Graeme R. Newman
Ronald V. Clarke

POLICIJSKA DEJAVNOST PROTI TERORIZMU

UNIVERZA V MARIBORU
FAKULTETA ZA VARNOSTNE VEDE

Graeme R. NEWMAN in Ronald V. CLARKE

POLICIJSKA DEJAVNOST PROTI TERORIZMU

Učbenik za vodilno osebje na policijskih postajah

Urednika dodanih slovenskih prispevkov:
IZTOK PODBREGAR, ANDREJ SOTLAR

LJUBLJANA, januar 2010

Graeme R. Newman in Ronald V. Clarke

POLICIJSKA DEJAVNOST PROTI TERORIZMU:
Učbenik za vodilno osebje na policijskih postajah

Urednika dodanih slovenskih prispevkov:
Iztok PODBREGAR, Andrej SOTLAR

Avtorji dodanih slovenskih prispevkov:
Bojan Dobovšek
Teodora Ivanuša
Iztok Podbregar
Andrej Sotlar
Bojan Tičar

Recenzenta:
Gorazd Meško, Peter Umek

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

351.74:343.326

NEWMAN, Graeme R.
Policijska dejavnost proti terorizmu : učbenik za vodilno osebje na policijskih postajah / Graeme R. Newman in Ronald V. Clarke ; urednika dodanih slovenskih prispevkov Iztok Podbregar, Andrej Sotlar. - Ljubljana : Fakulteta za varnostne vede, 2010

ISBN 978-961-6821-00-1
1. Clarke, Ronald V.
249269760

Izdajatelj: Fakulteta za varnostne vede, Univerza v Mariboru, Ljubljana
Prevod: Adela Trunkl
Lektor: Marinka Milenković
Oblikovanje besedila: Tipografija, d.o.o.
Tisk: Tipografija, d.o.o.
Naklada: 300 izvodov

Ljubljana, 2010

VSEBINA

Predgovor

Pričujoča publikacija je rezultat sodelovanja Fakultete za varnostne vede Univerze v Mariboru s 'School of Criminal Justice' pri Rutgers University, Newark, ZDA. To je že druga publikacija v seriji prevodov in priredb ameriških avtorjev, ki jih izdaja Fakulteta za varnostne vede. Prvi prevod in priredba je bil *Priročnik za policijske (kriminalistične) analitike - v 60 korakih do rešitve problema (2008),* ki je v slovenskem jeziku objavljen tudi na spletni strani ameriškega Centra za v probleme usmerjeno policijsko delo (http://www.popcenter.org/library/translations/).

V začetku leta 2008 smo dobili dovoljenje za prevod in priredbo ter dopolnilo izvirnika s slovenskimi besedili, ki prispevajo k večjemu razumevanju in kontekstualizaciji prevoda in priredbe priročnika, ki sta ga napisala Graeme R. Newman in Ronald V. Clarke (http://www.popcenter.org/library/reading/pdfs/PolicingTerrorism.pdf). Priročnik z naslovom *'Policing Terrorism: An Executive's Guide'* (2008) sta dodatno uredila izr. prof. dr. Iztok Podbregar in doc. dr. Andrej Sotlar. Urednika sta povabila raziskovalce in visokošolske učitelje Fakultete za varnostne vede Univerze v Mariboru, ki so kakovostno dopolnili prevod in priredbo ameriškega dela o vlogi policije in ukrepih v primeru terorističnega napada. Dopolnila in komentarje slovenskih avtorjev je treba razumeti kot pojasnilo, kako bi bilo mogoče ameriški priročnik uporabiti v Sloveniji. Priročniku, ki sta ga napisala Newman in Clarke, so Bojan Dobovšek, Teodora Ivanuša, Iztok Podbregar, Andrej Sotlar in Bojan Tičar dodali poglavja, ki dodatno razširjajo spekter obravnavanih tem v zvezi s terorizmom in policijsko dejavnostjo.

Petdeset nasvetov z razlagami v petdesetih poglavjih priročnika je mogoče razumeti kot pripomoček policijskim šefom pri organizaciji policijskega dela. Želja avtorjev je, da bi priročnik policijskim šefom pomagal čim bolje razumeti teroristične napade, značilnosti teroristov ter jim dati priporočila za čim bolj učinkovito, zakonito in legitimno policijsko dejavnost. Poleg petdesetih poglavij, v katerih avtorja osveščata policijske šefe s pragmatičnimi navodili, so slovenski avtorji dodali razprave o pomembnih razsežnostih policijske dejavnosti (kriminalistike), pravne ureditve odzivanja na terorizem, kriznega menedžmenta in varnostnih študij, ki omogočajo celovitejši pogled na policijsko delo v zvezi s terorističnimi napadi. Mnenje

strokovnjakov in javnosti je, da v Sloveniji terorizem ne predstavlja resne grožnje. Kljub temu napotki, predstavljeni v priročniku, niso odveč.

Priročnik je mogoče uporabiti kot dopolnilno gradivo pri nekaterih predmetih na Fakulteti za varnostne vede Univerze v Mariboru, kjer se študenti srečujejo s tujimi varnostnimi modeli in domačo prakso zagotavljanja varnosti. Priročnik je izziv za študenta, strokovnjaka in vsakega, ki ga to področje zanima, da kritično razmišlja o napotkih za ravnanje policistov. Je tudi izhodišče za širšo razpravo o vzrokih, okoliščinah in odzivih na terorizem. Priročnik priporočam v branje policistom in drugim družbenim nadzorovalcem ter raziskovalcem na področju varnosti, kriminologije, policijske dejavnosti in širše.

Prepričan sem, da je pričujoči prevod in priredba ter dopolnilo Newmanovega in Clarkeovega priročnika kakovosten prispevek k pragmatičnem razmišljanju o policijski dejavnosti na področju nadzorovanja in preprečevanja posledic terorizma in pomemben kamenček v mozaiku publikacij v okviru založniške dejavnosti Fakultete za varnostne vede Univerze v Mariboru.

Prof. dr. Gorazd Meško
Dekan Fakultete za varnostne vede UM

Uvod k slovenski izdaji

Pred Vami je vsebinsko izjemno delo, kjer sta ameriška avtorja Newman in Clark v obliki Vodiča podala zelo natančna navodila vodstvenemu osebju na policijskih postajah širom Združenih držav Amerike, kako organizirati policijsko dejavnost v boju proti teorizmu.

V kriznem managementu se namesto klasičnih načrtov reševanja posameznih kriz vse bolj uveljavlja pristop v obliki priročnikov. Le ta omogoča uporabnikom, da dobijo podrobne usmeritve za reševanje posameznih kriznih razmer, v tem primeru dejavnosti proti terorizmu, hkrati pa omogočajo fleksibilno prilagajanje vsebin konkretnim razmeram in izkušnjam uporabnika priročnika. Tega vodila sta se držala tudi avtorja, ki sta zelo izčrpno in s konkretnimi ponazoritvami in analizami opisala tako teroristično grožnjo, še bolj pa možen in zaželen odgovor policijskih sil v Združenih državah Amerike.

Zakonodaja, sistem organiziranosti varnostnih sil in nenazadnje tudi grožnja teorizma se v ZDA precej razlikuje od razmer v Sloveniji. Zato smo se pri prevodu priročnika v slovenski jezik, odločili, da zaradi lažjega razumevanja in sledenja vsebine, posamezna poglavja, sicer vsebinsko odličnega priročnika, dopolnimo in aktualiziramo s prispevki in pojasnili slovenskih avtorjev. Naš namen je bil, da na ta način bralcu lažje vzpodbudimo razmišljanja o protiteroristični dejavnosti pri nas in v naši regiji. Prispevki slovenskih avtorjev so umeščeni na konec izvornih poglavij in opozarjajo na morebitno specifičnost slovenskih razmer (npr. glede zaznavanja in odzivanja na teroristične grožnje – A. Sotlar) oziroma na širši kontekst boja proti terorizmu (npr. vprašanje vloge in organizacije obveščevalno-varnostne dejavnosti v boju proti terorizmu – I. Podbregar; sprege med terorizmom in organiziranim kriminalom – B. Dobovšek ali ogroženosti in zaščite slovenske kritične infratsrukture – T. Ivanuša). Za lažje razumevanje normativno-pravne urejenosti boja proti terorizmu v Sloveniji pa je že na začetku priročnika dodan tudi daljši prispevek B. Tičarja.

Vejamemo, da bo tako dopolnjen priročnik zanimivo in koristno branje vsem, ki delujejo v policiji in v drugih organih in službah sistema nacionalne varnosti, kakor tudi raziskovalcem in študentom, in nenazadnje tudi novinarjem, ki spremljajo in poročajo o fenomenu terorizma.

izr. prof. dr. Iztok Podbregar in doc. dr. Andrej Sotlar
Urednika slovenske izdaje

Uvod k ameriški izdaji

Ta projekt temelji na Sporazumu o sodelovanju številka 2007-CK-WX-K008, ki ga je odobril Urad za v skupnost usmerjeno policijsko službo (Office of Community Oriented Policing Service) ameriškega ministrstva za pravosodje. Mnenja avtorjev niso nujno uradna stališča ali pogledi ameriškega ministrstva za pravosodje. Poudarjamo, da pričujoče delo zgolj ponazarja nekatere vidike policijske dejavnosti in odzivanja na terorizem, ki dopolnjuje dosedanje razprave o policijski dejavnosti in terorizmu.

Spletne reference, navedene v tej publikaciji, so bile veljavne julija 2008. Ker se spletne strani nenehno spreminjajo, tako avtorja kot tudi Urad za v skupnost usmerjene policijske službe ne morejo jamčiti za njihovo sedanjo veljavnost.

Pisanje Grahama Newmana in Ronalda Clarka je treba razumeti kot pogled dveh kriminologov na ameriško videnje policijske dejavnosti in terorizma, pri čemer je nekatera načela mogoče uporabiti na globalni ravni (opomba urednikov).

Direktorjevo pismo

Neposredno po 11. septembru 2001 sem sklical sestanek vodij petih pomembnejših izvršnih organizacij na področju kazenskega pregona v Združenih državah Amerike. Povedali so mi, da je skupnostna policijska dejavnost v tem trenutku bolj pomembna kot kadarkoli prej. Od takrat je Urad za v skupnost usmerjeno policijsko službo (COPS urad) večkrat sklical zvezne agencije, predstavnike zasebnega sektorja, vodje organov kazenskega pregona iz cele države, vključno z javno varnostjo in policijo za nadzor plemenskih skupnosti, da bi preučili nove načine reševanja v zvezi z nasilnimi zločini in nenehno grožnjo terorizma. V vsaki od teh razprav smo se vedno znova vračali k osrednji vlogi, ki jih imajo načela skupnostne policijske dejavnosti v okviru preprečevanja in odzivanja na teroristične grožnje.

Od 11. septembra so zvezne, lokalne in specializirane agencije kazenskega pregona dobile številne nove naloge. Delovne zadolžitve že tako zaposlenih postaj so se občutno povečale in vključujejo še odkrivanje potencialnih teroristov, zaščito ranljivih tarč in usklajevanje prvega odziva. Ne glede na to, ali ste načelnik policije v majhnem mestu ali v velemestu, je v vaši pristojnosti, da zagotovite pripravo načrtov za preprečevanje napadov in da se odzovete hitro in učinkovito, kolikor bi do napada prišlo. Ta priročnik, namenjen vodjem policijskih postaj, šerifom in drugim vodstvenim delavcem, vam bo pomagal pri soočanju z novimi izzivi, ki jih vključuje zoperstavljanje grožnjam terorizma. Jasno izraža in povzema pisanja o temeljnih sestavinah protiterorističnega načrta.

Slovita avtorja, Graeme Newman, ugledni profesor na univerzi v Albany, newyorški državni univerzi, in Ron Clark, univerzitetni profesor na Rutgersu, državni univerzi v New Jerseyju, sta oblikovala več izvirnih napotkov za preprečevanje terorizma, ki so lahko zelo koristni za vašo policijsko enoto. Čeprav smo prepričani, da je priročnik uporaben za enote vseh velikosti, bo še posebej uporaben za majhne in srednje velike policijske postaje, ki imajo omejena sredstva za preprečevanje terorizma in odzivanje nanj. Ta vodič bo v pomoč tudi agencijam pri oblikovanju prednostnih nalog in pripravi utemeljenih, trajnostnih odzivov pri soočanju z dodatnimi odgovornostmi.

Po več letih dela v organih kazenskega pregona in skoraj sedemletnem direktorovanju uradu COPS še nisem naletel na uspešno in trajno strategijo zmanjševanja kriminalitete in preprečevanja terorizma, ki bi bila v skladu z demokratičnimi načeli naše države in bi gradila na sodelovanju z državljani in vključevanju načela reševanja problemov. Sodelovanje s skupnostjo in reševanje problemov v okviru policijske dejavnosti nista zadnja ostanka minule dobe, temveč sta tako sodobna, kot je sodobna vojna proti terorju, in tako aktualna kot današnje novice.

Po obisku tragičnega prizorišča bombnega napada v Londonu leta 2005 je BBC navajala besede načelnika policijske uprave Los Angelesa, Billa Brattona, ki je rekel:

> *Pri soočanju z resnim mednarodnim kriminalom se je treba osredotočiti na skupnost. V kolikor policija ne sodeluje s skupnostmi v tako etnično raznolikem mestu, kot je London, je igre konec, vedno se bomo lovili.*

Ob istem terorističnem napadu je gospod Ian Blair, poveljnik britanske metropolitanske policije, izjavil:

> *Ne policija in ne obveščevalna služba nista tisti, ki bosta premagali terorizem. Skupnost je tista, ki bo premagala terorizem.*

V boju proti kriminaliteti in pri varovanju svoje domovine bomo preizkušali številne prijeme in pripravili veliko strategiji ter možnih rešitev. To je dobro, saj moramo ostati previdni in se moramo upirati samozadovoljstvu, ki lahko zasenči vsak dolgotrajni boj. V prizadevanju, da bi bile naše skupnosti varnejše, moramo vztrajati pri načelih, za katera vemo, da delujejo. Usmeriti se moramo na neposredne vzroke problemov, ki jih želimo rešiti, združiti se moramo s tistimi, ki nam lahko najbolj pomagajo pri reševanju težav in pripraviti moramo naše organizacije na to, da se bodo bolje borile proti pojavom, ki najbolj ogrožajo mir našega naroda. Ta priročnik naj bi vam pomagal ravno pri tem.

Carl Peed, direktor
COPS urad

Zahvala

Obstaja nevarnost, da bi bil lahko priročnik, kot je ta, ki sva ga napisala dva akademika, daleč od resničnega življenja. Tej pasti sva se skušala izogniti, in če sva se ji, je za to zaslužna predvsem pomoč, gostoljubnost in odprtost članov anaheimske (Kalifornija) policijske postaje, na katero sva se obrnila na začetku priprave priročnika. Tisti, ki so nama pomagali, so: načelnik John Welter, preiskovalec Christopher Schneider, poročnik Chuck O'Connor, poročnik David Vangsness, narednik Brian McElhaney in narednik James Wilkes. Predstavili so naju tudi Thomasu J. Woodu, pomočniku direktorja mestne uprave mesta Anaheim, ki nama je omogočil dragocen vpogled v probleme domovinske varnosti, s katerimi se sooča to srednje veliko mesto, in naredniku Johnu Hargravsu iz šerifovega urada v losangeleškem okraju, urad za nujne operacije, ki nama je predstavil delo operacijskega centra. Pomemben vpogled v probleme, s katerimi se srečuje zasebni sektor v okviru soočanja s terorizmom, nama je omogočil Damion Ellis, pomočnik direktorja urada za varnost v Hilton Anaheimu, Bernard E. Heimos, pristojen za odnose z gosti v Marriott hotelu v Anaheimu ter John J. Amabile, operativni direktor varnostnih operacij zabavišča Disneyland.

Za koristne pripombe sva dolžnika Garyju Cordnerju, Johnu Ecku, Georgu Kellingu in Nicku Rossu; anonimnim recenzentom, ki so nama pomagali predstaviti najino sporočilo; Mikeu Scottu, direktorju centra za problemsko naravnano policijsko dejavnost, ki ni le natančno pregledal priročnik, temveč je podpiral najina prizadevanja v dolgem obdobju, ko sva ga pripravljala; Jonu Shaneu, ki je ponudil odlične praktične predloge in osnoval 19. napotek (orig. 20. napotek); in končno Phyllis Schultze, stebru najine raziskave, ki je vedno našla gradivo, ki sva ga želela in potrebovala.

Napotek 01: Najprej preberi to

Rečeno je že bilo, da je 11. september spremenil vse. To velja tudi za lokalne policijske agencije in njihove načelnike**.** Vedno bolj je jasno, da zvezne agencije, kot sta FBI (zvezni urad za preiskave op.prev.) in ameriške obveščevalne službe, ne morejo več same varovati Združenih držav Amerike pred morebitnimi bodočimi napadi. Sodelovati morajo z drugimi javnimi in zasebnimi službami, in kar je najbolj pomembno, z lokalno policijo. Lokalna policija lahko odkrije morebitne teroriste, ki živijo in delujejo v njihovih okoliših, pomagajo lahko varovati ranljive tarče in lahko usklajujejo prvi odziv na teroristične napade. To so nove zahtevne naloge, ki občutno širijo delovne zadolžitve že tako obremenjenih policijskih postaj. Številne postaje sicer pozdravljajo te nove zadolžitve, vendar ne smejo zmanjševati njihovega pomena, ker izvoljeni uradniki in javnost vse bolj pričakujejo, da bo policija pripravljena na tovrstne dogodke.

»**Protiterorizem moramo vtkati v vsakodnevno delo postaj.** Vključiti bi ga bilo treba v dnevni red vsakega sestanka in ta nova vloga mora biti dodeljena policistom na cesti, tako da preprečevanje terorizma postane del njihovega vsakodnevnega razmišljanja.«

Vir: Kelling, George L. in William K. Bratton, Policing Terrorism, Civic Bulletin 43, New York: Manhattan Institute for Policy Research, September 2006.

Ta priročnik naj bi bil v pomoč vodjem policijskih okolišev in drugim vodstvenim delavcem pri soočanju z novimi izzivi, ki jih zajema zoperstavljanje grožnjam terorizma, s povzemanjem literature o bistvenih sestavinah protiterorističnega načrta. Ne obravnava posebnosti, kot so (1) nadzor osumljenih teroristov; (2) varovanje različnih ranljivih tarč, kot so pristanišča in kemični obrati; ali (3) vzpostavljanje medoperativnosti v brezžičnih komunikacijah za odziv na katastrofe med agencijami, kot so gasilci, policija in nujno zdravniško osebje. Nižji uradniki sicer rabijo o tem podrobna navodila, vodje pa želijo bolj splošne informacije o širšem seznamu zadev, ki jim bodo pomagale razviti načrte in politike za zoperstavljanje teroristični grožnji. Ta priročnik skuša zadovoljiti potrebe vodij in drugih vodstvenih delavcev s povzemanjem informacij približno 49 izvirnih ključnih tem v obliki nasvetov za predstojnike.

Morda imate občutek, da takega priročnika ne potrebujete, ker je vaše mesto premajhno in nepomembno, da bi pritegnilo pozornost teroristov. Morda imate prav, pa tudi če samo zato, ker je v ZDA na tisoče mest in velemest, teroristični napadi pa so redki. Kljub temu pa nekateri strokovnjaki menijo, da lahko prav ta občutek nepomembnosti pritegne teroriste, ker napad na nepomembno in nepričakovano tarčo utegne povzročiti več strahu – kar je pomemben cilj teroristov – kakor bi napad na pričakovano tarčo. Ne glede na to, ali je to res ali ne, ne smete tvegati življenj ljudi v vaši skupnosti: pripraviti morate načrte za preprečitev napada in hiter ter učinkovit odziv, če se napad zgodi.

Po drugi strani si lahko tudi mislite, da je priročnika ne potrebujete, ker ste že imeli nekaj izkušenj v spoprijemanju s terorizmom ali ste prestali kakšen protiteroristični trening. Morda imate osebje, ki je sposobno razviti natančne protiteroristične načrte; vsekakor ste morda že vzpostavili mnoge od potrebnih ukrepov in postopkov. Kljub temu pa ste le redki v tako ugodnem položaju. Bolj verjetno je, da niste še imeli izkušenj s terorizmom, da niste imeli nikakršnega protiterorističnega izobraževanja, da niste imeli časa za preučevanje poročil in knjig na to temo in da vaše osebje nima strokovnega znanja, da bi vam pomagalo pri oblikovanju protiterorističnih načrtov. Čeprav bo priročnik verjetno najbolj v pomoč tistim, ki sodijo v skupino slednjih, upava, da bodo zaradi ukvarjanja z nekaterimi manj znanimi temami in tehnikami, uvideli uporabno vrednost priročnika tudi bolj zreli protiteroristični strokovnjaki.

PRIROČNIK SESTAVLJA ŠEST DELOV

I. Pripravite sebe in svojo agencijo.
II. Razumite grožnjo.
III. Razvijte načrt in podporno mrežo.
IV. Zberite informacije.
V. Okrepite tarče.
VI. V primeru napada bodite pripravljeni.

Prvi trije deli obsegajo pripravljalne korake, medtem ko četrti do šesti del bolj poglobljeno obravnavajo tri ključne sestavine protiterorističnega na-

črta: (1) razvijanje obveščanja o možnih teroristih; (2) odkrivanje in zaščita pomembnejših tarč; in (3) razširitev odzivnih zmožnosti ob katastrofah.

Vsak od šestih delov vsebuje ločene napotke, ki povzemajo posamezne teme ali postopke. Te napotke sva poskušala razvrstiti po logičnem vrstnem redu, čeprav v prve tri dele vpeljujeva nekatere ključne teme, ki jih podrobneje razvijeva na koncu priročnika.

Priročnik je dovolj kratek, da ga lahko preberete ob koncu tedna, kar bi bilo vredno storiti, posebej, če imate malo osnovnega znanja o protiterorizmu. Kasneje bi ga morali imeti pri roki, da bi si lahko na hitro osvežili spomin glede določene teme. Tistim, ki imate izkušnje s terorizmom, bo morda bolj ustrezalo brskanje po kazalu in prebiranje samo tistih napotkov, za katere menite, da vam lahko nudijo nove informacije. Celo izkušeni bralci bi ga morali imeti pri roki kot uporaben napotek za usmerjanje njihovega protiterorističnega dela.

Ker vas ima večina običajno malo časa za dodatno branje in morda nimate dostopa do specializiranih knjižnic, kjer je na voljo veliko informacij, v priročniku nisva navajala virov v celoti kot pri akademskih delih. Občasno boste morda rabili več informacij, kot jih nudi priročnik; zato sva na koncu številnih napotkov navedla ključna poročila in druge publikacije, ki jih lahko pridobite razmeroma enostavno, večinoma kar na internetu. Kolikor rabite pomoč pri pridobivanju teh virov, nama lahko pošljete elektronsko sporočilo na naslednja naslova: gnewman@popcenter.org ali rvgclarke@aol.com. Pišite nama tudi, če menite, da sva v priročniku izpustila pomembne informacije ali menite, da je treba zaradi hitro spreminjajoče se narave področja o nekaterih nasvetih ponovno razmisliti. To nama bo pomagalo pri pripravi prihodnjih izdaj priročnika.

Ureditev preprečevanja terorizma v pravnem redu Republike Slovenije

Bojan Tičar

1. IZHODIŠČE

Beseda terorizem izvira iz latinske besede *terreo*, ki je v antičnem času pomenila strah ali prestrašenost. V novodobnem smislu je sodobno pojmovanje terorizma izpeljano iz staro-francoskega samostalnika *terreur*, ki je - podobno kot v latinščini - označeval strah in grozo. Francozi so za poimenovanje terorizma pomembni zato, ker so dejansko pojem terorizma v sodobnem smislu tudi prvi udejanjili. Nastal je v času francoske revolucije oziroma v obdobju po njej. Pet let po revoluciji, med 5. septembrom 1794 (ustanovitev revolucionarnega »Odbora za javno varnost«) in 28. julijem 1795 (obgalvljenje M. Robespierra) v Franciji namreč nastane t.i. *čas vladavine terorja*[1]. Povzročilo ga je politično rivalstvo med Girondini in Jakobinci, posledica pa je bilo masovno obglavljanje t.i. sovražnikov revolucije. Ocenjujejo, da je bilo v tem času pobitih od 16.000 do 40.000 t.i. izdajalcev. To je bil čas splošnega družbenega strahu, ki so ga sistematično razvili vodje odstranjevanja izdajalcev med revolucionarnimi odbori. Skrajnost *obdobja vladavine terorja* se kaže tudi v tem, da so na koncu preganjalci izdajalcev in ustvarjalci državnega terorizma sami končali pod giljotino (*fr.: guilliotine*)[2]. Ko se je francoska revolucija izrodila, je beseda terorizem prevzela označevanje državnega nasilja in eksekucij z javnim obglavljanjem[3].

Danes v pravnih redih sodobnih držav ni enotne pravne definicije terorizma. Predvsem ne takšne, ki bi na mednarodni ravni na enak način de-

---

1 Ideja državnega terorizma se kaže v izjavi Maximiliena de Robespierra, 1794 (ang.): »To punish the oppressors of humanity is clemency; to forgive them is barbarity«. Vir: Jordan David (1996), Robespierre and the Politics of Virtue, Yearbook of European Studies, European Cultural Foundation.

2 Tako je na primer končal tudi glavni protagonist vladavine terorja Maximillien de Robespierre; glej: Robespierre: the force of circumstance by J. L. Carr (Constable, 1972), stran 10.

3 Glej: Andress, David (2006). The Terror: The Merciless War for Freedom in Revolutionary France. Farrar, Straus and Giroux, New York.

finirala ta pojem.[4] Različni pravni redi opredeljujejo pojem terorizem različno. Na splošno pa povsod velja, da terorizem pomeni sistematično in organizirano nasilno dejavnost skupin ljudi, ki so nedržavno ali državno organizirane, s ciljem uničenja ali poškodovanja oseb in/ali premoženja in to iz političnih, verskih ali gospodarskih namenov. Teroristična dejavnost je javna dejavnost, saj je usmerjena predvsem na vplivanje in oblikovanje javnega mnenja in na ustrahovanje širše družbene skupnosti. Terorizem lahko razdelimo v več skupin:

a) **Nacionalistično-separatistični terorizem**. Ta oblika terorizma predstavlja delovanje ekstremnih skupin, ki stremijo k oblikovanju samostojne etnične države. Navadno to počno s pritegnitvijo javne pozornosti z nasilnimi dejanji v boju za osamosvojitev. Nacionalistične teroristične organizacije praviloma ne pretiravajo z nasilnimi dejanji. K nasilju se zatekajo do mere, da postanejo vidne in prepoznavne v domači in tuji javnosti. Običajno ne gredo čez mejo prepoznavnosti, saj bi na ta način izgubile mednarodno ali lokalno razumevanje svojih problemov. V državah članicah EU se kot najvidnejši nacionalistični teroristični organizaciji danes pojavljata predvsem Irska republikanska armada (ang.: *Irish Republican Army*, *IRA*)[5] in Baskovska domovina in svoboda (ang: *Basque Homeland and Freedom*; *Euskadi ta Askatasuna*, *ETA*)[6]. IRA se bori na območju severne Irske, ki spada pod britansko državno oblast. IRA se zavzema za priključitev severnega dela irskega otoka Republiki Irski. ETA si v Španiji prizadeva za odcepitev in osamosvojitev Baskije.

b) **Levičarski terorizem.** Ta oblika terorizma se bori proti kapitalističnemu političnemu sistemu. Bori se za zlom sedanjega političnega sistema in za to, da bi ga nadomestil novi, skrajno levo usmerjeni družbenopolitični sistem. Običajno je to komunistični ali socialistični politični sistem vladavine. Teroristične skupine te vrste navadno širijo prepričanje o trpljenju ljudstva. Tarče terorističnih napadov mnogokrat postanejo premožni in politično vplivni posamezniki, simbolni in dejanski predstavniki napada-

4 Glej: Angus Martyn (2002), The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September, Australian Law and Bills Digest Group, Parliament of Australia- http://www.aph.gov.au/library/Pubs/CIB/2001-02/02cib08.htm (22.102009).

5 Glej: Durney James (1997), The Volunteer: Uniforms, weapons and history of the Irish Republican Army 1913-1997, stran. 8.

6 Vir: Woodworth Paddy (2003). Dirty War, Clean Hands: ETA, the GAL and Spanish Democracy, Second Edition,Yale Nota Bene.

nega političnega sistema. Le-ti so po mnenju levičarskih teroristov najprimernejši za ugrabitev in/ali usmrtitev. Med organizacije levega terorizma z delovanjem na območju Evropske unije se umeščata na primer skupini, aktivni v 70-tih in začetku 80-tih let prejšnjega stoletja, kot sta *Baader-Mainhof Group (Nem.: Rote Armee Fraktion -R.A.F.)*[7] iz Nemčije, in *Rdeče brigade* (it.: Brigatte rosse)[8] iz Italije.

c) **Desničarski terorizem.** Tretja oblika terorizma predstavlja ekstremne skupine posameznikov, ki so praviloma ohlapno in kratkotrajno organizirane. Običajno veljajo za najšibkejše in slabo vplivne teroristične skupine. Načeloma so v te skupine vključeni t.i. *obritoglavci*. Med te sodijo ekstremni nacionalisti, fašisti, šovinisti in rasisti, ki si prizadevajo za odpravo socialno-liberalnih političnih sistemov ter vzpostavitev nacionalističnih (fašističnih) držav na »svoji« zemlji. Neofašistični teroristi navadno izvajajo napade na priseljence in begunce, prihajajoče iz drugih dežel. V Evropi je desničarski terorizem značilen za »stare« članice EU.

d) **Anarhistični terorizem**[9]**.** Četrta, zgodovinska oblika terorizma, se je razvila zaradi obsežnega vseevropskega pojava atentatov zlasti konec 19. in v začetku 20. stoletja. Gre za obliko terorizma, ki napada na prvem mestu najvišje politike, državno imetje, državne ustanove in sploh veljavni politični sistem države. Leta 1901 so anarhisti ubili ameriškega predsednika Willaima McKinleya[10]. Danes je ta politični tip terorizma aktualen v obliki t.i. *antiglobalističnih demonstracij*. Te so se začele ob koncu 90. let prejšnjega stoletja in se redno pojavljajo še danes. Pogosto so označene kot delovanje anarhistično usmerjenih terorističnih skupin.

e) **Državni terorizem.** V sodobnem smislu je to sinonim za organiziranje terorističnih skupin s podporo radikalnih držav, navadno pa je njihov mehanizem za zunanjo politiko. Tovrstni terorizem je mnogokrat

---

7 Vir: Aust Stefan (1987), The Baader-Meinhof Group: The Inside Story of a Phenomenon, The Bodley Head Ltd.

8 Vir: Franceschini Alberto (2005), Brigades rouges . L'Histoire secrète des Red Brigades racontée par leur fondateur,. Entretien avec Giovanni Fasanella.« Editions Panama.

9 Glej; Anarchism; Encyclopædia Britannica. Encyclopædia Britannica Premium Service. 2006. http://www.britannica.com/eb/article-9117285 (22.10.2009).

10 Vir: Gould Lewis L (1980), The Presidency of William McKinley, standard history of his term, University Press of Kansas.

označen kot uporaba nadomestnih bojevnikov – 'orožja za najem'. Država lahko podpira oziroma izvaja notranjepolitični terorizem tudi proti svojim (političnim) nasprotnikom. Teorije o tem, katere države oziroma državne institucije podpirajo ali izvajajo državni terorizem, se med seboj najbolj razlikujejo.
Pod pojem državnega terorizma po razumevanju ZDA sodijo države na t.i osi zla (*ang.: axis of evil*)[11], kot so Iran, Irak in Severna Koreja.
Po drugi strani pa predvsem islamske države označujejo Združene države Amerike za eno najbolj nasilnih terorističnih držav,ravno tako tudi njene zaveznice, npr. Veliko Britanijo ter Izrael, katerega državnost po mnenju večine islamskih držav sloni na ponavljajočih se dejanjih državnega terorizma.

f) **Mednarodni verski terorizem.** Zadnja, v sodobnem času najpogostejša in družbeno najnevarnejša oblika terorizma, je islamski, fundamentalni, verski terorizem. Po 11. septembru 2001, ko sta se dve ugrabljeni potniški letali zaleteli in do tal porušili nebotičnika newyorškega *World Trade Centra*, ter pri tem pobili skoraj 3000 žrtev, je mednarodni islamsko-fundamentalni verski terorizem postal problem celotne »zahodne civilizacije«. Ne samo problem Združenih držav Amerike, ampak tudi Evropske unije in njenih članic.

Razsežnosti vsakokratnega in različnega terorizma ter potreba po zanesljivem in učinkovitem varstvu pred njim narekujejo danes *najvišjo stopnjo javnega interesa*, zahtevo po javni in državni varnosti[12].

Vprašanje varnosti državljanov, nacionalne varnosti držav članic EU in globalne vojne proti terorizmu je v zadnjem času potisnjeno v senco drugih svetovnih kriz, zlasti vse hujše krize svetovnega gospodarstva[13]. Kljub temu pa ostaja vprašanje, do kod segajo dopustne metode v boju proti terorizmu, odprto vprašanje sodobnega pravnega reda Republike Slovenije kot članice EU. Kako naj se v slovenskem pravnem redu zakonodajalec

---

11 Pojem je uvedel leta 29.januarja 2002 ameriški predsednik George W. Bush v State of Union Adress: »This is a regime that has something to hide from the civilized world. States like these, and their terrorist allies, constitute an **axis of evil**, arming to threaten the peace of the world. By seeking weapons of mass destruction, these regimes pose a grave and growing danger. They could provide these arms to terrorists, giving them the means to match their hatre«.

12 Tako Tudi: Teršek Andraž, Pravna praksa, Gospodarski vestnik d.d., letnik 2001, številka 29, stran 4.

13 Glej: Velkavrh A., Pravna praksa, Gospodarski vestnik d.d., letnik 2009, številka 8, stran 25.

učinkovito pripravi na preprečevanje in sankcioniranje terorizma? Pravno ureditev odkrivanja in preprečevanja terorizma v Republiki Sloveniji bomo prikazali v nadaljevanju.

2. POZITIVNO-PRAVNA UREDITEV PREPREČEVANJA TERORIZMA V REPUBLIKI SLOVENIJI

Pravno-sistemsko so teroristična dejanja zajeta predvsem v veljavnem Kazenskem zakoniku Republike Slovenije (Uradni list RS, št 55/2008 in 66/2008 – v nadaljevanju KZ-1). V členih 108., 109., 110. in 111. so kogentno regulirana kazniva dejanja, ki v slovenskem pravnem redu pomenijo kazniva dejanja terorizma. Razdeljena so v štiri sklope: (1) terorizem, (2) financiranje terorizma, (3) ščuvanje in javno poveličevanje terorističnih dejanj ter (4) novačenje in usposabljanje za terorizem.

Prejšnji kazenski zakonik (KZ) je razlikoval med terorizmom (prejšnji 355. člen KZ) in mednarodnim terorizmom (prejšnji 388. člen KZ). Od leta 2004 smo dobili tudi posebno kaznivo dejanje financiranja terorizma (prejšnji 388. a člen)[14].

KZ-1 (2008) je odpravil razdelitev na notranji in mednarodni terorizem. Vse nove inkriminacije so oblikovane na podlagi mednarodnih pravnih aktov, zlasti na podlagi *»Okvirnega sklepa Sveta Evropske unije o boju proti terorizmu«*[15]. Navedeni pravni vir navaja dve vrsti kaznivih dejanj: terorizem in kazniva dejanja, povezana s terorizmom. Kaznivo dejanje terorizma sestavljajo objektivni in subjektivni zakonski znaki. Objektivni zakonski znak sestavljajo alternativno našteta izvršitvena ravnanja, ki so kot kazniva dejanja opredeljena v državi podpisnici, subjektivni zakonski znak pa je poseben naklep, ki povzroči, da kaznivo dejanje postane teroristično kaznivo dejanje (ustrahovanje javnosti, prisiljevanje oblasti, da nekaj stori ali nečesa ne stori, ali destabilizacija javne organizacije)[16].

---

14 Glej: Zgaga Sabina (2009), Pravna praksa, Gospodrski vestnik d.d., številka 26, stran 15.

15 Council Framework Decision on Combating Terrorism (2002/475/JHA), UL L 164, 22. junij 2002.

16 Zgaga Sabina (2009), ibidem.

V veljavnem slovenskem KZ-1 je pod pojmom terorizem definirano kaznivo dejanje z normo:

Terorizem

108. člen

(1) Kdor z namenom, da bi uničil ali hudo ogrozil ustavne, gospodarske, socialne ali politične temelje Republike Slovenije ali druge države ali mednarodne organizacije, da bi hudo zastrašil prebivalstvo oziroma da bi prisilil vlado Republike Slovenije ali druge države ali mednarodno organizacijo, da nekaj stori ali opusti, stori ali grozi, da bo storil, eno ali več od naslednjih dejanj:
- napad na življenje in telo ali na človekove pravice in svoboščine,
- ugrabitev ali zajetje talcev,
- precejšnje uničenje državnih ali javnih objektov ali predstavništev tujih držav, revoznega sistema, infrastrukture, informacijskega sistema, pričvrščenih ploščadi v epikontinentalnem pasu, javnega kraja ali zasebne lastnine,
- ugrabitev letala, ladje ali javnega prevoznega sredstva,
- proizvodnjo, posest, nakup, prevoz, dobavo ali uporabo orožja, razstreliva, jedrskega, biološkega ali kemičnega orožja,
- raziskovanje in razvoj jedrskega, biološkega ali kemičnega orožja,
- ogrožanje varnosti s spuščanjem nevarnih snovi oziroma povzročanjem požarov, poplav ali eksplozij, – motnjo ali prekinitev oskrbe z vodo, elektriko ali drugimi za življenje ljudi osnovnimi naravnimi viri, ki lahko ogrozijo življenje ljudi.

Splošno zagrožena kazen za tovrstna dejanja je 3 do 15 let zapora.

V drugem odstavku 108. člena je v skladu z mednarodno pravno ureditvijo[17] kot kvalificirano kaznivo dejanje urejen t. i. *jedrski terorizem*. Gre za izvršitvena ravnanja terorizma v zvezi z jedrskim materialom. V tretjem odstavku istega člena je urejeno kaznivo dejanje pomoči kot samostojno kaznivo dejanje, če je izvršeno v povezavi s terorističnimi dejavnostmi iz prvega ali drugega odstavka.

[17] International Convention for the Suppression of Acts of Nuclear Terrorism, sprejeta leta 2005 pod okriljem Združenih narodov

V slovenski ureditvi je inkriminirana pomoč pri pripravljanju terorističnih kaznivih dejanj, pomoč pri izvršitvi kaznivih dejanj terorizma pa je kazniva že po določbah splošnega dela kazenskega zakonika (KZ-1).

