiteroristično telefonsko linijo in posneli pogovore med uslužbenci te linije ter tudi pogovore, ki so jih sami imeli z osebjem te službe (SIOL 2012a). Še istega dne so policisti pridržali najstnika, stara 16 in 17 let, ki naj bi bila člana organizacije Team Poison. Ta je za hekerski napad prevzela odgovornost, telefonske linije pa naj bi napadla zaradi neutemeljenega zapiranja ljudi, obdolženih terorizma, in zaradi nedavne odločitve Velike Britanije, da nekatere pridržane, ki so bili osumljeni terorizma, deportira v ZDA. Ob tem naj bi jih motili tudi načrti britanske vlade, da sprejmejo t. i. zakon o »vohljanju«, ki bi varnostnim agencijam dovoljeval več dostopa do osebnih komunikacij. Člani Team Poison naj bi za napad uporabili razpoložljiv in vsakomur dostopen software, svojo aktivnost pa so, da bi prikrili sledi, speljali prek strežnika v Maleziji (Telegraph 2012).

Podobno se je zgodilo tudi v Nemčiji. Tam so hekerji odkrili trojanskega konja, program, ki naj bi ga oblasti uporabljale za nadzor zasebne uporabe spleta, elektronske pošte in pogovorov v klepetalnicah. Ker so v klubu hekerjev iz Berlina Chaos Computer Club (CCC) menili, da je tak program protizakonit in protiustaven, so zahtevali, da se ga uniči. Čeprav je nemška zvezna policija zanikala uporabo tega 'trojanca', so policije kar pet nemških zveznih dežel priznale uporabo t. i. Bundestrojaner ali zveznega trojanskega konja pri nadzoru kriminalcev, povezanih s preprodajo drog. Ob tem pa so zagotovile, da nikoli ni šlo za protizakonito rabo tega programa . Bundestrojaner je namreč le oddaljeno preiskovanje oziroma program za nadzor vsebin, do katerih uporabniki dostopajo prek interneta. Za vsak posamezni primer naj bi bil prilagojen, odobriti pa ga mora tudi sodišče. Prikrita preiskava se izvaja tako, da se na računalnik osumljenca namesti ustrezen program, trojanski konj, ki neopazno pregleda vsebino podatkov na računalniku,

[33] Avstralska protiteroristična telefonska linija se imenuje The National Security Hotline.

pošto, shranjene dokumente, obiskane spletne strani itd. Tovrstne podatke je mogoče analizirati in ločiti pomembne od nepomembnih že v računalniku preiskovanca. Program se kasneje neopazno uniči (Podpečan v Vidic 2011).

8 ŠTUDIJA PRIMERA PREPREČENEGA TERORISTIČNEGA NAPADA

Vprašanje, na katerega si skušam v tej magistrski nalogi odgovoriti, je, ali programi za preprečevanje terorističnih dejanj delujejo. Sama sem v času pisanja naloge najverjetneje večstokrat v različne iskalnike na svetovnem spletu vtipkala besedo terorizem ali pa besedno zvezo, ki jo je vsebovala. Iz podatkov v moji knjižnični članski izkaznici bi prav tako lahko ugotovili, da sem brala nenavadno veliko literature na temo terorizma. Še več, precejšen odstotek e-pošte in SMS-sporočil se je navezoval na področje terorizma. Obiskovala sem spletne strani, namenjene podpornikom različnih terorističnih organizacij, spremljala twite, si prek spleta ogledala nekaj dokumentarcev na temo terorizma ter odkrivanja in preprečevanja morebitnih terorističnih napadov. Če tovrstni programi delujejo, se je nekje zagotovo ob mojem imenu prižgala »rdeča luč«. Ker v času nastajanja magistrske naloge nisem dobila nobenega obiska s strani organov pregona ali varnostnoobveščevalnih služb,[34] lahko sklepam, da računalniški programi za odkrivanje in preprečevanje terorističnih dejanj ne delujejo dovolj dobro, ali pa, da tovrstni programi delujejo zelo dobro in so ob zgoraj naštetih informacijah pri oblikovanju odločitve upoštevali še naslednje podatke in informacije: oseba je študentka, ki je v iskalnike velikokrat vtipkala tudi besedno zvezo »magistrska naloga«, njena kartoteka ne vsebuje nobenih zaznamkov, potovala ni v nobeno od glede na terorizem potencialno rizičnih držav . Iz tega sledi, da jo to področje zanima in mu je namenila veliko svojega časa zgolj zaradi pisanja magistrske naloge. To sklepanje je skladno z informacijsko piramido.

[34] Da to ni tako zelo nemogoče, zagotovo ve Tomi Sluga iz Radgone. 20. maja 2001, le nekaj dni pred srečanjem Busha in Putina v Ljubljani, je na naslov Bele hiše poslal elektronsko pismo: "Rešite Zemljo, vi tepci, ubili vas bomo v Ljubljani. Dobrodošli!" Čez nekaj tednov so na njegova vrata potrkali možje postave in mu zasegli računalnik. Ameriški varnostni organi so namreč slovensko policijo obvestili, kaj je zagrešil. Na prvem sojenju je bil obsojen na štiri mesece zaporne pogojne kazni. Decembra 2005 je višje mariborsko sodišče sodbo razveljavilo, na ponovljenem sojenju pa je bil leta 2007 oproščen. (Bedek 2007)

Kaj pa teroristični napadi, ki so jih varnostnoobveščevalne službe in organi pregona preprečili? Eden izmed najodmevnejših poskusov razstrelitve letala z vnosom tekočega eksploziva[35] je in še vpliva na način potovanja potnikov.

Trojica teroristov je namreč leta 2006 nameravala na letala pretihotapiti tekoči eksploziv, in sicer v steklenicah brezalkoholnih pijač, v baterijah in drugih izdelkih, ki so bili običajni v ročni prtljagi potnikov. Eksploziv naj bi detonirali, ko bi bila letala v zraku. Britanski varnostni organi so tedaj preprečili tragedijo, zaradi terorističnega načrta pa so bili sprejeti poostreni ukrepi glede vnosa tekočin na letala. Sodišče je kasneje presodilo, da je trojica vodila teroristično zaroto, v kateri bi, če bi uspela, umrlo največ ljudi po terorističnem napadu v ZDA 11. septembra 2001. To je bila do takrat obveščevalna operacija brez primere, v kateri je sodelovalo na stotine policistov. Zbrali so 26.000 dokazov, opravili 102 hišni preiskavi, zasegli 80 osebnih računalnikov in drugih elektronskih naprav, kar 226 računalnikov iz internetnih lokalov, 15.000 CD-jev, 500 mehkih diskov, zbrali 14.000 gigabajtov podatkov, obiskali Japonsko (zaradi tipa baterij, ki so jih teroristi uporabili), Pakistan, Južno Afriko, Mavricius in Belgijo (Met Police 2007). Zgodba[36] se je pričela kmalu po Al Kaidinih napadih 11. septembra 2001. Ameriška vojska je vstopila v Afganistan, desetletja trajajoča kriza z begunci se je zaostrila. The Islamic Medical Association, dobrodelna organizacija v Londonu, je zbirala denar in opremo za begunce na meji med Afganistanom in Pakistanom. Abdull Ahmed Ali in Assad Sarwar sta z zbrano pomočjo odpotovala v begunsko taborišče ter bila zgrožena nad tem, kar sta tam videla. Ali, vodja kasnejše trojice teroristov, je zaradi nakopičene jeze poiskal somišljenike pri radikalnih islamistih, ki so vse bolj zahtevali maščevanje nad Britanci.

[35] Prepoved vnosa tekočin na letala v EU-ju ostaja, saj je Evropska komisija julija letos sklenila, da rok za odpravo prepovedi preloži. Za to bodo potrebne izkušnje z novo opremo, s katero bodo na letališčih preverjali steklenice in embalažo tekočin. Trenutno lahko potniki na letališčih v Evropski uniji v ročni prtljagi na letala prinesejo tekočino v embalaži z največ 100 mililitri kapacitete. Embalaže morajo biti shranjene v prozornih plastičnih vrečkah. S tem želijo preprečiti, da bi teroristi na letala pretihotapili eksplozivne snovi. Sprva je bilo predvideno, da bi EU prepoved, ki jo je uvedel leta 2006 zaradi terorističnih groženj, odpravil že leta 2011(STA, 18. julij 2012). http://www.rtvslo.si/evropska-unija/prepoved-vnosa-tekocin-na-letala-v-eu-ju-ostaja/287666

[36] Zgodbo sem povzela po dokumentarcu Liquid Bomb Plot na National Geographic ter po člankih na BBC News, Reuters in STA.

Obveščevalci, ki so imeli te radikalne ektremiste ves čas pod budnim očesom, so postali pozorni na Alija. Agenti MI5 so pri njegovem povratku v Veliko Britanijo junija 2006 na skrivaj preverili njegovo prtljago in našli po njihovem mnenju neobičajno pijačo v prahu, Tang, in večje število velikih baterij. V tednih, ki so sledili, so Metropolitanska policija in MI5 pričele operacijo, ki je postala največja v zgodovini Združenega kraljestva. Med tem časom je Ali pričel pošiljati elektronsko pošto v Pakistan. Vsebina zakodiranih sporočil je postala jasna šele po aretacijah: bila so sporočila Jihadskim sodelavcem, povratna sporočila so dala zeleno luč za nadaljevanje projekta ali prezentacije, kot so ga poimenovali. Sarwar je medtem kupoval neobičajne predmete, vodikov peroksid, sicer legalno kemikalijo, ki pa lahko postane smrtonosna.[37] Komunikacija prek elektronske pošte se je nadaljevala. Ko so agentje MI5 vdrli v Alijevo stanovanje, so bili presenečeni nad najdenim (glej prilogo 2). Kar so našli, je še najbolj spominjalo na laboratorij za izdelavo bomb, vendar nekoliko neobičajen. 3. avgusta je mikrokamera zabeležila Alija in sostorilca Tanvirja Husseina, kako izdelujeta neznane predmete iz plastenk. Obveščevalci so kasneje opazovali Ahmeda Alija še v internetnem lokalu, ko je kar dve uri raziskoval urnike letov. Stvari so kmalu postale jasne. Plastenke so postajale bombe, sicer majhne, vendar dovolj velike, da v trup letala naredijo luknjo.[38]

To je samo ena izmed odmevnih protiterorističnih operacij in hkrati prikaz uspešnega sodelovanja različnih resorjev in agencij, ki se ukvarjajo z bojem proti terorizmu. Policisti, varnostniki na letališčih, protiobveščevalne službe, v tem primeru MI5, ter tehnologija – nadzorne kamere, ki so zabeležile nakupe pripomočkov za izdelavo bomb, internet, elektronska pošta (glej prilogo 1) – so samo v sodelovanju in ob delitvi informacij lahko preprečili načrtovani morilski načrt. Ob delu je bilo tudi nekaj napak,

[37] Tudi v tem primeru so teroristi pri komunikaciji uporabljali t. i. odprto kodo. »Vodica po britju Calvin Clein« je bila, kot se je kasneje izkazalo, koda za vodikov peroksid. Količina vodice po britju CK je namreč ustrezala količini vodikovega peroksida, ki ga je Sarwar kupoval.