Ta odstavek inkriminira tudi pripravljanje kaznivih dejanj iz prvega ali drugega odstavka istega člena[18].

V slovenskem sistemu je zakonodajalec oblikoval pripravljalno dejanje kot posebno kaznivo dejanje (lat.: *delictum sui generis)*, pri tem pa je poudaril, da gre za pripravljalno fazo terorizma. Torej je zgoraj omenjena določba o pomoči pri pripravljanju kaznivih dejanj dejansko odveč, saj je pomoč pri kaznivem dejanju (čeprav gre za pripravljalno dejanje kot posebno kaznivo dejanje) kazniva že po določbah splošnega dela KZ-1[19].

V zvezi z udeležbo pri terorizmu zahteva navedeni okvirni sklep EU še to, da država članica EU inkriminira vodenje in sodelovanje v teroristični skupini. V KZ-1 je tako predvideno kvalificirano kaznivo dejanje, če je temeljno kaznivo dejanje izvršeno v hudodelski združbi ali skupini, ki ima namen izvrševati kazniva dejanja, poleg tega je inkriminirana ustanovitev in vodenje take skupine ter sodelovanje v njej. Ta ureditev je specialna glede na 294. člen KZ-1, ki ureja hudodelsko združevanje na splošno. Pri obravnavanju terorizma je treba upoštevati tudi novi 41. člen o odgovornosti članov in vodij hudodelske združbe. V njem so določeni pogoji, kdaj vodja oziroma član združbe odgovarja kot storilec, čeprav kaznivega dejanja sam ni izvršil[20].

Kaznivo dejanje financiranja terorizma ostaja kaznivo, in sicer tudi v primeru, če zbrani denar ali sredstva niso bila uporabljena za izvršitev terorizma, novo pa je kaznivo dejanje novačenja in usposabljanja za terorizem. Tudi to kaznivo dejanje je povzeto po Konvenciji Sveta Evrope o preprečevanju terorizma[21]. Financiranje terorizma je kaznivo dejanje, ki ga je zakonodajalec predpisal tako:

---

18 Zgaga Sabina (2009), ibidem.

19 Ibidem.

20 Zgaga Sabina (2009), ibidem.

21 Council of Europe's Convention on the Prevention of Terrorism, sprejeta v Varšavi, 16. maja 2005.

Financiranje terorizma

109. člen

(1) Kdor zagotovi ali zbere denar ali premoženje z namenom, da bo deloma ali v celoti uporabljeno za storitev dejanj iz 108. člena tega zakonika, se kaznuje z zaporom od enega do desetih let.
(2) Enako se kaznuje storilec dejanja iz prejšnjega odstavka tudi, če z namenom zagotovljen ali zbran denar ali premoženje ni bil dejansko uporabljen za storitev v prejšnjem odstavku navedenih kaznivih dejanj.
(3) Če je bilo dejanje iz prejšnjih odstavkov storjeno v teroristični hudodelski združbi ali skupini za izvrševanje terorističnih kaznivih dejanj, se storilec kaznuje z zaporom od treh do petnajstih let.
(4) Denar in premoženje iz prejšnjih odstavkov se vzameta.

Ščuvanje kot nova inkriminacija. Pomembna določba v zvezi z udeležbo v kaznivem dejanju terorizma je tudi nova inkriminacija ščuvanja (in javnega poveličevanja) terorističnih dejanj. V zakonu je ščuvanje definirano kot:

Ščuvanje in javno poveličevanje terorističnih dejanj

110. člen

(1) Kdor ščuva k storitvi kaznivih dejanj iz 108. člena tega zakonika s tem da razširja sporočila ali jih daje na razpolago drugim osebam na kakšen drug način z namenom spodbujati teroristična kazniva dejanja in tako povzroči nevarnost za izvršitev enega ali več takih kaznivih dejanj, se kaznuje z zaporom od enega do desetih let.
(2) Enako se kaznuje, kdor neposredno ali posredno javno poveličuje ali zagovarja kazniva dejanja iz 108. člena ali kaznivo dejanje iz prejšnjega odstavka s tem, da z namenom iz prejšnjega odstavka razširja sporočila ali jih daje na razpolago javnosti in s tem povzroči nevarnost za izvršitev enega ali več takih dejanj.
(3) Pregon za kazniva dejanja iz prejšnjih odstavkov se začne z dovoljenjem ministra za pravosodje.

V enem delu gre za napeljevanje, ki je kaznivo že po določbah splošnega dela KZ-1, v delu, v katerem je ščuvanje širše od napeljevanja, pa gre za novo inkriminacijo. Ta inkriminacija je povzeta po navedeni konvenciji.

Zadnje kaznivo dejanje je novačenje in usposabljanje za terorizem. To je predpisano na naslednji način:

Novačenje in usposabljanje za terorizem

111. člen

(1) Kdor novači za terorizem s tem, da spodbuja drugo osebo k storitvi kaznivih dejanj iz 108. člena tega zakonika ali k sodelovanju pri naročilu takega terorističnega kaznivega dejanja ali k priključitvi k teroristični hudodelski združbi ali skupini za izvrševanje terorističnih kaznivih dejanj, ki jih stori ta hudodelska združba ali skupina, se kaznuje z zaporom od enega do desetih let.

(2) Enako se kaznuje, kdor usposablja druge za kazniva dejanja iz 108. člena tega zakonika s tem, da priskrbi navodila za izdelavo in uporabo razstreliva, strelno ali drugo orožje, škodljive ali nevarne snovi, jih usposablja za druge posebne metode ali tehnologijo za izvedbo ali sodelovanje pri terorističnem dejanju.

To so vsa kazniva dejanja v slovenskem pozitivnem KZ-1, ki opredeljujejo terorizem. Načelno vsebujejo dovolj široko, splošno in abstraktno pravno podlago za pregon vseh vrst terorizma. Menimo, da je sodobna pravna ureditev preprečevanja terorizma, kot je zajeta v slovenskem KZ-1, primerna in učinkovita podlaga za boj proti terorizmu.

3. ZAKLJUČEK

Končali bomo s sposojeno mislijo: »*Naša civilizacija, če hočemo ali ne, je v vojni s terorizmom. Ker je Evropa po drugi svetovni vojni svojo energijo usmerila k preprečevanju "novega Hitlerja", je zanemarila druge oblike internacionalnih konfliktov. Združeni narodi so resda zmanjšali napetosti med nacijami in spodbujali meddržavne dialoge, vendar so dodatno odrinili marginalne skupine brez mednarodne subjektivitete. Če je ena takih skupin postala dovolj močna, da je nevarna zahodnemu svetu, je v boju z njo potreben mednarodni konsenz. Vendar je omahljiva previdnost Evrope, ko gre za vojne zadeve, prej vrlina kot slabost. Tisti, ki se ustraši vojne tam, kjer je ni, in začne svojo "preventivno obrambo", je kmalu v vojni, ki jo je sam začel*«[22].

[22] Juren Andrej (2004), Nacionalni in mednarodni terorizem v Španiji. Pravna praksa, Gospodarski vestnik d.d., letnik 2004, številka 15, stran 15.

Literatura in viri:

- *Andress, D. (2006). The Terror: The Merciless War for Freedom in Revolutionary France. Farrar, Straus and Giroux, New York.*
- *Angus, M. (2002). The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September, Australian Law and Bills Digest Group, Parliament of Australia- http://www.aph.gov.au/library/Pubs/CIB/2001-02/02cib08.htm (22.102009).*
- *Aust, S. (1987). The Baader-Meinhof Group: The Inside Story of a Phenomenon. The Bodley Head Ltd.*
- *Council Framework Decision on Combating Terrorism (2002/475/JHA), UL L 164, 22. junij 2002.*
- *Council of Europe's Convention on the Prevention of Terrorism, sprejeta v Varšavi, 16. maja 2005.*
- *Durney, J. (1997). The Volunteer: Uniforms, weapons and history of the Irish Republican Army 1913-1997, stran. 8.*
- *Encyclopædia Britannica. Encyclopædia Britannica Premium Service. 2006. http://www.britannica.com/eb/article-9117285 (22.10.2009).*
- *Franceschini, A. (2005). Brigades rouges . L'Histoire secrète des Red Brigades racontée par leur fondateur,. Entretien avec Giovanni Fasanella." Editions Panama.*
- *Gould Lewis, L. (1980). The Presidency of William McKinley, standard history of his term, University Press of Kansas.*
- *International Convention for the Suppression of Acts of Nuclear Terrorism, sprejeta leta 2005 pod okriljem Združenih narodov*
- *Jordan, D. (1996). Robespierre and the Politics of Virtue, Yearbook of European Studies, European Cultural Foundation.*
- *Juren, A. (2004). Nacionalni in mednarodni terorizem v Španiji. Pravna praksa, Gospodarski vestnik d.d., letnik 2004, številka 15, stran 15.*
- *Kazenski zakonik Republike Slovenije (Uradni list RS, št 55/2008 in 66/2008).*
- *Teršek, A. (2001). Pravna praksa. Gospodarski vestnik d.d., letnik 2001, številka 29, stran 4.*
- *Velkavrh, A. (2009). Pravna praksa. Gospodarski vestnik d.d., letnik 2009, številka 8, stran 25.*
- *Woodworth, P. (2003). Dirty War, Clean Hands: ETA, the GAL and Spanish Democracy, Second Edition,Yale Nota Bene.*
- *Zgaga, S. (2009). Pravna praksa. Gospodrski vestnik d.d., številka 26, stran 15.*

I.

Pripravite sebe in svojo organizacijo

Napotek 02: Sprejmite novo vlogo

Po začetnem pretresu zaradi 11.septembra vas je morda, tako kot številne druge načelnike, potrlo premišljevanje o prihodnosti policijske dejavnosti. Kar naenkrat je tu namesto kriminala terorizem kot največja grožnja družbenemu redu in obveščevalne agencije so postale najpomembnejši varuh družbe ter prevzele vlogo, ki jo je tradicionalno imela policija. Ko se je vlada trudila, da bi našla denar za nove protiteroristične pobude, so rezi v zveznih sredstvih za policijske programe opozorili na spremenjen status policijske dejavnosti. Vendar so se začele stvari kmalu ponovno spreminjati. Čeprav se sredstva, namenjena za boj proti kriminalu, niso vrnila na prejšnjo stopnjo, so policijski voditelji, kot sta William Bratton in George Kelling, začeli opozarjati na večjo vlogo policije v boju proti terorizmu iz dveh razlogov: (1) terorizem se ne razlikuje dosti od običajnega kriminala in (2) lokalna policija ima največ možnosti, da izve za lokalne teroristične grožnje, prepozna tarče, ki so najbolj na ogrožene in usklajuje prvi odziv na napade.

Za opravljanje te vloge boste morali nekateri veliko spremeniti. Če poveljujete veliki postaji v mestu s številnimi nedavno priseljenimi prebivalci in številnimi privlačnimi tarčami, se boste verjetno morali pripraviti na obsežnejše spremembe, kot če poveljujete, recimo, majhnim podeželskim enotam v notranjosti Amerike. Kakršenkoli je že vaš položaj, sprejmite spremembe, saj so te v skladu z najboljšo prakso v policijski dejavnosti. Poudarjajo preprečevanje, služenje skupnosti, čim boljše izkoriščanje podatkov, ki jih zberete, in vzpostavljanje sodelovanja z drugimi agencijami in organizacijami. Ti postopki vam ne bodo le pomagali pri spoprijemanju z grožnjo terorizma, temveč tudi izboljšati boj zoper kriminaliteto.

Kriminal in terorizem

Nekateri strokovnjaki poudarjajo razliko med terorizmom in običajno kriminaliteto in trdijo, da teroriste motivirajo višji nameni kot zločince ter da so bolje izurjeni in bolje organizirani. V resnici se storilci kaznivih dejanj zelo razlikujejo glede na svoje motivacije in zavzetost. Nekateri serijski morilci, na primer, načrtujejo zločine prav tako natančno kot katerikoli terorist in so enako odločni, da jih bodo uspešno izpeljali. Razlika med teroristi in drugimi storilci kaznivih dejanj verjetno ni večja, kot je razlika med različnimi vrstami storilcev. Seveda je veliko podobnosti med teroristi in organiziranimi kriminalci, posebej tistimi, ki so vključeni v mednarodni kriminal. Poleg tega teroristi pogosto zakrivijo običajna kazniva dejanja – rop, razpečevanje mamil, prevare – ki so ne le podpora napadu, temveč tudi način pridobivanja sredstev za lastno preživetje. Z vidika policijske dejavnosti je treba še veliko povedati o teroristih kot hudodelcih s političnim ozadjem.

Kljub temu boste morali spoznati nekatera osnovna dejstva o terorizmu (glej 2. del tega priročnika). Posebej pomembno je, da ne podležemo nepremišljeno številnim stereotipom, ki jih širijo nekateri mediji in politiki (glej napotek 6). Nameniti boste morali tudi sredstva za soočenje z nekaterimi novimi zahtevami, ki jih prinaša terorizem, upravljali boste morali s subvencijami za boj proti terorizmu, ki jih bo pridobila vaša postaja. To lahko pomeni, da boste morali ustanoviti protiteroristično enoto in jo oskrbeti z osebjem ali, če ste manjša agencija, uvesti obveščevalno enoto, ki se bo osredotočala na hudodelstva, ki podpirajo terorizem.

Preprečevanje in varnost (napotki 19, 29 – 36)

Številne pobude za preventivne policijske dejavnosti, še posebej »razbita okna« (op. prev. glej »Teorija razbitih oken« v članku iz leta 1982 kriminologa Jamesa Q. Wilsona in Georgea Kellinga) in problemsko naravnano delovanje policije enako poudarjajo preprečevanje kriminalitete kot njeno odkrivanje in pregon. Če upoštevamo, da je lahko posledica terorističnega napada izguba življenj, postane preprečevanje še bolj pomembno. Prav zato boste morali povečati varnost ob večjih dogodkih in pomnožiti patrulje v pristaniščih, na mostovih in ob drugi pomembni infrastrukturi. Morda boste morali opravljati varnostne raziskave in nuditi okrepitve na

ranljivih lokacijah. Če je tako, se prepričajte, da so policisti, ki prevzemajo te naloge, ustrezno usposobljeni.

Skupnostne policijske dejavnosti (napotek 26 in 27)

Kot drugi načelniki boste za pospešitev komunikacije s prebivalci določenih skupnosti tudi vi morali uporabiti policiste za skupnostno policijsko dejavnost. S peš patruljiranjem in v pogovorih s prebivalci ter lastniki lokalnih podjetij bodo verjetno izvedeli za nove prišleke in opazili tudi majhne spremembe v njihovih soseskah. Stalni prebivalci verjetno poznajo odgovorne vodje priseljenskih skupnosti, zato bi jih lahko prosili za pomoč pri spremljanju sumljivih aktivnosti. To so nekateri od številnih razlogov za oblikovanje programa skupnostne policijske dejavnosti zlasti tam, kjer je grožnja terorizma ustvarila napetosti med prebivalci soseske in policijo. Za prilagoditev skupnostne policijske dejavnosti tem novim izzivom boste morda potrebovali posebno usposabljanje in veščine.

Obveščevalni podatki in informacije (napotek 20-27)

V majhnih agencijah verjetno krožijo med policisti informacije o sumljivih aktivnostih, ker se policisti med seboj poznajo. V večjih agencijah pa je možno, da policisti, ki delajo v istem delokrogu v različnih izmenah, zanemarijo izmenjavo takih informacij, zato boste morda morali uvesti bolj formalne postopke komuniciranje. Terorizem poudarja potrebo po izmenjavi informacij in dejansko se bo v okviru zvezne izmenjave informacij (angl. Federal Information Sharing Environment – ISE), osnovane leta 2004, od vaše postaje pričakovala izmenjava informacij tako znotraj enote kot tudi z državno policijo, FBI, spojitvenimi centri in drugimi lokalnimi agencijami. Za izvedbo te dejavnosti boste morda morali posodobiti svoj informacijski sistem in zaposliti ustrezno usposobljene analitike. Morda boste morali določiti vsaj enega uslužbenca za zvezo za področje terorizma (terrorism liaison officer – TLO), ki bo pregledoval in prenašal informacije ustreznim agencijam v okviru ISE. Informacije za usposabljanje vašega TLO lahko pridobite na http://www.tlo.org/training/index.htm. Če jih še niste, si priskrbite smernice spojitvenega centra, ki sta jih družno oblikovala ministrstvo za pravosodje in ministrstvo za domovinsko varnost zaradi lažje izmenjave informacij med agencijami kazenskega pregona. Smernice so dostopne na

http://fas.org/irp/agency/ise/guidelines.pdf. Še en koristen dokument je *Nacionalni načrt izmenjave kazenskih obveščevalnih informacij*, ki ga je oktobra 2003 objavil biro pravosodne asistence (angl. Bureau of Justice Assistance – BJA): http://www.it.ojp.gov/documents/NCISP_Plan.pdf. Oktobra 2007 je predsednik Bush razglasil novo Nacionalno strategijo za izmenjavo podatkov, ki določa prednosti pri izmenjavi podatkov in oblikuje integrirane nacionalne mehanizme za izmenjavo podatkov, sorodnih tistim o terorizmu, med zveznimi, državnimi, lokalnimi policisti, zasebnim sektorjem in tujimi partnerji. Podrobnosti o tej strategiji in njeni uporabi lahko najdete pri Uradu direktorja nacionalne obveščevalne dejavnosti (Office of the Director of National Intelligence), http://www.ise.gov/.

Partnerstvo (napotek 16 in 17)

Zbiranje informacij o terorističnih grožnjah si lahko olajšate s sodelovanjem s subjekti zasebne varnosti in podjetji. Banke, ustanove za vnovčenje čekov, službe za prenos denarja, kot je Western Union, vam lahko dajo podatke o sumljivih finančnih transakcijah; agencije za najem avtomobilov, moteli in nepremičninski agenti vas lahko obveščajo o prišlekih in začasnih gostih; izvajalci zasebne varnosti vas lahko obvestijo o organiziranih goljufijah in medmrežni kriminalitei, ki bi lahko financirala terorizem. To osebje je tudi neposredno odgovorno za varovanje večine infrastrukture na vašem območju in se pogosto prvo odzove na nezgodo. Usklajevanje lahko zmanjša pritiske na vašo preobremenjeno enoto.

Priprave na katastrofo že zdaj zahtevajo tesno sodelovanje z županom ali upraviteljem mesta, ter z drugimi mestnimi ustanovamu, kot so gasilci, nujna zdravniška pomoč, bolnišnice in šole. Vendar pa teroristična grožnja pomeni, da boste morali prilagoditi svoje načrte tako, da bodo upoštevali tudi manj običajne groženje. Na primer, odvisno od vaše lokacije, boste morda morali računati na možnost napada z orožjem za množično uničenje (weapons of mass destruction – WMD), vključno s kemičnimi, biološkimi, jedrskimi ali radiološkimi sredstvi. Morda boste morali upoštevati možnost, da bodo mostovi in tuneli na morebitnih evakuacijskih poteh namerno uničeni. Verjetnost, da bodo tovrstne napade izpeljali brez opozorila, zahteva povečano pogostnost in dodelanost vaj za usposabljanje.

Morda boste želeli vzpostaviti partnerstvo z lokalnimi časopisi in radijskimi postajami. Z objavljanjem, kaj počnete, da bi se zoperstavili grožnji teroriz-

ma, lahko mediji pripomorejo k pomirjanju zaskrbljene javnosti. Lahko tudi pomagajo prepričati skupine priseljencev, da se bo z njimi ravnalo pošteno in da bo policija trdno ukrepala proti zločinom iz sovraštva. Mediji lahko igrajo vitalno vlogo v izrednih razmerah z obveščanjem javnosti o okoliščinah in odzivih nanje. Veliko bolj verjetno je, da bodo pomagali, če sebe vidijo kot partnerja v spoprijemanjem s terorizmom. Večina navedenega je v skladu z običajno skupnostno dejavnostjo policije (napotek 27). Če torej že imate program skupnostne policijske dejavnosti, ga bo preprosto razširiti tako, da bo vključeval tudi odziv na teroristične grožnje.

Kako se je policijska postaja Long Beach (Kalifornija) prilagodila terorističnim grožnjam

- Z oblikovanjem protiteroristične enote in določitvijo uslužbenca za zveze (TLO).
- Z določitvijo policistov za ocenjevanje in zaščito kritične infrastrukture, kot so pristanišče, letališče in čistilne naprave.
- Z napotitvijo policistov na usposabljanje za nove veščine, kot sta odziv na orožje za množično uničenje in prepoznavanje znamenj terorizma.
- Z ustanovitvijo pristaniške policijske enote, opremljene z majhnimi čolni.
- Z določitvijo policistov za odziv na področjih z visoko rastjo prebivalstva.
- Z izboljšanjem opaznosti in odzivnega časa z razporeditvijo policistov - namesto dveh ena oseba v avtu.
- Z zmanjšanjem osebja na manj pomembnih programih, kot je izobraževanje o odpornosti na zlorabe drog (Drug Abuse Resistance Education – D.A.R.E).
- Z zmanjšanjem števila peš patrulj in kadra v oddelku za mamila.
- Z vlogami za pridobitev dodatnih sredstev za pokritje povečanih potreb tako od mestne uprave za lokalne potrebe kot tudi od zvezne vlade za državne potrebe.

Vir: Raymond, Barbara, Laura J. Hickman, Laura Miller in Jennifer S. Wong., Police Personnel Challenges After September 11: Anticipating Expanded Duties and a Changing Labor Pool. Santa Monica, California; RAND Corporation, 2005.

Napotek 03: **Vedite, da je strah sovražnik**

V času velike ekonomske depresije je Franklin D. Roosevelt zbral Američane z opominom, da »...je edina stvar, ki se je moramo bati, strah sam – brezimna, nespametna, neupravičena groza, ki paralizira trud, da bi umik preoblikovali v napredek.« Njegove besede so še bolj prikladne po 11. septembru, ker je zdaj veliko ljudi strah, da bodo v nekem obdobju svojega življenja postali žrtve terorističnega napada. Dejansko jih veliko bolj skrbi zares majhno tveganje, da jih bodo ubili teroristi, kakor pa veliko večja nevarnost, da bodo umrli v avtomobilskem trčenju ali kakšni drugi nesreči.

Kot že dobro veste, nesorazmerje med tveganjem in strahom omogoča kriminaliteo. Strah pred kriminaliteto se je v dveh desetletjih, od sredine 1980. let. nenehno večal, medtem ko je število prijav kaznivih dejanj nenehno padalo. Tisti, ki se najbolj bojijo kriminalitete – starejši na primer – so pogosto najmanj verjetne žrtve. Dejansko, večina ljudi ne sodi o nevarnosti, da bi postala žrtev zločina in terorizma (ali katerekoli katastrofe) na podlagi statističnih podatkov; bolj verjetno je, da bo nanje vplivalo časopisno in televizijsko poročanje o zastrašujočih dogodkih. Tako se ljudje pogosto bolj bojijo, da bodo umrli v strmoglavljenju letala ali zaradi napada morskega psa, kot na bolj običajne načine, kot je avtomobilska nesreča. Zdi se tudi, da se jih veliko boji, da bodo izgubili življenje v obsežni katastrofi, kot je teroristični napad, kar pa je prav tako malo verjetno.

Boj ko smo prestrašeni, bolj bodo teroristi ocenjevali svoje napade kot uspešne. Ne samo da pretiran strah znižuje kakovost našega življenja, temveč, kot trdi David Altheide v Terorizem in politika strahu (Terrorism and the Politics of Fear), strah »omejuje naše intelektualne in moralne zmožnosti, nas ščuva ene proti drugim, spremeni naše vedenje in naše gledišče ter nas naredi ranljive v odnosu do tistih, ki nas želijo nadzirati, da bi uresničili svoje lastne cilje.« Ta strah lahko vodi državo v trošenje milijard dolarjev za varnostne ukrepe, v omejevanje pomembnih svoboščin in v sprejemanje radikalnih sprememb v zunanji politiki.

Morda se ne zdi pomembno, vendar je lokalni odziv na grožnjo terorizma prav tako pod vplivom strahu kakor odziv na nacionalni ravni. Čeprav malo strahu lahko olajša izvedbo stvari, lahko previsoka stopnja strahu – kar je nek akademik opisal kot **»umetni občutek nevarnosti« - vodi v tratenje sredstev in delovne sile**. Da bi preprečili to potrato, vas bo mor-

da celo mikalo, da bi sledili nasvetu senatorja Johna McCaina, navedenega v knjigi Zakaj je pogum pomemben: Pot do pogumnejšega življenja (Why Courage Matters: The Way to a Braver Life): »Pojdite v prekleto dvigalo! Letite s prekletim letalom! Preračunajte verjetnost, da vas poškodujejo teroristi! Še vedno je približno tako verjetno, kot da vas odnese na morje val plime... Skoraj zagotovo bo z vami vse v redu...«

Čeprav je to racionalen odziv na grožnjo terorizma, boste verjetno ugotovili, da je neučinkovit: ljudje občudujejo pogumne voditelje, vendar še bolj cenijo tiste, ki razumejo njihove strahove in so ustrezno previdni. Reči bi morali: »Veliko ljudi je razumljivo prestrašenih«; ne pa: »Ničesar se ni treba bati«. Zmanjševanje strahu bi moralo biti pomemben del protiterorističnega načrta. Na srečo je lažje zmanjšati strah pred napadom kot dejansko tveganje napada. Namreč, kako zmanjšati tisto, kar je za večino okolij resnično majhno tveganje? Poleg tega večina ukrepov, ki jih lahko izpeljete za zmanjšanje strahu, kot je razvidno iz spodnjega seznama tovrstnih ukrepov, ni draga.

1. Pri oblikovanju protiterorističnega načrta za skupnost se s svojimi partnerji sporazumevajte čim bolj odprto (glej napotek 16-18). Celovito utemeljite svoje odločitve in prijazno sprejmite njihove prispevke, soglasje in sodelovanje. Bolj verjetno boste uspeli, če jih boste obravnavali kot enakovredne partnerje ter jim dodelili odgovornost za uporabo posameznih delov protiterorističnega načrta. Če čutite, da z javnostjo ne morete biti neposredni, razložite to svojim partnerjem.
2. Ocenite vse predloge - tako za zmanjševanje strahu kot tudi za zmanjševanje tveganja. V okoljih, kjer je tveganje zanemarljivo, se osredotočite na predloge za zmanjšanje strahu. Ko je strah zmanjšan, boste lahko oblikovali bolj racionalen načrt za zmanjševanje tveganja.
3. Prepričajte se, ali lahko razložite in zagovarjate načrt pred javnostjo.
4. Posebno pozornost namenite manjšinam in priseljenskim skupinam, zlasti njihovemu strahu, da bodo žrtve zločinov iz sovraštva. Ob posebno občutljivih trenutkih, kot npr. takrat, ko je stopnja teroristične ogroženosti povišana, povejte, da ne boste dopuščali zločinov iz sovraštva; hkrati pa se zavedajte, da se bodo nekatere manjšinske skupnosti počutile neupravičeno zapostavljene, ne glede na to, kako se boste trudili, da bi ublažili njihove skrbi.
5. Pridobite pomoč lokalnih medijskih hiš pri predstavitvi svojega načrta, izogibajte se zastraševalnim taktikam poročanja o terorizmu ter govoru o podpori, če je majhna verjetnost napada.

6. Če se napad ponovno zgodi, v ZDA ali drugje, naj vam bodo jasne njegove posledice za vaše mesto ali okoliš - v večini primerov jih ne bo. Skrbno ocenite lokalni pomen nacionalnih opozoril o stopnji teroristične ogroženosti in, če je treba, uravnotežite potrebne akcije s prizadevanji za pomiritev skupnosti in osebja svoje postaje.
7. Soočite se z lastnimi strahovi, da bo terorizem prizadel vas ali vašo družino (kar je zelo malo verjetno); s strahovi pred svojimi profesionalnimi pristojnostmi v okviru nove protiteroristične vloge (vsi se učimo); z obtožbami, da ste sprejeli nepotrebne varnostne ukrepe ali, da niste sprejeli tistih, ki so bili nujni (kasnejši uvidi so krasna stvar).

Več o tem:

1. *Altheide, David L. Terrorism and the Politics of Fear. Lanham, Maryland: AltaMira Press, 2006.*
2. *McCain, John, with Mark Salter, Why Courage Matters: The Way to a Braver Life. New York; Random House, 2004.*

Napotek 04: Pripravite se na opozorila o stopnji teroristične ogroženosti

Svetovalni sistem domovinske varnosti (The Homeland Security Advisory System – HSAS) so uvedli kmalu po 11. septembru za opozarjanje države o morebitnih terorističnih napadih. Sestavlja ga pet (barvnih) stopenj ogroženosti, vsaka pa je povezana s predlogi zaščitnih ukrepov.

1. Rdeča: resna stopnja.
2. Oranžna: visoka stopnja.
3. Rumena: povišana stopnja.
4. Modra: stopnja previdnosti.
5. Zelena: nizka stopnja.

Večino časa je veljala za državo rrumena, srednja (povišana) stopnja, čeprav je bila ob različnih okoliščinah stopnja ogroženosti dvignjena na oranžno (visoko). Za obdobja, ko je vaš predel na oranžni stopnji (ali kadar odločevalni letalski opozorilni sistem teroristične ogroženosti označi lokalno letališče z oranžno stopnjo), morate imeti pripravljen odzivni načrt. Načrt naj sestavljajo zdravorazumski ukrepi, ki jih vi in drugi – občinski uradniki, podjetja in prebivalci – lahko izpeljete v svojem okolju. (Glej seznam teh ukrepov v okvirju.) Ne glede na dejansko verjetnost napada – ali resnično učinkovitost ukrepov – lahko ukrepi pomagajo pomiriti prebivalce in jim dajo občutek, da so zavarovani pred morebitnim napadom.

Sistem HSAS so mediji na široko kritizirali. Tudi vi se boste morda morali soočiti s kritikami, ko boste vzpostavljali odzivni načrt. Ker je malo verjetno, da bo v bližnji prihodnosti stopnja ogroženosti padla pod rumeno, se sistemu očita, da je prej tristopenjski kot pa petstopenjski. Prav tako se mu očita, da ne nudi jasnih opredelitev, kaj določa povišano, visoko in resno stanje in da ne nudi praktičnih nasvetov, kaj narediti v vsakem primeru. Vendar pa je njegova največja pomanjkljivost ta, da ne sloni na trdnih dokazih kot na primer vremenska opozorila. Vremenska opozorila temeljijo na meteoroloških podatkih, ki pokrivajo široko paleto natančno merljivih vremenskih spremenljivk – zračni tlak, hitrost vetra, predvideno plimovanje, temperatura, pričakovane padavine itd. Zelo težko je seveda dobiti zanesljive informacije o pripravljajočem se terorističnem napadu, še težje je nekatere grožnje pripisati določenim tarčam ali področjem države. Tako

je za vsak sum napada na stotine ali tisoče mest opozorjenih na grožnjo, ker nimamo ustrezne metode za razvrščanje tarč glede na njihovo potencialno ogroženost. To seveda vodi v porabo sredstev in nepotrebne varnostne ukrepe. Pri obsežnem delu populacije lahko vzbudi tudi nepotrebno prestrašenost, kar lahko vzame veljavo sistemu, če do napada ne pride. Da bi rešili ta problem, so se nekatera nedavna opozorila osredotočila na določeno področje države ali poseben industrijski sektor. Razmišlja se tudi o drugih izboljšavah in izboljšuje se usklajenost z nekaterimi drugimi državnimi in zveznimi sistemi opozarjanja. Medtem pa ni druge možnosti, kot da se upošteva HSAS in prepričati je treba tudi druge, da storijo enako. Pregled seznama ukrepov ob opozorilu – nudiva seznam za oranžno opozorilo, ki je najbolj običajno – je lahko koristen tudi zato, ker poudarja kompleksnost odziva in veliko število vključenih oseb in skupin.

Več o tem:

Kemp, Roger L., »Homeland Security: Common Sense Measures to Safeguard your Community,« The Police Chief 73 (February 2006).

Seznam priporočenih ukrepov in odzivov na oranžno opozorilo

Seznam za vodje policije

- Skrbno nadzorujte vse varnostne in obveščevalne podatke zveznih, državnih in lokalnih agencij kazenskega pregona.
- Dovolite dostop do vseh pomembnih objektov le nujnemu osebju.
- Zagotovite, da bodo policisti uveljavljali omejitve parkiranja vozil ob pomembnih javnih zgradbah.
- Okrepite obrambne ukrepe ob ključnih strukturah in ob večjih javnih dogodkih.
- Opozorite policijsko in gasilsko osebje, da bo pozorno, ko se bo odzivalo na izgrede.
- Preglejte stavbe in parkirišča, če so kje sumljivi paketi.
- Nadzorujte vse občinske zbiralnike in razvodja, čistilne naprave in druge pomembne javne objekte.
- Izvajajte naključne cestne kontrole na območjih, kjer je pomembna infrastruktura.

- Svetujte vsemu osebju, kako naj ravna ob nepredvidljivih dogodkih, katere hitre spremembe, naloge, dela in sklopi pomoči so potrebni ter kakšna naj bo družinska oskrba in podpora ob zaostritvi razmer. Imejte pripravljen načrt družinske pripravljenosti.
- Razpršite in postavite sredstva postaje za nujne primere, vključno z rezervnimi vozili in poveljniškimi točkami, na različne lokacije v okolišu.
- Od poveljnika terenskega operativnega urada zahtevajte, da identificira potencialne poveljniške točke in določi zbirna mesta po vsem okolišu in to informacijo posreduje uradu načelnika.
- Uskladite javne informacije z županovim kabinetom, mestno agencijo za obvladovanje izrednih razmer, gasilsko postajo in nujno medicinsko službo.
- Od načelnikov zahtevajte, da pregledajo opremo za operativno pripravljenost.
- Kjer je to primerno, dvignete ograde in ovire za nadzor pretoka prometa.
- Sodelujte z mestom pri določitvi in objavi evakuacijskih poti.

Seznam za mestne uradnike (župane in člane mestnega sveta, mestne upravitelje, vodje gasilcev, direktorje javnih del in drugo osebje za izredne razmere)

- Preglejte lokalne načrte za odziv v izrednih razmerah in se pripravite na aktiviranje operacijskega centra za nujne primere.
- Uskladite odzivne načrte s kolegi na drugih vladnih ravneh.
- Tesno sodelujte z okrožnimi zdravstvenimi uslužbenci pri odkrivanju prenosljivih bolezni.
- Vse enote za obvladovanje izrednih razmerah in specializirane odzivne ekipe naj bodo v stanju pripravljenosti.
- Zagotovite, da bodo zaposleni posebej pozorni na sumljive pakete ali zavoje brez lastnika, in članke, ki so jih prejeli prek sistemov javne in zasebne pošte.
- Pomembna odzivna vozila hranite na varovanih območjih; če je mogoče v pokritem parkirnem objektu.

Seznam za podjetja

- Prepričajte se, da so ustrezne varnostne naprave nameščene in da pravilno delujejo.

- Uslužbencem naročite, da svojim nadrejenim poročajo o sumljivih dejavnostih, paketih in ljudeh.
- Preglejte vse torbe in pakete osebja in od uslužbencev zahtevajte, da gredo skozi detektor kovin, če je ta na voljo.
- Nadzorujte dostope do podzemne garaže in nakladalne doke; ravno tako zaprta parkirišča ob zgradbah in v infrastrukturi.
- Preglejte in aktivirajte sistem za odkrivanje vdorov, zunanjo razsvetljavo, varnostno ograjo in sistem zaklepanja.
- Preglejte vse dostave; kjer je to primerno, sprejemajte pošiljke le na odmaknjenih lokacijah.
- Uslužbence opozorite na poostreno varnostno politiko in ustrezne evakuacijske postopke v zgradbi.
- Imejte pripravljen načrt za umik v zaklonišče.

Seznam za prebivalce

- Zaradi preiskovanja prtljage in drugih poostrenih varnostnih ukrepov v javnih zgradbah in drugih objektih pričakujte zastoje.
- S klici v klicni center 911 poročajte lokalnim agencijam kazenskega pregona o vseh sumljivih dejavnostih na pomembnih javnih objektih ali v njihovi bližini.
- Ne puščajte nenadzorovanih paketov in aktovk na javnih območjih.
- Pripravite komplete za oskrbo v izrednih razmerah in se z družino pogovorite o načrtih za izredne razmere.
- Bodite pozorni na svojo okolico, ne izpostavljajte se nevarnim okoliščinam in skrbno nadzorujte aktivnosti svojih otrok.
- Za zagotavljanje varnosti otrok in njihove čustvene dobrobiti vzdržujte tesne stike s svojo družino in sosedi.
- Spremljajte svetovne dogodke in lokalne okoliščine kot tudi opozorila lokalne vlade glede ogroženosti.

(Za nadaljnje predloge glej http://www.ready.gov.)

Napotek 05: Pričakujte večjo pozornost javnosti

Grožnja terorizma povečuje obseg vašega dela in odgovornosti, prav tako se bo občutno povečala tudi vaša javna prepoznavnost v mestu ali velemestu. Lokalni mediji bodo od vas zahtevali, da komentirate tveganje za napad. Redno vas bodo prosili, da govorite na srečanjih Lionsov, Elksov, Rotary kluba in podobnih organizacij. Manjšinske skupnosti bodo hotele zagotovila, da so zavarovane pred zločini iz sovraštva in da jih policija ne bo po krivici izpostavljala. Z lokalnimi podjetji in korporacijami boste sodelovali pri izboljševanju njihove varnosti. In morali se boste posvetovati z bolnišnicami, klinikami in šolami (ne glede na to, ali sodijo pod mestno upravo ali ne), da se prepričate, ali delajo vse, kar lahko, da se zavarujejo.

Vendar pa je najbolj pomembno to, da se bodo mestne oblasti verjetno zanašale na vaš odziv na grožnjo terorizma. Obravnavali vas bodo kot lokalnega strokovnjaka za terorizem in kot osrednji vir informacij, ki prihajajo od zveznih oblasti. Od vas bodo pričakovali, da boste osnovali lokalne obveščevalne službe za oskrbo z nasveti o varnosti mestne infrastrukture, da boste sklenili dogovore o medsebojni pomoči s sosednjimi policijskimi postajami za delitev sredstev (npr. specialne enote - SWAT team), oddelke za odstranjevanje bomb in poskrbeli za pogosto spregledane tolmače ter poskušali povečati sredstva postaje in mestne sredstva s pridobivanjem in upravljanjem zveznih ter državnih subvencij za boj proti terorizmu.

Ob operacijah v izrednih razmerah boste morali igrati bolj pomembno vlogo. V okviru načrta operacij v izrednih razmerah, kakršnega ima sedaj večina mest, imajo policijske postaje in druge mestne agencije nekatere omejene odgovornosti. Značilen načrt (kot ga je opisalo mednarodno združenje uprav mest/okrožij - International City/County Management Association) je opisan v spodnjem seznamu. Ta načrt odgovornosti postaj vključuje preiskavo kaznivih dejanj, varovanje lastnine, nadzor prometa in vodenje evakuacij. V kolikor bi imele posledice terorističnega napada katastrofalne razsežnosti, se te dolžnosti razširijo. Dejansko je treba skoraj vsak vidik načrta prilagoditi, ker je katastrofa kot posledica terorizma v nekaterih pomembnih vidikih drugačna od drugih katastrof (glej napotek 37). Na primer, običajno ni predhodnega opozorila za nevarnost še enega napada, zato je javni strah toliko večji in verjetno se poveča tudi medijska pozornost z občutno več tujega poročanja. Če napad vključuje jedrska, kemična in biološka sredstva, je potrebnih veliko odzivov, vključno z zaščito

pred kontaminacijo tistih, ki so ukrepali, in z zagotavljanjem zdravniške oskrbe poškodovanim v napadu.

Z vašega stališča bo zaradi terorističnega napada katastrofalnih razsežnosti treba prilagoditi vodstvene odgovornosti v treh pomembnih pogledih.

1. **Varnost prizorišča.** Po začetnem napadu bi teroristi lahko podtaknili bombe, da bi pobili reševalne delavce. Po napadu 11. septembra na Svetovni trgovinski center je policija v vozilih, ki so vstopala na kraj katastrofe, iskala eksploziv in drugo orožje.
2. **Varnost centra operacij v izrednih razmerah.** Poleg poostrene varnosti na prizorišču katastrofe boste morali poostriti varnost tudi v centru operacij v izrednih razmerah (Emergency operations center – EOC), da župan, voditelji skupnosti in drugi mestni uradniki ne bi postali tarče teroristov.
3. **Zavarovanje kraja zločina.** Za razliko od naravnih katastrof zahtevajo teroristični napadi kriminalistično preiskavo; delovati boste morali hitro, da bi pridobili in zavarovali dokaze. Pripravite seznam ljudi, ki jim boste odobrili dostop na prizorišče in ne dovolite prostovoljcem in civilistom, da se prosto gibljejo na kraju napada, kot bi to dovolili ob običajnih katastrofah. Narediti morate vse, kar lahko, za ohranitev neokrnjenosti dokazov. Prepričajte se, da dokazi niso prinešeni na lokacijo ali odnešeni z nje in hranite natančno evidenco o skrbniški verigi dokazov. V primeru požiga zagotovite, da izpušni dim iz generatorjev in drugih motoriziranih naprav ne uniči ruševin in uniči dokaze, ki bi pokazali, da so bili uporabljeni pospeševalniki.

Še zadnja točka o reševanju. Načrti operacij v izrednih razmerah pogosto zanemarjajo vlogo podjetij pri odzivih na katastrofo. Podjetja imajo velik interes, da si skupnost hitro opomore, zato so pogosto pripravljena dati ogromno sredstev in včasih lahko pomoč priskrbijo veliko bolj učinkovito kakor vladne agencije (glej okvir). Vaš odnos z zasebnimi varnostnimi strokovnjaki pomeni pomembno povezavo med vlado in podjetji; zagotovite, da bo mesto pri odzivu na katastrofo v celoti pridobilo potencialne prispevke.

»V odzivu na orkana Katrina in Rita so se podjetja, kot sta Wal-Mart in Home Depot, izkazala kot veliko bolj spretna pri oskrbi z delovno silo, materialom in logistiko kakor mnogi organi zvezne oblasti. Medtem ko so tovornjaki z ledom, ki jih je najela zvezna agencija za obvladovanje

izrednih razmerah (Federal Emergency Management Agency – FEMA), obtičali več dni brez napotkov, kam morajo iti, so nacionalni trgovci na drobno organizirali pomembne distribucijske točke za hrano, vodo, obleke, generatorje in drugo oskrbo. Misisipi Power, podružnica Southern Company, je ponovno vzpostavila elektriko stotisočem odjemalcev veliko pred načrtovanim rokom. Varnostna služba družbe Guardsmark je v enem tednu izsledila vse svoje pogrešane zaposlene, ki so živeli in delali na prizadetem območju, in jim priskrbela avtomobile, nujno oskrbo ter pomoč pri selitvi. Pri Johnson Controls so kupili avtodome v Viskonsinu in jih dostavili v kampe na območju katastrofe, tako da so njihovi uslužbenci imeli začasna bivališča. Čeprav sta bila Katrina in Rita naravni katastrofi, ki ju ni povzročil človek, se je pokazalo, da bo ljudem veliko bolje, ko bo zvezna oblast sprejela zasebni sektor kot partnerja pri preprečevanju in odzivanju na morebitne katastrofalne teroristične napade.«

Vir: Flynn, Stephen E., and Daniel B. Prieto, Neglected Defense: Mobilizing the Private Sector to Support Homeland Security, Council Special Report No. 13. New York: Council on Foreign Relations, 2005.

Primer načrta operacij v izrednih razmerah – Kaj kdo dela?

Župan/upravnik mesta

- Sproži mestni načrt za izredne razmere
- Če je treba, začasno prekliče odloke
- Uporabi vsa mestna sredstva, kjer je to potrebno
- Po potrebi premesti mestno osebje, opremo in funkcije
- Sodeluje z uradnikom za javno informiranje - za posredovanje informacij javnosti

Vodja v izrednih razmerah

- Svetuje županu in upravitelju mesta
- Usmerja razvoj mestnega načrta z drugimi postajami
- Vzpostavi sistem zbiranja, analize, poročanja in razpečevanja informacij
- Vodi vaje z vsemi agencijami in organizacijami v skupnosti
- Usklajuje donacije in vzajemno pomoč
- Nadzira evakuacijo
- Usmerja operacije centra operacij v izrednih razmerah (EOC)
- Sodeluje z uradnikom za javno informiranje - za posredovanje informacij javnosti

Gasilci

- Zadušitev ognja
- Nujna medicinska služba
- Iskanje in reševanje
- Radiološka ocena

Policija

- Kazenski pregon
- Kriminalistična preiskava

Urad za nadzor in stanovanjsko vzdrževanje/inženiring

- Oceni škodo
- Izloči poškodovano strukturo
- Uskladi obnovo servisov
- Javna dela
- Odstranjuje ruševine
- Obnovi vodne in kanalizacijske storitve
- Težka oprema

Inženiring

- Parki in rekreacija
- Odstranjevanje ruševin

Javne zgradbe in objekti

- Zagotovitev uradov za državna in zvezna sredstva

Zavetišča

Mrliški oglednik

- Identifikacija žrtev
- Mrliška služba
- Finance
- Računovodstvo
- Nabava
- Osebje
- Zagotovi dobrobit družin tistih, ki so se odzvali
- Usklajuje prostovoljce
- Oddelek za urbanizem
- Ocena škode

Pravne zadeve

- Javne informacije
- Akreditacija medijev in nadzor lokacije
- EOC zastopništvo
- Evakuacije
- Komunikacije
- Nadzor prometa

Napotek 06: Podvomite v predpostavke

Včasih je težko vedeti, kaj verjeti o terorizmu. Za večino izmed nas so glavni vir informacij mediji, ki nas bombardirajo z zgodbami o terorističnih grozotah, pogosto iz oddaljenih delov sveta, začinjenimi s komentarji strokovnjakov - včasih vprašljivega ugleda. Zapomnite si, da osrednja naloga medijev ni informiranje, temveč obdrževanje in zabavanje občinstva. Zgodbe so predstavljene tako, da so videti pomembne in želijo vzbuditi čustva občinstva. Televizijski napovedovalci običajno sledijo zgodbi – recimo o samomorilskem napadu v Šri Lanki – s spraševanjem domnevnega strokovnjaka, ali smo v ZDA ustrezno pripravljeni na spoprijemanje s tovrstnimi dogodki. Z oblikovanjem taktične predpostavke, da je lahko pričakovati samomorilske napade tudi tu, tisti, ki intervjuva, naredi zgodbo pomembno za življenje gledalcev in dvigne stopnjo njihovega strahu, čeprav v resnici nismo skoraj nikoli ustrezno pripravljeni na redke in nepredvidljive dogodke. Posledica tega je, da bodo gledalci v iskanju bodisi zagotovil ali pa nadaljnjega vznemirjenja bolj verjetno ponovno gledali isti kanal. »Strokovnjaki« imajo morda svoje razloge za zbujanje strahu in bodite prepričani, da sledijo zasebnim ciljem, ki so za sedanjo administracijo ali proti njej, posledica pa je, da so gledalci manj informirani ali bolj zmedeni kot kdajkoli.

Vedno poskušajte identificirati in kritično oceniti predpostavke, na katerih temeljijo informacije, ki vam jih posredujejo. Spodaj so naštete nekatere najbolj običajne in najbolj vprašljive predpostavke o terorizmu.

1. **Mit: Kdorkoli je lahko terorist.** Čeprav drži, da so teroristi vseh oblik in velikosti, je večina teroristov mladih moških. Zelo malo verjetno je, da bo terorist sivolasa babica iz srednjega zahoda, tudi če se sumljivo obnaša. Veliko bolj verjetno je, da je zbegana ali nepoučena in tako bi moral razmišljati tudi policist, ko pristopa k njej. Sumničenje bi morali prihraniti za tiste, ki bolj ustrezajo profilu terorista.
2. **Mit: Vsak priseljenec je sumljiv.** Tisti, ki najbolj ustrezajo profilu terorista (vsaj za sedaj), so mladi moški priseljenci bližnjevzhodnjaškega videza. Seveda je tudi v okviru te skupine le manjšina teroristov, tistih, ki želijo biti teroristi, ali le privržencev teroristov. Drugačno obravnavanje v okviru priložnostnih srečanj bi lahko ogrozilo odnose s skupino, ki lahko vašim policistom sicer priskrbi dragocene informacije o zares sumljivi dejavnosti.

3. **Mit: Teroristi so ponoreli fanatiki.** Ne glede na to, kako močno se ne strinjate z razlogi za njihova dejanja, si morate zapomniti, da večino teroristov vodi trezen razum. Kot vsi organizirani kriminalci tudi oni natančno načrtujejo svoja dejanja, se poskušajo izogniti aretaciji in so odločeni, da jim bo uspelo.
4. **Mit: Teroristi si želijo smrti.** Kot smo spoznali na lastni izkušnji, so nekateri teroristi pripravljeni umreti za svoje ideale. Toda številni teroristi so previdni, kadar gre za njihovo življenje. Ne samo, da imajo enake želje po uspehu in sreči kot vsi ostali, ampak bi raje zbežali in kasneje ponovno napadli, kot pa tvegali, da jim spodleti in izgubijo življenje.
5. **Mit: Teroristi so hudobni geniji.** Vsak terorist nima pameti Osame Bin Ladna. Večinoma so običajni, zmotljivi posamezniki. Lahko sicer natančno načrtujejo svoja dejanja, vendar so vključeni v tvegane posle. Ne morejo predvideti vseh ovir in občasno bodo prisiljeni improvizirati in tvegati. Nekatere njihove odločitve bodo neuspešne in jih bodo nemara vodile v smrt.
6. **Mit: Teroristi lahko napadejo kjerkoli.** Teoretično teroristi lahko napadejo kjerkoli, praktično pa morajo varčevati s svojimi viri in napasti tam, ker bodo dosegli največji učinek. Če razmišljamo kot teroristi, lahko predvidimo njihove izbire in se temu primerno odzovemo z zavarovanjem najbolj ranljivih tarč.
7. **Mit: Teroristov ni mogoče ustaviti.** Večina terorističnih skupin deluje eno do dve leti preden razpadejo. Podatki govorijo o bistvenem zmanjšanju terorizma. Ugrabitve letal v 1970. letih in zavzemanje ambasad v 1980. letih sta le dva primera. Če natančno preučimo korake, ki jih morajo izpeljati teroristi za izvedbo svojih dejanj, in potem s posredovanjem naredimo ta dejanja bolj tvegana, ter če zavarujemo tarče, ki so najbolj privlačne, lahko občutno zmanjšamo uspeh teroristov.
8. **Mit: Vojno proti terorizmu je mogoče dobiti.** Čeprav lahko teroriste oviramo in zmanjšamo njihovo uspešnost, nikoli ne bomo dobili tako imenovane vojne proti terorizmu. Zmaga pomeni, da bi bil terorizem za vedno odstranjen s sveta. To je tako malo verjetno, kot zmagati v vojni s kriminaliteto.
9. **Mit: Če se lahko zgodi v Izraelu (Londonu, Madridu, Delhiju), se lahko zgodi tudi tukaj.** Domnevamo, da se oblika terorizma, ki je možna v Londonu in Delhiju (ali kjerkoli drugje prek morja), lahko ponovno uprizori v ZDA. Vsak oblika terorizma je odvisna od priložnosti, ki jih nudi določeno okolje. To okolje je v različnih državah le redko enako. Rutinske samomorilske bombne napade, ki jih Palestinci izvajajo pro-

ti Izraelu, omogoča stalen dotok prostovoljnih bombnih napadalcev in majhnost ter bližina teh dveh držav. Takih pogojev v ZDA ni.

10. **Mit: Pripraviti se moramo na jedrski napad.** Večina strokovnjakov se strinja, da je verjetnost, da nas bodo teroristi napadli z jedrskim orožjem, majhna. Logistika izdelave, nakupa ali kraje jedrske bombe in potem njene dostave, je preveč zahtevna. Po drugi strani se večina strokovnjakov strinja, da bi lahko teroristi v vsakem našem velikem mestu brez težav podtaknili bombo v ročnem kovčku (naprave za radiološko razprševanje). Ni verjetno, da bi to povzročilo množične žrtve, kljub temu bi bila posledica takega dogodka splošna panika.
11. **Mit: Boj proti terorizmu je naloga agentov FBI**. Ne glede na to, kako učinkovita sta, FBI in CIA ne moreta sama poraziti terorizma. temveč morata združiti podporo javnosti, zasebnega sektorja in predvsem lokalnih in državnih policijskih agencij. Kot ta priročnik kaže, igrajo lokalne policijske agencije ključno vlogo v zbiranju obveščevalnih podatkov o teroristih, pri pomoči zaščite ranljivih tarč in pri odzivu na napad.
12. **Mit: Izmenjava informacij je ključ do zmage nad terorizmom.** Poročilo o 11. septembru je jasno pokazalo napake zvezne obveščevalne agencije pri usklajevanju operacij. Od takrat je bilo veliko storjenega za izboljšanje komunikacije med FBI in CIA ter za izboljšanje izmenjave podatkov med lokalnimi, državnimi in zveznimi agencijami. Ne glede na to, koliko izboljšamo zbiranje in obdelovanje obveščevalnih podatkov, se ne smemo vedno zanašati samo na obveščevalne podatke. Zmanjšati moramo tudi možnosti za terorizem z zaščito najbolj ranljivih tarč in z nadzorom orodja in orožja, ki ga teroristi navadno uporabljajo.

Napotek 07: Prepoznajte omejitve pristopa »Odstranite jih!«

Poznavalci kazenskega prava so kritični do ideje, da lahko premagamo in zmanjšamo kriminaliteto z aretacijami kršiteljev, z zapiranjem najhujših med njimi. Naštetih je nekaj razlogov, zakaj poznavalci verjamemo, da je ta politika neustrezna.

- Kljub velikim naporom policije se le majhen delež kaznivih dejanj zaključi z aretacijo in kaznovanjem. Poleg tega ni znano, kako povečati ta delež. Skrajne represivne ukrepe in večje število patrulj se lahko vzdržuje le kratko obdobje in v vsakem primeru je rezultat le peščica aretacij. Detektivsko delo je tako zamudno, da se uporablja le v najbolj resnih primerih. Tudi hitrejši odzivni čas policiji ne pomaga dosti, saj hudodelci pogosto veliko prej zbežijo, preden prizadeti pokličejo policijo.
- V desetletjih kriminalističnega raziskovanja nismo uspeli ugotoviti povezave med strogimi kaznimi in zmanjšanjem obsega kriminalitete. Statistični podatki ne dokazujejo, da smrtna kazen odvrne od umora. Ker večina kršiteljev ne verjame, da jih bodo ujeli, strogih kazni ne jemljejo resno; drugi se ne zmenijo, če jih ulovijo, ker storijo kazniva dejanja v stanju opitosti ali v afektu.
- Visoka stopnja zapornih kazni ne zagotavlja nižje stopnje kriminalitete. Stopnja zapornih kazni v ZDA je na primer veliko večja kakor v številnih drugih zahodnih državah, vendar pa na splošno stopnja kriminalitete ni nič nižja; dejansko je stopnja nasilnih zločinov v ZDA veliko višja.
- Nabora prestopnikov ni nikoli konec. V vsaki generaciji mladih jih bo 5 do 10 odstotkov postalo rednih kršiteljev zakona; torej, ne glede na to, koliko prestopnikov aretiramo in spravimo v zapor, bodo drugi takoj zasedli njihova mesta.
- Visoka stopnja zapornih kazni ima visoke ekonomske in socialne stroške tako za celotno družbo kot tudi za zapornike in njihove družine.

Nekateri od teh razlogov pojasnjujejo, zakaj se ne moremo zanašati na odstranitev teroristov – t.j., da jih identificiramo in ulovimo ali pokončamo. Ujeti teroriste ni lahko. Bolj kot običajni kriminalci se potrudijo skriti svoje delovanje, zato je njihova izsledite v včasih vodila v uporabo vprašljivih postopkov. Tudi kadar poznamo njihove identitete, jih ne moremo vedno ujeti. Tako je še posebej takrat, kadar delujejo prek morja, v državah, ki

podpirajo njihove cilje: doslej je bilo dosti naporov, da bi našli Osamo Bin Ladna, neplodnih. Tisti, ki so pripravljeni umreti za svoja prepričanja, jih strah pred smrtjo ali kaznijo verjetno ne bo odvrnil od dejanj. Iz varnostnih razlogov se jim ne more soditi v okviru javne razprave in tudi, ko se jih obsodi, so težavni zaporniki. Pravzaprav je verjetno najvišji strošek zapiranja teroristov, da se njihovi somišljeniki čutijo poklicane načrtovati nove zločine, da bi izsilili njihovo izpustitev.

Ubijanje teroristov prinaša velike stroške. Ustvarja še več zagrenjenosti med že tako sovražnim prebivalstvom, s čimer se konflikt, ki je temelj terorističnih dejanj, še težje razrešuje. Upravičuje uporabo nasilja in podpira mnenje, da se borijo proti neusmiljenemu sovražniku. Iz teroristov naredi mučenike in vplivne simbole za novačenje med dovzetnimi mladimi moškimi, ki jih želijo teroristi pritegniti.

To ne pomeni, da ne smemo kaznovati teroristov, ko jih ulovimo. Za svoja dejanja si zaslužijo kazen in prav je, da jih lovimo. Nekateri bi lahko trdili, da je tudi prav, da odstranimo teroristične voditelje, posebno karizmatične posameznike, ki imajo precejšen vpliv na svoje privržence in so težko nadomestljivi. Uboj teh voditeljev bi lahko učinkovito obglavil organizacijo in pustil telo, da oveni, s čimer bi rešili življenja številnih nedolžnih ljudi.

Ne smemo dovoliti, da pristop »Odstranite jih!« obvlada naš odziv na terorizem. **Zapiranje ali celo ubijanje teroristov ne bo izkoreninilo terorizma, tako kot stroge kazni ne ustavijo kriminalitete.** Kot narod moramo pristopiti k terorizmu z več plati. Truditi se moramo za diplomatske in vojaške rešitve. Poskušati moramo izboljšati gospodarske in izobraževalne možnosti za pripadnike tujcev, tako tistih, ki bi lahko postali nezadovoljni in sovražni, kot tudi tistih, ki so v nevarnosti, da jih bodo posrkale teroristične organizacije. Delati moramo na preprečevanju terorističnih napadov z utrjevanjem tarč in nadzorom orodja in orožja, ki ga uporabljajo. In ko napadejo, se moramo odzvati hitro in učinkovito, da bi zmanjšali število smrtnih žrtev in gmotno škodo kot posledice napada.

Toda, kaj vse to pomeni za vas? Kako vam lahko to znanje pomaga zavarovati skupnost pred terorizmom? Jasno je, da kot lokalni upravitelj policije ne morete vplivati na oblikovanje zunanje politike tako pri razporejanju tuje pomoči kot tudi pri začetku diplomatskih ali vojaških akcij. Toda tudi vi morate slediti večstranskemu načrtu. V vašem primeru naj bi načrt vse-

boval tri ključne elemente: (1) razvijanje lokalnih obveščevalnih informacij o možnih terorističnih dejavnostih; (2) utrjevanje najbolj ranljivih tarč v vašem območju; in (3) razvijanje učinkovitih odzivnih in reševalnih postopkov. Poskusiti morate vzdrževati primerno ravnotežje med temi tremi elementi. Še posebej se ne zanašajte preveč na moč obveščevalnih podatkov pri zaščiti pred terorizmom. To je le del tistega, kar morate narediti za zaščito svoje skupnosti. Lahko se vam oprosti, da niste odkrili terorističnega načrta, vendar pa ni opravičila, če vam ne uspe zavarovati ključnih tarč ali se nerodno odzovete ob napadu.

Napotek 08: Poznati morate lokalne ranljive točke

Ena od najbolj frustrirajočih stvari glede teroristične grožnje je, da je nemogoče vedeti, kako resna je. Na srečo je terorizem redek; tako redek, da ste lahko prepričani o zelo majhni verjetnosti, da bo vaše mesto izbrano za napad. Glede na dogajanje v pretekli zgodovini imate skoraj gotovo prav. Res je, da imate morda tarče, ki bi lahko privabile teroriste – vodni zbiralnik, mestno dvorano, šole, avtobusno ali železniško postajo – vendar, kot kaže spodnja tabela, ima tovrstne tarče večina mest. Vprašajte se, ali je kakšen razlog za to, da bi teroriste bolj pritegnilo vaše mesto kot na stotine drugih podobnih mest. Ker so teroristični napadi tako redki, vam raziskave ne morejo odgovoriti na to vprašanje. Za druga kazniva dejanja je mogoče analizirati vzorec pojavljanja in identificirati dejavnike tveganja, vendar pa to ni mogoče pri terorizmu, vsaj v ZDA ne.

Na osnovi povedanega je mogoče izpeljati nekatere logične zaključke o tem, zakaj je neko mesto izpostavljeno tveganju napada. Treba je analizirati dve ključni točki: prvič, cilje terorizma (povzročitev žrtev, ustvarjanje strahu in pritegnitev pozornost medijev); drugič, logične težave, s katerimi se soočajo teroristi pri pripravi napada (na primer, pridobitev ustreznega orožja, pridobitev dostopa do tarče in težave pri izvedbi napada čez morje). Mesto je v večji nevarnosti napada, kadar: (1) je znamenito – ker teroristi želijo pritegniti čim večjo pozornost; (2) je pomembno – ker teroristi želijo škoditi državi; (3) je dostopno – ker teroristi želijo zmanjšati tveganje in napor; (4) v njem živi veliko priseljencev – ker z vključenjem v priseljensko skupnost tuji teroristi lažje delujejo; in (5) gre za domači terorizem (glej Napotek 11), je v njem raziskovalna univerza ali institucija, ki zadržuje laboratorijske živali, ali trgovske ustanove, ki jih ekoteroristi zaznavajo kot škodljive za okolje. To pomeni, da se bo nevarnosti napada za vaše mesto povečala, če je:

- zgodovinsko
- turistični center
- glavno mesto zvezne države
- veliko, z veliko prebivalci
- znano po kakšnem ikonskem proizvodu
- v bližini večjega vojaškega oporišče
- center zveznih služb
- finančni, trgovinski ali proizvodni center

- v bližini vhodnega pristanišča v ZDA
- v bližini mednarodnega letališča
- cilj nedavnih priseljevanj (posebno islamskih)
- sedež živalskih raziskovalnih laboratorijev, kjer delajo poskuse na živalih
- osrednji sedež naftnih rafinerij, kogeneratorski obrati ali jedrski objekti
- večji komunikacijski in računalniški center
- transportni center.

Tudi to spoznanje ne pove veliko, ker tudi če je vaše mesto v večji nevarnosti kakor druga, je dejansko tveganje napada še vedno zelo majhno. Vendar pa zaradi pretresljivih posledic morebitne pomote ne morete tvegati, da ga bodo teroristi spregledali. Skušnjavi, da bi prezrli še tako majhno tveganje, mestne oblasti in skupnost ne bodo podlegle. Če nič drugega, jih boste težko prepričali, da je tveganje resnično majhno. Kaj lahko naredite, da se zavarujete pred izgubo časa, volje in sredstev pri poskusu preprečevanja zelo malo verjetnega dogodka? Predlagava naslednje:

- Majhno verjetnost napada postavite na stran in se osredotočite na pretresljive posledice.
- Osredotočenost na posledice vam bo pomagala pri soočenju s ciniki in skeptiki, ki trdijo, da je preprečevanje izguba časa – da teroristi ne bodo nikoli napadli vašega mesta, da jih ne morete ustaviti, če se oni tako odločijo, in da nihče ne bo nikoli vedel, ali so vaši varnostni ukrepi zmanjšali tveganje.
- Vložite čim več časa, volje in sredstev v preprečevalna dejanja (vključno z izboljšanjem obveščevalnih podatkov), pri čemer morate biti še vedno sposobni izpolonjevati osrednje policijske dolžnosti.
- Prizadevajte si izboljšati osnovno varnost na vseh ogroženih objektih.
- Mestne oblasti, podjetja in vodje skupnosti prosite, da razvrstijo tarče, za katere menijo, da so bolj ogrožene, po pomenu. Kot podporo temu procesu uporabite IVIL UZBL (angl. EVIL DONE) in KDORUP (angl. CARVER) (glej napoteka 28 in 29). Ti akronimi zajemajo značilnosti, zaradi katerih so zgradbe in objekti v nevarnost, da bodo napadene. Obstaja nekaj prekrivanj med temi značilnostmi in tistimi, zaradi katerih je vaše mesto v nevarnosti; na primer, za teroriste je pomembno, da so tako stavbe in mesta, ki jih izberejo, pomembna in znamenita – nekatere druge značilnosti pa se nanašajo samo na zgradbe.

- Predvidevajte, kako bi se napad najverjetneje zgodil. Na okoliščine poglejte z zornega kota terorista: razmislite, kako bi lahko izpeljali tak napad in katere pomanjkljivosti bi lahko izrabili.
- Začenši z objekti na vrhu seznama, razmislite o seriji ukrepov, ki presegajo izboljšanje osnovne varnosti, in razvijte načrt uporabe teh ukrepov. To vključuje aktivno iskanje novih sredstev pri podjetjih, državi in zveznih virih.
- Predstavljajte si svojo nočno moro: kakšne vrste napada se najbolj bojite? S tem misliva specifične vrste napada na določen objekt v vašem okolju. Lahko je to tolpa teroristov, oboroženih z avtomatičnim orožjem, ki napade osnovno šolo; bomba v parku v središču mesta; tovornjak bomba, ki se zaleti v lokalno kemično tovarno. Kakršenkoli je že ta napad, se morate s problemom soočiti ob hladni dnevni svetlobi in ne po tem, ko se že zgodi in je morala na najnižji točki. Morda boste ugotovili, da je tak napad tako malo verjeten, da lahko tako možnost prezrete, ali pa boste odkrili resnične pomanjkljivosti, glede katerih lahko kaj naredite. S potrebnim ukrepanjem se boste vsaj lahko tolažili, da ste naredili vse, kar je bilo v vaši moči za zaščito skupnosti.
- Po soočenju z vašo osebno nočno moro namenite enako pozornost naslednjemu najhujšemu scenariju in se z njim spoprimite na enak način in tako naprej.

Preberite več o tem:

Verjetno ima vsaka policijska jurisdikcija enega ali več ogroženih objektov. Kako jih prepoznati in odstraniti pomanjkljivosti, lahko izveste v problemsko naravnanem vodiču za policijo COPS urada (angl. Office of Community Oriented Policing Service), Problem-Solving Tools Series No. 6: Understanding Risky Facilities, by Ronald V. Clarke and John E. Eck, 2007.

http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=410

»Katere vrste objektov naj bi zavarovali v vašem mestu ali v njegovi bližini?«

(Odgovori 725-ih mest, pridobljeni z raziskavo po elektronski pošti, september 2002)

	V mestu (procent)	V okolici (procent)
Oskrba z vodo	39	82
Vladni objekti	25	77
Šole	26	66
Prevozni sistem	33	66
Bolnišnice	35	62
IT infrastruktura	27	61
Stadioni/prizorišča	28	31
Pristanišča	37	29
Druge velike zgradbe	22	28
Elektrarne	38	26
Druge zvezne zgradbe	31	21
Vojska	29	17
Mednarodna meja	8	5

Vir: Hoene, Christopher, Mark Baldassare, in Christiana Brennan, Homeland Security and America's Cities, Research Brief on America's Cities, Issue 2002-2. Washington, D.C.: National League of Cities, 2000.

II.

Razumite grožnjo

NAPOTEK 09: **Na terorizem glejte kot na kriminaliteto**

Jasno je, da se policijske postaje spoprijemajo s kriminaliteto vsak dan; odvisno od obsega in vrste okoliša, izkusijo celotno paleto hudodelstev, od umorov do nepomembne tatvine in prekrškov. Ker je terorizem v primerjavi z drugim kriminalom redek pojav, bi lahko pričakovali, da bo povprečna postaja vzpostavila popolnoma nov pristop v boju proti kriminaliteti, da bi se lahko spoprijeli z njim. Pa je to res?

Teroristi so tudi hudodelci. Veliko terorističnih skupin izvaja običajna kazniva dejanja, kot so bančni ropi, trgovanje z mamili, tatvine identitete in pranje denarja, da bi s tem podpirale svoje teroristične aktivnosti. Poleg tega se vedenje, ki vključuje terorizem – celo samomorilski terorizem – le malo razlikuje od vedenja običajnih storilcev kaznivih dejanj.

»Številni teroristi, posebej tujci, ki so v Združenih državah ilegalno, morajo živeti življenje ubežnika – kar pomeni, da morajo izvrševati kazniva dejanja, ne le zato, da izpeljejo napad, temveč preprosto zato, da se vzdržujejo. Vzdržujejo se z ilegalnimi dokumenti, z vlamljanjem in ropanjem, razpečevanjem mamil, sleparstvom in tako naprej. Z drugimi besedami, niso vsi ilegalni priseljenci ali ubežniki tudi teroristi, vendar številni teroristi morajo za preživetje v ZDA živeti podtalno, kot ilegalni priseljenci in ubežniki.«

Vir: Kelling, George L. and William K. Bratton, Policing Terrorism, Civic Bulletin 43. New York: Manhattan Institute for Policy Research, September 2006.

Terorizem je zločin s političnimi motivi. Kaj mora terorist narediti drugače kot običajni storilec kaznivega dejanja, da bi uspešno izpeljal svoj

namen? Preučite naslednji primer, ki primerja samomorilskega bombnega napadalca in serijskega morilca.

1. **Vedenje terorista:** Samomorilski bombni napadalec mora narediti več korakov, da izpelje svojo nalogo. Pridobiti mora eksplozivni pas, ki ga lahko skrije na sebi; izbrati mora tarčo; ugotoviti mora, kako doseči tarčo, ne da bi ga ujeli; in imeti mora rezervni načrt v primeru, da ga ulovijo preden doseže svojo tarčo ali preden uspe detonirati bombo.
2. **Vedenje serijskega morilca:** Serijski morilec mora narediti več korakov, da ubije svojo žrtev. Izbrati mora tarčo in ugotoviti najboljši način za dostop do nje ter izvesti umor ne da bi ga ujeli; odločiti se mora, s kakšno metodo bo moril; odločiti se mora, kako se bo znebil trupla; in načrtovati mora pot pobega.

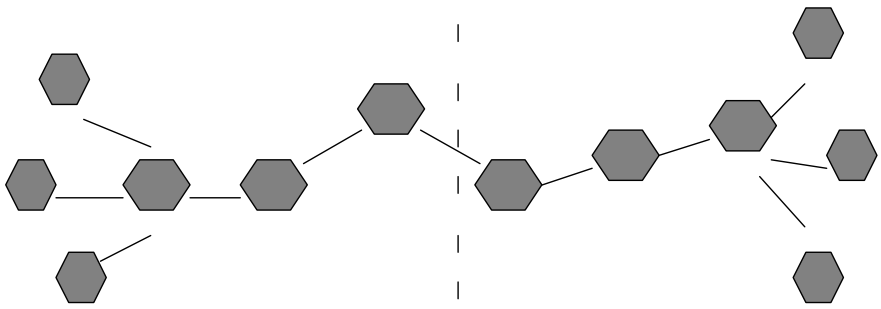
Skupni element teh dveh primerov je logično zaporedje korakov, ki jih morata narediti oba, terorist in serijski morilec, da bi uspešno izpeljala svojo nalogo.

Priložnost dela terorista. Specifične priložnosti in okoliščine vsakega kaznivega ali terorističnega dejanje so odvisne od specifičnih zahtev zločina. Na primer, če je strelno orožje na voljo, bo storilec morda izbral pištolo kot sredstvo za izpeljavo zločina (npr. roparski napad na trgovino z alkoholnimi pijačami); to lahko spremeni njegovo oceno o priložnostih in tarčah. Podobno bi terorist raje podtaknil bombo v avto ali avtobus, kot da bi izpeljal samomorilski bombni napad, kadar je na voljo veliko eksploziva, vendar nobenega eksplozivnega telovnika. V vsakem primeru so načrti napada, bodisi kriminalni ali teroristični, odvisni od možnosti.

Je kriminaliteta in potem je kriminaliteta. Čeprav splošna kategorija kriminalitete obsega širok razpon dejavnosti, večino storilcev vodi isti logični vzgib: želja po tem, da bi izpeljali dejanje, ne da bi jih pri tem prijeli. Kljub temu vsaka posebna priložnost za hudodelstvo ustvari popolnoma drugačen niz izbir in dejavnosti; in sicer, zaporedje dejavnosti, ki jih je treba izpeljati za vlom v neko bivališče v predmestni soseski, je čisto drugačno od tistega, ki ga zahteva vlom v visok stanovanjski kompleks. Dejansko **je razlika med izvedbami različnih vrst običajnega kriminala lahko velika in nemara celo večja, kot je domnevna razlika med kriminaliteto in terorizmom.**

Stvar skupine? Nekateri trdijo, da je bistvena razlika med kaznivim dejanjem in terorizmom ta, da teroristično dejanje vedno izpelje organizirana skupina. Številne, morda celo večina knjig o protiterorizmu poudarja organizacijske strukture in razsežnosti terorističnih skupin. Čeprav ne povsem uspešno, se policijske postaje že desetletja spoprijemajo z organizirano kriminaliteto številnih oblik. Nedavne raziskave o skupinah organiziranega kriminala so pokazale, da na splošno kriminalne organizacije niso enotne, kakor se je prej domnevalo (glej okvir), temveč da nastanejo in se razidejo glede na priložnosti in okoliščine. Raziskave so podobno pokazale, da večina terorističnih skupin razpade v dveh letih. V tem smislu so izpostavljene organizacijske razlike med drugo kriminaliteto in terorizmom nedosledne, čeprav so izzivi, s katerimi se sooča policija na lokalni ravni pri spoprijemanju z organiziranim kriminalom, precejšnji.

Na kratko, če na terorizem gledate kot na eno od oblik kriminalitete in ga analizirate v skladu s tem, je največja ovira pri reševanju problema odstranjena. Tako kot veliko različnih vrst kriminala zahteva različne prilagojene odzive, enako velja za terorizem.



Na lokalni ravni so teroristične mreže precej podobne organiziranim kriminalnim mrežam, posebej tistim, ki delujejo prek meje. Verižna mreža, upodobljena zgoraj, je običajna pri kriminalističnih organizacijah (vključno s terorističnimi skupinami), ki prenašajo nezakonite proizvode (pištole, mamila, ilegalne priseljence, denar) od vira do porabnika. Vsak akter v verigi ima dve funkciji: kupuje od predhodnih akterjev in prodaja naslednjemu. Jasna točka intervencije je meja; ali je

to najbolj učinkovita točka posega, je odvisno od različnih elementov, vključno z zveznimi, državnimi in lokalnimi zakoni ter odnosom med lokalno policijo in mejnimi agenti. Končna točka, na kateri potekajo dogovori med prodajalci in odjemalci, je morda bolj učinkovita točka intervencije za lokalno policijo. Identifikacija orodij in pogojev, ki lajšajo tako dejavnost, je v vsakem primeru lahko pomemben prvi korak pri varovanju lokalne skupnosti pred terorističnimi napadi in organiziranim kriminalom.

Napotek 10: Terorizem ima veliko oblik

Kriminaliteta je prikladen konstrukt za medije in laike v vsakdanjih pogovorih, vendar ima omejeno uporabnost v vsaki resni razpravi o zmanjšanju obsega kriminala, ker ta vključuje številne vrste dejanj, ki jih zagreši obsežna množica storilcev, od katerih vsak obvlada zelo različne veščine in ima za svoje dejanje različne razloge. Ko poskušamo identificirati učinkovite ukrepe omejevanja kriminalitete, je bistveno, da se osredotočimo na posamezne oblike kaznivih dejanj, bodisi na bančni rop, posilstvo, razpečevanje mamil, izsiljevanje, vlom, požig ali tatvino identitete. Čeprav številna različna dejanja, ki jih vključuje svetovni terorizem, niso tako raznolika kot tista, ki jih vključuje svetovna kriminaliteta, velja isto načelo: v okviru razmišljanja o tem, kako se braniti pred terorizmom, morate upoštevati tako njegove številne oblike kakor tudi, za katere vrste napada ste najbolj ranljivi – ker ukrepi, ki bi preprečili eno obliko napada, morda ne bodo preprečili druge. Čeprav smo nagnjeni k razmišljanju o terorističnih dejanjih kot razsežnih, spektakularnih dogodkih, je veliko tudi običajnih kaznivih dejanj, kot sta ugrabitev ali umor. Tu je kratek seznam različnih oblik terorizma:

- avto ali tovornjak bomba,
- samomorilski bombni napadi,
- zaletavanje v objekte (tovornjak, letalo, ladja),
- improvizirane eksplozivne naprave (angl. Improvised explosive devices – IED) in druge podtaknjene bombe,
- pisemske bombe/antraks,
- umazane bombe (naprava za radiološko razprševanje),
- kemični/nuklearni/biološki napadi,
- atentati,
- ostrostrelski napadi,
- zasede,
- streljanje iz mimo vozečega vozila,
- zavzetje talcev,
- ugrabitve,
- ugrabitve letal,
- ugrabitve vlakov,
- ugrabitve ladij in
- raketni napadi in napadi z izstrelki.