[38] Leta 2001 je Richard Reid poskušal ubiti vseh 197 potnikov in članov posadke letala družbe American Airlines na poti iz Pariza v Miami. Med poletom je želel sprožiti v športnih copatih skrito majhno razstrelivo. Tako varnostno obveščevalne službe kot organi pregona so pričakovali, da bodo teroristi še poskušali z uporabo majhnih eksplozivnih sredstev.

predvsem pa očitkov, da so vodje protiteroristične akcije načrtovalce napada predolgo opazovali in jim sledili ter s tem potencialno ogrozili življenja morebitnih žrtev napada.[39]

Iz opisanega izhaja, da je oblikovanje učinkovitega koncepta sistemske zaščite, tako na nacionalnih kot na globalnem nivoju, nujno. Samo uspešno in intenzivno sodelovanje med inštitucijami v ZDA in v Evropi ter zbiranje in preglednost informacij na enem mestu zagotavlja uspešnost boja tako proti organiziranemu kriminalu kot posredno tudi proti pojavu mednarodnega terorizma.

9 INFORMACIJSKI VIDIK BOJA PROTI MEDNARODNEMU TERORIZMU KOT GROŽNJA SVOBOŠČINAM IN ČLOVEKOVIM PRAVICAM V DEMOKRACIJI

Metode, ki lahko pogosto zagotovijo uspeh pri odkrivanju načrtovanja terorističnih dejanj, so pogosto v konfliktu z osnovnimi človekovimi pravicami in svoboščinami. Obveščevalno-varnostne službe v primerjavi z drugimi varnostnimi organi pri izvajanju svojih nalog posegajo najgloblje v človekove pravice in temeljne svoboščine. Pomembno je seveda zagotavljane ravnotežja med varnostjo in demokracijo in človekovimi pravicami (Anžič 2002, 456).

Poznamo tri vrste zasebnosti. Prva je zasebnost v prostoru, ki se nanaša na željo posameznika, da ima možnost biti sam; druga je zasebnost osebnosti, ki se nanaša na svobodo misli, opredelitve in izražanja; tretja pa je informacijska zasebnost (Čebulj 1992, 7). In prav tretja vrsta zasebnosti je največkrat zanemarjena. Obveščevalne službe zbirajo in preučujejo med drugim tudi osebne podatke. Najpomembnejše pogosto pridobijo z uporabo posebnih metod in ukrepov, ki posegajo v zasebnost. Če ti posegi niso v skladu z veljavnimi zakoni in predpisi, govorimo o kršenju ali zlorabi človekovih pravic. Z bojem proti terorizmu sovpada vrsta zelo zaskrbljujočih premikov v okviru sistema varstva

[39] Kar nekaj britanskih medijev se je v času sojenja trojici teroristov glede na urnike in načrte napadalcev spraševalo, ali niso morebiti britanska vlada in MI5 z aretacijami čakale predolgo. Prvi načrt za izvedbo napada je namreč datiral teden dni pred dejansko aretacijo (Daily Mail Newspaper, 15. avgust 2006).

človekovih pravic in varstva osebnih podatkov. Dogajajo se krivice glede sodnega varstva, poštenega sojenja v razumnem roku in pravice do zasebnosti, ki jih izvajajo države, ki naj bi bile zgled spoštovanja človekovih pravic. Opravičevanje teh dejanj s strahom pred terorizmom še dodatno razburja borce za človekove pravice in javnost. Dr. Petra Roter je v intervjuju za RTV Slovenija dejala, da terorizem nedvomno je velik problem, a odziv demokratičnih držav daje slutiti, da nimajo odgovorov, kako ohranjati in izboljševati varstvo pravic in temeljnih svoboščin posameznikov, hkrati pa zagotavljati tudi njihovo varnost. (RTV SLO 2007.) Dodala je še, da se je v obdobju po 11. septembru 2001 spremenil vrstni red temeljnih vrednot posameznikov: danes naša temeljna vrednota ni več svoboda, ampak varnost. To posledično večа pričakovanja, da država varnost zagotovi – pogosto se zdi, da za vsako ceno. Vendar pa je danes posameznik zaradi uporabe sodobnik tehnologij v vsakem primeru izpostavljen nadzoru. Uporaba interneta že a priori ne nudi zasebnosti, to si mora uporabnik zagotoviti sam. Največkrat ljudje z uporabo Googla, Facebooka, Twitterja in drugih iskalnikov ter socialnih omrežij prostovoljno sporočamo podatke o svojem zasebnem življenju, svojih navadah, prijateljih, potovanjih in nakupih. Zato je varovanje osebnih podatkov v informacijski dobi vsak dan na preizkušnji. Informacijska tehnologija omogoča posameznikom, skupinam, organizacijam, ne nazadnje tudi državam, da obdelujejo in shranjujejo ogromne količine osebnih in drugih podatkov (Črnčec 2009, 229). Avtor še dodaja, da ima vsak, ki mu je omogočeno povezati različne skupine osebnih podatkov, ki so v bazah podatkov, neomejeno možnost, da spremlja posameznika na vsakem koraku ter tako posega v njegovo zasebnost brez njegove vednosti.

Skladno z razvojem in napredkom tehnologije, še bolj intenzivno pa po napadih 11. septembra, se je povečal tudi nadzor. Če za primer vzamemo samo videonadzor, ki se uporablja pri varovanju pomembnih objektov, kot so letališča, vladne stavbe, pa tudi športni objekti, avtoceste in podobno, lahko ugotovimo, da smo dnevno, večinoma brez vednosti posneti mnogokrat. Tudi v Sloveniji se je število videokamer v zadnjih letih občutno povečalo, jih je pa v primerjavi z ZDA ali pa Veliko Britanijo nedvomno manj.[40]

[40] Po nekaterih ocenah je bilo v Veliki Britaniji leta 2007 nameščenih skoraj 5 milijonov nadzornih kamer, kar je ena na 12 ljudi. Ocenjujejo, da je Londončan dnevno lahko posnet kar 300-krat (Svete 2011, 164).