Katero dejanje bodo izbrali teroristi? Vrsta napada, ki jo izbere tako imenovani terorist, je odvisna od pričakovanih koristi dejanja kot tudi od priložnosti za uspešno izvedbo napada. Okvir 1 navaja te možne koristi. Vsako teroristično dejanje ne prinese vseh koristi. Na primer, ugrabitev letala se lahko konča z zajetjem talcem, ki jih lahko teroristi zamenjajo za vladne koncesije. Po drugi strani, čeprav razstrelitev letala z bombo lahko ubije veliko ljudi in zbudi velik strah, ne dopušča veliko prostora za pogajanja.

Okvir 1. Cilji teroristov.

Teroristi želijo s svojim delovanjem doseči tako dolgoročne kot tudi kratkoročne cilje. Vseeno pa imajo teroristi veliko težav z neposrednim povezovanjem tistega, kar morajo narediti za uspešno izvedbo operacije, z dolgoročnimi cilji, kot je strmoglavljenje neke oblasti. Razumevanje teh dolgoročnih ciljev nam na splošno daje le malo smernic glede tega, katere tarče bodo izbrali. Izjema od tega pravila so enoproblemski teroristi. Spodaj je seznam možnih dolgoročnih in kratkoročnih koristi od terorističnih dejanj.

- Povzročiti čim večjo škodo in čim več smrtnih žrtev.
- Ustvariti vzdušje strahu.
- Ustvariti medijsko senzacijo.
- Razrvati vsakodnevno življenje.
- Prekiniti specifično dejavnost (npr. rekrutiranje policijskih kadetov).
- Prekiniti trgovino in industrijo.
- Demoralizirati varnostne sile.
- Izsiliti koncesije (npr. izpustitev zapornikov, odpoklic čet, spremembo politike).
- Uničiti ideološkega nasprotnika ali žaljivo ikono.
- Ponižati uradnike in oblasti.
- Izsiliti skrajni vladni povračilni ukrep.
- Pretirano povečati zaznavo terorističnе grožnje, tako da razmeroma majhna teroristična skupina uveljavlja velik vpliv.
- Ustvariti občutek o neki nadvse prodorni sili: »notranji sovražnik«.
- Razkazovati se somišljenikom in s tem utrditi teroristično skupino.
- Prestrašiti politične tekmece ali teroristične frakcije.

- Vzdrževati disciplino znotraj skupine.
- Testirati ali »okrvaviti« nove rekrute; zasledovalci vlakov (train followers).
- Prestrašiti prebivalstvo.
- Izrabiti ugotovljene šibkosti demokracije (t.j. pravna država, svoboda govora, zakoni proti mučenju in pripor).
- Zlomiti sovražnikovo voljo.

Preberite več o dolgoročnih in kratkoročnih ciljih:

Headquarters, Department of the Army. Field Manual 7-98, "Operations in Low-Intensity Conflict," Section 3.6, Combating Terrorism. Washington, D.C.: U.S. Government Printing Office, October 1993.

Torej, glede na ostale elemente – razpoložljivost orožja, dostopnost tarče itd. – se lahko zdi teroristični skupini detonacija tempirane obcestne bombe bolj učinkovita kot samomorilska detonacija v restavraciji. V tistem trenutku, ko sta tarči različni, so koristi vsakega od vsake drugačne. Vsako od teh dveh dejanj zahteva tudi drugačen niz odločitev in drugačen niz dejanj. Enoproblemsko usmerjeni teroristi bodo izbrali tarče, ki so neposredno povezane z njihovo zadevo. Vendar morajo tudi v tem primeru še vedno izbirati med različnimi opcijami. Kateri laboratorij z živalmi? Katero univerzo? Katero mesto? (Glej okvir 2 za primerjavo verjetnih koristi za teroriste v primeru dveh razvpitih napadov).

Posamezni in večkratni napadi. Kompleksnost in težavnost terorističnega napada določa, kako pogosto se lahko izvede določena vrsta napada. Največja težava je oddaljenost od tarče. Če je tarča daleč od domačega oporišča teroristov (npr. Svetovni trgovinski center je bil v Združenih državah, Al Kaida pa v Afganistanu), je podpora večkratnim napadom posebno težka. Če pa je tarča bližje domu, kot v primeru irske republikanske armade (IRA) na Severnem Irskem, potem se lahko uporabi večkratne napade podobne vrste in ti lahko celo postanejo rutina. Zato je pomembno razlikovati med rutinskim terorizmom in enkratnimi napadi. Rutinski terorizem se v Združenih državah ni prijel. Trije večji teroristični napadi v nedavni preteklosti – napada na Svetovni trgovinski center leta 1996 in leta 2001 ter bombni napad na zvezno zgradbo Alfreda P. Murraha v Oklahomi City, Oklahoma leta 1995 – so bili enkratni napadi. Eden je bil

domač; druga dva na Svetovni trgovinski center so organizirali tuji teroristi (Al Kaida), ki so izrabili domače okoliščine za lažjo izvedbo obeh napadov (t.j., priseljenske skupnosti so zagotovile krinko za tuje operativce).

Okvir 2. Koristi teroristov od napadov na Svetovni trgovinski center in USS Cole (rušilec ZDA).

	Napad na Svetovni trgovinski center (New York City, 11. september 2001)		Napad na USS Cole (Port of Aden, Jemen, 12. October, 2000)	
Cilj	Rezultat*	Premislek	Rezultat*	Premislek
Uniči in ubij	10	Tarča je popolnoma uničena; po podatkih je bilo ubitih približno 2.750 ljudi.	3	Obsežno uničenje ladje, ki pa se ni potopila. Dvanajst vojakov je bilo ubitih.
Strah	9	Strah je s časom upadel.	3	Državljani Združenih držav niso bili neposredno prizadeti, ker se je dejanje zgodilo na oddaljeni lokaciji.
Ustvari medijsko senzacijo	10	Ne potrebuje komentarja.	4	Dogodek je bil obsežno medijsko pokrit, zaradi izgube življenj in inovativne metode napada.
Razrvati vsakdanje življenje	9	Takojšnji pretres v New York Cityu, vendar so se varnostni ukrepi zdaj že spojili z vsakdanjim življenjem.	1	Pretres je bil omejen na USS Cole, mornarico Združenih držav in diplomatsko in vladno osebje.
Prekiniti trgovanje	9	Drastičen vpliv z nekaterimi dolgoročnimi učinki.	1	Dogodek je bil omejen na operacije mornarice in vojske.
Izsiliti privolitev oblasti v svoje zahteve	1	Ni bilo nobenih zahtev, a Al Kaida je dosledno zahtevala umik Združenih držav iz bližnjevzhodne regije.	1	Varnost je bila izboljšana; Združene države se niso umaknile iz pristanišča.

Izsiliti pretiran odziv oblasti	9	Združene države so sprejele doktrino vojne preden se grožnja materializira. (angl. Preemptive war)	1	Nobene silne reakcije oblasti, ki bi dala teroristom zadoščenje.
Izkoristiti šibkosti demokracije	9	Invazija na Irak je vodila v silovito politično nestrinjanje doma in med zavezniki.	1	Ljudi je spodbudilo k podpori družinam in vojski.
Nadvse prodorna sila	9	Nenehna skrb glede spečih celic v Združenih državah.	4	Dogodek je bil omejen na vojaško tarčo v tujih vodah, čeprav so bile vključene speče celice.
Ponižanje	10	Oblast Združenih držav se je izkazala za ranljivo v odnosu do peščice tujih operativcev.	3	Čeprav so bila izgubljena življenja, je bilo videti, da je mornariško osebje ravnalo pogumno.
*10=najvišji rezultat, 1=najnižji rezultat				

Vir: Clarke, Ronald V. and Graeme R. Newman, Outsmarting the Terrorists. Westport, Connecticut: Praeger Security International, 2006.

Napotek 11: Ne tratite časa z razlago razlogov za terorizem

Trdimo, da je terorizem kriminaliteta s političnimi razlogi. Obstajajo seveda izjeme od te definicije; na primer, nekoga, ki je prekršil volilni zakon iz političnih razlogov, ne bi šteli za terorista. Drugi trdijo, da teroriste žene verski fanatizem, čeprav je tudi v tem primeru najbolj pomemben razlog politični, ker je temeljni cilj strmoglavljenje posvetne oblasti. V vsakem primeru je najino stališče, da je bolj produktivno razmišljati o terorizmu kot kriminaliteti kot razmišljati o njem kot o dejanjih s popolnoma drugačno iniciativo, ki jo žene fanatična ali skrajna ideologija – tudi če je slednje res, lahko glede tega naredite le malo, medtem ko če razmišljate o terorizmu kot kriminalu, so vam lahko policijske izkušnje uporabno vodilo pri spoprijemanju s terorističnimi dejanji.

Temeljni vzroki terorizma. Za preprečitev tistega, kar želijo hudodelci narediti, razumevanje globoko zakoreninjenih vzrokov ni posebej pomembno. To je zato, ker so tovrstne analize vedno oddaljene od delovanja kršiteljev v resničnem času, ko izvajajo svoja dejanja. Po predolgotrajni raziskavi, na primer, lahko ugotovimo, da je storilca gnalo v serijska posilstva očetovo zlorabljanje v otroštvu. Toda, kakšne preprečevalne ukrepe lahko policija uporabi na podlagi tega odkritja? Preteklosti ne moremo spremeniti; prav tako ne moremo spremeniti družinskega življenja, tako da starši ne bodo več zlorabljali svojih otrok. Najbolj razširjen vzrok, ki ga pripisujemo današnjemu terorizmu, je gospodarsko in politično zatiranje. Ta vzrok ni dokazan, vendar, tudi če bi bil resničen, kakšen pomen ima to za vodjo policije v majhnem mestu, ki se poskuša odločiti, kaj naj naredi tukaj in zdaj?

Motivacija in ideološka predanost. Zelo razširjeno je mnenje, da so teroristi veliko bolj predani svoji nalogi kot običajni storilci kaznivih dejanj. Cilj teroristov dojemamo kot višji od tistih, ki ženejo običajne storilce kaznivih dejanj – terorista žene verski ali politični ideal, medtem ko hudodelca žene zgolj pohlep. Kdo lahko sodi, kateri cilj je več vreden? Poznavanje motivacije teroristov in drugih hudodelcev nam ne pove, kako predani so. Ne zamenjajte predanosti z motiviranostjo.

Zdi se, da je samomorilski bombni napadalec veliko bolj predan svoji nalogi kot bančni ropar, vendar pa raziskave o samomorilskih bombnih napadalcih ne potrjujejo te domneve. Dejansko postanejo ljudje samomorilski bombni napadalci prej iz številnih drugih razlogov kot zaradi verske gorečnosti, npr.

zaradi denarja za njihove družine in javnega odobravanja, če omenimo le dva. Poleg tega, ker mora samomorilski bombni napadalec za uspešno dokončanje svoje naloge umreti, je stopnja njegove predanosti idealu sporna: ima le eno možnost za uspeh. Po drugi strani pa imajo bančni roparji številne priložnosti – vsaj dokler jih ne ulovijo. Tako bi lahko nekdo zaključil, da so vztrajni bančni roparji bolj predani kot samomorilski bombni napadalci. Skratka, kakršnakoli je temeljna motivacija, tako terorist kot tudi storilec katerega koli kaznivega dejanja želita uspešno dokončati svoja dejanja. Brez take predanosti terorist ne bi dorasel nalogi – in enako velja za bančnega roparja.

Ideologije in izbira tarč. Če bi preučevali teroristične ideologije, bi dobili kakšen namig o tem, kdaj in kje bodo udarili? Vemo, da na primer v Palestini samomorilski bombni napadalci redko napadejo verske tarče. Raje imajo polno zasedene restavracije, avtobuse in trgovine. Njihove tarče so operativno usmerjene; to pomeni, da želijo ubiti čim več ljudi na krajih, s katerimi so dobro seznanjeni. Čeprav teroristične skupine dejansko žene politični ali verski fanatizem, ko pride do izbiranja posebne tarče ali orožja, ideologijo pogosto nadvlada operativni dejavnik. Zato teroristi 11. septembra niso izbrali Bele hiše (premajhna tarča), kljub temu, da je Osama Bin Laden to želel. Torej, kjer primanjkuje sredstev, poraba delovne sile za študije o zapletenosti teroristične ideologije jemlje sredstva temu, kar je zares pomembno: ocenjevanju operativnih dejavnikov, ki vplivajo na uspešno dokončanje vsake teroristične naloge, in načrtovanju načinov oviranja vsakega koraka terorističnega napada. Kot bomo videli v nadaljnjih korakih, se to lahko naredi brez poglobljenega razumevanja fanatičnih ali skrajnih nazorov teroristov.

Širša slika. Za teroristično dejanje se združuje veliko dejavnikov. Nekateri, kot sta gospodarsko ozadje in družinska vzgoja terorista, se zgodijo daleč od dejanskega terorističnega dejanja; drugi, kot so dostopnost tarče in orožja, se zgodijo blizu terorističnega dejanja. Številni dejavniki, ki pripomorejo k nastanku terorizma, so oddaljeni od točke, kjer se policija odloča o razvrščanju sredstev in delovne sile. Lokalna policija ne more upati, da se bo spoprijela s temi oddaljenimi vzroki, vendar pa z usmerjanjem na štiri stebre teroristične priložnosti – tarča, orožje, orodje in olajševalne okoliščine – ki vse dopuščajo posredovanje, policija lahko nadzoruje priložnosti za teroristično dejanje in načrtovanje. To pomeni, da je treba **na lokalnem nivoju odkriti priložnosti, ki jih lahko terorist izrabi, in tam tudi sprejeti ukrepe za zmanjšanje teh priložnosti.** Zato ste kot lokalni vodja policije pomemben akter pri spoprijemanju s terorizmom.

Napotek 12: Mislite kot terorist

Teroristi so običajni ljudje. Prvi korak k razumevanju razmišljenja terorista je spoznanje, da so teroristi ljudje z običajnimi potrebami in omejitvami. O svoji nalogi se odločajo enako, kot se mi odločamo o nalogah, ki jih izvršujemo vsak dan na delovnem mestu ali v domačem okolju. Teroristi se morajo odločiti glede tarče, kako jo bodo dosegli, katero orodje bodo uporabili in s katerim orožjem bodo opravili delo. V vsaki situaciji, za vsako posamezno teroristično dejanje so te odločitve izredno težke, ker okoliščine, ki prevladujejo na kraju in v času naloge, omogočajo tako priložnosti za uspeh kot postavljajo omejitve glede tega, kaj lahko terorist doseže.

Načrtovanje napada na Svetovni trgovinski center. Cilj prvega napada na Svetovni trgovinski center leta 1993 je bil razstrelitev ene stolpnice, ki bi se prevrnila na drugo. Za izvedbo te naloge je bilo treba narediti številne korake.

1. Nadzorovati notranjost in zunanjost zgradbe, da bi ocenili, koliko eksploziva bo potrebno.
2. Določiti najboljše mesto za detonacijo eksploziva.
3. Pridobiti potrebno količino eksploziva.
4. Pridobiti sredstvo za prevoz eksploziva (v tem primeru je to bil velik najet tovornjak).
5. Pridobiti potrebno tehnologijo in usposobljene ljudi za detonacijo eksploziva.
6. Izbrati in izučiti operativce za izvedbo naloge.
7. Načrtovati pot pobega.
8. Omogočiti dostop do zgradbe (skozi parkirno garažo) in nastaviti eksploziv na želeni lokaciji.

Čeprav je napad povzročil precejšnjo škodo in smrtne žrtve, je štel za neuspelega, ker ni popolnoma dosegel cilja: uničenja Dvojčkov. Pri načrtovanju drugega napada je bil izziv teroristom – očitno je bil v tem primeru načrtovalec Osama Bin Laden – odpraviti pomanjkljivosti prvega načrta. Dejanje je bilo izvedeno z uporabo komercialnih potniških letal kot vodenih izstrelkov, usmerjenih v tarče v slogu kamikaze. Teroristom je uspelo, ker so spremenili orožje, ne pa zato, ker bi spremenili tarčo.

Slaba obramba omogoča terorizem. Napad na Svetovni trgovinski center je omogočila slaba obramba. Prvi napad je izrabil slabo varnost v parkirni garaži pod Dvojčkoma, zato je imel tovornjak z bombo lahek dostop. Drugi uspešen napad je izkoristil površno letališko varnost, ki je bila osnovana na domnevi, da tisti, ki ugrabijo letalo, niso pripravljeni umreti.

Zakaj sta bila Dvojčka tarča? V igri sta bila vsaj dva elementa: prvi napad je uspel zaradi slabe varnosti; v drugem napadu sta izstopali lahki tarči. Kot bomo videli kasneje, obstajajo številne lastnosti, zaradi katerih je neka tarča bolj privlačna kot ostale.

Vsako teroristično dejanje poteka po načrtovanih stopnjah, podobnih tistim, ki smo jih že opisali, čeprav so dejanske odločitve teroristov povezane z določeno obliko terorizma. Spremljajoči okvir kaže, kako zapletena je lahko priprava preprostih samomorilskih bombnih napadov, kakršni se rutinsko dogajajo v Izraelu. In tudi ta primer je precej poenostavljen.

Iz zgornjih opažanj lahko potegnemo nekaj pomembnih zaključkov, ki vplivajo na odziv na grožnjo terorističnega napada na lokalnem nivoju.

- Teroristične tarče niso izbrane naključno. Tarnanje, da »ne moremo zaščititi vsega«, temelji na lažni domnevi, da teroristi izbirajo svoje tarče naključno. Res je, da ne moremo zavarovati vsega, vendar je tudi res, da nam vsega ni treba zaščititi. Teroristi se prav tako kot mi soočajo s težkimi odločitvami. Odločiti se morajo, katere tarče napasti, izbrati jih morajo na osnovi ocene uspešnosti napada, ki je utemeljena na dostopnosti orožja, orodja in na okoliščinah, ki jim bodo omogočile izpeljati nalogo. Poleg tega teroristi večinoma delujejo v sovražnem okolju, v katerem so preganjani, še posebej, če poskušajo pripraviti operacijo v tuji državi, daleč od domačega oporišča.
- Veliko je priložnosti, da se prepreči teroristom doseči tarče. Zaradi kompleksne logistike teroristične operacije – in še posebej njihove potrebe po orodju, orožju in podpori skupnosti v bližini predvidene tarče – igra pri identifikaciji ranljivih točk lokalna policija pomembno vlogo. Policijske postaje, ki imajo tesne delovne odnose z lokalnimi skupnostmi, imajo boljše možnosti, da preprečijo teroristom doseganje njihovih tarč.
- Dostopnost atraktivnih tarč bo določila vrsto terorističnega napada. Težje ko je tarča dostopna, bolj posebno in inovativno mora biti orodje in orožje, ki ga uporabijo za dostop do nje. Temu sledi, da trdnejša ko

je tarča, težje je načrtovanje in potrebnih je več sredstev za podporo operacijam.

Priprava samomorilskega bombnega napada

Obstajajo tri osnovne stopnje izpeljave klasičnega samomorilskega bombnega napada, ko terorist, opasan z bombo, vstopi v restavracijo:

1. Priprava: osebje, tarča in orodje.
2. Operacija: spraviti bombnega napadalca do tarče.
3. Posledice: prevzemanje odgovornosti in načrt novega napada.

Tabela prikazuje korake za pripravo takšnega napada. Upoštevajte, da smo ta primer izbrali, ker je o tovrstnih napadih na voljo več informacij, ne pa zato, ker bi bilo verjetneje, da se bo tak napad (ki je običajen v Izraelu) zgodil v Združenih državah.

Potrebno dejanje	Potrebna sredstva
1. korak – Priprava varne osnove za operacijo	
• Najti prijazno lokacijo za varno hišo • Pripraviti njeno uporabo	• Skladišče za shranjevanje bombnih priprav • Zarota skupnosti v podporo varni hiši
2. korak – Izbor tarče ali tarč	
• Najti atraktivne tarče, ki ustrezajo nalogi • Izbrati primerno pot za dostop do tarče • Ogled tarče za ocenitev logistike in dostopnosti	• Zemljevidi in poizvedovanje o okolici tarče • Obveščevalni viri iz lokacije tarče in predlagana pot do tarče
3. korak - Izbor kandidata za bombni napad	
• Uporaba mreže za izbor kandidata • Začeti z indoktrinacijo bombnega napadalca • Plačila staršem bombnega napadalca	• Pridobivanje mladih navdušencev • Organizacijska mreža za identifikacijo kandidatov
4. korak – Določanje lokacije detonacije	
• Izbrati lokacijo (npr. na avtobusni postaji X, pred živahno tržnico Y) • Izbratii alternativno lokacijo, če načrt spodleti	• Natančne informacije lokalnih prebivalcev na lokaciji tarče; poizvedovanje

Potrebno dejanje	Potrebna sredstva
5. korak – Določanje poti do tarče	
• Načrt poti do tarče in način prevoza (avtobus, taki ali peš) • Priprava alternativne poti	• Natančno poznavanje območja tarče in poti • V pomoč je podpora lokalnih prebivalcev
6. korak – Vzpostavitev skupinske predanosti	
• Sestanki skupinske predanosti za povezovanje zarotnikov med sabo in nalogo	• Zaupanja vredni prostovoljci za spodbujanje procesa skupinske predanosti
7. korak – Izurjenje bombnih napadalcev	
• Uporaba bombnih telovnikov in postopek detonacije • Ponavljanje poti do tarče	• Eksploziv in oblačila za prekrivanje • Strokovnjaki za oceno bombnega telovnika
8. korak – Priprava propagande	
• Razglasitev mučeništva bombnega napadalca • Posnet video, v katerem bombni napadalec izraža svojo predanost nalogi	• Videokamera, osebni računalnik in programska oprema za videomontažo, material za plakate • Fotografije bombnih napadalcev

Vir: Clarke, Ronald V. and Graeme R. Newman, Outsmarting the Terrorists. Westport, Connecticut: Praeger Security International, 2006.

Napotek 13: Zamenjajte »Kaj če?« s »Koliko verjetno?«

Od 11. septembra je predstava o novem napadu teroristične skupine iz tujine podžigala uradni odziv na terorizem in prestrašila javnost. Stopnja dnevne grožnje terorja, ki se prikazuje na TV postajah v času poročil, vzdržuje stopnjo strahu. Ko smo prestrašeni, se ukvarjamo z možnostmi, da bo prišlo do vseh vrst katastrof in velika verjetnost je, da smo v interakciji z državljani, predstavniki skupnosti in lokalnimi uradniki pod pritiskom teh možnosti. Kaj če teroristi zastrupijo mestni vodovod? Kaj če terorist sproži umazano bombo v lokalni športni dvorani? Kaj če oborožen človek zasede osnovno šolo? Kaj če? Kaj če? Nekdo si zamisli vse vrste grozovitih scenarijev – in mogoče se bodo ti zgodili. Vendar je pri tem pomembno vprašanje: kako verjetno je, da se bodo zgodili v vašem okrožju?

Kako naj bi se odzvali na vsako nočno moro? Dejstvo je, da je kakršenkoli teroristični napad zelo malo verjeten. Odzivanje na grožnjo, kot da je najhujši napad neizbežen, bo samo povečalo strah med volivci in vas temeljito oviralo pri oblikovanju metodičnega načrta za zaščito vaše skupnosti. Za oblikovanje logičnega načrta morate oceniti, katere posebne značilnosti vašega mesta – katere posebno atraktivne tarče – bi lahko vodile teroriste v napad. Takšne tarče lahko odkrijete z isto vrsto logike, ki se uporablja za identifikacijo izdelkov, ki so privlačni za tatove.

Identifikacija privlačnih tarč. Predmete, ki so najbolj priljubljena tarča tatvin, določijo življenje ljudi, ki jih imajo v lasti, in podjetja, ki jih izdelujejo. Priljubljenost teh dobrin (npr. avtomobili, iPodi, DVD-ji) pomeni, da je veliko takih predmetov na voljo za krajo in da je veliko ljudi pripravljenih kupiti jih od tatov. Z uporabo tega pristopa lahko identificiramo lastnosti, zaradi katerih so izdelki privlačni in na podlagi teh lastnosti sklepamo o možnostih, da jih bodo tatovi izbrali. Akronim SPRDPU (angl. CRAVED) pomaga identificirati lastnosti izdelkov, ki jih tatovi izbirajo.

1. Mogoče jih je skriti (angl. **C**oncealable) (tatovi skrijejo iPod pod plašč).
2. So prenosni (angl. **R**emovable) (iPod, iztrgan iz verižice okoli vratu žrtve).
3. So razpoložljivi (angl. **A**vailable) (nenadoma ima vsakdo iPod).
4. So dragoceni (angl. **V**aluable) (iPod-i so dragi).

5. So prijetni (angl. **E**njoyable) (iPod-i so prijetni).
6. So uporabni (angl. **D**isposable) (vsakdo ga želi).

V bistvu je vsak izdelek mogoče ukrasti, vendar, kot vidimo iz te analize, vsak izdelek ne bo ukraden. Dejansko, večino izdelkov komaj kdaj ukradejo. Podobno, čeprav je mogoče, da bi vsako zgradbo ali osebo lahko napadli teroristi, je verjetnost, da bi večino napadli, zelo majhna. Večina zgradb in oseb preprosto niso atraktivne tarče za teroriste, ki želijo od vsakega napada največje koristi. Čeprav je res, da ne moremo zavarovati vsega, je res tudi, da vse ne potrebuje zaščite, ali vsaj ne enake stopnje zaščite.

Lastnosti tarč, ki so za teroriste atraktivne, lahko povzamemo z akronimom IVIL UZBL (angl. EVIL DONE – zlo opravljeno – op. prev.).

1. Izpostavljenost (angl. **E**xposed) (Dvojčka sta bila najvišji stavbi v okolici).
2. Vitalnost (angl. **V**ital) (električno omrežje, transportni sistemi, komunikacijski sistemi).
3. Ikon(ičnost) (angl. **I**conic) (simbolične vrednosti za sovražnika, npr. Kip svobode).
4. Legitimnost (angl. **L**egitimate) (somišljeniki teroristov so se veselili, ko sta se Dvojčka zrušila).
5. Uničljivost (angl. **D**estructible) (vladalo je mnenje, da sta Dvojčka neuničljiva).
6. Zasedenost (angl. **O**ccupied) (ubiti čim večje število ljudi).
7. Bližina (angl. **N**ear) (na dosegu teroristične skupine; blizu doma).
8. Lahkost (angl. **E**asy) (zvezno stavbo Alfreda P. Murraha je zadela avto bomba, ki je bila nastavljena ne dlje od 8 čevljev od njenega perimetra).

Kako zavarujemo tarče pred tatvino, je precej očitno iz analize njihove atraktivnosti. Na primer, iPod-ov ne bi smeli razstaviti na odprtih prodajnih pultih, zapakirani naj bi bili v velikih škatlah, ne bi se jih smelo nositi okoli vratu in tako naprej. Isto velja za tarče teroristov. Preprosta betonska pregrada, primerno oddaljena od stavbe Murrah, bi Timothyu McVeighu močno otežila njeno razstrelitev. Razmišljanje o tem, kako bi teroristi našli način, da bi Dvojčka izpostavili in ju naredili lažje dostopna, bi morda vodilo v to, da bi se zračni napad predvidel; dejansko so ta pristop preučevali, vendar opozorilo ni bilo upoštevano.

Seveda vsaka tarča teroristov nima vseh naštetih lastnosti do enake mere. Poleg tega novo in inovativno orožje ali orodje lahko vpliva na uničljivost in dostopnost tarče. Na primer, okoli Bele hiše so postavili »jekleni obroč«, narejen iz betonskih pregrad in jeklene zaščite, vendar je to ne bi zaščitilo pred zračnim napadom, za katerega obsojeni Al-Kaidin terorist Zacarias Moussaoui trdi, da ga je načrtoval za 11. september.

IVIL UZBL (angl. EVIL DONE) nam omogoča, da oblikujemo nekaj zelo dobrih domnev o tarčah, za katere je večja verjetnost, da bodo napadene, in o obliki teh napadov. (Za več podrobnosti o IVIL UZBL (angl. EVIL DONE) glej napotek 28); to pomeni, da nam ni treba vsega ščititi do enake stopnje, celo ob soočenju z napadom. Obstajajo drugi logični načini napovedovanja, katere tarče bodo bolj verjetno napadene in katere tarče bodo, v kolikor bodo napadene, povzročile največ gorja. Zavarovalne agencije se spopadajo s tem problemom odkar delujejo: gre za ocenjevanje ranljivosti tarče za napad in pričakovanih izgub v primeru uspešnega napada.

Ranljivost se nanaša na značilnost tarče, ki privlači pozornost terorista, kot je opisano v IVIL UZBL (angl. EVIL DONE). Ranljivost tarče lahko zmanjšamo z :

- oceno privlačnosti potencialnih tarč in uvedbo primerne preprečevalne tehnike;
- zmanjšanjem priložnosti, da bi teroristi prišli do orožja, s katerim lažje izkoristijo ranljivost tarč;
- zmanjšanjem priložnosti, da bi teroristi izkoristili orodja, kot so nove komunikacijske tehnologije, ki lahko olajšajo organizacijo njihovih napadov in doseganje njihovih tarč;
- nadzorom lokalnih razmer, ki bi lahko teroristom olajšale dostop do tarč, orodja in orožja.

Pričakovana izguba se nanaša na predvidene poškodbe in škodo zaradi uspešnega napada. Na primer, napad na električno omrežje bi lahko bil katastrofalen, ker je omrežje sestavni del infrastrukture, od katerega je družba odvisna; kakorkoli, razpoložljivost rezervnega sistema lahko močno zmanjša izgubo. Čeprav bi utegnil biti neprijeten, napad na električno omrežje ne bi neposredno ubil ali poškodoval veliko ljudi, kot bi se to zgodilo, če bi bile uničene večje zasedene poslovne stavbe. Pogostost

napadov seveda povečuje izgubo. Na primer, število izgubljenih življenj v preteklih 30 letih zaradi terorizma IRE (domači terorizem) je skoraj enak številu ubitih v enkratnem napadu 11. septembra (v tujini načrtovan terorizem). Vendar pa v nasprotju s Severno Irsko, redkost v tujini načrtovanih napadov na Združene države pomeni, da jih je težko z gotovostjo predvideti. Resnično so manj predvidljivi od potresov – čeprav lahko povzročijo prav takšno uničenje. Zato se moramo bolj osredotočiti na zmanjševanje ranljivosti, saj s tem zmanjšamo tudi izgube. Na lokalni ravni je napad tujih teroristov zelo malo verjeten, čeprav so morda nekateri kraji, kot so velika mesta, ki imajo številne privlačne tarče, bolj ogroženi od drugih.

Napotek 14: Pazite se domačega terorizma

Takojšen odziv institucij kazenskega pregona in medijev na bombni napad na zvezno zgradbo Alfreda P. Murraha leta 1995 v Oklahoma City v Oklahomi je bil, da je šlo za delo tujih fanatikov. Vendar se je izkazalo, da je šlo za domačega fanatika. Od 1998 do 2004 je bilo 98 primerov domačega terorizma, posledica katerih je bilo 177 smrtnih žrtev. Na žalost je tudi 2.817 ljudi izgubilo življenje v peščici tujih napadov, ki so se zgodili v istem času. Čeprav je bilo torej v Združenih državah veliko več primerov domačega terorizma, je bilo v teh primerih smrtnih žrtev občutno manj kot pri napadih, ki so jo povzročili tuji teroristi.

Problemsko usmerjeni teroristi. Z nekaj manjšimi izjemami želijo domači teroristi v Združenih državah reševati s terorističnimi dejanji določene probleme in uporabljajo nasilje za pospeševanje svojih načel. Te vrste teroristi so ekoteroristi, nasprotniki splava in različne sovražne skupine. Med slednjimi sta Fronta za osvoboditev zemlje (Earth Liberation Front – ELF) in Fronta za osvoboditev živali (Animal Liberation Front – ALF), ki sta bili najbolj aktivni v zadnjih letih. Nobena od teh skupin ni povzročila smrti kakega posameznika, so pa povzročale občutno gmotno škodo. Nekaj smrtnih žrtev so povzročili nasprotniki splava, ki se nagibajo k temu, da delujejo sami. Razen bombnega napada v Oklahoma Cityju je bilo malo vojaških napadov, napad Timothya McVeigha pa je bil najbolj smrtonosen.

Načrtovanje teh napadov na splošno sledi opisanim načelom terorističnega (in kriminalnega) načrtovanja: tarče napada domačih teroristov so blizu njihovim operacijskim bazam. Ni naključje, da je McVeigh raje napadel stavbo zveznega urada v Oklahoma Cityju kot pa katero v Washington D.C., centru oblasti, ki jo je tako močno preziral. McVeigh se je v Oklahoma Cityju zaradi bližine svojih povezav , zaradi česar je lažje izpeljal pripravo bombe (glej okvir), počutil udobno. Podobno tudi ELF in ALF izvajajo svoje dejavnosti na posebnih lokacijah - na splošno na daljnem zahodu, regija Velikih jezer (Great Lakes) in v severovzhodnih Združenih državah. Poleg tega je zaradi njihove naravnanosti lažje predvideti, katere tarče bodo te skupine napadle. Za ALF je možna tarča vsaka struktura ali organizacija, ki uporablja živali, vključno z univerzami z raziskovalnimi živalskimi laboratoriji. Za ELF so možne tarče trgovci špor-

tnih terenskih vozil in načrtovalci zemljišč v bližini območij divjine. V teh primerih lahko občutno zožimo seznam tarč, ki jih moramo varovati.

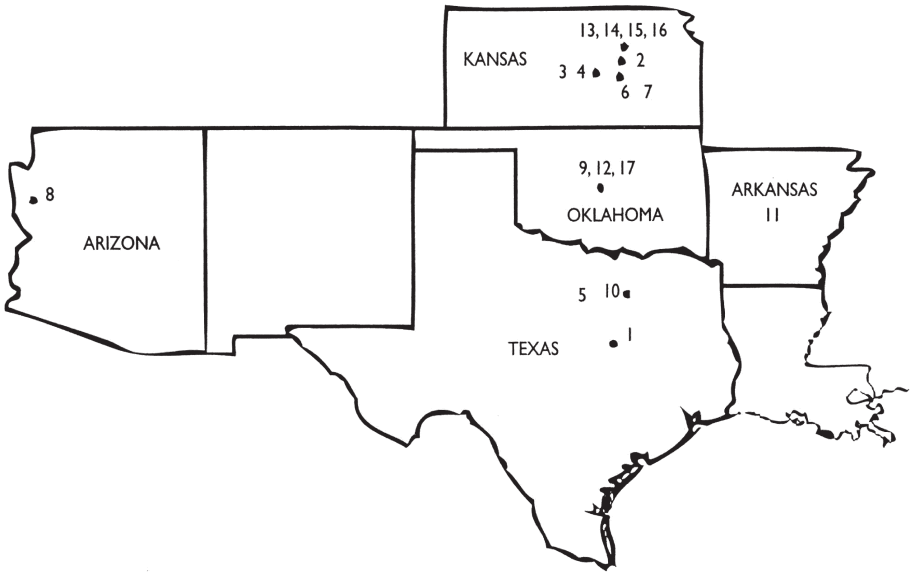
Rutinski terorizem v Združenih državah. Nobena od teh domačih terorističnih skupin ni bila zmožna izvajati rutinskih in ponavljajočih se napadov na stopnji IRE na Severnem Irskem ali različnih terorističnih skupin v Palestini. Verjetno zato, ker nimajo organizacijskih zmožnosti za podpiranje številnih napadov. Lahko je tudi, da se ne zavzemajo za nasilna sredstva kakor druge teroristične skupine. Izjema od te splošne resnice so bili nasilni protivojni protesti in protesti Črne moči (Black power), ki so potekali v času vietnamske vojne, in serija bombnih napadov, ki jih je v New York Cityju izvedlo gibanje za osvoboditev Puerto Rica (Puerto Rico Liberation movement) v 1960. in 1970. letih. Slednje je bila koalicija domačih in tujih terorističnih skupin, ki so izrabili kritje dobro vpeljane portoriške priseljenske skupnosti v New York Cityju za izvajanje ponavljajočih se bombnih napadov manjših razsežnosti na banke in druge zgradbe. Sodelovalo je majhno število teroristov, ki so jih sčasoma ulovili in zaprli ali ubili v akciji. Napadi so hitro prenehali.

Se lahko spet zgodi kaj podobnega? Če je tako, katero orožje, orodje in olajševalne okoliščine bi lahko okrepile domači terorizem? Naštejmo nekaj možnosti.

- Široko razširjena dostopnost majhnega orožja v Združenih državah, posebej med mestnimi tolpami.
- Dolga zgodovina nasilja med latinskimi in drugimi tolpami v velikih mestih ZDA.
- Tolpe, sestavljene iz bivših paravojaških skrajnežev, kot je Mara Salvatrucha, ki izvira iz El Salvadorja.
- Izgon članov tolp v njihove domovine in na ta način ustvarjanje dejanskih mednarodnih kriminalnih mrež.
- Obstoj dobro vpeljanih priseljenskih skupnosti, ki nudijo kulturno kritje potencialnim teroristom.

Nihče ne ve, ali se bodo – s pravim razlogom in vodjo – ti pogoji izkazali kot pomemben domač teroristični problem.

Potovanje do bombnega napada



Legenda zemljevida

1. *Marec 1993: McVeigh gre v Waco, da bi si ogledal spopad med pripadniki sekte Branch Davidians in uradom za alkohol, tobak, strelno orožje in eksploziv (Bureau of Alcohol, Tobacco, Firearms in Explosives – ATF). Dogodek v Wacu naj bi podžgal njegovo odločitev, da bo napadel zvezno stavbo v Oklahoma City.*
2. *22. september 1994: McVeigh najame skladišče v Heringtonu, v Kansasu. McVeigh in zarotnik Terry Nichols zbereta material za izdelavo bombe in ga shranita v skladišču preden sestavita napravo.*
3. *23. september 1994: McVeigh kupi 10 vreč umetnega gnojila pri Mid-Kansas Cooperative Association v McPhersonu, Kansas.*
4. *30. september 1994: McVeigh in Nichols kupita štirideset 50 funtov težkih vreč amonijevega nitrata v McPhersonu, Kansas.*
5. *30. september 1994: McVeigh kupi tri sode nitrometana, vsakega za 950 dolarjev od V.P. Racing, lociranega južno od Dallasa, Teksas.*
6. *1. oktober 1994: McVeigh in Nicholas ukradeta eksploziv iz skladiščnih prostorov v Marionu, Kansas.*
7. *3. oktober 1994: McVeigh in Nichols ukradeta od Martin Mariette Quarry v Marionu v Kansasu dinamitne palice, 544 električnih detonacijskih kapic (pokrovov) in 93 običajnih detonacijskih kapic.*
8. *3. oktober 1994: McVeigh in Nichols odpeljeta ukradeni eksploziv v Kingman, Arizona, kjer je McVeigh najel drugi skladiščni prostor.*
9. *10. oktober 1994: McVeigh in Nichols se na poti, ko gresta kupit nitrometan na Dallasovo dirkališče, peljeta skozi Oklahoma City.*
10. *10. oktober 1994: Peljeta se mimo zvezne stavbe Murrah in ocenita, koliko časa bo McVeigh rabil za umik s kraja, kjer bo nastavljena bomba.*
11. *5. november 1994: McVeigh in Nichols oropata prodajalca strelnega orožja v Arkansasu.*
12. *18. december 1994: V spremstvu starega prijatelja, Mikea Fortiera, McVeigh odpotuje v Oklahoma City in potrdi izbor stavbe Murrah kot tarčo, medtem ko predhodno zavrne zgradbi v Kansas Cityu, Kansas in v Littleu, prav tako Kansas.*

Nekaj razmišljanj o (policijskem) zaznavanju teroristične grožnje v Sloveniji

Andrej Sotlar

Verjetno se je policistom najtežje spopadati s tistimi viri in vrstami groženj, ki se redko ali celo nikoli ne pojavljajo v njihovem delovnem in življenjskem okolju. V kolikor odmislimo države, kot so Afganistan, Irak, Pakistan in Izrael, teroristični napadi v večini držav pač niso tako pogosti kot ropi, umori, preprodaja drog in druga podobna kazniva dejanja. To še posebej velja za Slovenijo, ki se v času svoje samostojnosti komajda spomni nekaj dejanj, ki bi lahko imela teroristično ozadje (sem grožnje z nasiljem in ustrahovanje, ki sta posledica motivacij organiziranega kriminala ali neuravnovešenih posameznikov, zagotovo ne sodijo).

Odsotnost realne vsakodnevne grožnje nujno vpliva tudi na zaznavanje problema pri laični in strokovni javnosti ter političnih elitah. Javnomnenjske raziskave že vsa leta (tudi po 11. septembru) kažejo na izredno nizko stopnjo zaznavanja teroristične grožnje med prebivalci Slovenije. Koliko lahko takšna percepcija uspava tudi pripadnike nacionalnovarnostnega sistema (policiste, obveščevalce, vojake, pripadnike zaščite in reševanja in druge), je težko oceniti, vsekakor pa daljša odsotnost neke grožnje (in posledično skromnejše operativne izkušnje) zagotovo ne pripomore k izostritvi njihovega »protiterorističnega občutka«.

V nadaljevanju so predstavljeni nekateri napotki in priporočila, ki naj policistom olajšajo soočenje s kaznivimi dejanji teroristične narave. Terorizem je namreč prav to – zelo težko kriminalno dejanje, ki ima ponavadi globoke neposredne in posredne vzroke, ki jih policisti sicer lahko razumejo, vendar njihov odziv nanje ne more in ne sme biti posledica njihove lastne zaznave, morda celo simpatij do protagonistov določenega političnega, etničnega ali gospodarsko-socialnega problema, iz katerega tudi terorizem skuša črpati svojo legitimnost. Na tem mestu se kar sama ponuja primerjava policijskega pristopa h klasičnemu kriminalu. Tudi mnogi policisti razumejo in obžalujejo, da so npr. dejanja množičnega posiljevalca lahko zgolj posledica dejstva, da je bil storilec v mladosti tudi sam zlorabljan,

vendar jih to ne bo zaustavilo v nameri, da ga čim prej primejo in preprečijo, da stori še več gorja. V obeh primerih, tako ko gre za klasična kazniva dejanja, kot če gre za kazniva dejanja v povezavi s terorizmom, je kazenski zakonik zagotovo glavno vodilo policijskega dela.

Novi Kazenski zakonik Republike Slovenije (Ur. l. RS, št. 55/2008) je nabor dejanj z obeležji terorizma še razširil. Tako imamo sedaj štiri kazniva dejanja, ki se neposredno nanašajo na terorizem: Terorizem (108. člen KZ), Financiranje terorizma (109. člen KZ), Ščuvanje in javno poveličevanje terorističnih dejanj (110. člen KZ) in Novačenje in usposabljanje za terorizem (111. člen KZ). Vendar pa preprečevanje in preganjanje terorizma še zdaleč nima samo svoje nacionalne dimenzije. Zavezanost protiterorističnemu boju je namreč tudi splošni civilizacijski in mednarodno-pravni imperativ, na operativni ravni pa stvar utečenega mednarodnega policijskega in pravosodnega sodelovanja. Grožnjo terorizma gre namreč razumeti zelo praktično – nekaj, kar se je v naši državi morda začelo z navidez »nedolžnim« kaznivim dejanjem (npr. z opravljeno finančno transakcijo med člani ali simpatizerji teroristične skupine), se lahko hitro konča z veliko človeško tragedijo v drugi državi, tragedijo, v kateri pa so lahko udeleženi državljani številnih držav, tudi tistih, ki niso bile cilj/tarča terorističnega akta. Zato so tudi razprave o ločnicah med »(domačim) terorizmom« in »mednarodnim terorizmom« prej stvar akademskih in filozofskih razprav kot pa vsakodnevnega policijskega dela, ki se ne sprašuje o nacionalnih in zunanjepolitičnih interesih, ampak prej o interesih ljudi, ki jim je potrebno zagotoviti varnost, saj predstavljajo najmanj zaščiteno potencialno tarčo.

Za policiste, ki morajo biti vedno na preži, to seveda še ni vse. Terorizem pozna namreč bogat nabor kaznivih dejanj, ki pravzaprav omogočajo, da teroristična dejavnost sploh (pre)živi. Ropi, preprodaja drog in orožja, umori, ugrabitve, izsiljevanja, nezakoniti prestopi meje in podobno so lahko nekakšna pripravljalna dejanja (nekatera so hkrati tudi končna oblika terorističnega dejanja), zgolj vrh ledene gore, medtem ko se načrtuje in pripravlja »klasično« teroristično kaznivo dejanje. Zato so policisti, ki se ponavadi (če odmislimo neposredne oškodovance) prvi soočijo s kaznivim dejanjem, lahko celo priča začetku nečesa globljega in nevarnejšega, kot se zdi na prvi pogled. V tej luči se nam tudi vsakodnevno policijsko delo pokaže precej bolj pomembno tudi, ko gre za teroristične grožnje, s katerimi se ponavadi po svetu predvsem ukvarjajo »elitne« službe - kot npr. obveščevalno-varnostne službe, posebni oddelki kriminalistične policije,

specialne (protiteroristične) policijske in vojaške enote itd. Vse prevečkrat namreč pozabljamo, da se vsako teroristično dejanje zgodi v neki lokalni skupnosti, torej tam, kjer delujejo policijske postaje in njihovi policisti, ki najbolje poznajo lokalne razmere in bi vsaj hipotetično morali razpolagati tudi z največ informacijami, ki so kasneje lahko še kako pomembne za omenjene protiteroristične službe.

Slovenskim policistom naj bodo zato pri soočenju s teroristično grožnjo in ob prebiranju napotkov ameriških strokovnjakov v pomoč naslednja priporočila, nekakšen dekalog policijskega protiterorističnega dela:

1. Nobena družba ni imuna na teroristične grožnje in napade.
2. Na terorizem bomo bolje pripravljeni, če bomo naš miselni in besedni slovar spremenili iz »Če« v »Ko« ali »Kdaj« (bo prišlo do terorističnega dejanja).
3. Vsak teroristični napad je najprej in vedno predvsem hudo kriminalno dejanje.
4. Čeprav lahko razumemo vzroke in motivacijo za teroristične napade, dejanj samih ne moremo opravičevati.
5. Policisti ne odpravljajo vzrokov za terorizem, pač pa ga preprečujejo in preiskujejo.
6. Dilema »varnost ali svoboda« je lažna dilema, saj se vrednoti ne izključujeta, ampak medsebojno pogojujeta.
7. Policisti imajo pomembnejšo vlogo pri preprečevanju in preiskovanju terorizma, kot je videti na prvi pogled, saj se teroristični akt vedno zgodi v njihovem lokalnem delovnem in/ali življenjskem okolju.
8. Boj proti terorizmu zahteva vrhunsko poznavanje policijske taktike in hkrati nekonvencialno razmišljanje – potrebno je misliti onkraj mogočega, verjetnega in zamisljivega.
9. Človeško življenje ima največjo vrednost, zato morajo biti policijski postopki usmerjeni najprej v varovanje in zaščito ljudi, torej v preprečevanje samega terorističnega dejanja.
10. Teroristi so, ne glede na to, kaj storijo ali nameravajo storiti, še vedno ljudje, ki jim gredo vse civilizacijske pridobitve osumljenim v predkazenskem postopku, kar od policistov zahteva strogo spoštovanje zakonov, najvišjo profesionalnost in visoko stopnjo etične in moralne drže, naj bo to ob soočenju s hudim terorističnim dejanjem še tako težko.

III.

Oblikujte načrt in podporno mrežo

Napotek 15: Zajemite v načrt tri osnove protiterorizma

Ta napotek nudi pregled treh glavnih sestavin protiterorističnega načrta, ki ga natančno opisujeva v zadnjih treh delih priročnika.

1. Zbiranje informacij o možnih terorističnih dejavnostih (Napotki 21-28).
2. Utrjevanje tarč (Napotki 29-36).
3. Pripravljenost na odziv v primeru napada (Napotki 37-50).

Ironično je, da je odziv na napad najmanj problematična sestavina vsakega protiterorističnega napada. Nedvomno ste sami že vzpostavili načrt za spoprijemanje s konvencionalnimi katastrofami. Z nekaj popravki vam ta načrt operacij lahko pomaga pri soočenju s terorističnim napadom. Na primer, predvideti boste morali možne nadaljnje napade na reševalce in razmislite o možnosti, da bodo napadalci uporabili orožje za množično uničevanje, vendar so tudi v teh primerih potrebna dejanja relativno jasna in specifična. Če ste vzpostavljenim postopkom natančno sledili in da tesno sodelujete s tistimi, ki nosijo najvišjo odgovornost za načrt v izrednih razmerah, bi morala biti vaša skupnost dobro pripravljena na odziv in obnovo po terorističnem napadu. Kolikor ne boste natančno načrtovali in bodo stvari šle narobe, lahko pričakujete, da vas bodo kritizirali, in to upravičeno.

Glede ostalih dveh sestavin stvari še zdaleč niso tako jasne. Veliko manj je smernic o tem, kako določiti, katere tarče zavarovati in kako pridobiti podatke o teroristih. Še posebej je nejasno, koliko truda naj bi vložili v zbiranje podatkov. Seveda morate spodbujati policiste za skupnostno policijsko dejavnost, da opazujejo možne teroristične dejavnosti v svojih soseskah – posebej priseljenskih soseskah. Vsako informacijo, o kateri poročajo, morate takoj posredovati FBI, ki ima najvišjo odgovornost pri

preiskovanju teroristov v vašem okolišu. Za skupno dobro morate tudi vi sodelovati v lokalni delovni skupini za terorizem (Joint Terrorism Task Force) in enega od vaših policistov usposobiti kot uradnika za zvezo za področje terorizma (http://www.tlo.org/training/index.htm). Ali boste vlagali v bolj formalne metode zbiranja in izmenjave obveščevalnih informacij, bo odvisno od velikosti vašega okoliša in vaše presoje o njegovi ranljivosti. Za večino manjših okolišev je vprašljivo, ali bi bila investicija upravičena, ker je nevarnost terorizma tako majhna, da bi kakršenkoli poseben sistem za zbiranje in izmenjavo informacij obrodil zelo malo koristi in bi bil hitro neuporaben. Natančna preučitev nacionalnega načrta za izmenjavo kazenskih informacij (National Criminal Intelligence Sharing Plan) vam lahko pomaga pri odločitvi, koliko virov investirati v izmenjavo informacij in zbiranje. (http://www.it.ojp.gov/topic.jsp?topic_id=93)

V majhnih, malo ogroženih okoliših je utrjevanje tarč nekoliko problematično. Za začetek, še vedno ni jasno, kako si razlagati 11. september. Hkrati prevladuje prepričanje, da napad pomeni, da bodo Združene države v prihodnosti pod nenehno grožnjo napadov teroristov prek morja. Vendar pa po sedmih letih ni bilo v Združenih državah nobene ponovitve napada. Ali zato, ker so bile varnostne sile uspešne pri prestrezanju in odvračanju vseh kasnejših napadov, ali pa gre preprosto za geografski vpliv – namreč teroristi zelo težko napadejo Združene države prek morja – ni znano. Torej, čeprav je globalni terorizem verjetno nepreklicno tukaj, ne moremo vedeti, kdaj ali kje bodo spet napadli Združene države. Ta negotovost spodkopava argument, ki govori v prid obsežnemu utrjevanju tarč, posebej glede vloženih stroškov in truda. Vsa podzemna jedrska zaklonišča, ki so ob koncu hladne vojne postala presežek, svarijo pred tem, da politiko vodi strah.

Zelo malo je smernic glede tega, katere tarče utrditi, kako jih utrditi in katerim dati prednost. Leta 2006, na primer, je nacionalna baza podatkov ministrstva za domovinsko varnost (Department of Homeland Security's (DHS) National Asset Database (NAD) naštela 77.069 kritičnih lokacij zveznih držav, ko so se potegovale za sredstva iz zveznih fondov za boj proti terorizmu. Vključene so bile številne malo verjetne tarče, vključno s starim Macdonaldovim živalskim vrtom za otroke, kjer se živali lahko ljubkuje in hrani, parada dneva mul, Searsov trgovinski center in Nixova unovčevalnica čekov. Seznam Indiane vsebuje 50 odstotkov več lokacij kot seznam New Yorka in vključuje podjetja, kot je Amish Country Popcorn. Ko so novinarji New York Timesa (12. julija 2006) pobarali lastnika te ustanove

s petimi zaposlenimi, kako da je vključen v seznam, se je ta zdel tako zmeden kot vsi ostali: »Tukaj so samo vozovi amišev in traktorji. Morda zato, ker popovka eksplodira?« To se je zgodilo en mesec potem, ko je DHS napovedal zaključek svojega nacionalnega načrta za zaščito infrastrukture (National Infrastructure Protection Plan – NIPP), načrta, ki temelji na obvladovanju tveganja (glej napotek 18; za več informacij o ranljivosti in oceni tveganja, dveh ključnih konceptov, ki jih je sprejel NIPP, glej napotek 28-32. V skladu z NIPP, ki še vedno čaka uresničitev, bo za vas verjetno najbolj smiselno slediti tristopenjskemu pristopu k utrjevanju tarč.

1. Čim prej zaščitite izpostavljene tarče. Ker so nekatere tarče v zasebni lasti, je vaša naloga, da se povežete z lastniki, jim ponudite nasvete, za katere se čutite kvalificirani, spodbujate lastnike, da si priskrbijo strokovno varnostno svetovanje ter delujete kot posrednik med podjetji in državo ter zveznimi agencijami, ki lahko nudijo pomoč pri uresničevanju utrjevalnih ukrepov.
2. Sestavite prednostni seznam ostalih tarč, ki rabijo obsežno utrjevanje, kot tudi časovni razpored za zagotavljanje, da se to stori.
3. Razvijte daljši seznam vseh možnih tarč, ki bi jih bilo treba zaščititi z nekaj osnovnimi utrjevalnimi ukrepi, in spremljajte načrte lastnikov teh objektov, da bodo pripravili osnovne varnostne ukrepe (napotek 32).

Pri prepričevanju lastnikov objektov, da pripravijo varnostne ukrepe, jim razložite, da jih bodo taki ukrepi ščitili tako pred terorizmom kot tudi pred običajnim kriminalom. Postopki, zaradi katerih teroristi težje dostopajo do objektov, bodo prav tako pripomogli k odvračanju vlomilcev in vandalov. V bistvu bi morala biti kriterij vaših protiterorističnih prizadevanj uporaba tistih utrjevalnih ukrepov, ki nudijo dvojno korist. **Ker je tveganje za teroristični napad na nekaterih lokacijah precej nizko, bo protiteroristične ukrepe, ki koristijo običajnim policijskim operacijam, lažje zagovarjati tako z družbenega kot tudi s finančnega vidika.**

Napotek 16: Sodelujte s podjetji

Vlada in podjetja so neugodni partnerji in to velja tudi, ko gre za kriminal. Policija se pogosto zadovolji s tem, da se podjetja sama varujejo pred kriminalom in spoprijemajo s storilci na svoj način. Občasno ta dogovor odpove in se trgovci pritožujejo, da lokalna policija ne preganja tatov ali pa policija trdi, da trgovine naredijo premalo za varovanje svojega blaga.

Ko gre za terorizem, pa morajo vlada in podjetja pozabiti stare navade in sodelovati iz številnih pomembnih razlogov. Prvič, podjetja imajo v lasti 85 odstotkov državne infrastrukture, kot so zbiralniki, kemične tovarne, transportni sistemi, pristanišča, letala, komunikacije itd., ki so zelo možne tarče terorističnih napadov. Drugič, teroristi pogosto izberejo tarče zaradi njihove simbolne ali ikonične vrednosti – teroristi so 11. septembra izbrali za tarčo Svetovni trgovinski center, ki je simbol kapitalizma – in nekatera podjetja se identificirajo z ameriškim načinom življenja. Taka podjetja so tudi McDonald's, Wal-Mart, Starbucks, Nike, Hilton in Marriott. Zato nekatere spletne strani trdijo, da je Starbucks protimuslimanski in kljub njegovemu prizadevanju, da bi opozoril na okoljske težave, je podjetje postalo tarča radikalne levice. In še to. Nekateri domači teroristi izbirajo za tarče podjetja, kot so mlečne farme, mesarije in klinike za splav (glej napotek 14, orig. napotek 15). Kot je izjavil bivši minister za domovinsko varnost, Tom Ridge: »Smo okolje, bogato s tarčami, in zasebni sektor ima v lasti večji del teh tarč.«

Podjetja so v Združenih državah neločljivo povezana s civilnim življenjem. Nahajajo se v skupnostih, kjer živijo njihovi zaposleni, stranke in kupci. Pogosto so locirana dovolj blizu ostalih prebivalcev, tako da je napad na podjetje nevaren tudi za skupnost. Tako kot si podjetja prizadevajo zaščititi svoje zaposlene pred katastrofalno škodo, bi si morali prizadevati tudi za zaščito svojih sosesk in skupnosti.

Podjetja niso zgolj tarče, so tudi pomemben vir informacij in virov. Banke lahko nudijo informacije o finančnih transakcijah sumljivih organizacij, telefonska in kreditna podjetja lahko pomagajo pri sledenju sumljivih oseb, podjetja za najem avtomobilov in moteli lahko poročajo o nedavnih obiskovalcih in trgovine za kmetijsko oskrbo lahko izsledijo prodaje vnetljivih gnojil. Podjetja vedno sodelujejo in pomagajo, kadar se zgodijo velike katastrofe. Bolj pomembno kot to pa je, da so vodje podjetij enako lojalni in domoljubni kot katerikoli drugi član skupnosti (glej okvir 1).

Okvir 1: Korporacije niso samo zgradbe, stroji in papirji.

»Korporacije niso samo zgradbe, stroji in papirji; so zaposleni, delničarji, upravljavci in direktorji, ki so vsi domoljubni, lojalni in spoštujejo družbene vrednote našega naroda, osebne svoboščine in tržno gospodarstvo. Ko podjetje sprejme ukrepe za zaščito sebe in drugih, bi del računa za to moral, in neizbežno bo moral, vključevati podporo naše države in zavarovanje njenih ljudi.«

Vir: Susman, Thomas. Terrorism: Real Threats. Real Costs. Joint Solutions. Washington, D.C.: The Business Roundtable, 2003.
http://www.businessroundtable.org/pdf/984.pdf.

Sodelujte s podjetji: (1) da bodo njihovi prostori, objekti in operacije bolj varni; (2) pri oblikovanju načrta za izredne razmere, za primer neposrednega napada; in (3) jih vključite v načrtovanje reševanja in obnove v primeru napada v vašem okolišu. Kontaktne točke s podjetji bi lahko vključevale:

- rutinske klice podjetjem s strani območnih policistov;
- redna predavanja o terorizmu na srečanjih Lions-ov, Elks-ov, Rotary kluba in podobnih organizacij;
- fizične preiskave trgovin na drobno in drugih komercialnih ustanov, ki jih izvajajo policisti, usposobljeni za varnost prizorišč;
- sestanke z izvršnimi direktorji velikih podjetij in stike z lokalnimi in regionalnimi upravljavci;
- redna srečanja z varnostnimi upravljavci velikih podjetij.

Varnostni upravljavci velikih podjetij se bodo verjetno izkazali kot najbolj koristni partnerji (glej napotek 17), vendar si zapomnite, da velika podjetja niso nujno v največji nevarnosti za napad. Podjetja, ki so najbolj v nevarnosti sodijo v štiri glavne skupine, in sicer so to podjetja, v katera bi morali usmeriti svojo energijo: (1) podjetja, ki so odgovorna za infrastrukturo, kot so zbiralniki in elektrarne; (2) tista, ki so odgovorna za objekte, v katerih se zbira veliko ljudi; (3) tista, ki bi v primeru, da bi bila napadena, povzročila stransko škodo, npr. kemične in biološke tovarne; in (4) tista, ki so komercialne ikone, kot je McDonalds in druga podjetja, ki sva jih omenila zgoraj.

Morda boste presenečeni nad nesodelovanjem določenega podjetja. Za tak odziv so številni razlogi: nekatera podjetja so morda preprosto pripravljena živeti z neznano in verjetno zelo majhno nevarnostjo napada; druga podjetja so v letih, ki so pretekla od 11. septembra, morda dobila lažen občutek varnosti; spet druga podjetja so morda pripravljena tvegati s podstandardno varnostjo, ker verjamejo, da jih bo vlada rešila, če se bo zgodilo najhujše. Poleg tega so zaradi svojega finančnega in upraviteljskega okolja nekatera podjetja morda omejena, na primer:

- podjetja, ki so v lasti nacionalnih verig, se morda morajo uskladiti z varnostnimi ukrepi, ki jih določi uprava;
- podjetja se morda bojijo, da se bodo zaradi obsežnih varnostnih stroškov znašla v nekonkurenčnem položaju;
- na današnjih trgih, ko je pomembno uloviti pravi trenutek, se vse, kar upočasni operacije podjetja, zaznava kot protikonkurenčno;
- podjetja morda niso naklonjena uvajanju novih dragih varnostnih postopkov.

Številna podjetja se bojijo, da bo temeljita varnostna ocena pokazala resne pomanjkljivosti, za odpravo katerih bodo morali zapraviti velike vsote denarja, da jih ne bi obtožili namerne malomarnosti, če bi se zgodilo kaj slabega (glej primer Las Vegas v okviru 2).

Okvir 2. Spodleteli sestanek.

Leta 2004 so informacije obveščevalnih agencij ZDA navajale, da so islamski teroristi izbrali za tarče lasvegaške igralnice. V prizadevanjih, da bi bili proaktivni, je FBI sklical sestanek v Las Vegasu in povabil varnostne direktorje vseh večjih igralnic, da se seznanijo z informacijo. Edina, ki sta se udeležila sestanka, sta bila dva lokalna policista. V notranjih dopisih ministrstva za pravosodje so trdili, da je bila želja po izognitvi odgovornosti eden od razlogov, da se noben varnostni direktor igralnic ni udeležil sestanka.

Vir: Garcia, Mary Lynn, »Risk Management,« v The Handbook of Security, ed. Martin L. Gill, Basingstoke, England: Palgrave Macmillan Ltd., 2006.

Iz vseh teh razlogov **je treba izpostavljati ukrepe z dvojno koristjo: tiste, ki bodo zaščitili podjetja ne samo pred terorizmom, temveč tudi pred kriminalom**, kar lahko prispeva h povečanju dobička. Taki ukrepi presegajo okvire prve ravni varnostne pripravljenosti – obrobna varnost, odkrivanje vsiljivcev in varnostniki ter obhodi, vključujejo bančno politiko spoznaj-svojo-stranko, poostritev zahtev po identifikacijskih dokumentih strank v podjetjih, ki dajejo avtomobile v najem, motelov ter preverjanje kriminalnih dosjejev morebitnih najemnikov s strani upraviteljev stanovanjskih kompleksov.

Napotek 17: Sodelovanje s subjekti zasebnega varovanja

Kljub nalogam, ki so skupne policiji in subjektom zasebnega varovanja, se bodo policisti v skupnosti verjetno prej srečali z duhovnikom, podjetnimi skupinami in sosedskimi združenji kot z lokalnimi varnostnimi strokovnjaki. Dejansko lahko zasebni varnostniki nudijo neprecenljivo pomoč pri varovanju večine infrastrukture in zagotavljajo nadzor nad kriminalom na krajih, kjer se ljudje zadržujejo večji del svojega vsakdana: na delu, v javnem transportu, izobraževalnih ustanovah, nakupovalnih centrih in celo v zaprtih skupnostih. Čeprav javni sektor nadzira informacije o terorizmu in obveščevalne informacije, je zasebni sektor tisti, ki nadzira večji del ranljivih in verjetnih tarč napada.

Koristi

V Združenih državah uslužbenci zasebnega varovanja številčno presegajo policiste v razmerju tri proti ena. Sodelovanje z zasebnim varovanjem v okolišu vam bo omogočilo, da za uresničevanje protiterorističnih odgovornosti pokličete na pomoč veliko obsežnejšo skupino moških in žensk. Zlasti bi vam pomagalo pri naslednjem:

- zaščiti kritične infrastrukture v vaši skupnosti, ki jo varujejo subjekti zasebnega varovanja, in zagotovivti hitre obnove v primeru napada;
- pridobivanju učinkovite pomoči zasebnega varovanja v izrednih razmerah. Ker se varnostniki pogosto prvi odzovejo, policija lahko usklajuje z njimi evakuacije, odkrbo s hrano in druge potrebe v izrednih razmerah;
- izboljšavi pretoka informacij v obe smeri. Sodelovanje vam bo omogočalo, da boste zasebnemu sektorju učinkovito posredovali informacije o ogroženosti in narobe, zasebnemu sektorju bo omogočilo neposreden dostop do pravih ljudi, kadar bodo rabili pomoč ali bodo želeli posredovati informacije;
- izrabi znanja zasebnega sektorja, kjer ga vaši postaji primanjkuje, kot npr. v zvezi z goljufijami in spletno kriminaliteto.
- pridobivanju dostopa do virov in objektov zasebnega sektorja, kar vam bo pomagalo izpolnjevati izobraževalne in operativne potrebe.

Zaupanje

Prevzemite pobudo za partnerstvo, da bi pa dosegli polno sodelovanje, se potrudite, da bodo vaši kolegi iz zasebnega sektorja dobili javno priznanje za svoje delo. Z njimi delajte kot s sebi enakimi. To je morda lažje za vas kakor za nekatere od vaših policistov, ki se jim morda zdi, da osebje zasebnega varovanja ni usposobljeno, zlasti v rokovanju z orožjem; da je slabo organizirano in premalo odgovorno za svoja dejanja; in celo, da so to bili neuspeli policijski kandidati, ki niso mogli dobiti značke. Tako mišljenje je odraz omejenega vrednotenja zmogljivosti zasebnega varstva, njegovega strokovnega znanja in virov. Po drugi strani pa varnostniki policiste morda dojemajo kot nesramne in nezainteresirane za svoje področje – dokler ti ne iščejo dela po upokojitvi. Skupno delo bo morda odpravilo napačne predstave in predsodke.

Verjetno je najbolj kritično vprašanje obdelava občutljivih podatkov. Vašim policistom je morda neprijetno izmenjavati informacije o ogroženosti s podjetji, ki so v lasti tujih subjektov; druge informacije, kot so kriminalne zgodovine, pa so zavarovane z zakoni o varstvu zasebnosti. Po drugi strani se zasebni varnostniki morda bojijo, da bodo informacije o lastništvu podjetij zaradi zakonov o svobodi informiranja postale javne. Morda na partnerskih sestankih ne bodo govorili odkrito, da ne bi konkurenti izvedeli za njihove težave, ali zato, ker se bojijo, da bodo obdolženi protimonopolnih kršitev ali celo kaznivih dejanj. Nazadnje, morda ne prijavljajo primerov spletne kriminalitete, da vaša postaja ne bi zasegla zapisov in računalnikov. Z eno besedo, vse temelji na medsebojnem zaupanju, za razvoj tega pa so potrebni čas in potrpežljiva pogajanja.

Organizacija

Kot je omenjeno v napotku 16 , je eden od najboljših načinov pristopanja k velikim podjetjem v skupnosti prek njihovih varnostnikov, vendar obstaja veliko drugih varnostnih strokovnjakov v vaši skupnosti, vključno z lokalnimi varnostnimi svetovalci, ponudniki varnostnih storitev, direktorji družb za protivlomne alarme in monterji varnostne strojne opreme in sistemov. Morda mislite, da že imate dobre neformalne stike s temi skupinami, ki zaposlujejo številne policiste v pokoju, vendar pa višja delovna mesta v agencijah zasebnega varovanja dandanes vedno bolj zasedajo direktorji, ki napredujejo od znotraj; mreže »dobri stari fantje« izginjajo. V

skladu z DHS je cilj preprečevanja terorizma dosegati boljše rezultate prek formaliziranega odnosa med policijo in zasebnim varovanjem, bodisi prek koordinacijskih dogovorov ali prek memorandumov o soglasju. Formalizacija kaže zaposlenim obeh strani, da je sodelovanje prednostna naloga organizacije.

Kako začeti?

- Vključite vrhunske varnostne strokovnjake s svojega področja. Dovolite jim, da predlagajo druge, ki bi morali biti vključeni.
- Pojasnite namen sodelovanja in določite cilje za boljše sodelovanje in usklajevanje.
- Natančno določite, kakšno mora biti sodelovanje, da bi izpolnilo svojo nalogo. (Glej okvir za tipične dejavnosti)
- Identificirajte vire, ki jih bo sodelovanje rabilo, da bi doseglo cilje in najdite načine, da si jih zagotovite.
- Najdite fizični in logistični dom partnerstva in določite policiste, ki bodo koordinirali njegovo delovanje.
- Odločite se, kako bodo člani partnerstva komunicirali, tako rutinsko kot tudi v izrednih razmerah.
- Ustvarite identiteto partnerstva z logotipom, brošurami ali spletnimi stranmi in uporabite to identiteto za pridobivanje sredstev in rekrutiranje novih članov.

Več o tem: Office of Community Oriented Policing Service. National Policy Summit: Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2004.

http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RIC=246

Nekaj dejavnosti partnerstva policija/subjekti zasebna varovanja

Mreženje

- Redni sestanki za obravnavanje problemov in kot pomoč vsaki strani pri razumevanju problemov ter motiviranju druge.
- Predavanja strokovnjakov s področja zasebnega varovanja v centrih za usposabljanje policistov.
- Govori ene skupine na konferencah druge.
- Imeniki stikov lokalne policije in subjektov zasebnega varovanja.
- Priznanja in nagrade ene skupine drugi.

Izmenjava informacij

- Informacije, ki jih ima policija o kazenskih obsodbah, grožnjah in nesrečah, kjer to dovoljuje zakon.
- Informacije, ki jih ima zasebni sektor o podjetniškem kriminalu in sumljivih zaposlenih.

Preprečevanje kriminalitete

- Skupno sodelovanje pri varnosti in zaščiti za podjetniško izboljšanje okrožij.
- Posvetovanje glede preprečevanja situacijskega kriminala in skupnostne policijske dejavnosti.
- Posebne operacije v zvezi z lokalnimi težavami, kot so goljufije s čeki in lažni alarmi.
- Skupna podpora sosedski straži (angl. Neighborhood Watch) in nacionalni nočni straži (National Night Out)

Delitev virov

- Tehnična in logistična izvedenska mnenja.
- Specializirana oprema in objekti, kot so dvorane, učilnice in sejne sobe.
- Poslovni prostor za skupnostno policijsko dejavnost.

Urjenje

- Gostovanje govornikov o temah, ki so v skupnem interesu.
- Izmenjava usposabljanj in ekspertiz. Korporacije lahko nudijo policiji usposabljanje vodstva, agencije za zasebno varovanje lahko usposabljajo organe kazenskega pregona o varnostnih ukrepih, institucije kazenskega pregona lahko učijo varnostnike, kako pričati na sodišču ali kako zbirati dokaze v skladu s procesnimi standardi.

Zakonodaja

- Pripraviti in podpirati zakonske osnutke in odloke glede tem, kot so standard varnostnikov in koncesiranje, alarmi in računalniški kriminal.
- Sledenje zakonodaji, pomembni za institucije kazenskega pregona in varnostne operacije.

Operacije

- Skupne preiskave zapletenih finančnih goljufij in računalniškega kriminala.
- Kritično načrtovanje ukrepanja ob naravnih nesrečah, šolskem streljanju in nasilju na delovnem mestu.

Vir: Bureau of Justice Assistance, Operation Cooperation: Guidelines for Partnerships between Law Enforcement & Private Security Organizations. Washington, D.C.: U.S. Department of Justice, 2000.

Napotek 18: Spoznajte obvladovanje tveganja

Če tega še niste naredili, identificirajte tarče v svojem okolišu, ki so v večji nevarnosti, da jih bodo napadli teroristi, in zato najbolj potrebujejo varovanje. V majhnih mestih to verjetno ne bo težko, saj je morda le nekaj tarč, zanimivih za teroriste – recimo vodni zbiralnik, kemična tovarna in dve ali tri lokalne šole. Skupaj z vodstvom teh objektov oblikujte načrt za zaščito pred možnimi grožnjami. Če je vaš okoliš velik, postane postopek identifikacije groženj in določitev prednostnih nalog veliko večji izziv preprosto zato, ker obstaja toliko več tarč, ki jih je treba upoštevati, in toliko več groženj ter posledic, ki jih je treba pretehtati. Zato boste morda hoteli osnovati formalno ocenjevanje tveganja kot del programa obvladovanja tveganja.

Obvladovanje tveganja je postopek, ki ga uporabljajo podjetja za identifikacijo, določanje prednostnih nalog in spoprijemanje z večjim tveganjem v zvezi z dobičkom in nadaljevanje operacij. Grožnjo lahko pomenijo naravni pojavi (orkan, snežna nevihta, padec telefonskega ali računalniškega sistema, virusne epidemije ali celo nepričakovana smrt izvršnega direktorja) ali zlonamerne dejavnosti ljudi (sabotaža, rop, prevara, vdiranje v računalniške sisteme). Z obvladovanjem tveganja se vse bolj ukvarjajo vladne agencije; DHS zagovarja njegovo uporabo pri ocenjevanju in odzivanju na teroristične grožnje.

Obvladovanje tveganja je lahko visoko tehnološko, še posebej takrat, ko obstajajo podatki za kvantitativno oceno tveganja in pripravo protiukrepov. Inštituti, strokovna združenja in časopisi zadovoljujejo potrebe uporabnikov. Midva ne bova podala natančnega tehničnega opisa; namesto tega bova predstavila dovolj informacij, da presodite, ali morate pripraviti formalno študijo o obvladovanju tveganja v vašem okolišu. Povedala vam bova tudi, kako pripraviti študijo o obvladovanju tveganja, ki morda ne bo v skladu s strokovnimi standardi, vendar bo zadovoljila vaše potrebe. Pri tem sva veliko črpala iz odličnih smernic (glej okvir), ki jih je oblikoval ASIS International (prej American Society of Industrial Security).

Prvi korak vaje obvladovanja tveganja je ocena tveganja. Pri oceni terorističnega tveganja analiza poskuša odgovoriti na naslednja vprašanja: Katere tarče bi lahko bile napadene in kako? Kolikšna je verjetnost, da bo tarča napadena? Odgovori na ti vprašanji ocenijo ranljivost tarč. Kakšne bi bile tako kratkoročne kot tudi dolgoročne posledice za vaše mesto? Odgovor na to

vprašanje oceni pričakovano izgubo. Odgovori na ta vprašanja torej pomagajo identificirati, ovrednotiti in prednostno določiti tveganja. Obvladovanje tveganja gradi na teh odgovorih pri naslavljanju drugega niza vprašanj. Kakšne ukrepe je mogoče sprejeti za zmanjšanje tveganja napada? Kateri so z njimi povezani dogovori o stroških, koristih in tveganju? Kako bi njihova izbira ovirala prihodnje možnosti? To se imenuje blaženje.

Morda se sprašujete, kolikšna je vrednost študije o obvladovanju tveganja, ki temelji na tem postopku. V zvezi s pripravo potrebnih ocen je na vsaki od sedmih stopenj toliko težav, da bo rezultat nujno negotov in omejen. Čeprav to drži, bo morda vseeno vredno izpeljati postopek, ker vas bo to prisililo v natančen pregled vsake morebitne tarče. Rezultat bo morda nepričakovan, bo pa tudi v pomoč. Morda boste ugotovili, da tarča, za katero vsi mislijo, da je najbolj ranljiva, že ima varnostne mehanizme, ki občutno znižujejo njeno ogroženost. V luči teh informacij boste pozornost usmerili na manj ogrožene tarče, ki niso pripravile minimalnih varnostnih ukrepov.

Več o tem: Department of Homeland Security, National Infrastructure Protection Plan. Washington, D.C., 2006. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

Dewar, James A. Assumption-Based Planning: A Tool for Reducing Avoidable Surprises. New York: Cambridge University Press, 2002.

Smernice ASIS International o splošni varnostni oceni tveganja

Čeprav naj bi bile te smernice v pomoč varnostnim strokovnjakom pri ugotavljanju tveganj v zvezi s kriminaliteto na določeni lokaciji in naj bi prispevale k oceni možnih rešitev, jih je mogoče uporabiti pri oceni tveganja za teroristični napad. Če ne morete najeti strokovnega svetovalca za obvladovanje tveganja, lahko uporabite smernice za pripravo svoje študije, še posebej, če vam pri tem pomaga izobražen varnostni strokovnjak.

Ko boste enkrat identificirali najbolj ogrožene tarče, za vsako uporabite sedemstopenjske smernice. Prilagodila sva opis smernic ukrepom ob grožnji terorističnega napada.

1. **Za vsako tarčo identificirajte ogrožene ljudi in sredstva (lastnina, omrežja in informacije).**
- Ljudje vključujejo vse tiste, ki so povezani s podjetjem in sosednjimi skupnostmi.
- Lastnina vključuje zgradbe in neotipljiva sredstva, kot je intelektualna lastnina.
- Omrežja vključujejo vse sisteme, infrastrukturo in opremo, ki je povezana s podatki, telekomunikacijami in računalniško obdelavo.
- Informacije vključujejo različne vrste zaupnih in zasebnih podatkov.