Tovrsten nadzor seveda odpira številna vprašanja o ravnovesju med varnostjo in zasebnostjo. Zaradi uporabe mobilnih telefonov, ki jih ima danes domala vsak, se lahko zaradi omrežja, ki spremlja menjavo baznih postaj, osebi natanko sledi in določa njeno lokacijo. Še najbolj nesorazmerno poseganje v zasebnost posameznika predstavljajo biometrične metode. Digitalno fotografiranje obraza in jemanje prstnih odtisov sta postala predpogoj za vstop v ZDA. Tukaj so še skeniranje šarenice ter razvoj novih tehnik, kot je naprava, ki lahko človeka prepozna po značilnem odmevu njegovega notranjega ušesa (Svete 2011, 221). Svojo sled dnevno puščamo tudi z uporabo interneta. Lahko bi rekli, da je Google, največji iskalnik na svetu, tudi največji sistem nadzora ljudi. Mnogo informacij o sebi na internetu objavljamo prostovoljno,[41] druge, kot so npr. podatki o bančnih računih, lahko posamezniki z dovolj tehničnega znanja, če seveda ne uporabljamo ustreznih zaščit, z lahkoto zlorabijo. V človekove pravice in svoboščine pa posegajo tudi država in obveščevalne službe, vendar mora biti to storjeno pod točno določenimi pogoji, opredeljenimi z zakonom. Nekatere države so po napadih 11. septembra spremenile zakonodajo na področju poseganja v človekove pravice v korist države. ZDA so prva država, ki je dala večja pooblastila obveščevalnim službam. Le dober mesec po napadu na dvojčka v New Yorku je sprejela patriotski zakon,[42] ki med drugim ob zgoraj omenjenem olajšuje uporabo posebnih oblik pridobivanja podatkov, izboljšuje njihovo izmenjavo med varnostnimi in obveščevalnimi službami ter strožje kaznuje kazniva dejanja, povezana s terorizmom. Kljub kritikam, da zakon daje preširoke pristojnosti varnostnim organom in tako krši načelo zasebnosti, so lahko na njegovi podlagi obveščevalci in policija spremljali izmenjavo elektronskih sporočil brez posebnih odredb sodišča, le pod pogojem, da je posameznik osumljen sodelovanja v terorističnih dejavnostih (Črnčec 2009, 220). Če so bili pomisleki o primernosti tega zakona pred leti še sekundarni, tudi zaradi brezpogojne podpore takratnega predsednika Busha, pa je sedaj zakon, verjetno tudi zaradi časovne oddaljenosti napadov 11. septembra vse bolj na udaru.

[41] Facebook, Twitter, Google+ in podobna socialna omrežja so polna najintimnejših podatkov o posameznikih, ki jih lahko nekdo preprosto zlorabi. Z objavljanjem počitniških fotografij v realnem času dajemo vedeti, da je naša hiša v tem trenutku prazna, z objavami na Zidu razkrivamo svoje politične usmeritve …

[42] Partiotski zakon ali USA PATRIOT Act – Uniting and Strengthening America by Providing Appropriate Tools Recquired to Intercept and Obstruct Terrorism.

V določbah so ključni trije ukrepi: t. i. "mobilni nadzor" komunikacij osumljencev z uporabo več telefonskih linij, načelo "samotnega volka", ki omogoča nadzorovanje osebe, za katero se domneva, da sama pripravlja teroristične dejavnosti, in možnost, da imajo pristojni organi dostop do "vseh otipljivih podatkov" v zvezi z osumljencem, kot je na primer elektronska pošta (RTV SLO 2011). Vendar pa je zakon, vključno s temi tremi spornimi odločbami, predsednik Barack Obama leta 2011 podaljšal. Evropske države pa se niso v večji meri pridružile ZDA pri zaostrovanju protiterorističnih zakonov, ki globoko posegajo v človekove pravice. Najpomembneje namreč je, da se ne glede na stopnjo ogroženosti ali velikost grožnje ne pozabijo osnovne človekove pravice.

10 ZAKLJUČEK IN VERIFIKACIJA HIPOTEZ

Po koncu hladne vojne smo priča številnim spremembam v mednarodnem politično-varnostnem okolju. Zmanjšana stopnja napetosti sicer ne pomeni, da je danes možnost izbruha obsežnega vojaškega konflikta in vojne izničena, vendar pa je ta možnost malo verjetna. Prav iz tega razloga se je odprl miselni prostor za zaznavanje večjega števila nevojaških virov ogrožanja varnosti (Prezelj 2001, 849). Globalna vojaška grožnja ni več primarna, zato pa so prihodnja varnostna tveganja in grožnje težje predvidljivi. Med najaktualnejša tveganja in grožnje nedvomno sodita terorizem in organizirani kriminal. Ta je v preteklosti spadal v domeno nacionalne države, dejavniki, kot so okrepljena ekonomska soodvisnost, razvoj transporta in komunikacij ter globalni finančni trg, pa so povečali njegovo okolje. Tako organizirani kriminal kot terorizem predstavljata izziv ne samo nacionalni, temveč tudi mednarodni varnosti.

Eden izmed poglavitnih razlogov, da je do napadov 11. septembra 2001 prišlo, je po mnenju številnih prav nezadostno sodelovanje med institucijami oziroma resorji, ki se ukvarjajo z bojem proti terorizmu. Na zaslišanjih pred komisijo, ki je preiskovala okoliščine terorističnih napadov, je takratni ameriški pravosodni minister John Ashcroft obtožil nekdanjo pomočnico pravosodne ministrice Jamie Gorelick, da je s tem, ko je leta 1995 izdala navodila oziroma pravilnik delovanja FBI, ki je zahteval ločenost med

kriminalističnim in obveščevalnim delom, pripomogla k temu, da načrtovani napadi niso bili uspešno zaznani (STA 2002). Prav prepletenost kriminalnega in obveščevalnega dela vsakega posameznega organa, ki se ukvarja z bojem proti terorizmu, je ključno za njegovo uspešno delovanje. Danes je kriminal še bolj kot nekoč prepleten s terorističnim delovanjem skupin, saj številnim prav kriminalno delovanje predstavlja osnovni vir dohodka. Intenzivno in pregledno sodelovanje med inštitucijami, ki se ukvarjajo z bojem proti terorizmu, povečuje možnost uspešnega boja proti mednarodnemu terorizmu.