2. **Natančno navedite vse vrste napadov in ranljivosti.** Teroristični napadi se lahko izvedejo na različne načine (tovornjaki bombe, zaseganje talcev, streljanja) in za vsako zgradbo, ki je ogrožena, poskusite odkriti obliko napada, za katero je ranljiva. Analiza ranljivosti bi morala upoštevati vse, kar bi se lahko izrabilo za izvedbo napada. Ta proces bi moral izpostaviti šibke točke in bo v pomoč pri oblikovanju nadaljnih analiz in protiukrepov.
3. **Ocenite verjetnost vsake oblike napada.** Tu vstopate na področje ugibanja – kjer je najvarnejša ocena nič. Lažje bo razvrstiti oblike napada kakor oceniti verjetnost. Na primer, zbiralnik bo verjetneje okužen kot tarča bombnega napada.
4. **Določite posledice napada.** Določite verjetne posledice napada za vsako tarčo. Poskušajte oceniti verjetno število mrtvih in ranjenih, izgubo lastnine, prekinitev normalnega življenja, stroške reševanja in obnove in čustveni vpliv (predvsem prestrašenost) na skupnost.
5. **Ugotovite možnosti za ublažitev tveganja.** Identificirajte možnosti za preprečitev ali ublažitev škode. Te lahko segajo od pasivnega sprejemanja tveganja prek vrste varnostnih možnosti, vključno z namestitvijo opreme in računalniške strojne opreme, spremembo politik, postopkov in vodstvenih praks ter najemanja in usposabljanja varnostnega osebja.
6. **Preučite izvedljivost svojih možnosti.** Na tej stopnji bi morali upoštevati praktične vidike vsake možnosti ali strategiji. Finančni stroški so pomemben element, vendar je enako pomembno, ali bo strategija močno ovirala delovanje podjetja. Na primer, strogi nadzori dostopanja v nakupovalni center ali stadion lahko ustvarijo negativno ozračje, ki odvrača ljudi od tega, da bi vstopili v objekt. Izziv je najti ravnotežje med trdno varnostno strategijo in operacijskimi

potrebami podjetja ter med vplivom na ljudi, ki jih varnostni program zadeva.

7. **Analizirajte stroške in koristi.** V končnem koraku premislite o stroških in koristih dane varnostne strategije. Določite tako stroške strategije (finančne, vodstvene, socialne in okoljske) kot tudi različne koristi, ne le o zmanjšanju škode, ki bi lahko bila posledica napada, temveč tudi o drugih koristih, kot je zmanjšanje tveganja za kriminal.

Vir: ASIS International, General Security Assessment. An ASIS International Guideline. Alexandira, Virginia, 2003. http://www.asisoneline.org/guidelines/guidelinesgsra.pdf

Napotek 19: Pridobite sredstva za boj proti terorizmu

Subvencijska sredstva vam lahko pomagajo izpolnjevati obveznosti glede priprave na teroristični napad s plačilom opreme, usposabljanja in nadur. Če ste uspešni pri pridobivanju subvencij, se bo vaš celotni proračun močno povečal. Poleg pomoči pri izpolnjevanju obveznosti lahko ta sredstva omogočijo razvoj vaše postaje na načine, kot ste si vedno želeli.

Če boste oblikovali enoto za boj proti terorizmu, je lahko pisanje vlog za podporo in upravljanje s podporo ena od njenih glavnih nalog. S toliko denarja poskrbite, da boste izbrali energičnega in ambicioznega policista za vodenje enote. On ali ona bo zelo zaposlen/a s pridobivanjem in upravljanjem podpore in lahko znatno prispeva k vaši bilanci. Subvencije lahko pritekajo iz zveznih, državnih in zasebnih virov.

Zvezni viri. Zvezne agencije, ki ponujajo protiteroristično podporo, nudijo različne stopnje financiranja, ponujajo različne priložnosti in imajo različne pogoje in postopke prijave. Navajava seznam nekaterih potencialnih virov, viri za nekatere bolj specifične namene pa so podrobno navedeni drugje v tem priročniku.

- **Ministrstvo za domovinsko varnost** (http://www.dhs.gov): DHS vsako leto nudi milijone dolarjev podpore za opremo, tehnično podporo in usposabljanje.
- **Protiterorizem** (http://www.counterterrorismtraining.gov): Ta vir je nastal na osnovi priporočil protiteroristične delovne skupine za usklajevanje usposabljanja ministrstva za pravosodje Združenih držav (U.S. Department of Justice's Counter-Terrorism Training Coordination Working Group). Nudi protiteroristično orodje institucijam kazenskega pregona in prvim odzivnim skupnostim.
- **Subvencija.gov (Grants.gov)** (http://www.grants.gov): Ta vir je nastal na podlagi predsednikove pobude za izboljšanje dostopa javnosti do vladnih služb leta 2002. Agencije kazenskega pregona lahko pregledajo prošnje za subvencije in se prijavijo prek spleta.
- **Državno in lokalno protiteroristično usposabljanje** (http://www.slatt.org): program SLATT je skupen trud FBI in urada za pravosodno pomoč (Bureau of Justice Assistance – BJA). Usklajuje ga inšti-

tut za medvladne raziskave (Institute for Intergovernmental Research) (http://www.iir.com) in zagotavlja specializirano policijsko usposabljanje za spoprijemanje s terorizmom in kriminalnim ekstremizmom.

- **Urad za pravosodno pomoč** (http://www.ojp.usdoj.gov/BJA): BJA je eden od najmočnejših virov zveznega financiranja. Njegov programski oddelek usklajuje državne in lokalne subvencije.
- **Urad za v skupnost usmerjene policijske službe** (http://www.cops.usdoj.gov): Urad za v skupnost usmerjene policijske službe ministrstva za pravosodje Združenih držav (urad COPS) je razširil svojo prvotno vlogo zagotavljanja virov za skupnostno policijsko dejavnost, tako da vključuje tudi zagotavljanje virov za boj proti terorizmu.
- **Nacionalni inštitut za pravosodje (National Institute of Justice)** (http://www.ojp.usdoj.gov/nij): Čeprav nacionalni inštitut za pravosodje ne daje programskih subvencij, izvaja raziskave in vrednoti nepovratna sredstva. Preden se odobri financiranje, se od agencij kazenskega pregona običajno zahteva sodelovanje z raziskovalnimi inštituti ali univerzami.
- **Urad za žrtve zločinov (angl. Office for Victims of Crime)** (http://www.ojp.usdoj.gov/ovc): Urad za žrtve zločinov hitro zagotavlja sredstva za podporo žrtvam zločinov. Tudi ta urad je razširil svojo vlogo, tako da vključuje zagotavljanje sredstev za žrtve terorizma in množičnega nasilja.

Državne subvencije. Državne upravne agencije (State administrative agencies – SAA) so zadolžene za usklajevanje državnega in zveznega financiranja ter za prenos zveznih sredstev na lokalne okoliše. Pooblaščene SAA se razlikujejo od ene do druge zvezne države. V New Jerseyju je pooblaščena SAA Urad za državno varnost in pripravljenost (Office of Homeland Security and Preparedness); v Kaliforniji je to Kalifornijski urad za domovinsko varnost (California Office of Homeland Security). Da bi našli svoj pooblaščeni SAA stik, obiščite http://www.ojp.usdoj.gov/odp/contact_state.htm.

Zasebne fundacije. Agencije kazenskega pregona pogosto spregledajo na tisoče fundacij, ki vsako leto financirajo programska področja. Spletna poizvedba vas bo zasula s tovrstnimi možnostmi; na srečo obstajajo vodila, ki vam bodo pomagala izbrati fundacijo, ki financira programe v vaši zvezni državi in na vašem geografskem področju. Na voljo so pri: Research Grants Guides, Inc., P.O. Box 1214, Loxahatchee, FL 33470 (telefon: 561.795.6129; faks: 561.795.7794). Da bi našli vir financiranja, morate samo pregledati

vodila za posebne kategorije (npr. sredstva za opremo, sredstva za stavbe) in zahtevati vlogo za subvencijo.

Vloga za financiranje. Koraki v okviru priprave vloge za subvencijo običajno vključujejo strateško načrtovanje in sestanke vodstvenega osebja, preden se začne dejansko pisanje. Shema prikazuje rubrike, ki sestavljajo običajno vlogo za subvencijo. Odvisno od lokalnih pogojev in vrste vloge za subvencijo, bi bila vaša razvojna ekipa morda zmožna skrajšati postopek.

Pisanje vloge za subvencijo. Preden začne pisati vlogo, mora vaša ekipa raziskati temo prek spleta. Začne naj z nacionalno referenčno službo za kazensko pravo (National Criminal Justice Reference Service) (http://www.ncjrs.org). Vlogo morate podpreti s statistikami o naravi in obsegu problema, ki ga imate, ter možnimi rešitvami, ki jih želite raziskati.

Statistični podatki morajo biti reprezentativni in zanesljivi; imejte v mislih, da poskušate prepričati ljudi, naj investirajo v vaš program. Vloga za subvencijo mora sama po sebi dosegati strokovne predstavitvene standarde: vključevati mora vse zahtevane oblike z izvirnimi podpisi; biti mora urejena in logična, jezikovno natančna, pravilno slovnično napisana, uporaba ločil naj bo pravilna – ne uporabljajte žargona, ne pišite v prvi osebi in preverite črkovanje besed in slovnico celotnega dokumenta, preden ga izročite v popravek komu drugemu.

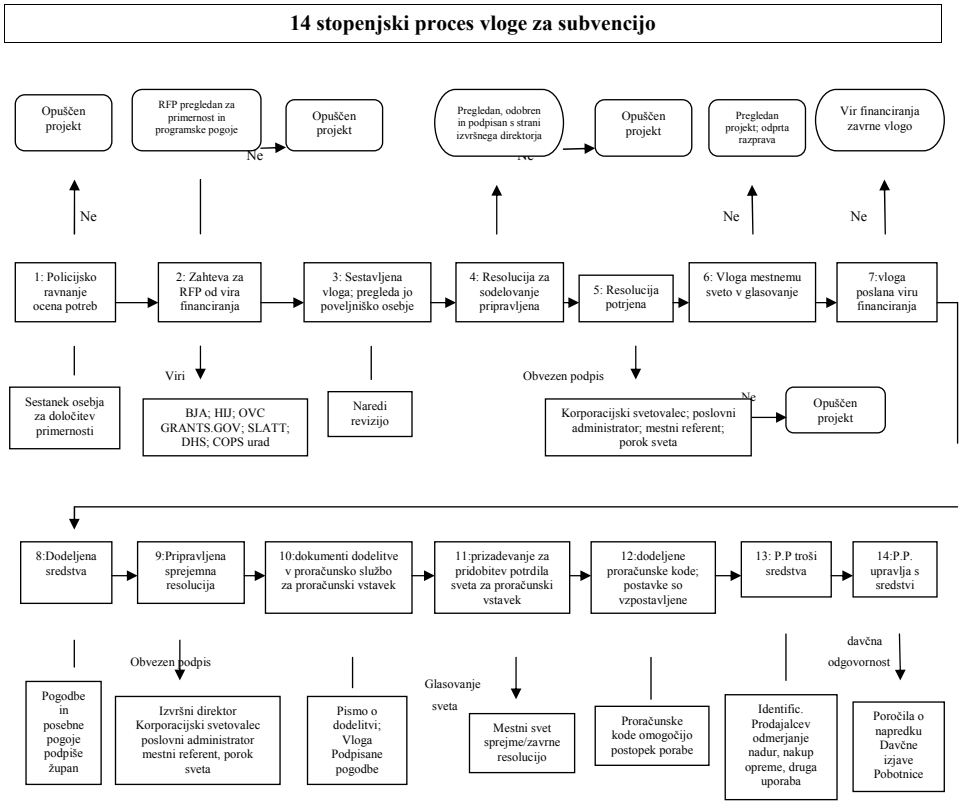
Vsaka vloga za subvencijo mora biti oblikovana v skladu z navodili v zahtevku za predlog (request for proposal – RFP); če ni nobenih navodil, sledite spodnjemu načrtu.

1. **Naslovnica:** vključite ime programa in identifikacijske podatke agencije.
2. **Vsebina:** številke strani se morajo ujemati z vsebino.
3. **Povzetek:** kratek opis vloge za subvencijo in zaprošenih finančnih sredstev.
4. **Navedba problema:** opredelite problem in podprite svoje ugotovitve z ustrezno statistiko
5. **Naloge in cilji:** prepričajte se, da so naloge uresničljive in cilji merljivi.
6. **Programska strategija:** opišite, kaj nameravate narediti in kako nameravate to izpeljati.
7. **Oris proračuna:** poleg izpolnjenih obrazcev za proračun, naj bi oris pojasnil, kako bodo sredstva porabljena in zakaj so potrebna.

8. **Dodatek:** priložite vso dokazno dokumentacijo, vključno s kopijami virov in povzetkov, kot je potrebno.

Upravljanje s sredstvi. Po dodelitvi subvencije mora vaša agencija izpolnjevati določene upravne zahteve za zagotavljanje odgovornosti. Vsak podporni program ima priročnik, ki opisuje upravne in računovodske odgovornosti prejemnika sredstev. Določa tudi enotno terminologijo, pogoje prejema sredstev, način dostopa do sredstev, vzdrževanje finančnih evidenc, zvezne revizijske zahteve, zahtevana poročila in obdobja poročanja, čas prejemanja subvencije in postopke za podaljšanje. Za zagotovitev enostavne uporabe subvencije večina agencij za subvencije ponuja tudi telefonsko podporo za tehnično pomoč.

Več o tem: Shane, Jon M., »Writing a Winning Grant Proposal,« FBI Law Enforcement Bulletin 72. Washington, D.C.: Federal Bureau of Investigation, May 2003.



Analiza tveganj razvoja organizirane kriminalitete in terorizma

Bojan Dobovšek

Obdobje, v katerem smo, opredeljujemo kot čas prehoda, saj ga zaznamujejo procesi ekonomske in politične tranzicije ter vstopanja novih držav v severnoatlantsko zvezo in Evropsko unijo. Pri tem se kot nova vira ogrožanja modernih družb vse pogosteje pojavljata organizirana kriminaliteta in terorizem. Čeprav imamo nacionalne in mednarodne podatke pa akademsko in strokovno literaturo o organiziranem kriminalu, nič od tega ne daje zanesljive slike o realni grožnji organiziranega kriminala (Vander Beken, 2004: 471-472) in terorizma. Problem izhaja že iz različnih definicij, ki povzročajo zmedo in nedoslednosti pri poročanju. Tako lahko resnost pojava različno ocenjujejo odvisno od situacije, od primera, različni avtorji različno (Paoli, 2002). Van Duyne (1996) pravi, da lahko merjenje organizirane kriminalitete in terorizma primerjamo s fantomom in da slike o teh virih ogrožanja ustvarja človeška domišljija. V tem delu se bomo osredotočili predvsem na predvidevanje orgožanj s strani organizirane kriminalitete, znanja in ugotovitve pa veljajo tudi za področje terorizma.

Iz dosedanjih razprav je razvidno, da je težko meriti količino organizirane kriminalitete oziroma jasno odgovoriti na prvi pogled lahka vprašanja, npr.: Ali je organizirane kriminalitete veliko? Kako resna je situacija? Ali je slab znak, da sedaj deluje več skupin organizirane kriminalitete kot včasih? Katere skupine so najbolj nevarne? Itd. Kot omenja tudi Levi (2003), je merjenje sprememb in ocena organizirane kriminalitete še vedno v povojih in ne povsem razdelano in uspešno. Za podrobnejšo predstavitev stanja smo analizirali delo Vander Bekena (2004), ki temelji na dveh belgijskih študijah, katerih namen je bil oblikovati metodologijo, s katero bo mogoče opravljati boljše raziskave in dobiti natančnejše ugotovitve o kvantiteti in kvaliteti organizirane kriminalitete po svetu. Namen tega dela je med drugim tudi olajšati oceno situacije glede ogrožanja sveta s strani organizirane kriminalitete, kar bo v pomoč zakonodajnim oblastem po svetu, da bodo lahko določale prednostne naloge in prave preventivne ukrepe pri kreiranju kriminalitetnih politik.

Ena izmed rešitev, kako zaobiti težave pri merjenju organizirane kriminalitete je, da analiziramo tveganja. Tveganje poznamo v poslovanju vseh industrijskih panog. Pogosto česa ne moremo narediti, ne da bi pri tem tvegali. Analiza tveganja na podjetniški ravni priskrbi vodstvu informacije, ki podpirajo odločitveni proces. Te analize so lahko kvalitativne ali kvantitativne. Pogosto so analize tveganja ocene tveganja in tveganega vodenja. Namen ocene tveganja je zagotoviti razumevanje dejavnikov, ki vplivajo na interesne dogodke pri stranki. Tako ocena tveganja omogoča analizo ekonomskega ravnotežja med tveganjem v podjetju in stroški izvedbe preventivnih in zaščitnih merjenj (Broder, 2000 v Vander Beken, 2004).

Stalnost analize tveganj in tveganosti pri ocenjevanju so začeli raziskovati tudi v obveščevalni dejavnosti znotraj policijskih in drugih varnostnih institucij. Na primer, Europol je identificiral oceno tveganj kot metodo, ki bo omogočila razvoj proaktivnega pristopa k informiranju policijskih enot. Po Europolovih navodilih za analitično delo je cilj ocenjevanja raziskovanje področij v družbi, kjer naj bi bile dejavne organizirane kriminalne skupine, pri tem pa bi indentificirali področja, ki so najbolj tvegana za nadaljnji razvoj takih skupin. Tako lahko definiramo tveganje kot možnost, da se bo nekaj zgodilo, kar bo vplivalo na nek objekt (objekt v tem smislu lahko pomeni tako osebo, predmet, pojem itd...) (Vander Beken, 2004).

Pri merjenju organizirane kriminalitete razumemo ocenjevanje tveganja kot sistematično analiziranje socio-ekonomskih in političnih spremenljivk in njihovih potencialnih vplivov na organizirano kriminaliteto. Kakovostno ocenjevanje tveganja omogoča identifikacijo trenutnih pogojev, ki vplivajo na organizirano kriminaliteto, saj opisuje in analizira okoliščine, v katerih pride do težav. Je orodje za povezovanje vzrokov ogrožanja z mogočimi posledicami. The Risk assessment Matrix (REM) - matrica za ocenjevanje tveganja (MOT), ki jo predlaga Vander Beken (2006), je orodje s katerim lahko primerjamo možne vire ogrožanja in s katerim lahko ocenjujemo tveganje.

Verjetnost ogrožanja s strani organiziranih kriminalni skupin (threat) je funkcija namena (intent) in sposobnosti (capability) identificiranih akterjev, da bi dosegli določen cilj. Namen se nanaša na »verjetnost poželenja, želje (desire) subjekta, da se bo lotil neke aktivnosti in na njegovo samozavest, da bo pri tem uspešen«. Sposobnost ali zmožnost pa je funkcija

razpoložljivih virov in znanja, ki jih ima subjekt za dosego ciljev. Vsakemu elementu (desire, resources, intent itd.) lahko dodelimo vrednost – ki je lahko kvalitetna ali kvantitena. Po tem modelu lahko ocenjujemo tveganje pri katerem koli pojavu. Pri tem pa je treba paziti, da je vsaka vrednost, ki jo vnašamo, oziroma vsak podatek, ki ga uporabljamo pri MOT, relevanten in točen. Kot vidimo, ima vsak atribut osnovo in merske potrebe za uspešno izvajanje podjetništva. MOT tako zagotavlja osnovo za razvoj širšega spektra policijskih strategij. Tako lahko policija in druge varnostne institucije vplivajo na vse štiri atribute, ki določajo namen in sposobnost delovanja. Na primer, neka skupina je lahko znana po tem, da ima močno željo in ustrezno raven samozavesti, da bo izvedla oziroma dosegla nek cilj. Podatki tudi nakazujejo, da ima potrebne vire in znanje za to. Zaključimo lahko, da je ta kriminalna skupina v primerjavi z neko drugo bolj ogrožajoča. Pri tem je ogrožanje lahko ekonomsko, čustveno, psihično, intelektualno in politično (Vander Beken, 2006).

Temelj metode MOT je v tem, da lahko razporedimo ogrožanje organizirane kriminalitete po nekem vrstnem redu, od večjega ogrožanja proti manjšemu, in se posvetimo najprej tistim ogrožanjem, ki jih ocenimo za večja. Vander Beken navaja tudi primere, pri katerih so uporabljali opisani model – MOT: primer Sleipnir, Kraljeva kanadska gorska policija, kot ga navaja Klerksa itd. (2000). Predlagano orodje temelji na treh ključnih domnevah: a) organizirani kriminal je poslovno motiviran z željo po finančnem dobičku, b) merjenje ogrožanja zahteva temeljito sliko okolja, v katerem kriminalna skupina deluje, c) metoda mora biti za uporabo čimbolj enostavna. Tako metoda temelji na analizi okolja (zbiranje in procesiranje informacij o okolju, v katerem skupine delujejo), oceni znanih organiziranih skupin, ki se ukvarjajo z organizirano kriminaliteto in njihovih protistrategij ter analizi zakonitih in nezakonitih trgov (tekmovanje med znanimi skupinami, število podjetij, število in vrste potencialnih vstopov v podjetje, ki vzpodbujajo dobičkanosnost, moč barantanja, dinamika poslovanja itd.) Za definicijo nelegalnega trga smo uporabili definicijo po Arlacchiju (1998), ki opredeljuje ilegalni trg kot prostor, v katerem se dobrine in storitve izmenjujejo in večina držav v svojih zakonodajah prepoveduje njihovo produkcijo, ponudbo in povpraševanje.

Projekt se idejno nadaljuje na evropski ravni s strani organizacije EDGE (tj. evropski interdisciplinarni analitski projekt) v sodelovanju z AGIS (institucijo, ki je podala zasnovo za projekt OCO). Projekt poteka v smeri razvijan-

ja metodologije, ki bi preučevala pretok kriminalnega denarja[23]. Projekt so razdelili na tri faze (Schulte in sodelavci, 2007: 6 – Project documents):

1. nacionalni in mednarodni tokovi kriminalnega denarja – popis s strani evropskih policij,
2. nacionalni in mednarodni tokovi kriminalnega denarja – ugotavljanje razvijanja do leta 2012,
3. ocena uporabljene metodologije scenarijev.

Kot lahko opazimo iz navedenih faz projekta, se nanašajo vse bolj ali manj na finančni pretok kapitala – želi se najti rešitev na vprašanje finančnega ozadja organizirane kriminalitete v povezavi s predpostavko, da ta izvira iz težnje po dobičku in da je posledično primorana v pranje tako pridobljenega denarja. Rezultat prve faze projekta naj bi bil priročnik, namenjen evropskim policijam o dokumentaciji in poznavanju povezav pretoka kriminalnega denarja, kar je skladno s celotno strukturo tega dela.

Ugotovitve projekta kažejo na večjo potrebo varnostnih organov po podatkih o pranju denarja. Prost pretok dobrin nakazuje trend pošiljanja večje količine denarja čez državne meje. Da bi se omejilo tako kriminalno delovanje, se predlaga dve poti:

– zmanjševanje administrativnih in drugih omejitev pri pregledu dejavnosti imigrantov;
– intenzivnejše varnostno pregledovanje na državnih mejah. (Schulte in sodelavci, 2007: 63, 64 – Volume 1)

Analiza raziskav pokaže, da je merjenje organizirane kriminalitete in terorizma brez jasnega koncepta in metodologije zelo tvegano. Takšna merjenja bolj prikazujejo dojemanje organizirane kriminalitete in terorizma v družbi, ne pa dejanskega stanja. Kljub temu pa so rezultati uporabni za oblikovalce politik boja proti kriminaliteti in terorizmu, če se le zavedajo omejitev in slabosti takšnih merjenj. Zaradi navedenega je cilj raziskovanja razviti metodološki okvir merjenja, ki bo omogočil odgovore za prihodnost. Dosedanje analize kažejo, da je pri analizi organizirane kriminalitete in terorizma treba upoštevati ekonomski položaj v družbi in opredeliti

[23] Prav pranju denarja in sledenju denarnih tokov je v zadnjem času dan največji poudarek v boju s terorizmom.

legalni in ilegalni trg, vlogo vpletenih na trgih ter se posvetiti metodologiji, temelječi na analizi tveganj, saj se organizirana kriminaliteta v času in prostoru spreminja.

RAZPRAVA

Rezultati so pokazali, da je ocena nevarnosti in obsega organizirane kriminalitete in terorizma arbitrarna in je namenjena predvsem operativni analizi, manj pa strateški analitiki z upoštevanjem drugih dejavnikov, ki vplivajo na določene oblike kriminalitete. Sodobne teorije o organizirani kriminaliteti izhajajo iz ekonomskih analiz dojemanja organizirane kriminalitete, za kar je potrebno podrobno analizirati tako legalni kot ilegalni trg. Najbolj kritični rezultat pri poskušanju razumevanja in analiziranja organizirane kriminalitete dobimo z upoštevanjem ekonomsko-podjetniškega vidika ocenjevanja organizirane kriminalitete pri ocenjevanju trgov. Iz navedenega lahko sklepamo, kako sta organizirana kriminaliteta in trg povezana, ter da moramo, če želimo izboljšati boj proti organizirani kriminaliteti, pri izbiranju strategij upoštevati, da je bolje spreminjati pravila trga kot pa le odstranjevati člane oziroma udeležence na trgu. Prav tako je pri pregonu tovrstne kriminalitete potrebno poleg tožilstva in policije pridobiti tudi finančne institucije, ki lahko nadzorujejo transakcije na trgih.

V nekaterih državah se je ilegalni trg izmaknil državni kontroli in ga ni mogoče nadzorovati. Kot vemo, so gospodarstva Tajske, Singapura in Hong Konga doživela razcvet prav zaradi vpliva denarja, pridobljenega s trgovanjem z drogo. Prav zato se večkrat zagovarja stališče, da je tudi umazani denar denar in da kot tak spodbuja gospodarstvo. Če si pobliže ogledamo gospodarsko situacijo v takšnih državah, lahko ugotovimo, da dotok kriminalnega denarja vodi v renominacijo lokalnih denarnih enot in s tem v inflacijo, spodbuja spekulativno investiranje, v državi se ustvarja nasilno vzdušje, kar negativno vpliva na tuje vlagatelje, kriminalne organizacije začno kapital vlagati v še dobro stoječa podjetja, ki jih nato uporabljajo za tihotapljenje droge, zato se država postopno umika s svetovnega gospodarskega in finančnega trga.

Kot vidimo, z vlaganjem v legalna podjetja ali z ustvarjanjem svojih podjetij organizirani kriminal vpliva na celotno gospodarstvo države. Ustvarja

se ilegalni trg kot vzporedni sistem trgu, ki ga nadzoruje država s svojo politiko. Organizirana kriminaliteta vzpostavi namesto trga, ki ga je prepovedala država, ilegalni trg, nad katerim ima monopol. Legalni in ilegalni trg sta med seboj tesno povezana. Spremembe, ki jih narekuje politika na legalnem trgu, se nujno odražajo tudi na ilegalnem trgu, ki ga nadzorujejo kriminalne organizacije. Iz tega sledi, da tisti, ki kreirajo varnostno politiko, ne morejo mimo dejstva, da poleg legalnih trgov obstajajo tudi ilegalni trgi. Ker se na takšnih trgih obračajo velika sredstva, ki jih ni moč natančno nadzorovati, so vprašljive vse primerljive statistike, ki temeljijo na uradno pridobljenih podatkih. Pri obravnavi gospodarskih značilnostih posameznih držav se srečujemo s problematičnimi kazalci, ker so primerjave večkrat nepregledne in slabo primerljive.

Poleg prehoda organizirane kriminalitete na področje gospodarstva raziskovalce tovrstne kriminalitete zanima predvsem prihodnost razvoja te kriminalitete in v ta namen razvijajo orodja, ki temeljijo na teorijah tveganja. Cilj je oblikovati tako metodologijo, s katero bo mogoče ugotavljati družbene trende, ki vplivajo na razvoj organizirane kriminalitete, in omogočiti zbiranje in obdelavo podatkov, ki se nanašajo na družbene vzroke za organizirano kriminaliteto. Tako bi prispevali k usklajevanju kriminalitetnih politik ter oblikovanju proaktivnih strategij odzivanja na organizirano kriminaliteto v EU in tudi širše. Po mnenju raziskovalcev zgornje ugotovitve veljajo tudi za terorizem, ki vse bolj posega v mednarodne denarne tokove.

LITERATURA IN VIRI:

- *Arlacchi, P. (1998). Some Observations on Illegal Markets, in V. Ruggiero (ed.), The New European Criminology: Crime and Social Order in Europe. London, Routledge.*
- *Broder, J. (2000). Risk Analysis and the Security Survey (2nd ed.). Boston: Butterworth, Heinemann.*
- *Klerks, P., Groot in de Hasj. (2000). Theorie en Praktijk van de Georganiseerde Criminaliteit. Rotterdam: Doctoral Thesis Erasmus Universiteit Rotterdam.*
- *Levi, M. (2003). The Organization of Serious Crimes, in M. Maguire, R. Morgan and R. Reiner (Eds.). The Oxford Handbook of Criminology. Oxford, Oxford University Press.*

- *Paoli, L. (2002). The paradoxes of organized crime, Crime Law and Social Change.*
- *Schulte, T. (vodja projekta), Boberg, M., El-Samalouti, P., Mähs, S., Mönnikes, M., Mückenhausen, F., Velten, T. (2007). Project documents: Criminal Money Management: Project outline and Questionnaire. A European Interdisciplinary Analysis Project - EDGE.*
- *Schulte, T. (vodja projekta), Boberg, M., El-Samalouti, P., Mähs, S., Mönnikes, M., Mückenhausen, F., Velten, T. (2007). Volume 1-First Results: Criminal Money Management: A manual about present methods of money transfers with criminal background. A European Interdisciplinary Analysis Project - EDGE.*
- *Vander Beken, T. (2004). Risky business: A risk-based methodology to measure organized crime. Crime, Law & Social Change. Netherlands.*
- *Vander Beken, T. (2006). European Organised Crime Scenarios for 2015. Maklu Publishers, Antwerpen/Apeldoornrime, Belgium.*
- *Van Duyne, P. (1996). "The Phantom and Threat of Organized Crime," Crime Law and Social Change.*

IV.

Zbiranje podatkov

Napotek 20: Pomagajte FBI – pridružite se skupni lokalni protiteroristični projektni skupini

Ministrstvo za pravosodje ZDA je ustvarilo raznovrstne protiteroristične projektne skupine in svete za izboljšanje izmenjave informacij. Kar zadeva vas, so med njimi najbolj pomembne Skupne protiteroristične projektne skupine (Joint Terrorism Task Forces – JTTF). Zdaj jih je več kot 100 po vsej državi, vključno s 56 območnimi izpostavami FBI. Čeprav je prvi JTTF nastal pred 11. septembrom, je njihovo število od napada močno naraslo. Njihova naloga je usklajevati prizadevanja agencij kazenskega pregona za odkrivanje, preprečevanje in odzivanje na teroristične napade na zvezni, državni in lokalni ravni. Primarno preiskovalne in analitične agencije, JTTF zaposlujejo preiskovalce FBI-ja, agente zveznih agencij, kot sta Urad za alkohol, tobak, strelno orožje in eksploziv (Bureau of Alcohol, Tobacco, Firearms and Explosives – ATF) in Urad za priseljevanje in carino (Bureau of Immigration and Customs Enforcement – ICE) ter detektive lokalnih policij in šerifovih uradov. JTTF so zaslužni za različne uspehe, vključno z aretacijo in obsodbo teroristov, ki so pripravili prvi napad na Svetovni trgovinski center leta 1993, ter tako imenovanega bombaša čevelj (shoe bomber), Richarda Reida.

Če je FBI-eva območna izpostava v vašem okolišu ali blizu njega, skoraj zagotovo že pripadate JTTF. Podobno je, če vodite veliko postajo. Če pa imate majhno, podeželsko enoto na območju, za katero je malo verjetno, da bo pritegnila pozornost teroristov, je možnost, da pripadate JTTF ali da bi s pridružitvijo eni od njih pridobili veliko korist, majhna. Priključitev JTTF je težka odločitev za postaje srednje velikosti, ki služijo mestom ali manjšim velemestom, oddaljenim od prejšnjih terorističnih dejavnosti. V praksi priključitev JTTF pomeni napotitev enega ali več vaših detektivov na delo v JTTF, in sicer polni delovni čas; naloge s krajšim delovnim časom

niso priporočljive, ker policist ne more polno sodelovati pri delu JTTF. Po priključitvi JTTF bo vaš policist imenovan za agenta FBI. FBI plačuje nadure in nudi potrebno opremo in potrebščine; vendar pa vaša postaja še naprej financira policistovo plačo. To je precejšnje breme glede sredstev za vašo postajo. Poleg tega se od policistov, ki so dodeljeni JTTF, pričakuje, da bodo ostali vsaj eno leto, ker lahko traja 6 mesecev ali več za pridobitev dovoljenja za dostop do strogo zaupnih podatkov.

Glavna korist sodelovanja v JTTF je sodelovanje pri ustvarjanju države, ki je varnejša pred napadi. Sodelovanje pomaga FBI-ju v preiskavah, ki bodo nekega dne morda povezane s primerom na vašem območju. Malo je verjetno, da boste s sodelovanjem v projektni skupini dobili kakršnokoli zgodnejše opozorilo o resni teroristični ogroženosti, kakor bi ga prejeli sicer; prav tako vam sodelovanje ne bo v veliko pomoč v malo verjetnem primeru napada. Za to obstajajo različni razlogi. Prvi in glavni razlog je, da vas bo FBI nemudoma obvestil o kakršnikoli resni grožnji na vašem območju ne glede na to, ali sodelujete v JTTF ali ne. Drugi razlog je, da vam vaš predstavnik v JTTF ne more vedno zaupati informacij, še posebej, kadar so informacije strogo zaupne. Tretji razlog, ki ga je izpostavil William Bratton in tudi drugi, JTTF vključuje primarno preiskovalne agencije. Z drugimi besedami JTTF ne izmenjuje obveščevalnih podatkov FBI z drugimi agencijami. Da bi zadovoljili to potrebo, je FBI nedavno začel ustanavljati terenske obveščevalne skupine (Field Intelligence Groups) v vseh 56 območnih izpostavah

Dovoljenje za dostop do zaupnih podatkov se je včasih izkazalo za oviro pri operacijah JTTF. Ne le, da je lahko postopek za pridobitev dovoljenja za dostop do strogo zaupnih informacij izredno dolgotrajen (iz razlogov, ki so opisani v okvirju 1), temveč se to lahko odraža tudi v strokovni zavisti, če ima terenski policist JTTF dovoljenje do zaupnih podatkov višje stopnje kakor njegov predstojnik. Resnično se je zgodilo, da je tak položaj vodil v umik predstavnika policijske agencije iz lokalne JTTF. Leta 2005 se je Portland v Oregonu umaknil iz lokalne JTTF, ker FBI ni želel dovoliti dostopa do strogo zaupnih podatkov mestnemu pravnemu zastopniku (glej okvir 2). Župan je želel pridobiti to dovoljenje, ker je trdil, da brez njega ne bi mogli ugotoviti, ali njegovi predstavniki v JTTF ustrezajo zahtevam stroge zakonodaje zvezne države s področja državljanskih svoboščin.

Okvir 1: Dovoljenje za dostop do strogo zaupnih podatkov

Poleg preverjanja rojstnih podatkov, izobrazbe, bivališča, zadolženosti, zaposlenosti in dokumentov o vojaški službi, je treba opraviti tudi osebne razgovore s kandidati, delodajalci, sosedi, družabniki in referenčnimi osebami. Neskladja in neugodne informacije je treba preiskati in razrešiti.

Okvir 2: Mestni odpoklic iz JTTF

Aprila 2005 je Portland v Oregonu postal prva enota v državi, ki se je umaknila iz JTTF. To se je zgodilo po mesecih nesoglasij med mestom in FBI zaradi želje mesta po nadzoru nad portlandskim policistom, ki je bil dodeljen JTTF. Znano je, da je Portland liberalen, vendar je za razumevanje te odločitve treba razjasniti nekaj ozadja. Septembra 2002 je *The Portland Tribune* razkril ogromno število dokumentov o aktivistih od 1960. do 1980. let, ki jih je hranila portlandska policija. Leta 1981 je bil sprejet državni zakon, ki od mesta zahteva, da prekine preiskovanje aktivističnih skupin brez utemeljenega suma o vpletenosti v kriminalne dejavnosti in uniči vse zapise o tem. Ne le, da dokumenti niso bili uničeni, temveč je mesto še naprej obdržalo dokumente, navkljub temu, da zakon narekuje drugače.

Ne dolgo za tem je FBI aretirala lokalnega muslimanskega duhovnika, Mohameda Abdirahmana Kariyea, za katerega je trdila, da je imel sledi TNT na prtljagi, želel pa se je vkrcati na letalo na portlandskem mednarodnem letališču. Testi so kasneje pokazali, da na potovalki ni bilo sledi eksploziva. Nato je FBI aretirala zaradi sodelovanja v bombnem napadu v Madridu marca 2004 še enega Portlandčana, Brandona Mayfielda. Mayfield, odvetnik, ki je prestopil v islam, je obiskoval isto mošejo kot Kariye. FBI je trdila, da se Mayfieldovi prstni odtisi ujemajo s tistimi na torbi, ki so jo našli v bližini napadene železniške postaje. Španska državna policija je FBI-ju jasno povedala, da to ne drži; ko je bil na podlagi istih prstnih odtisov kasneje aretiran državljan Alžirije, so Mayfielda izpustili brez obtožbe. S skoraj neprecedenčno potezo je

zvezna oblast pozneje Mayfieldu plačala 2 milijona dolarjev odškodnine in se uradno opravičila odvetniku in njegovi družini.

Prav ta zgodovina policijskih izgredov in šušmarjenje preiskovalcev FBI-ja je botrovalo nezadovoljstvu Portlanda z JFFT. Zadeva je dosegla vrhunec z izvolitvijo novega župana, Toma Potterja, nekdanjega policijskega vodje, ki je dosledno izražal nezadovoljstvo zaradi mestnega dogovora z JFFT. Kot je običajno, je Portlandov JFFT predstavnik dobil dovoljenje za dostop do strogo zaupnih podatkov, vendar tisti, ki so podpisovali njegov plačilni list, tega dovoljenja niso imeli, zato niso mogli nadzirati uradnih dejavnosti svojega zaposlenega. Potterjev poskus, da bi popravil situacijo, je propadel, ko je FBI odklonil dodelitev mestnemu pravnemu zastopniku enak dostop do zaupnih podatkov, kot ga je imel predstavnik Portlanda pri JFFT. Tako župan ne bi mogel ugotoviti, ali so dejanja njegovega policista v skladu z državnimi zakoni glede državljanskih pravic, ki so strožji od enakih zakonov na zvezni ravni.

Vir: Kershew, Sarah, »In Portland, Ore., a Bid To Pull Out of Terror Task Force,« The New Nork Times, April 23, 2005.

Napotek 21: Vedite, zakaj ne rabite vedenjskega profiliranja

Vsak policijski načelnik ve, da je rasno profiliranje nezakonito in zelo netočno. Čeprav je res, da so tuji teroristi najpogosteje mladi moški iz muslimanskih držav, večina takih posameznikov v Združenih državah nima ne terorističnega znanja ne želje po napadu. Zato iščejo načine za zoženje iskanja. Eden od njih je vedenjsko profiliranje, ki poskuša odkriti znake laganja ali izmikanja pri izpraševanih osumljencih. Problem tega pristopa je, da smo vsi nekoliko izurjeni v prevarah; celo najbolj pošten med nami je navajen reči, kako močno uživa na dolgočasni svečani večerji ali da mu je všeč grozno darilo za rojstni dan. Take vrste bele laži gladijo družbene interakcije. Da jih lahko izrečemo, moramo nekaj vedeti o igri – ali vsaj, kako prikriti svoje občutke. Ko laži postanejo resnejše – staršem, delodajalcem, zakoncem – se moramo bolj potruditi, da smo videti iskreni. In narobe, da bi se zavarovali pred zavajanjem, se naučimo prepoznavati izdajalske znake: zardevanje, izogibanje očesnemu stiku, jecljanje, nedosledne zgodbe itd.

Državljani rutinsko lažejo policiji, vendar policija hitro prepozna običajne izgovore (»Nisem videl stop znaka«; »Še vedno je gorela zelena luč«; » Pozabil sem plačati«) in verjame, da lahko na podlagi obnašanja osebe ugotovi, kdaj ta laže. Četudi policist lahko razloči med resnico in izmišljotino v vsakdanjih interakcijah z državljani, je to veliko težje, ko se o resnih zločinih zaslišuje utrjene kršitelje. Kršitelji so verjetno bolj spretni lažnivci, ki lahko veliko več izgubijo, če jih ulovijo. Ti znajo nadzorovati svoja čustva in skriti svoje občutke. Zato policija išče načine, kako spregledati te zvijače in razkriti laži. Tako se je na tisoče policijskih preiskovalcev izurilo v Reid tehniki razgovorov in zasliševanja, ki je namenjena pomoči pri razlikovanju resnice od laži; s tem namenom se vsak dan izvede veliko število poligrafskih razgovorov.

Tako tehnika Reid kot tudi poligraf se opirata na zaznana znamenja anksioznosti med izpraševanjem: pri uporabi poligrafa z merjenjem fizioloških odzivov kože, ki kažejo na stres; pri uporabi tehnike Reid z natančnim opazovanjem telesnih gibov in značilnosti govora (npr. višina in hitrost). Obe tehniki se uporabljata v razgovorih v formalnih okoliščinah in nista primerni za terenske razgovore; vendar je teroriste mogoče srečati na te-

renu, ko si ogledujejo tarče ali se odpravljajo na misijo in bilo bi zelo koristno spregledati njihove zgodbe. Na primer, tri izmed ugrabiteljev letal 11. septembra je policija izprašala med rutinskimi kontrolami prometa, vendar nihče od njih ni vzbudil posebnega suma. Po drugi strani so v Alžiriji rojenega Ahmeda Ressama, tako imenovanega milenijskega bombnega napadalca, prejeli v Port Angelesu v Washingtonu 14. decembra 1999, ko je poskušal pretihotapiti opremo za izdelavo bombe čez kanadsko mejo. Med rutinskim izpraševanjem je carinska agentka Diana Dean postala sumničava, ker se ji je Ressamov potovalni načrt zdel nenavaden, on sam pa je bil nekomunikativen, nemiren in je deloval nervozno.

Aretacija Ressama odpira mikavno možnost, da bi policisti, izurjeni za odkrivanje take vrste znakov, kot jih je opazila Diana Dean, v okviru rutinskih izpraševanj lahko odkrivali teroriste. **To je obljuba vedenjskega profiliranja: iskanje znakov živčnosti na izrazih obraza, majhne spremembe v drži in nenavadno govorjenje ali kretnje rok.** Izraelske varnostne sile že vrsto let uporabljajo vedenjsko profiliranje na letališču Ben Gurion v Tel Avivu, kjer še nikoli ni bilo kako letalo ugrabljeno. To je spodbudilo, da milejšo različico izraelskega postopka ocenjujejo na letališču Logan v Bostonu, vzletni točki dveh letal, ki sta se zaleteli v Dvojčka. Vendar pa je vedenjsko profiliranje le eden od elementov izraelskega uspeha: uporablja se v kombinaciji z natančnimi obveznimi pregledi vsakega potnika in temeljitimi razgovori o njegovih razlogih za potovanje.

Čeprav je delo profesorja Paula Ekmana z Univerze v Kalifoniji v San Franciscu do neke mere dokazalo učinkovitost vedenjskega profiliranja, celo on sam izraža zadržke pred uporabo izključno tega postopka. Več kot 40 let profesor Ekman raziskuje odnos med izrazi na obrazu in čustvi. Zabeležil je več kot 10.000 možnih kombinacij premikov obraznih mišic, ki odražajo občutke. Spoznal je, kako ujeti neželene »mikroizraze«, ki migetajo po obrazu, ko oseba laže. Na žalost, lahko le redki ljudje brez njegovih dolgoletnih izkušenj natančno zaznajo te mikroizraze. Večina skupin, ki jih je poučeval, vključno s policijo, je bilo le malo uspešnjših od naključne skupine pri zaznavi izrečene laži. Agentje tajne službe ZDA so se bolje odrezali kot ostale skupine, vendar je bila tudi njihova natančnost le 10 odstotkov boljša od naključja.

Čeprav se z intenzivnim usposabljanjem policisti lahko naučijo zaznavati laži, lahko urjenje ljudem tudi pomaga zakriti anksioznost, kadar lažejo. V

vsakem primeru pa ima anksioznost pri izpraševanju številne izvore. Oseba, ki govori resnico, na primer, se lahko boji policije ali se samo boji, da mu ne bodo verjeli. Lahko je zamenjati anksioznost z lažjo, napaka, ki jo je Ekman poimenoval »Otelova napaka« (glej okvir). Otelova napaka ne le, da postavlja pod vprašaj nespornost vedenjskega profiliranja, temveč tudi nespornost poligrafa, ki prej zaznava anksioznost kakor laž. Dejansko, znanstveno preučevanje ni podprlo trditve o zmožnosti poligrafa, da je sposoben zaznati laž, kljub temu pa je še vedno lahko dragocen dodatek pri zasliševanju, še posebej, kadar kršitelji verjamejo, da je natančen.

Otelova napaka

V Shakespearovi drami Otelo po krivem obdolži svojo ženo, Desmondo, nezvestobe in ji zagrozi, da jo bo ubil. Otelo si narobe razlaga njen prestrašen izraz kot posledico krivde in umori nesrečno žensko.

Le malo je razlogov za predpostavko, da je policiste mogoče usposobiti za zaznavanje laži teroristov v okviru rutinskega patruljiranja. Ob hkratni majhni verjetnosti, da bo neki policist srečal terorista, to nakazuje, da ni smotrno investirati v tovrstno usposabljanje policistov. Bolje bi bilo zagotoviti, da so vaši policisti pozorni na sumljivo vedenje, kot sta postopanje v bližini ali poskus nezakonitega dostopa do pomembnih objektov. To ne pomeni, da cariniki, letališki selektorji in drugi, za katere je bolj verjetno, da bodo v okviru svojega rutinskega dela naleteli na teroriste, s tovrstnim usposabljanjem ne bi nič pridobili. Čeprav koristno, 9-tedensko usposabljanje, kakršnega so deležni skrbno izbrani izraelski varnostni uslužbenci na letališču Ben Gurion, z vidika stroškov verjetno ne bi bilo učinkovito.

Več o tem: Schubert, Siri, »A Look Tells All,« Scientific American Mind, October/November 2006.

Napotek 22: Spodbujajte policijsko dejavnost na osnovi obveščevalnih informacij – vendar se zavedajte njihovih omejitev

Akademski komentator, Vincent Henry, pravi: »Večina policistov, določenih za patruljiranje in naloge pregona, dnevno neuradno zbira, analizira in širi informacije s področja kriminalitete. Policisti v interakciji z javnostjo, občasno ali aktivno pridobivajo informacije o soseskah in ljudeh, ki v njih živijo, in jih običajno na nek način osnovno analizirajo, da bi bolje razumeli dogajanje v skupnosti in njihove težave s kriminalom. V številnih primerih izmenjujejo te osnovne obveščevalne informacije z drugimi člani agencije.«

Policijska dejavnost na osnovi zbranih podatkov je poskus izrabe tega rutinskega dela ne le za njen tradicionalni namen - reševanje problemov v zvezi s kriminaliteto, temveč proaktivno, za preprečevanje ali odvračanje od kaznivih dejanj in zdaj tudi od terorizma. Za to se uporabljajo računalniški sistemi, ki zbirajo in strukturirajo osnutke informacij v enostavno dostopne oblike. V tej obliki so osnutki informacij primerjalni podatki; podatki pa niso obveščevalne informacije. Da bi postali obveščevalne informacije, jih morajo analizirati usposobljeni policisti z znanjem in izkušnjami, ki nato priporočajo ustrezne ukrepe na podlagi vzorcev v podatkih. Na primer, opazijo lahko številne manjše nakupe materiala za izdelavo bombe in povežejo začetek nakupov s prihodom sumljive skupine na območje. Te obveščevalne informacije se potem lahko uporabi za določitev skupine za intenzivni nadzor in za prošnjo trgovinam, da vodijo sistematičen zapisnik o tovrstnih nakupih. Obveščevalne informacije je mogoče uporabiti tudi za podporo zakonodaji, ki naj oteži nakup tovrstnih kemikalij.

Izraz policijsko delovanje na podlagi obveščevalnih informacij (intelligence-led policing) je skoval Kent Constabulary v Združenem kraljestvu, ki je razvil ta koncept kot odgovor na velik porast vlomov in tatvin avtomobilov v času zmanjševanja policijskih proračunov. Višji vodstveni delavci so verjeli, da je za številne od teh kaznivih dejanj odgovorno majhno število posameznikov in da bi bilo stopnjo kriminalitete najbolje znižati z ustanavljanjem obveščevalnih enot, ki bi odkrivale kršitelje. Za te enote so dobili sredstva, ko so zmanjšali odzive na klice na pomoč. V treh letih je obseg kriminalitete upadel za 25 odstotkov. Policijsko delovanje na podlagi informacij je zdaj osnova nacionalnega obveščevalnega modela (National

Intelligence Model), ki je vzpostavil nove standarde zbiranja in obdelave podatkov v 43 policijskih skupinah v Združenem kraljestvu.

V Združenih državah je policijska dejavnost na osnovi obveščevalnih informacij pritegnila pozornost kot način »povezovanja točk« (connect the dots), fraza, ki jo je popularizirala komisija 11. septembra. Z drugimi besedami, to je način kombiniranja nepovezanih informacij o terorističnih dejavnostih, ki postanejo smiselne šele, ko se obravnavajo skupaj. Policijska postaja v New York Cityju je vodilna v policijskih dejavnostih na osnovi tovrstnih informacij v boju proti terorizmu. Ima več kot 1000 policistov za protiterorizem, ima najete obveščevalne in protiteroristične strokovnjake, ima policiste, ki tekoče govorijo številne jezike, spremlja poročevalske službe in obveščevalna poročila in ima celo svoje agente v državah, ki so žarišča terorizma. Nobena druga domača policijska postaja se ne more primerjati s takimi naložbami, četudi številne velike postaje z več sto ali morda več tisoč policisti imajo organizirano obveščevalno dejavnost. Potrebna je le računalniška baza podatkov, obveščevalni policisti in analitiki ter obveščevalni vodja – čeprav se vse to navadno prej uporablja za podporo preiskovanju, kakor za usmerjanje operacij.

Nekatere od preostalih 17.000 postaj v državi, ki imajo na ducate do stotine zapriseženih zaposlenih, bi bile zmožne razviti obveščevalno dejavnost za notranjo rabo, toda tiste z manj osebja ne zaposlujejo obveščevalcev. Če že koga zadolžijo za obveščevalne operacije, ima ta oseba običajno različne odgovornosti in je pogosto policist za mamila, kriminalne tolpe in protiterorizem. V nekaterih primerih so bili ti policisti usposabljani za obveščevalno dejavnost in so sposobni razumeti analitične podatke, vendar v večini primerov to ne drži.

Vzpostavite obveščevalne naloge. Če v okviru svoje postaje še nimate obveščevalne službe, lahko zadovoljite te potrebe v naslednjih korakih:

1. Pripravite izjavo o nameri, da bi radi uvedli izmenjavo obveščevalnih informacij glede resnih kaznivih dejanj.
2. Enega policista ali civilnega analitika določite kot kontakno osebo za obveščevalne informacije.
3. Tega posameznika zadolžite za pripravo rednih kratkih poročil o terorizmu na podlagi obveščevalnih podatkov, zbranih iz javnih virov in od drugih policijskih agencij.

4. Zagotovite, da bodo poročila o sumljivih dejavnostih, ki jih posredujejo patruljni policisti in drugi, posredovana tej osebi.
5. Pridružite se regionalnemu obveščevalnemu centru; če ta ni na voljo, sodelujte z drugimi lokalnimi agencijami in ustanovite regionalni center.
6. Zagotovite zavarovanje zasebnih podatkov (glej okvir).

Bodite pripravljeni na cinizem in odpor. Patruljni policisti, ki ne bodo takoj sprevideli uporabnosti obveščevalnih podatkov, jih bodo morda zaznavali kot sredstvo za preusmerjanje politike od tradicionalnih policijskih modelov in starejši policisti, ki bodo manj razumeli pomen obveščevalnih podatkov, bodo skeptični glede njihove vrednosti.

Čeprav vas spodbujava, da vzpostavite osnovno obveščevalno službo, ne pričakujte preveč od te investicije. Za to sta dva razloga:

1. Obveščevalne informacije so visoko strokovno delo, ki pogosto presega sposobnosti vaših policistov. Z besedami Gregorya Trevertona iz korporacije RAND: »(Obveščevalne informacije) obsegajo pridobitev globljega in širšega razumevanja danega problema, da bi bili zmožni odkriti vzorce. Cilj je stalno povezovanje točk z védenjem, da se narava in položaj točk nenehno spreminjata. To lahko pomeni, da namesto izkušenj o določenem segmentu problema, potrebujemo številne pare oči, ki preučujejo podatke v zvezi z odkrivanjem prihajajočih groženj.«
2. Neuporabne informacije so veliko pogostejše kot uporabne. Čeprav pogosto slišimo zgodbe o obveščevalnih uspehih, ki so rezultat prejetih namigov ali nadzorovanj, ne slišimo o nadzoru, ki ni pokazal rezultatov ali vseh navidezno obetajočih namigov, ki niso vodili nikamor.

Več o tem:

1. *Henry, Vincent, »The Need for a Coordinated and Stategic Local Police Approach to Terrorism: A Practitoner's Perspective,« Police Practice and Research 3 (4) (2002): 319-336.*
2. *Treverton, Gregory F., The Next Steps in Reshaping Intelligence, Occasional Paper. Santa Monica, California: RAND Corporation, 2005.*

Pravne zadeve in zasebnost

V 1960. letih so lokalne policijske postaje zašle v težave zaradi nezakonitega vohunjenja za mirovniškimi skupinami in skupinami za državljanske pravice. Da bi to preprečili, je v nedavnem poročilu ministrstvo za pravosodje izpostavilo naslednje smernice.

Informacije, ki vstopajo v obveščevalni sistem, bi morale imeti kazensko naravo ali pa naj bi šlo vsaj za utemeljeni sum, da gre za kaznivo dejanje, in morale bi biti ovrednotene, da se preveri zanesljivost vira in točnost podatkov.

Informacije, ki vstopajo v obveščevalni sistem, ne bi smele kršiti varovanja zasebnosti in državljanskih svoboščin njihovih subjektov.

Informacije, ki se jih obdrži v obveščevalnem sistemu, morajo biti posodobljene ali prečiščene vsakih 5 let.

Agencije morajo slediti temu, kdo je prejel informacije.

Informacije iz obveščevalnega sistema so lahko posredovane le tistim, ki imajo za to pravico in vedo ali bi morali vedeti, da bi lahko izvajali funkcijo kazenskega pregona.

Vir: Peterson, Marilyn. Intelligence-Led Policing: The New Intelligence Architecture. NCJ 210681. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Assistance, September 2005.

Napotek 23: Ločite med sanjami in resničnostjo izmenjave informacij

Komisija 11. septembra je ostro kritizirala neuspeh FBI in CIA, ki nista pred napadom »povezala točk«; to je, nista prepoznala vzorcev v razpršenih delih informacij o ugrabiteljih, ki so pritegnili pozornost različnih zveznih agencij. Komisija je nadaljevala z navedbami, da morajo te agencije izmenjevati kritične informacije o osumljenih terorizma bolj usklajeno in pravočasno. Dejansko se izmenjava informacij ne bi smela ustaviti na zvezni ravni. Zvezne agencije morajo bolj odprto izmenjevati informacije z državno in lokalno policijo. Poleg tega se morajo na te agencije obrniti za informacije o osumljenih terorističnih dejavnosti k lokalnim okolišem – sledi, ki jih agentje FBI sami verjetno nikoli ne bi odkrili. Kakor je nekdanji direktor CIA, R. James Woolsey, navedel v svojem govoru v kongresu: »Tok izmenjave informacij bo bolj verjetno prej stekel iz lokalnih predelov v Washington kot obratno.« Prav tako morajo tudi državne in lokalne agencije najti načine za medsebojno izmenjavo informacij. Dejstvo, da se je lokalna policija med kontrolami prometa pred napadom 11. septembra znašla iz oči v oči s tremi ugrabitelji, se pogosto navaja kot usodno izgubljena priložnost.

Potreba po izmenjavi informacij je jasna; manj jasno je, kako jo uresničiti. Obstaja več kot 17.000 državnih in lokalnih agencij kazenskega pregona v Združenih državah, relativno malo izmed njih jih ima možnost, da zbirajo obveščevalne podatke (glej napotek 22). Še veliko manj jih ve, kako analizirati zbrane informacije tako, da bi jih lahko produktivno delili z drugimi agencijami. V kolikor te agencije ne bodo razvile obveščevalne službe, bodo ostale zunaj kroga. Veliko se dela na tem, da se olajša izmenjava informacij med agencijami, ki imajo obveščevalne službe. Na primer FBI je ustanovil Skupne protiteroristične projektne skupine (Joint Terrorism Task Forces) v vseh regionalnih okrožjih (glej napotek 20) čeprav so očitno osnovane tako, da ne služijo toliko potrebam lokalnih institucij kazenskega pregona, temveč bolj preiskavam FBI.

V duhu prave izmenjave informacij FBI vzpostavlja sistem, ki bo državnim in lokalnim policijam omogočal ugotoviti, ali je osumljenec na zveznih seznamih opazovanih teroristov. To bo zahtevalo integracijo (v času pisanja) devetih seznamov in razvoj sistema, ki omogoča dostop do združenega seznama v realnem času. »Fuzijski centri«, ki se ustanavljajo v številnih zveznih državah, predstavljajo tretjo iniciativo za izmenjavo informacij.

Združevali bodo informacije različnih okolišev in jih dajali na voljo patruljnim policistom, detektivom, vodstvu in drugemu osebju. Naloga takega centra je lahko omejena zgolj na protiterorizem, vendar pogosto vključuje tudi druga značilna kazniva dejanja, kot so tatvine identitet, zavarovalniške prevare, pranje denarja in oboroženi ropi.

Nazadnje se seznanite še s številnimi smernicami in dokumenti o izmenjavi informacij, ki jih je izdelal Urad direktorja nacionalne obveščevalne službe (Office of the Director of National Intelligence), zlasti s 100-dnevnim načrtom za integracijo in sodelovanje. http://www.fas.org/irp/dni/100-day-plan.pdf.

»Čeprav potreba po izmenjavi podatkov ni nova, je izmenjava informacij med okoliši in različnimi ravnmi oblasti bolj pomembna v sedanjem ogroženem okolju, kakor je bila kdajkoli v boju proti kriminalu. Ker je državni in lokalni kazenski pregon decentraliziran, mora preseči svoj tradicionalni odpor do izmenjave informacij.«

Vir: Kelling George L. in William K. Bratton, Policing Terrorism, Civic Bulletin 43, New York; Manhattan Institute for Policy Research, September 2006.

»Organi lokalnega kazenskega pregona pogosto sklepajo, da zvezne agencije zadržujejo podrobne, relevantne in pomembne informacije iz številnih razlogov. Nisem prepričan, da to drži. FBI se tako kot mi ponovno uči igre zbiranja obveščevalnih podatkov in moramo se zavedati, da morda včasih informacij pač nimajo.«

Vir: Flynn, Edward A., Protecting Your Community form Terrorism; The Strategies for Local Law Enforcement Series. Volume 1: Local-Federal Partnerships. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2003, p 29.

Ovire pri izmenjavi informacij

Glavna ovira za pravočasno izmenjavo informacij je, da večini lokalnih postaj primanjkuje tako osebja, izurjenega v okviru splošnega obveščevalnega učnega načrta, kakor tudi tehnologije za pridobivanje, analizo in uporabo neobdelanih obveščevalnih podatkov (glej napotek 20). Dejansko, ve-

čini lokalnih postaj primanjkuje primerno usposobljenih kriminalističnih analitikov, kaj šele obveščevalnih analitikov. V večini postaj kriminalistično analizo štejejo za bolj pomembno od obveščevalne analize, preprosto zato, ker prva lahko prinese bolj očitne in oprijemljive koristi za vsakodnevno policijsko delo. Številne lokalne postaje nimajo računalniške in programske opreme za podporo nacionalnega sistema obveščevalnih podatkov. Celo v okviru iste enote je medsebojna povezanost med računalniškimi sistemi pogosto slaba. Brez poenotenja in medsebojne povezanosti lahko sanje o elektronski mreži, prek katere se hitro posreduje informacije in se jih primerja, ostanejo zgolj to: sanje.

Druge ovire pri izmenjavi informacij vključujejo naslednje:

1. Tajnost vira je zaščitni znak obveščevalnih agencij; varovanje virov in preprečevanje uhajanja informacij je bilo v zgodovini zelo pomembno. Zato doktrina tajnosti vodi politiko izmenjave podatkov. Na žalost pa v praksi ta doktrina ovira izmenjavo informacij in ovira tudi sveže in nove poglede, ko nove oči preučujejo stare informacije. Lokalne postaje se še vedno pritožujejo, da informacije, ki jih odstopi FBI, pogosto vsebujejo le malo več od tistega, kar izveš na kabelski televizijski postaji ali v novinarskih objavah v medijih. Čeprav se veliko govori o potrebi po večjem zaupanju, se o tem, kako to storiti med 17.000 agencijami, nikoli zares ne razpravlja. Bolj realistično je pričakovati, da bomo našli načine za izmenjavo informacij brez podrobnosti o virih.
2. Posebej na zgodnjih stopnjah preiskave je verjetno, da bodo preiskovalci močno ščitili svoje informacije. Ne le zato, da bi preprečili njihovo uhajanje, ki bi lahko ogrozilo preiskavo, temveč tudi zato, ker (razumljivo) želijo požeti slavo ob uspešni aretaciji teroristov. Izmenjava informacij lahko pomeni delitev slave – ali celo prikrajšanost zanjo.
3. Terorizem, celo sum terorizma, je redek. Ljudje so težko nenehno pozorni, še posebno, ko se zdi, da se nič ne dogaja, in težko je vzdrževati delovno moralo tistih, ki opazujejo.
4. Bistvo preprečevanja je zaustaviti nekaj, da se ne bi zgodilo. Težko je dokazati, da so bila tovrstna prizadevanja uspešna, kadar postaja, ki zbira koristne informacije, ni tista, ki izvaja akcije preprečevanja. Še enkrat, to dejstvo nasprotuje obveščevalni funkciji in - bolj natančno - izmenjavi podatkov.

Več o tem: D'Amico, Joseph, »Stopping Crime in Real Time,« The Police Chief 73 (September 2006). http://www.policechiefmagazine.org/

»Pomembno je vedeti, da so zvezni organi kazenskega pregona odgovorni za preiskovanje vseh bombnih in terorističnih napadov. Državne ali lokalne agencije se lahko pozove k navzočnosti pri preiskavi na številne načine, vendar njihova vloga zagotovo ne bo vloga primarne preiskovalne agencije. Glede na zgodovino nesoglasij med organi zveznega in lokalnega kazenskega pregona, nagibanje k malenkostnim zavistim in napačnemu razumevanju, ki preraste v prave konjske dirke, in glede na obsežno medijsko pozornost ter pritiske javnosti, ki neizbežno spremljajo preiskave, je tudi vprašljivo, ali bo določena teroristična preiskava napredovala hitro in gladko. V sedanjem vzdušju kazenskega pregona so konflikti praktično neizbežni.

Vir: Henry, Vincent, »The Need for a Coordinated and Strategic Local Police Approach to Terrorism,« Police Practice and Research 3 (4) (2002): 319-336.

Napotek 24: Spoznajte omejitve videokamer

Kmalu po samomorilskem bombnem napadu v londonski podzemni železnici julija 2005 so svetovne televizijske postaje predvajale videoposnetek štirih bombnih napadalcev, ko so vstopali v podzemno železnico. Slike so jasno govorile v prid videonadzoru in vsak, ki jih je videl, ni mogel spregledati njihove preiskovalne vrednosti (glej okvir). Zato je zelo verjetno, da vas bodo v vašem mestu silili, da namestite videokamere za zaščito pred terorizmom, četudi se ljudje v Združenih državah bolj upirajo videonadzoru kakor v Združenem kraljestvu. Ta odpor večinoma temelji na skrbi za zasebnost, ki ima v realnosti malo osnove. Raziskave, ki so jih izpeljali v Združenem Kraljestvu ali drugje, na splošno ugotavljajo, da ljudje dobro sprejemajo kamere. Malo jim je mar, da jih fotografirajo, da so le ceste zaradi kamer bolj varne. Ljudje v Združenih državah bi bili verjetno enakega mnenja, če bi vedeli, da jih bodo kamere zaščitile pred terorizmom. V vsakem primeru so ljudje že navajeni na videvanje kamer v bankah, trgovinah, bencinskih črpalkah, poslovnih stavbah, šolah in na univerzitetnih območjih.

Slike iz londonske podzemne železnice so nazoren dokaz vrednosti videonadzora pri preiskovanju terorizma. Vendar, ali imamo dokaz, da lahko videokamere dejansko preprečijo napad? Na to vprašanje ni jasnega odgovora, delno zato, ker so videokamere dokaj nove in so se dokazi o njihovi uporabi šele začeli nabirati. Kljub temu je v povezavi s COPS uradom dr. Jerry Ratcliffe z Univerze Temple pred kratkim pregledal raziskave o učinkovitosti videonadzora pri preprečevanju kriminalitete na javnih mestih (glej »Preberi več«). Analiziral je rezultate več kot 30 objavljenih študij, večino katerih so izvedli v Združenem kraljestvu. Opazil je, da je težko dokazati učinkovitost videokamer, ker se jih pogosto uporablja skupaj z drugimi tehnikami preprečevanja kriminalitete in je težko ločevati njihove učinke od učinkov drugih ukrepov. Težko je tudi vedeti, ali kamere znižujejo kriminal, ali pa ga preprosto preženejo na področja zunaj dometa kamere. Kljub tem težavam je uspel potegniti naslednje zaključke:

1. Videokamere delujejo, vendar niso rešitev za vse težave. Delujejo na različne načine v različnih okoliščinah.
2. Videokamere najbolj učinkovito delujejo v povezavi z drugimi situacijskimi preprečevalnimi ukrepi, t.j. ukrepi, ki povečujejo težavnost izvedbe dejanja in zvišujejo tveganje za prijetje (glej http://www.popcenter.org/25techniques.htm).

3. Videokamere bolje delujejo na majhnih, dobro označenih lokacijah (na primer parkiriščih) kakor na obsežnih področjih (kot je središče mesta).
4. Videokamere so bolj učinkovite v boju proti premoženjski kriminaliteti kakor proti nasilju ali neredu.
5. Videokamere najbolje delujejo, kadar so tesno povezane s policijskimi operacijami.

Iz tega povzetka je razvidno, da so videokamere lahko koristne pri preprečevanju kriminalitete, kadar so skrbno prilagojene okoliščinam. Ni pa jasno, ali lahko preprečijo terorizem, čeprav obstajajo dobri razlogi za domnevo, da vse, kar poveča tveganje za teroriste, verjetno ima nekakšno zastraševalno vrednost. Zato sva midva naklonjena vključevanju videokamer v vsak načrt za izboljšanje osnovne varnosti določenih ogroženih tarč, zlasti zato, ker bodo kamere koristile preprečevanju kriminala nasploh. Ali naj se jih namesti na javnih cestah ali v središču mesta, je težja odločitev, ker je njihova vrednost pri preprečevanju kriminalitete v takih okoliščinah manj jasna. Kljub temu lahko pomirijo javnost in bi morda lahko bile uporabne v primeru teroristične aktivnosti. Veliko bo odvisno od dodelanosti in velikosti sistema in potemtakem tudi od njegove cene. Dr. Ratcliffe je oblikoval sestavne dele celovitega videonadzornega sistema:

- ena ali več kamer, ki so usmerjene na javno površino;
- mehanizem za oddajanje videopodob na enega ali več monitorjev;
- videomonitorji za ogledovanje prizorov – običajno s priloženo snemalno napravo;
- operater kamere, npr. policist ali varnostnik.

Izboljšave vključujejo naslednje:

- zmožnost prenosa podob prek spleta;
- nadzorni senzorji za priklop kamere;
- navadna in infrardeča osvetljava za izboljšanje kakovosti slike ponoči;
- zmožnost obračanja in nagibanja, kar operaterju omogoča spremembo smeri snemanja kamere, približevanja in izostritve;
- tehnologije prepoznavanja obrazov in sistemi za ocenjevanje lokacij dogodkov s strelnim orožjem;
- obveščevalni sistemi za zaznavo nenavadnih aktivnosti, kot so cestni pretepi (ti so še v razvoju).

Vrednost videokamer za massachusetski urad za nadzor zalivskega tranzita

Več kot 450 varnostnih kamer, ki oprezajo za potencialnimi teroristi na »T-ju«, zdaj pomaga loviti domnevne storilce kaznivih dejanj. Tranzitni policist massachusetskega urada za nadzor zalivskega tranzita (Massachusetts Bay Transit Authority – MBTA) je aretiral 27-letnega moškega, osumljenega oboroženega ropa potnika na postaji Back Bay. Policist je povedal, da so podobni primeri pogosto ostali nerazrešeni in da bi bila aretacija veliko manj verjetna brez digitalnih posnetkov nadzorne kamere na postaji.

Mreža kamer »nam zelo pomaga pri identifikaciji osumljencev, ki v preteklosti običajno ne bi bili identificirani,« je povedal narednik, detektiv Michael Adamson. »Upamo, da se bo razvedelo, da so kamere nameščene in bodo ljudje dobro razmislili o svojih dejanjih, preden bodo storili kaznivo dejanje na MBTA.«

Rekel je tudi, da so detektivi s pomočjo kamer vedno bolj uspešni in jih zdaj redno uporabljajo za oženje seznama osumljencev. Rekel je, da celo kadar policija s pomočjo digitalnih posnetkov ni zmožna identificirati osumljenca, običajno dobi ustrezne sledi z občutno boljšim opisom osumljenca, da opis vključuje podrobnosti o oblačilih in razpoznavnih značilnosti, kot so znamenja in tetovaže.

Policija je povedala, da je v roparskem napadu v Back Bayu v poznih večernih urah žrtev opisala svojega napadalca kot moškega s tetovažo na vratu. Tranzitna policija je žrtvi pokazala slike več kot 100 znanih storilcev s tetoviranim vratom. Ko jih je žrtev nekaj izbrala, je policija pregledala posnetke digitalnih nadzornih kamer v Back Bayu in našla posnetek moškega, ki je vstopal na postajo v času ropa. To je pomagalo pridobiti nalog za aretacijo osumljenca.

Vir: Daniel, Mac in Suzanne Smalley, »Antiterror Cameras Capturing Crime on T,« The Boston Globe, January 29, 2007.

Katerikoli sistem izberete, se boste soočili s številnimi logističnimi vprašanji: Kam postaviti kamere? Ali združiti kamere za preprečevanje kriminalitete z obstoječimi kamerami za nadzor prometa? Kako nadzirati kame-

re? Kako se odzvati na incidente? Kako komunicirati s policisti na terenu? Kako shranjevati posnetke in kako dolgo? Kako obvladovati zaskrbljenost javnosti? Kot smo že povedali, bo javnost verjetno podprla uporabo kamer v protiteroristične namene in v vsakem primeru **večina sistemov ne bo ogrožala ustavnega varstva pred neutemeljenimi preiskavami in zasegom**. Morda boste še vedno morali dokazovati, da stroga pravila prepovedujejo policistom neprimerno usmeritev kamere in da bodo posnetki iz trgovin dostopni le tistim, ki jih morajo videti. Vsekakor bi bilo **glede te zadeve** razumno **zaprositi za lokalno pravno svetovanje**.

Več o tem: Ratcliffe, Jerry. Video Surveillance of Public Places, Problem-Oriented Guides for Police, Response Guides Series No. 4. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006.

http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=226

Napotek 25: Ne zanašajte se na previdnost javnosti

Elektronski avtocestni znaki ob velikih mestih pogosto prikazujejo brezplačno klicno številko in naprošajo javnost, da »prijavi sumljiva vedenja.« To je morda na prvi pogled dobra zamisel, vendar nedoločna opozorila državljanom, naj bodo previdni, zvišujejo strah in podžigajo večinoma nepotrebne klice na pomoč. Dejansko obstajajo številni razlogi, da se ne zanašate na previdnost javnosti.

1. V sredstvih množičnega prevoza je smiselno spodbujati ljudi, da prijavijo torbe ali pakete brez lastnika, ker vsak lahko prepozna tovrstne predmete in brez težav razume, da morda vsebujejo bombe. Na avtocestnih znakih pa sumljivo vedenje ni opredeljeno in ni nikakršnega soglasja o tem, kaj je sumljivo vedenje (glej okvir 1).
2. Brez jasne opredelitve sumljivega vedenja se lahko prijavlja ali celo nadleguje ljudi na podlagi predsodkov ali sumničenj tistih, ki jih označijo za sumljive – na primer temnopolti pešci v prevladujoče beli soseski.
3. Pozivi javnosti k pomoči pri prijavljanju sumljivega vedenja ni zastonj. Od tistih, ki pozivajo k prijavam, zahteva, da odgovarjajo na telefonske klice in se pogovarjajo s klicatelji ali poslušajo posnetke kasneje – ko je že prepozno, če bi opozorilo bilo resnično.
4. Po poslušanju je treba prijave oceniti ali celo preiskati. To trati nezadostna sredstva, ker je velika večina prijav neutemeljena.
5. Terorizem je skrajno redek pojav. Javnost se bo hitro naveličala opozoril, naj bo oprezna, če se nič ne zgodi. Še huje, to lahko spodbudi cinizem v odnosu do protiterorističnih prizadevanj.

Poleg pomislekov, ki so bili podrobno predstavljeni zgoraj, obstajajo še številni drugi dejavniki, ki govorijo proti vzpostavitvi vroče linije za pridobivanje informacij od javnosti. Na primer, ljudje lahko izrabijo vročo linijo za nadlegovanje tistih, ki jih ne marajo; vroče linije privabljajo čudake in šaljivce; in končno, morda boste ugotovili, da se morate zagovarjati pred jeznimi klicatelji, katerih prijave ste ocenili za neutemeljene.

Če ima pozivanje splošne javnosti k poročanju o sumljivem vedenju omejeno vrednost, je bolj smiselno, da omejite svoje pozive na posameznike in podjetje, ki bodo bolj verjetno prišli v stik s potencialnimi teroristi. Ali

Okvir 1: Sedem opozorilnih znamenj terorizma

Na spletnem seznamu sumljivega vedenja so številne objave (seznam je sestavil Urad državnega tožilca Združenih držav na Havajih), vendar pa ni jasno, koliko dosežejo in informirajo splošno javnost. Čeprav so nekateri kazalci lahko uporabni (npr. nenavadni nakupi kemikalij), jih je večina nejasnih in vključujejo običajne, vsakodnevne dejavnosti (npr. fotografiranje; glej okvir 2).

1. **Nadzor:** sumljivo kontroliranje tarče; nenavadno fotografiranje tarč; izdelovanje zemljevidov in diagramov; poskusi pridobiti tehnične načrte vladnih zgradb in podjetij.
2. **Izvabljanje:** poskusi pridobiti omejene informacije o določenem kraju, osebi ali operaciji; poskusi namestitve ključnih ljudi na občutljiva delovna mesta; prizadevanja ugotoviti prednosti in slabosti tarče.
3. **Testiranje varnosti:** vožnja mimo tarče ali poskusi varnostnih kršitev, da bi ugotovili odzivni čas.
4. **Pridobivanje potrebščin:** nakupovanje ali tatvina eksploziva, streliva ali orožja; nezakonito skladiščenje velikih količin kemikalij, kot je nitratno gnojilo; kraja policijskih uniform ali identifikacijskih značk.
5. **Sumljivi ljudje, ki ne sodijo zraven:** vedenje, ki ni v skladu z normami, ljudje, ki se nenavadno obnašajo; samonaložena osamitev ali nesocialno vedenje; priročniki za usposabljanje in protiameriška ali protisemitska propaganda.
6. **Poskusne vožnje:** vaje na ali ob območju tarče, da bi odkrili napake in predvideli težave; to lahko vključuje označevanje poti, nadziranje policijskih frekvenc in ugotavljanje časovne usklajenosti semaforskih luči.
7. **Indikacije bombnega napadalca:** ***(angl. ALERT)*** *samomorilski bombni napadalci*: sami in nervozni; ohlapna in okorna oblačila, ki niso v skladu z vremenskimi razmerami; razkrite žice; tog srednji del telesa – zaradi eksplozivnega pasu ali oklepa; stisnjene roke – lahko drži detonacijsko napravo. *Bombni tovornjaki:* nakup ali tatvina večje količine eksploziva, goriva, detonacijskih kapic in kemikalij, kot so dušikova kislina, žveplova kislina, sečni kristali,

tekoči nitrometan ali amonijev nitrat; najeti ali samo-skladiščni prostori za skladiščenje kemikalij; dostava kemikalij v stanovanjske ali samo-skladiščne objekte; nenavadne vonjave; zarjavela kovina ali svetli madeži v stanovanjih, motelih ali samo-skladiščnih enotah; najem, tatvina ali nakup tovornjaka ali kombija z najmanj 1 tono nosilnosti; testne eksplozije na odmaknjenih, podeželskih področjih; kemijske ožganine ali manjkajoči prsti na rokah.