V magistrski nalogi sem zagotovo potrdila glavno hipotezo, da je ključ učinkovitega boja proti terorizmu informacija – zbiranje podatkov, pravilna interpretacija in preglednost zbranih podatkov, oblikovanje informacij in njihova izmenjava med inštitucijami oziroma resorji, ki se ukvarjajo z bojem proti mednarodnemu terorizmu. Še več, informacija je postala oblika vojskovanja (Črnčec 2009, 67). »Informacija ni le sredstvo, ki povečuje učinkovitost smrtonosnih tehnologij, kot je bilo znano v preteklosti, ampak omogoča nove možnosti za nesmrtonosne napade, ki lahko onesposobijo, porazijo, odvrnejo ali prisilijo nasprotnika« (Bishop v Črnčec 2009, 67). Samo hitra in pravočasna pridobitev informacije omogoča ustrezen odziv.

Pomožna hipoteza, ki predvideva, da bi enotna definicija terorizma izboljšala uspešnost delovanja nacionalno-varnostnega sistema v boju proti terorizmu in da je zato ključnega pomena poenotenje stališč mednarodne skupnosti, je prav tako verificirana. Vendar pa je popolno poenotenje definicije terorizma skoraj nemogoče. Enotnih stališč nimajo niti inštitucije, ki preganjajo dejanja, povezana s terorizmom, znotraj ene države. Definicija terorizma je ne nazadnje odvisna od tistega, ki ga definira. Tudi številni strokovnjaki, ki se ukvarjajo s tem pojavom, menijo, da obča, abstraktna formulacija terorizma ni možna. Tudi zato ne, ker se ves čas spreminja. Z razvojem tehnologije je dobil nove razsežnosti, pojavile so se nove definicije, nove klasifikacije.

Druga pomožna hipoteza predvideva, da teroristične organizacije potrebujejo za svoje delovanje ogromno sredstev, zato je sodoben boj usmerjen k omejevanju le-teh . Velike

finančne pritoke zanje predstavlja organizirani kriminal. Teroristi in skupine organiziranega kriminala sodelujejo vsakodnevno, razlike med njimi so vse bolj zabrisane. Nekoč sta ti dve skupini veljali za popolnoma različni grožnji – motiv teroristov je bila ideologija, motiv kriminalnih skupin pa pohlep. Danes povezovanje terorističnih in kriminalnih skupin omogoča številne sinergične učinke, naraščajoča povezanost med kriminalom in terorizmom pa spreminja naravo boja proti terorizmu in zahteva nove strategije. Omejevanje finančnih virov je pomembna faza v boju proti terorizmu, zahteva pa tesno sodelovanje tako inštitucij za preprečevanje kriminala kot inštitucij, ki se borijo proti terorizmu.

11 LITERATURA

- ACLU. 2004. *Matrix: Miths and Reality.* Dostopno prek: http://www.aclu.org/technology-and-liberty/matrix-myths-and-reality (10. februar 2004).
- Agrell, Wilhelm. 1987. *The Changing Role of National Intelligence Services. V Intelligence for economic development: an inquiry into the role of knowledge industry* (uredila Stevan Dedijer in Nicolas Jequier), 31–40. Oxford, Hamburg, New York: Berg Publishers Limited.
- Albanese, Jay S. 2003. *Organized crime: world perspectives.* Upper Sadle River (N. J.): Prentice Hall, cop.
- Anžič, Andrej. 2002. *Mednarodni terorizem – varnostni izziv in dileme*. Teorija in praksa 2002, 454–466.
- *A secure Europe in a better world. European security strategy*. Bruselj, 12. december 2003. Dostopno prek: http://www.consilium.europa.eu/ uedocs/cmsUpload/ 78367 (12.avgust 2010).
- Bailey, Chris. 2005. *Surveillance and the Interception of Communications*. Dostopno prek: http://www.tni.org/archives/asem-seoul_011bailey1 (18. julij 2005).
- Balzer, J. A. 1996. *International Police Cooperation: Opportunities and Obstacles*; Policing in Central and Eastern European Europe ed. by Pagon, VPVŠ, Ljubljana.
- Boj proti terorizmu – Strategija in načrt ukrepanja. Marec 2012. Fight Against Terrorism: Dostopno prek: http://europa.eu/legislation_summaries/ justice_freedom_security/ fight_against_terrorism/index_sl.htm (14. julij 2012).
- Burgess, Marc. 2003. *Terrorism: The Problems of Definition.* Dostopno prek: http://studies.agentura.ru/centres/cdi/definition/ (1. avgust 2003).

- Buzan, Barry. 1993. *People, States and Fear, The National Security Problem in International Relations,* 1–34, 35–56, 112–142, 328–355. Whatseheaf Book, Sussex, Brighton.
- Campbell, Duncan. 2000. *Interception Capabilities*. Dostopno prek: http://duncan.gn.apc.org/stoa_cover.htm (31. avgust 2012).
- Campbell, Duncan. 2001. *How the Terror Trail Went Unseen.* Dostopno prek: http://www.heise.de/tp/artikel/9/9751/1.html (10. avgust 2001).
- Carter, David L. 1997. *International Organized crime. Emerging Trends in entrepreneurial Crime.* Understanding Organized Crime in Global Perspective: A Reader, 131–148.
- Center for Defence Information, 2003, Dostopno prek: http://www.cdi.org/program/document.cfm?documentid=1564&programID=39&from_page=../friendlyversion/printversion.cfm (16.april 2011)
- Central Inteligence Agency. Dostopno prek: http://cia.gov (20.maj 2012)
- Chepessiuk, Ron. 2002. *Dangereus Alliance:Terrorism and organized Crime. Dostopno prek*: http://www.globalpolitician.com/print.asp?id=3435 (28. avgust 2012).
- CNN. 2001. *Timothy Mcveigh*. Dostopno prek: http://articles.cnn.com/2001-03-29/us/profile.mcveigh_1_timothy-mcveigh-oklahoma-city-bombing-religion-basic-training-fort-bragg?_s=PM:US (12. september 2012).

  CNVOS. 2011. *Odgovor na svetovni terorizem: Pobude OZN za okrepitev mednarodnega sodelovanja v boju proti terorizmu.* Dostopno prek: http://www.cnvos.si/article/id/3511/cid/92. 26. november 2012.
- Council on Foreign Relations. 2009. *Terrorists and the Internet.* Dostopno prek: http://www.cfr.org/terrorism-and-technology/terrorists-internet/p10005 (8. januar 2009).
- Council on Foreign Relations. 2012. *Hamas.* Dostopno prek: http://www.cfr.org/israel/hamas/p8968 (23. september 2012).
- Čebulj, Janez. 1992. Varstvo informacijske zasebnosti v Evropi in v Sloveniji. Ljubljana: Inštitut za javno upravo pri Pravni fakulteti.

- Črnčec, Damir. 2009. *Obveščevalna dejavnost v informacijski dobi*. Ljubljana: Defensor.
- Dobovšek, Bojan.1994. *Organiziran kriminal in nacionalna varnost*. 76–83. Zb. strok. znan. razpr. Višja šola notr. zadeve, december 1994, 7.
- --- 2002.*Organizirana kriminaliteta in terorizem*. 30–32. Slov. uprava, feb./mar. 2002, letn. 2, št. 1.
- Deklaracija o podpori resoluciji o terorizmu. 2002. Državni zbor Republike Slovenije. Dostopno prek: http://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=C12565E2005E8311C1256BCD002812BB&db=spr_akt&mandat=VI (31. maj 2002).
- Dnevnik. 2005. *Ameriški senat ni podaljšal veljavnosti patriotskega zakona.* Dostopno prek: http://www.dnevnik.si/novice/svet/156794. (23. september 2012).
- --- 2010. *Filipinski marinci ubili šest skrajnežev skupine Abu Sajaf.* Dostopno prek: http://www.dnevnik.si/novice/kronika/1042339326 (17. april 2012).
- --- 2012. *Europol: Evropi vse bolj grozijo volkovi samotarji, kot sta Breivik in Merah.* Dostopno prek: http://narocanje.dnevnik.si/novice/eu/1042526362 (26. april 2012).
- *Dostop do informacij in izmenjava informacij.* Marec 2012. Dostopno prek: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/index_sl.htm (14. avgust 2012)
- Drucker, Peter F. 2001. *Menedžerski izzivi v 21. stoletju*. Ljubljana: GV Založba.
- Duran, Khalid & Pohly, Michael. 2001. *Osama Bin Laden in mednarodni terorizem*. Učila International, založba, d. o. o., Tržič.
- Dvoršak, Anton, Bojan Dobovšek. Posebne operativne metode in sredstva pri zatiranju organiziranega kriminala – kriminalistični pogled. 83–93. Zb. strok. znan. razpr. Višja šola notr. zadeve, junij 1996.
- Europa. Dostopno prek: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/index_sl.htm (14. marec 2012)

- European Union. *Providing security in a changing world, Report on the Implementation of the European security Strategy.* 407/08. Bruselj. Dostopno prek: http://www.euun.europa.eu/documents/en/081211_EU%20Security%20Strategy.pdf (1. oktober 2009).
- Europol. Dostopno prek: http://europol.net (5. avgust 2011)
- Europolovo poročilo 2011. Dostopno prek: https://www.europol.europa.eu/sites/default/files/publications/qlab11001sln.pdf
- Expeditioner. 2010. How Many Americans Have a Passport. Dostopno prek: http://www.theexpeditioner.com/2010/02/17/how-many-americans-have-a-passport-2/ (17. februar 2010).
- FATF. 2012. Dostopno prek:http://www.fatf-gafi.org/ (12. avgust 2012).
- Federal Bureau of Investigation. Dostopno prek: http://fbi.gov (20. julij 2012).
- Ferfila, Bogomil. 2002: ZDA, FDV.
- Fox News. 2005. FBI Ditches Carnovore Surveillance System. Dostopno prek: http://www.foxnews.com/story/0,2933,144809,00.html (18. januar 2005).
- Friedman, Thomas. 2005–2006. The World is Flat: a brief history of the 21st century, 1st. Rev. New York: And expanded ed. Farrar, Straus and Giroux.
- Ghioni, Fabio. 2006. *The financing of terrorism through capital from a legitimate source.* Dostopno prek: http://www.zone-h.org/contact/author/4259 (2. januar 2006).
- Gartner, Heinz, Adrian Hyde-Price in Erich Reiter, ur. 2001. *Europe's New Security Challenges*. Boulder: Lynne Rienner Publishers.
- Gričar, Jože. 2002. Management informacijske tehnologije in e-poslovanja. V: Obveščevalna dejavnost v informacijski dobi, Črnčec, Damir.
- Grizold, Anton & Bogomil Ferfila. 2000. *Varnostne politike velesil,* Knjižna zbirka Profesija. FDV.
- Grizold, Anton.1999. Obrambni sistem Republike Slovenije, VPVŠ, Ljubljana.
- Guardian. 2011. *Osama Bin Laden is dead, Obama announces.* Dostopno prek: http://www.guardian.co.uk/world/2011/may/02/osama-bin-laden-dead-obama (2. maj 2011).

- Harris, Shane. 2006. *TIA Lives On*. National Journal. Dostopno prek: http://shaneharris.com/magazinestories/tia-lives-on/ (23. februar 2006).
- Howorth, Jolyon and Anand Menon.1997. *The European Union and National Defence Policy*. London: Routledge.
- Informacijski pooblaščenec. 2012. Splošno o SIS. Dostopno prek: https://www.ip-rs.si/varstvo-osebnih-podatkov/inspekcijski-nadzor/schengen/splosno-o-schengenskem-informacijskem-sistemu-sis/ (31. avgust 2012).
- Information Awareness Office. Dostopno prek: http://infowar.net/tia/www.darpa.mil/iao/HID.htm (7. marec 2003)
- --- Dostopno prek: http://infowar.net/tia/www.darpa.mil/iao/EELD.htm (14. april 2003)
- --- Dostopno prek: http://infowar.net/tia/www.darpa.mil/iao/Genisys.htm (2. februar 2003)
- In Sight. 2012. Criminal Groups in Colombia. Dostopno prek: http://www.insightcrime.org/criminal-groups/colombia/farc (19. avgust 2012).
- Internet Story. 2012. Dostopno prek: http://www.internet-story.com/arpa.htm (1. avgust 2012).
- King, Paul. 2009. *Teroristi in organizirani kriminal. Samo posel?*. Dostopno prek: http://www.nato.int/docu/review/2009/Organized_Crime/SL/index.htm (26. april 2012).
- Keohane, Robert O. 2002. Power *and Governance in a Partially Globalized World*. London and New York: Routledge.
- Komisija Evropskih skupnosti. 2005. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0695:FIN:SL:DOC (22. december 2005).
- Krause, Keith and Michael Williams, ur. 1997. *Critical Security Studies*. London: UCL Press.
- Krunič, Zoran. 1997. *Strategija posrednega nastopanja.* Ljubljana: Unigraf.
- Markoff, John. 2002. "Pentagon Plans a Computer System That Would Peek at Personal Data of Americans". *The New York Times*, 22. november 2002.

- Malešič, Marjan. 2000. *Slovenian Security Policy and NATO*. Groningen: University Press.
- Mednarodni inštitut za bližnjevzhodne in balkanske študije. 2011. Dostopno prek: http://www.ifimes.org/default.cfm?Jezik=si&Kat=11&ID=605 (26. maj 2011).
- Mednarodni terorizem z vidika mednarodnega prava. Dostopno prek: http://www2.arnes.si/~tlutar/dokument/terorizem.htm (4. december 2002).
- Miholič, Andrej. 2004. *Logistične značilnosti sodobnih terorističnih skupin*. Diplomsko delo. Ljubljana: FDV.
- Miller, John. 2003. The cell: Inside the 9/11 plot and why the FBI and CIA failed to stop it. New York: Hyperion, cop.
- National Strategy for Information Sharing. 2007. *Successes and Challanges in Improving Terrorist-Related Information Sharing.* Dostopno prek: http://ise.gov/sites/default/files/nsis_book.pdf (4. oktober 2007).
- National Security Hotline. 2012. Dostopno prek: http://www.ema.gov.au/agd/www/nationalsecurity.nsf/Page/The_National_Security_Hotline (17. julij 2012)
- Nettler, Gwynn. 1984. *Explaining Cime*. New York: McGraw – Hill.
- North Atlantic Treaty Organization. Dostopno prek: http://www.nato.com (13. junij 2012).
- Perri, Frank S., Terrance G. Lichtenwald in Paula MacKenzie. 2009. *Evil Twins: The Crime – Terror Nexus*. The Forensic Examiner. Dostopno prek: http://www.all-about-psychology.com/support-files/crime-terror-nexus.pdf (20. avgust 2012).
- Podpečan, Mitja. 2007. *Vas ta trenutek preiskujejo?*. Pravna praksa 8, 18. v Matjaž Vidic. 2001. *Ekstremizmi na internetu*. Magistrsko delo. Ljubljana: FDV.
- Poročilo Sveta Evrope. 2007. *Council Conclusions on cooperation to combat terrorist use of the Internet.* Dostopno prek: http://register.consilium.europa.eu/pdf/en/07/st08/st08457-re03.en07.pdf (29. maj 2007).

- Prezelj, Iztok. 2001. Grožnje varnosti, varnostna tveganja in izzivi v sodobni družbi. Razreševanje nekaterih terminoloških dilem. Teorija in praksa 38 (1/2001): 127–141.
- --- 2001. *Vojaško ogrožanje nacionalne in mednarodne varnosti po koncu hladne vojne.* 848–850. Teorija in praksa 38 (5).
- Računalniške novice. 2012. FBI v svoje vrste snubi celo Microsoft. Dostopno prek: http://www.racunalniske-novice.com/novice/dogodki-in-obvestila/fbi-v-svoje-vrste-snubi-celo-microsoft.html (9. maj 2012).
- Reuters. 2009. The End of Sri Lanka's Quarter Century War. Dostopno prek: http://www.reuters.com/article/2009/05/16/idUSCOL391456 (22. september 2012)
- Revija Nato. 2007. *Izzivi pred Afganistanom – kaj nas učijo izkušnje iz Kolumbije.* Dostopno prek: http://www.nato.int/docu/review/2007/issue3/slovene/art1.html (14. september 2007).
- RTV SLO. 2007. *Država mora zagotavljati dostojno življenje.* Intervju z dr. Petro Roter. Dostopno prek: http://www.rtvslo.si/svet/drzava-mora-zagotavljati-dostojno-zivljenje/80387 (10. december 2007).
- ---. 2011. Domoljubni zakon v kongresu dobil zaušnico. Dostopno prek: http://www.rtvslo.si/svet/domoljubni-zakon-v-kongresu-dobil-zausnico/250535 (9. februar 2011).
- Sarkesian, Sam, John Allen Williams in Stephen J. Cimbala. 2002. *U.S. National Security. Policymakers, Processes and Politics* (Third edition). Boulder: Lynne Rienner Publishers.
- Schengen Information System. 2012. Dostopno prek: http://www.euro-dollar-currency.com/schengen_information_system.htm (31.avgust 2012).
- SIOL. 2012a. *Hekerji vdrli v britansko protiteroristično telefonsko linijo* (http://www.siol.net/novice/crna_kronika/ 2012/04/ hekerji_vdrli_v_britansko _protiteroristicno_telefonsko_linijo.aspx (8. april 2012).
- --- 2012b. *Na Japonskem aretiran še zadnji odgovorni za napad s sarinom*. Dostopno prek: http://www.siol.net/novice/svet/2012/06/na_japonskem _aretiran_se zadnji_odgovorni_za_napad_s_sarinom.aspx (15. junij 2012).

- Slovenija in NATO. 2004. *Zakaj se je Slovenija odločila za NATO kot pomoč pri oblikovanju učinkovite obrambe države?* Dostopno prek: http://nato.gov.si/slo/slovenija-nato/slovenska-vojska-nato/faq/01/. 26. november 2012.
- Slovenska tiskovna agencija. Dostopno prek: http://sta.si. (2. september 2011)
- SOVA. 2009. Dostopno prek: http://sova.gov.si/ indexd461.html?sv_path=1103,17333 (17. jilij 2012).
- Sporočilo Komisije Evropskemu palamentu. 2004. *Za izboljšanje dostopa organov pregona do informacij*. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0429:SL:HTML (28. avgust 2004).
- Sprejeta besedila EU. Dostopno prek: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0577+0+DOC+XML+V0//SL (14. december 2011).
- Svete, Uroš. 2005. Varnost v informacijski družbi. Knjižna zbirka Varnostne študije. Ljubljana: Fakulteta za družbene vede.
- Svete, Uroš, Damijan Guštin in Damir Črnčec. 2011. *Asimetrija nacionalne varnosti: od zgodovinskih izkušenj do sodobnih izzivov.* Ljubljana: Defensor.
- Šuhel, Peter., Alois Paulin, Peter Šuhel ml. 2011. *Uvod v informatiko*. Ljubljana; Novo mesto; Nova Gorica: samozaložba.
- Telegraph. 2012. *Police arrests two teenagers after ani-terror hotline hacked.* Dostopno prek: http://www.telegraph.co.uk/news/9201137/Police-arrest-two-teenagers-after-anti-terror-hotline-hacked.html (4. avgust 2012)
- Teroristične organizacije na Twitterju: Od Hezbolaha prek talibanov do Al Šababa. Znanost in tehnologije. Dostopno prek: http://www.dnevnik.si/ novice/znanost/1042499570 (3. januar 2012).
- The United States Mission to the European Union. *Clinton Launches New Counterterrorism Partnership.* Dostopno prek: http://www.useu.be/ Terrorism/EUResponse/Feb2003AshcroftTerrorism.html (9. september 2004).

- TG Daily. 2012. FBI Steps up social media tracking. Dostopno prek: http://www.tgdaily.com/software-brief/61533-fbi-steps-up-social-media-tracking (20. februar 2012).
- U. S. department of State. Establishment of the Bureao of Counterterrorism. Special Breifing of Daniel Benjamin. 4. januar 2012. Dostopno prek: http://www.state.gov/j/ct/rls/rm/2012/180148.htm (6. avgsut 2012).
- United Nations. *International convention for the Suppression of the Financing of Terrorism.* Adopted by the General Assembly of the United Nations resolution 54/109, 9. december 1999. Dostopno prek: http://www.un.org. (7. maj 2012).
- United nations Office of Drugs and Crime. Definitions of Terrorism. Dostopno prek: http://www.unodc.org/unodc/terrorism_definitions.html. (28. julij 2003).
- United Nations. *UN Security Council Anti-Terrorism Resolution, Unanimous call for suppressing financing, improving international cooperation.* Security Council SC/7158 4385th Meeting, 28. September 2001. Dostopno prek: http://www.un.org (5. maj 2012)
- UNODC. 2012. *Drug Trafficing and Financing of Terrorism.* Dostopno prek: http://www.unodc.org/unodc/en/frontpage/drug-trafficking-and-the-financing-of-terrorism.html (28. avgust 2012).
- USA Today. 2009. *US Doubles the Number of DS&T Operatives*. Dostopno prek: (http://www.usatoday.com/tech/news/surveillance/2008-10-26-cia-gadgets_N.html (26. oktober 2009).
- Veselko, Vesna. 2004. *Preprečevanje pranja denarja: Primer Slovenije*, Diplomsko delo. Ljubljana: Ekonomska fakulteta, 49. str.
- Vogrin, Andreja, Iztok Prezelj in Bojko Bučar. 2008. *Človekova varnost v mednarodnih odnosih*. Ljubljana: Fakulteta za družbene vede.
- Vukosavljević, Bogdan. 2006. *Global Terrorism*. Ljubljana: Forma.
- Woodwiss, Michael.2001. *Organized crime and American power: a history.* Toronto, Buffalo: University of Toronto Press.
- Woodworth, Pady. 2002. *Dirty war, clean hands: ETA, the GAL and Spanish democracy.* New Haven: Yale Nota Bene.

- Wikipedia. 2012. *Information Awareness Office*. Dostopno prek: http://en.wikipedia.org/wiki/Information_Awareness_Office (14. maj 2012).
- Wilkinson, P., Stewart, A. M., ed. 1987. Contemporary research on terrorism. Aberdeen: Aberdeen University Press.
- 24ur.com. 2002. *Džamaja Islamija kriva za Bali.* Dostopno prek: http://www.24ur.com/novice/svet/dzamaja-islamija-kriva-za-bali.html (3.april 2012).
- --- 2011. *Večji napadi, ki so pretresli Rusijo*. Dostopno prek: http://www.24ur.com/novice/svet/vecji-napadi-ki-so-pretresli-rusijo.html (20. september 2012)
- --- 2012. Pentagon želi zaradi terorizma nadzirati Facebook in Twitter. Dostopno prek: Dostopno prek: http://24ur.com/novice/it/pentagon-zeli-zaradi-terorizma-nadzirati-facebook-in-twitter.html (31. julij 2012)

PRILOGA

Slika 1 – Osumljenec, posnet med kupovanjem prtljage, v katero so nameravali skriti plastenke s tekočim eksplozivom

Slika 2 – Hiša, v kateri so organi pregona odkrili laboratorij za izdelavo bomb s tekočim eksplozivom