Vir: U.S. Attorney's Office, District of Hawaii http://www.usdoj.gov/usao/hi/atac/terrorisminformation.pdf

bi bilo vredno vprašati agente za izposojo avtomobilov v vašem mestu, da obveščajo policijo o sumljivih strankah – na primer skupini tujih moških, ki so najeli velik kombi ali tovornjak? Bi bilo vredno prositi upravnike hotelov ali motelov, da vas obvestijo, ko se prijavijo gostje iz islamskih držav? Bi morali naročiti nepremičninskim posrednikom, da vam sporočajo, ko najemniki za kratek čas iščejo osamljene posesti ali plačajo najemnino v gotovini? Je vredno vprašati upravnika banke, da vas informira o rednih denarnih nakazilih iz čezoceanskih krajev?

To se morda zdijo utemeljene previdnosti, vendar morate vedeti, da je večina naštetih »sumljivih« dejavnosti zakonitih in nedolžnih. Dobro boste morali premisliti o kakovosti morebitnih informacij in o tem, kako jih boste zbrali in pregledali. Tovrstne prošnje se bodo na začetku morda končale z nekaj kapljajočimi informacijami, vendar se bodo vaši viri hitro izpraznili, če jih ne boste opominjali. Enota za terorizem bi lahko redno zastavljala taka vprašanja, četudi bi to morda tratilo čas, ki bi ga lahko bolje porabili na druge načine. Čeprav je verjetno več možnosti, da pridobite uporabne obveščevalne podatke na podlagi neposrednih vprašanj posameznikom kakor od širše javnosti, je še vedno zaradi majhne verjetnosti, da bodo teroristi izbrali vaše mesto, tudi to neproduktivno. **Boljši način zaposlitve javnosti v okviru vaših protiterorističnih prizadevanj je ta, da polno izkoristite obveščevalne funkcije skupnostne policijske dejavnosti**, kar je predmet Napotka 28.

Okvir 2: Opazovalci ptic, bodite previdni!

Domnevno zelo sumljivo vedenje je bilo popolnoma neškodljivo. Eden od avtorjev tega priročnika je bil nekoč zadržan izven države, medtem ko je fotografiral obalne ptice v jahtnem pristanišču, ki je bilo tik ob večjem zastarelem vojaškem objektu. Vedenje je bilo popolnoma nedolžno, kljub temu je velik telefotografski objektiv za fotografiranje ptic sprožil prijavo javnosti varnostnemu osebju.

Napotek 26: Služite priseljenskim skupnostim

Čeprav so se priseljenci včasih zbirali primarno v vhodnih državah, kot so Kalifornija, Florida, Illinois, Massachussets, New Jersey, New Nork in Teksas, so se zdaj začeli naseljevati na številnih drugih območjih. Velika verjetnost je, da je priseljenska skupnost danes tudi v vašem okolišu.

Zaradi težav pri policijskem obvladovanju priseljenskih skupnosti je lokalna policija pogosto pripravljena tem skupnostim pustiti, da se policijsko obvladujejo same, in posredovati zgolj takrat, ko se zgodi resno kriminalno dejanje. Enajsti september je vse to spremenil. Priseljenske skupnosti, še posebej arabske in azijske z muslimanskimi vezmi, so bile osumljene, da so potencialna gojišča terorizma. V začetku novembra 2001 je državni tožilec ZDA pozval zvezne, državne in lokalne agencije kazenskega pregona, da izvajajo »prostovoljne« razgovore s tisoči mladimi moškimi iz bližnjevzhodnih držav, ki so prišli v Združene države na podlagi začasnih vizumov.

Čeprav je bila večina teh moških popolnoma nedolžna, so oblasti imele nekaj vzrokov za sum. Prvi napad na Dvojčka je izvedla skupina, ki je prebivala v Jersey City v New Jerseyju, priseljenski skupnosti blizu Manhattna in napadalci so živeli v okviru ali blizu priseljenskih področij, ki ustrezajo njihovemu etničnemu in nacionalnemu izvoru. Le malo je dvomov o tem, da je Al Kaidine napade olajšala navzočnost priseljenskih skupnosti v Združenih državah. Zvezne agencije so to pravilno razumele – vendar morda ne tako, da je Al Kaida te skupnosti izrabila, ne da bi se te tega zavedale. Priseljenske skupnosti pomagajo novim prišlekom poiskati svojo pot v tuji državi, zlasti kadar ne poznajo jezika. Tujim operativcem pomagajo odpreti bančne račune in pridobiti kreditne kartice, da bi prišli do denarja iz tujine, si kupili avtomobile, našli stanovanje in tako naprej.

Obstaja verjetnost, da so nekatere od teh skupnosti finančno podprle Al Kaido, saj je obsežno zbiranje sredstev prek dobrodelnih ustanov in mošej v priseljenskih skupnostih dobro dokumentirano. V nekaterih primerih je videti, da je bil denar, zbran v okviru priseljenskih skupnosti za podporo dobrodelnim ustanovam v njihovih domovinah, preusmerjen v roke teroristov.

Tovrstna operacijska in finančna podpora terorizmu, četudi v veliki meri nenamerna, zadostuje za zahtevo po policijski pozornosti. Toda, ali niso morda te skupnosti vpletene v terorizem na veliko bolj resen način? Alo lahko tudi

same »proizvedejo« svoje, doma vzgojene teroriste, kakor muslimanske skupnosti v Britaniji, četudi z nekaj Al Kaidine podpore? Ne zdi se verjetno, da se bo to zgodilo tukaj, vsaj ne v bližnji prihodnosti. Muslimanske priseljenske skupnosti v Britaniji so na splošno starejše kakor tiste v Združenih državah; številni od teh priseljencev so prišli v državo, da bi opravljali dela, ki jih Britanci zaničujejo. Teroriste se ne izvablja iz skupin priseljencev prve generacije, temveč so to pripadniki druge, v Britaniji rojene generacije, ki so pogosto razočarani nad svojim zaposlitvenim statusom in gojijo zamere, ker se njihove muslimanske identitete ne spoštuje dovolj. V primerjavi z njimi so otroci azijskih priseljencev v Združenih državah uspešni na šolah, fakultetah in na trgu dela, delno zato, ker je veliko njihovih staršev imelo višjo izobrazbo, kar jim je pomagalo že pri vstopu v državo.

Do zdaj smo obravnavali priseljenske skupnosti kot možen vir terorizma in ne kot žrtve terorizma. Vsakič, ko se pojavi novica o preprečenem terorističnem načrtu, ali vsakič, ko se stopnja teroristične ogroženosti povzpne, priseljenci poročajo o svojem strahu – ne le strahu, da bi bili žrtve terorizma, temveč da bodo postali tarča nadaljnjih pregledov in omejitev s strani oblasti in sovražnosti ali celo sovraštva lokalnega prebivalstva.

Zaščita teh skupnosti in njihovo pomirjanje ter obenem zagotavljanje, da ne nudijo zavetja ali podpirajo terorizma, je težavno dejanje uravnoteženja. Videti je, da standardna skupnostna policijska dejavnost nudi največ upanja za zadovoljitev teh dveh potreb, toda za to je tudi nekaj pomembnih ovir. Te vključujejo dejstva, da: (1) se priseljenci pogosto bojijo in ne zaupajo policiji; (2) številni priseljenci vedo le malo o državljanskih pravicah, zakonih ZDA ali kazenskem pregonu; (3) jezikovne ovire preprečujejo učinkovito komunikacijo in zaupanje med priseljenci in policijo; (4) se priseljenci bojijo, da bodo stiki s policijo ogrozili njihov priseljenski status (težava, ki se je zaostrila, ker lokalna in državna policija vedno bolj sodeluje z zveznimi imigracijskimi organi); (5) čuta za skupno socializacijo, ki ga zahteva skupnostna policijska dejavnost, ni, saj so številni priseljenci bolj povezani s svojimi domovinami kakor z novimi domovi; (6) pomanjkanje volilne pravice med priseljenci zmanjšuje njihovo vlogo pri določanju prednostnih nalog policije in lokalnih oblasti.

Kljub temu lahko veliko naredite za premagovanje teh ovir ter uspešno izvršite skupnostno policijsko dejavnost v priseljenskih skupnostih. Tu je nekaj primerov:

- Namenite policiste izvajanju skupnostne policijske dejavnosti, ki bodo delali izključno s priseljenskimi skupnostmi. V večjih skupnostih vzpostavite policijske podpostaje.
- Uporabljajte etnične radijske in televizijske postaje, verske institucije in delodajalce za komunikacijo s priseljenskimi skupnostmi. To vam bo pomagalo doseči veliik del populacije kot tudi članov skupnosti (npr. mlajših priseljencev, otrok priseljencev in dnevnih delavcev), ki se običajno ne udeležujejo tradicionalnih sestankov v administrativni enoti.
- Zaposlite več tolmačev in ponudite policijski material v tujih jezikih. Obiščite Omejeno znanje angleščine (Limited English Proficiency): spletno stran zvezne agencije na spletnem naslovu http://www.lep.gov, ki opisuje izvršno odredbo 13166, katere vsebina se nanaša na izboljšanje dostopa do zveznih programov in uradov za tiste ljudi, katerih znanje angleščine je pomanjkljivo.
- Vključite priseljenske voditelje v oblikovanje in izvajanje učinkovitih programov medkulturnega izobraževanja za vaše policiste. Izurite policiste v učinkovitem sporazumevanju z različnimi pripadniki priseljenske skupnosti.
- Premagujte ovire, ki preprečujejo rekrutiranje policistov iz priseljenskih skupnosti ter ustvarjajo odpor do policije, in premagujte težave z administrativnimi in kulturnimi ovirami.
- Jasno opredelite in objavite vašo politiko kazenskega pregona do priseljencev.
- Skupnostne odvetnike obvestite o vlogi svoje postaje in politik. Prepričajte se, da bodo mediji natančno poročali o dialogu med policijo in priseljenci.

Rob Davis, načelnik policije v San Joseju v Kaliforniji, član mormonske veroizpovedi, je napovedal, da se bo pridružil lokalnim muslimanom pri enomesečnem postu ob ramadanu. Za to so ga navdahnili pogovori s 7.000 muslimani, ki živijo na območju zaliva. Vsako noč je nameraval pretrgati post z drugo muslimansko družino na svojem lastnem domu. Načelnik Davis je povedal: »Moram biti načelnik za vse in še posebej za tiste, ki so se čutili marginalizirane.«

Vir: McDonald, William F., »Police and Immigrants: Community and Security in Post-9/11 America,« in Justice and Safety in America's Immigrant Communities, ed. Martha King, Princeton, New Jersey: Princeton University: The Policy Research Institute for the Region, 2006. http://region.princeton.edu

Preberite več:

Briggs, Rachel, Catherine Fieschi in Hannah Lownsbrough, Bringing It Home: Community-Based Approaches to Counter-Terrorism. London: DEMOS, 2006. http://www.demos.co.uk/files/Bringing%20it%20Home%20-%20web.pdf

Shah, Susan, Insha Rahman in Anita Khashu, Overcoming Language Barriers: Solutions for Law Enforcement. New York: Vera Institute of Justice and the Office of Community Oriented Policing Services, 2007. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=403 in http://www.vera.org/overcominglangbarriers

Napotek 27: Naj bo skupnostna policijska dejavnost vaša prva obrambna vrsta

»Samo učinkoviti lokalni policijski ustanovi, ki uživa zaupanje državljanov, bo npr. lokalni trgovec iz dela mesta, kjer živijo številni novi priseljenci, verjetno sporočil, da se je v bližnje stanovanje pred kratkim nastanila skupina mladih moških iz tujine in da se obnašajo sumljivo. Lokalna policija je najbolje usposobljena, da zaščiti državljanske svoboščine in obenem legalno pridobi sledi.«

Ta navedek iz pričevanja nekdanjega direktorja CIA, Jamesa Woolseya, v kongresu leta 2004 je le eno od mnogih potrdil vloge lokalne policije v protiteroristični dejavnosti. Bistvo zbiranja vitalnih informacij so: pridobivanje zaupanja državljanov, redni in neformalni pogovori s ključnimi člani skupnosti in varovanje pravic in svoboščin skupnosti. Drugače rečeno, to je formula za učinkovito policijsko dejavnost v skupnosti. Kot številni drugi načelniki ste tudi vi morda že določili območne policiste za posebne soseske, tako da (1) lahko bolje služite skupnosti in (2) vam skupnost pomaga pri izpolnjevanju policijskih obveznosti. Brez dvoma pričakujete, da bodo vaši policisti preživeli veliko časa v teh soseskah, kjer bodo spoznavali prebivalce in lastnike podjetij ter se z njimi pogovarjali o lokalnih problemih in težavnih posameznikih. Glede na človeške žrtve, ki so lahko posledica terorističnega napada, boste morda ugotovili, da so državljani celo manj zadržani pri posredovanju informacij o sumljivih dejavnostih kakor za običajni kriminal. Dejansko ima zbiranje informacij prek skupnostne policijske dejavnosti številne prednosti pred tradicionalnim obveščevalnim delom. Z osredotočanjem na skupnostno policijsko dejavnost se lahko izognete naslednjemu:

- sestavljanju neosnovanih seznamov osumljencev,
- izvajanju dragih nadzorovanj osumljencev in krajev,
- soočanju z obtožbami zaradi profiliranja,
- prisluškovanju in spopadanju z njegovimi legalnimi in političnimi ovirami,
- vodenju tajnih (in zato sumljivih) operacij,
- spodkopavanju zaupanja skupnosti,
- delovanju proti svoji lastni skupnosti,
- obtožbam zavajanja.

Z usmerjanjem na skupnostno policijsko dejavnost pridobite naslednje koristi:

- zaupanje skupnosti,
- spoznanja o najbolj ogroženih tarčah,
- zmanjšanje kriminalitete kot tudi preprečevanje terorizma,
- globlje poznavanje skupnosti,
- tesnejše sodelovanje s podjetji,
- sloves odprtosti,
- spoštovanje.

»Lokalni policisti so vsakodnevno navzoči v skupnostih, ki so jih dolžni varovati. 'Obdelujejo rajon,' in bodo verjetno prej opazili še tako majhne spremembe v skupnostih, kjer patruljirajo. So v boljšem položaju za spoznavanje odgovornih vodij v islamskih in arabskih skupnostih, tako da se lahko obrnejo nanje po informacije ali pomoč pri oblikovanju informatorjev.«

Vir: Kelling, George L. in William K. Bratton, Policing Terrorism, Civic Bulletin 43, New York: Manhattan Institute for Policy Research, September 2006.

Rezultati policijske dejavnosti za skupnost bi se morali kazati v večji domačnosti vaših policistov v lokalnih skupnostih in boljši obveščenosti o kakršnihkoli sumljivih dejavnostih. To se bo zgodilo samo, če bodo odgovorni za zmanjšanje kriminala na svojih območjih; če bodo preživljali večino svojih delovnih ur na teh območjih; če bodo izstopili iz avtomobilov, se pogovarjajo s prebivalci in lastniki podjetij ter z njimi navezali stike in če bodo posvetili pozornost temu, kar moti prebivalce in lastnike podjetij ter naredili, kar lahko, za ublažitev teh problemov.

Prepričati se boste morali, da imajo ti policisti sredstva, so usposobljeni in imajo ustrezne delovne pogoje za izpolnjevanje svoje vloge. To vključuje:

- izbor policistov, ki so značajsko primerni za policijsko dejavnost za skupnost;
- zadržanje policistov na delovnem mestu dovolj dolgo, da pridobijo zaupanje skupnosti;

- povezovanje policistov z ustreznimi soseskami (na primer izbiranje policistov, ki živijo v bližini ali celo v soseski);
- zagotavljanje, da policisti obvladajo ustrezne jezike za komuniciranje z manjšinskimi prebivalci;
- vzpostavitev policijske podpostaje v soseski, kjer je to mogoče;
- gibljiv delovni čas za policiste in kadar je le mogoče, izogibanje odpoklicem iz njihovih sosesk zaradi nujnih primerov;
- usposabljanje policistov za opravljanje obveščevalne naloge s področja terorizma.

Svoje policiste za delo za skupnost boste morali nadzirati, da se ne bi preveč tesno identificirali s soseščino, kateri služijo, in se podredili njenim potrebam. Da bi zagotovili, da bodo izpolnjevali cilje, preverjajte kakovost in pogostost njihovih poročil ter se prepričajte, da si določajo in dosegajo konkretne cilje - zmanjševanje kriminalitete in nereda. Poleg tega boste morda morali okrepiti kriminalistične analitične zmogljivosti postaje z zaposlitvijo predanega in primerno usposobljenega osebja ter mu zagotovili najnovejšo tehnologijo. Končno, morali boste doseči, da bodo policisti razumeli, da je reševanje problemov enako cenjeno kot odkrivanje in aretiranje storilcev – in da bo enako nagrajeno s priznanji in napredovanji. Okvir vsebuje seznam organizacijskih sprememb, ki jih morate uvesti za izvajanje programa policijske dejavnosti za skupnost.

Vzpostavitev organizacijske predanosti policijski dejavnosti za skupnost

- Dodelite policiste specifičnim geografskim lokacijam za daljša obdobja.
- Vgradite načela v dejavnosti rekrutiranja in odločanja o izbirah.
- Vključite policijsko dejavnost za skupnost v ocenjevanje učinkovitosti in sistem nagrajevanja.
- Razvijte tehnološke in podatkovne sisteme, prek katerih bodo informacije bolj dostopne policistom in skupnosti.
- Usposobite celotno osebje za skupnostne policijske dejavnosti.
- Policistom dajte večja pooblastila in zvišajte njihovo odgovornost.
- Spodbujajte policiste, da predlagajo nove rešitve za dolgotrajne probleme.
- Poenostavite hierarhično strukturo.

- Povečajte transparentnost aktivnosti in procesa odločanja agencije.
- Vključite policijsko dejavnost za skupnost v urjenje terenskih policistov.
- Policistom dajte proste roke pri oblikovanju novih odzivov.
- Razvijte tehnološki sistem za podporo problemske analize in vrednotenja.
- Vgradite policijsko dejavnost za skupnost v misije in strateško načrtovanje.

Vir: Chapman, Robert and Matthew Scheider, Community Policing for Mayors: A Municipal Service Model for Policing and Beyond. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006.

http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=32

Obveščevalno-varnostna dejavnost in boj proti terorizmu

Iztok Podbregar

Pred več tisoč leti je v klasičnem kitajskem priročniku o umetnosti vojne mojster *Sun Cu* o izrekel več pomembnih misli rabi vohunov. Med drugim je povedal tudi naslednje:

»Velika vojaška operacija močno izčrpa narod. Bitka za enodnevnega zmagovalca se lahko vleče dolga leta. Če nisi pripravljen plačevati za obveščevalne podatke o nasprotnikovem stanju, nisi človečen - potem tudi nisi resničen vojaški voditelj, niti pravi pomočnik vlade, niti ne zmagoslavni poveljnik. Prav predznanje je tisto, ki pametni vladi z modrim vojaškim vodstvom omogoči, da druge premaga in izpelje izredne načrte.

Tega predznanja ne moremo dobiti od duhov niti ga ne moremo razkriti z analogijo niti si ga ne moremo razjasniti z izračuni. Dobimo ga lahko le od ljudi, ki poznajo sovražnikovo stanje. Ločimo pet vrst vohunov: lokalne, notranje, dvojne, mrtve, žive. Kadar deluje vseh pet vrst vohunov, ne da bi kdorkoli poznal njihove poti, rečemo temu organizacijska genialnost. Ta je za vodstva nadvse dragocena.

Lokalne vohune najamemo med domačini. Notranje vohune najamemo med sovražnikovimi uradniki. Dvojne vohune najamemo med sovražnikovimi vohuni. Mrtvi vohuni predajajo sovražnikovim vohunom prirejene podatke. Živi vohuni se po opravljeni nalogi vrnejo in nam poročajo.«

Sodobne države in tudi organizacije različnih vrst (neprofitne, profitne) se zavedajo pomena prednosti, ki jih pridobijo z pravočasnimi, točnimi, uporabnimi podatki in informacijami. V ta namen bolj ali manj organizirano pristopajo k obveščevalno varnostni dejavnosti. Obveščevalna dejavnost, v najširšem pomenu, je dejavnost zbiranja, analiziranja, združevanja in interpretiranja vseh razpoložljivih podatkov, ki zadevajo enega ali več vidikov vsebinskega področja, ki je neposredno ali potencialno pomembno za načrtovalce in izvajalce odločitev, ki jim pravimo uporabniki obveščevalnih informacij.

Obveščevalno-varnostno dejavnost delimo na tri zvrsti: obveščevalno, protiobveščevalno in varnostno. Pri obveščevalni dejavnosti gre za zbiranje podatkov, pomembnih za nacionalno varnost zunaj območja naše države. Slovenija je članica Evropske Unije (EU) in članica Nata. Postavlja se vprašanje, kje je območje obveščevalnega zbiranja podatkov? Ali zunaj območja Republike Slovenije, ali zunaj območja EU in Nata? Pravniki imajo verjetno zelo točne odgovore. Zbiranje obveščevalnih podatkov iz EU in Nata, smo pa del teh multilateralnih organizacij, za našo nacionalno varnost ni potrebno. Navodila in usmeritve uporabnikov informacij (predsednik Vlade, ministri idr.) so verjetno že bolj ohlapne, ker potrebujejo čim več podatkov za svoje odločitve. Izvajalci obveščevalne dejavnosti, ki pa se na terenu soočajo s pestrimi podatki iz ne-transparentnih in raznolikih virov ogrožanja, imajo na to spet drugačen pogled. Še posebej sedaj, ko smo tudi na področju obveščevalno varnostne dejavnosti soočeni s pestrim mednarodnim sodelovanjem in je na terenu čutiti močan partnersko konkurenčni odnos.

Druga zvrst je protiobveščevalna dejavnost, kjer naše nacionalne interese ščitimo pred delovanjem tujih obveščevalnih služb.

Po vstopu Republike Slovenije v EU in v postopni graditvi novih držav Zahodnega Balkana, smo soočeni s povečano tovrstno dejavnostjo na ozemlju naše države. Kot da se je del obveščevalnih dejavnosti drugih držav iz tradicionalnega središča, tj. Dunaja, preselil v Ljubljano in prav nič ni odveč prebirati zgodovinske vire iz tridesetih let prejšnjega stoletja o dogajanju v Ljubljani, v katerih lahko prepoznavamo mnoge modele, značilne za našo Ljubljano še danes.

Tretja zvrst je varnostna zvrst, kjer naše nacionalno ozemlje ščitimo pred vsemi varnostnimi grožnjami, vključno z nadnacionalnimi grožnjami (organizirani kriminal, terorizem itd). Slovenija je geopolitično tranzitna država in je križišče poti iz vseh smeri. Poleg mnogih koristi in pozitivnih učinkov pa takšen geopolitični položaj na žalost predstavlja tudi odlično infrastrukturo za tiste, ki mislijo ter delajo bolj sebično in ozko oziroma za nas negativno.

Obveščevalno-varnostna dejavnost je v bistvu proces dejavnosti od zajemanja, zbiranja podatkov, njihovega vrednotenja in analiziranja ter distribucije informacij do uporabnikov raznolikih obveščevalno varnostnih informacij, potrebnih pri odločanju.

O potrebnosti te dejavnosti v sodobnem svetu ne želim polemizirati. Že res, da so mnenja o tem različna, vendar se večina tistih, ki so bili v vlogi uporabnika obveščevalnih informacij, strinja, da te informacije potrebujejo. Prav tako pa po sicer maloštevilnih raziskavah lahko ugotavljamo, da je vsebina obveščevalnih informacij udeležena v odločitvah v zelo majhnem, a morda v ključnem odstotku.

Zdi se pa nujno odpreti razpravo o vse krajšem času, ki je na voljo za izvedbo celotnega obveščevalno varnostnega procesa, kjer smo razen s časom zelo omejeni tudi z razpoložljivimi viri, pri tem pa je vsak del procesa zelo pomemben za celoto.

Upravičeno lahko trdimo, da so vse krajši čas, omejeni kadrovski, finančni, infrastrukturni in drugi viri ter netransparentne grožnje v sodobnem tehnološkem okolju tisti dejavniki, ki zahtevajo reinženiring obveščevalno varnostne dejavnosti, torej iskanje vse boljših rešitev s tem, kar je na voljo.

V nadaljevanju bom poskušal predstaviti nekaj dilem, razmišljanj pa tudi rešitev za tiste, ki v Sloveniji gradijo naš nacionalni varnostni sistem in njegove pomembne subjekte obveščevalno varnostne dejavnosti, tj. Slovensko obveščevalno-varnostno agencijo (SOVA) in Obveščevalno varnostno službo Ministrstva za obrambo (OVS MORS) in Kriminalistične policije.

PRIDOBIVANJE PODATKOV

Za pridobivanje oziroma zajemanje podatkov obveščevalno-varnostna dejavnost:

- uporablja zelo specifične oblike operativnega dela, tj. tajno sodelovanje;
- uporablja posebne oblike pridobivanja podatkov - spremljanje mednarodnih sistemov zvez, tajni odkup dokumentov in predmetov ter tajno opazovanje, sledenje na odprtih ali javnih prostorih z uporabo tehničnih sredstev za dokumentiranje;
- sodeluje in izmenjuje podatke med subjekti obveščevalno-varnostne dejavnosti v Sloveniji;
- zbira javno dostopne podatke;
- mednarodno sodeluje s partnerji.

Za uspešno opravljanje obveščevalno varnostnih nalog je potrebno stalno skrbeti za:

– izgradnjo in razvoj kakovostne sodelavske mreže, ki bo sposobna zagotoviti ustrezne podatke;
– uvajanje novih metod na področju vrednotenja in analiziranja podatkov;
– razvoj tehnike, ki bo zagotavljala operativno naravnanost obveščevalne dejavnosti;
– varne komunikacije;
– neprestano prilagajanje novim izzivom;
– fleksibilnost in sposobnost prilagajanja novim situacijam;
– fleksibilen pritok novih kadrov in
– drugo.

V zvezi z navedenimi pogoji delovanja obveščevalno-varnostne dejavnosti in izvajanjem nalog pa je potrebno izpostaviti nekaj pomembnih dejstev.

Sodobna družba je zelo občutljiva za posege v zasebnost in človekove pravice. Tudi v slovenskem prostoru je tako, da smo do vseh posegov v človekove pravice, ki se dogajajo v naši bližini, največkrat povsem neobčutljivi. Ko pa se zgodi poseg, ki ga zaznamo osebno, se ponavadi zelo burno odzovemo. Lahko bi rekli, da smo neobčutljivi do posegov v zasebnost in pravice drugih v neposrednem okolju in izjemno občutljivi na neposredne posege v našo zasebnost.

Dejstvo je, da tradicionalna in demokratična obveščevalno-varnostna dejavnost predvsem pri pridobivanju podatkov temelji in deluje na podlagi zakonitih oziroma demokratično nadzorovanih posegov v človekove pravice.

Razvoj obveščevalno-varnostne dejavnosti pri disciplini zajemanja podatkov bo šel v bodoče najverjetneje v dve smereh:

1. Nadaljevanje pridobivanja podatkov s poseganjem v človekove pravice, kjer bo z razvojem tehnologije vedno več posegov v človekovo zasebnost, ki jih bodo izvajalci obveščevalno varnostne dejavnosti težko prepoznavali. Javnost za takšne posege ne bo občutljiva, ker jih ne bo zaznala, zakonodaja in nadzor pa bosta v izvedbenem smislu ves čas zaostajala za realnim delovanjem, torej ne bosta nadzirala te dejavnosti.

Gre za kompleksno vprašanje, ki zahteva poglobljeno znanstveno raziskovanje tega področja in vse bolj kompetentne izvajalce obveščevalno-varnostne dejavnosti ter seveda zelo občutljive nadzornike posegov v človekove pravice.

2. Pogostejše zajemanje podatkov iz javnih virov, kjer ni nobenih posegov v človekove pravice. Sodobno okolje praktično nudi skoraj vse potrebne podatke za odločanje. Problem je, kako v množici podatkov, ki nas globalno obkrožajo, pridobiti nujno potrebne in zadostne. Zato je potrebno vključiti sodobno informacijsko tehnologijo in motivirati k sodelovanju za pridobivanja tako imenovanih javnih podatkov zadostno število sodelavcev.

Pri tovrstnem zbiranju podatkov je nujno potrebno ugotoviti, na podlagi vrednotenja in razvrščanja, tisti najnujnejši in najmanjši nabor podatkov za pridobitev, pri katerih bo potreben le minimalni, vendar zakoniti poseg v človekove pravice.

Menim, da bi načrtovalci sprememb v slovenski obveščevalno varnostni skupnosti, skupaj z nadzorniki in iskalci pravnih rešitev, lahko po prej opisanih napotilih najhitreje izgradili sodoben zajem podatkov, ki bi dajal zadostne rezultate za odjemalce in tiste, ki odločitve sprejemajo.

Graditev tradicionalnega tajnega sodelovanja je predolgotrajna, predraga in večkrat ne daje rezultatov v realnem času. Še posebej zato, ker so različni posegi v SOVO in OVS v zadnjih letih najverjetneje precej omajali zaupanje med registriranimi tajnimi sodelavci in operativci služb. To sodelovanje je namreč živ organizem, ki diha in deluje odlično le, če ne percipira zunanjih motenj. Neprestano nastopanje tovrstnih služb v medijih kot posledica nekaterih nepremišljenih aktivnosti prejšnje vlade, je občutno vplivalo in motilo tajno pridobivanje podatkov in omejilo to občutljivo delovanje za daljši čas.

Javni viri imajo v obveščevalno varnostni dejavnosti vse bolj pomembno vlogo. Ne samo pri možnosti takojšnje informiranosti o aktualnih dogodkih, pač pa tudi pri širšem razumevanju razvoja dogajanj, možnosti preverjanja podatkov iz različnih virov in podobno.

Javni viri v obveščevalni dejavnosti pa niso samo zbirka novih časopisnih izrezkov ali klipov. Prav tako niso samo kvalitetno brskanje po internetu,

temveč lahko s sodobno mrežo sodelavcev tudi na terenu preverjamo javno dostopne podatke, lahko gradimo mreže javnih virov in jih krmilimo glede na potrebe in drugo.

Kot pa sem že poudaril, javni viri ne morejo v celoti nadomestiti tajnega sodelovanja. Vedno bo obstajala potreba po osebi, ki bo tajno, za potrebe in po naročilu obveščevalne službe, vzpostavila neposreden stik s ciljnim okoljem in realizirala nekatere naloge, zaradi česar je tajno sodelovanje eno najpomembnejših obrtnih orodij obveščevalno-varnostne dejavnosti.

Tajni sodelavec obveščevalne službe je oseba, ki načrtno, prostovoljno, tajno in neprekinjeno zbira tajne podatke za potrebe obveščevalno-varnostne dejavnosti.

Naštejmo nekaj elementov tajnega sodelovanja v sodobni obveščevalno-varnostni dejavnosti:

- **prostovoljnost**, ki se kaže v zavestni odločitvi posameznika za sodelovanje z obveščevalno službo. Pravega sodelovanja si ni mogoče predstavljati brez prostovoljne, zavestne odločitve posameznika, da sodeluje v obveščevalno-varnostni dejavnosti. V operativni praksi namreč ni več primerov, da bi kdo tajno sodeloval pod prisilo;
- **načrtnost in organiziranost**, ki se kaže v formalnopravni urejenosti tajnega sodelovanja in usklajenem delovanju pod vodstvom obveščevalne službe za vnaprej določen cilj;
- **tajnost,** ki je temeljno načelo tajnega sodelovanja in osnovna obligacija med obveščevalno službo in njenimi tajnimi sodelavci, pri čemer se je treba zavedati, da odkrit vir ni več vir. Cilj tajnosti sodelovanja je zaščita osebnosti tajnega sodelavca, zaščita zaupanja v obveščevalno službo in njene naloge;
- **trajnost oziroma stalnost**, ki je velikokrat pogoj za uspešno realizacijo nalog, kjer ni improvizacij, nenadnih vpadov, prekinitev in opustitev temveč sta pomembni doslednost in trajnost.

Danes se upravičeno postavlja vprašanje, ali je za vse naloge, ki jih izvaja neka obveščevalna služba, potrebno delovati po teh načelih. Na primer, če mora obveščevalna služba v nekem oddaljenem mestu preveriti kakšen rutinski podatek, ki je pri vsem tem še več ali manj javno dostopen, potrebuje za to več dni, da po vseh načelih sodelovanja organizira vse faze

tajnega pridobivanja podatka. Porabi lahko tudi veliko denarja, dodatno pa še zamuja ali zamudi glede na razpoložljiv - kratek čas obveščevalnega procesa. Verjetno je lažje in veliko hitreje poklicati znanca oziroma osebo iz javne mreže agencije in v nekaj minutah dobiti ali preveriti povsem javno dostopen podatek.

Formalno se tajno sodelovanje začne z registracijo sodelavca, konča pa se z deregistracijo sodelavca.

Tajno sodelovanje se postavlja po naslednjih fazah:

- določitev ciljnega okolja in osebe, prek katere bi lahko pridobivali operativne podatke,
- preverjanje kandidata za tajno sodelovanje,
- približevanje kandidatu za tajno sodelovanje in
- privolitev kandidata za tajno sodelovanje.

V fazah postavljanja tajnega sodelovanja lahko že z bežnim prebiranjem vseh dejavnikov in stopenj ugotovimo, da gre vsekakor za zelo kompleksne interdisciplinarne naloge v zelo kratkem razpoložljivem času.

Pravzaprav je danes težko pri posameznikih najti takšne interdisciplinarne kompetence, zato se v sodobnih obveščevalni službah vse bolj uveljavlja teamsko delo, kjer v celotnem procesu obveščevalne dejavnosti sodelujejo teami operativcev, analitikov, tehničnih strokovnjakov, psihologov, sociologov, ekonomistov, komunikologov itd.

Horizontalni procesni pristopi in delovanje so realnost in prihodnost obveščevalne dejavnosti, kar pa pri tradicionalistih obveščevalnih služb vzbuja nezaupanje in odpor. Pravilen teamski pristop zagotavlja kakovost in tajnost ter izjemno strokovnost v vseh fazah delovanja in daje rezultate v realnem času.

VREDNOTENJE IN ANALITIKA

Analitika se posredno ali neposredno vključuje v vse glavne faze obveščevalnega procesa, glavnina njenih nalog pa je povezana z **obdelavo podatkov (vrednotenje in analiziranje) in s pripravo ustreznih informacij za naslovnike.**

Usmerjanje obveščevalne dejavnosti se začne z natančno določitvijo informacijskih potreb in prioritet oziroma prednostnih nalog, ki iz njih izhajajo. V tej fazi je treba na osnovi želja, zahtev in naročil uporabnikov natančno opredeliti, katere podatke je treba zbrati. Skratka, analitiki morajo informacijske potrebe preoblikovati v cilje operativne raziskave – **usmerjevalna funkcija analitike**.

Zbrane podatke analitiki najprej ovrednotijo oziroma ugotavljajo njihov pomen glede

na aktualnost, vsebinsko oziroma informativno vrednost ter uporabnost, pri čemer upoštevajo tudi zanesljivost vira podatkov in stopnjo preverjenosti podatkov. Zgolj v vsebinskem smislu (kot povratna informacija operativi), lahko te naloge imenujemo tudi **kontrolna funkcija analitike.** Temu sledi faza analiziranja, v kateri analitiki podatke podrobno razčlenijo, ponovno integrirajo ter na koncu interpretirajo v obliki različnih analitičnih informacij.

Glede na ugotovitve in zaključke analiziranja pa je lahko funkcija analitike bodisi **deskriptivno - razlagalna** oziroma informativna (opisovanje dejanskega stanja ali tendenc v razvoju analiziranih pojavov, razlogov zanje in njihovih morebitnih posledic) bodisi **predlagalno - usmerjevalna** (predlaganje ukrepov, ki bi analizirano stanje usmerili v želeno smer).

Ker so vse dejavnosti v obveščevalnem procesu medsebojno tesno povezane in prepletene, je pogoj za doseganje optimalnih rezultatov na analitičnem področju dobro sodelovanje vseh delov omenjenega procesa.

Analitik mora biti posebej pozoren na možnost potvorjene ali neresnične informacije, kadar:

- podatkov iz informacij ni mogoče preveriti prek drugih virov (niti javno dostopnih virov),
- je podatek pridobil le en vir (je torej unikaten) in se ne ujema s podatki drugih virov o isti problematiki,
- vir posreduje podatke iz okolij, do katerih sam oziroma njegovi viri nimajo dostopa,
- vir posreduje podatke zaradi domneve, da takšne podatke ali ocene od njega pričakujejo.

Sodobna analitika mora imeti na voljo sodobna informacijska orodja in programe za vrednotenje, analiziranje in postavljanje analitičnih tez. Praktično je brez ustrezne informacijske tehnologije nemogoče v razpoložljivem času kakovostno sodelovati v obveščevalnem procesu.

UPORABNIKI, NJIHOVA PERCEPCIJA TER ŠIRITEV ŠTEVILA UPORABNIKOV

Obstaja več različnih načinov posredovanja informacij končnim prejemnikom, najpomembneje pa je, da jim omogočimo, da nam dajo povratne informacije na posredovane vsebine. Odzivi, mnenja ali sugestije prejemnikov so zelo pomembni, saj bodisi potrjujejo pravilno usmerjenost obveščevalnega dela bodisi dajejo usmeritve za prihodnje delo, skratka vplivajo na njegovo kakovost.

Trendi – prednosti in slabosti

Razvoj tehnologije posredovanja obveščevalnih podatkov prinaša v odnosu med obveščevalno službo in uporabniki njenih informacij spremembe. Aktualni trendi na tem področju gredo namreč v smeri uporabe **koncepta interneta** tudi za prenos obveščevalnih podatkov.

Tako naj bi obveščevalne službe v prihodnje oblikovale elektronske baze, v katere bi uvrščale svoje obveščevalne izdelke, uporabniki pa bi med slednjimi sami izbirali (deskanje) ustrezne informacije.

Tiskanja obveščevalnih izdelkov (papirna oblika) naj bi bilo tako v prihodnje vse manj, saj je tak postopek posredovanja tudi dolgotrajnejši od elektronskega.

Vzporedno naj bi se še bolj razvilo t.i. ustno brifiranje oziroma osebni stiki med oblikovalci obveščevalnih izdelkov in uporabniki.

Tradicionalno posredovanje obveščevalnih izdelkov, ki temelji na t.i. »push architecture«, naj bi nadomestil t.i. model »pull architecture«.

Sedanji način namreč predvideva, da analitik iz množice podatkov izbere tiste, za katere meni, da jih uporabnik potrebuje in mu jih posreduje v

predpisani obliki. Slabosti takšnega načina so, da analitik ne ve vedno natančno, katere informacije uporabnik v danem trenutku resnično potrebuje. Če je analitikovo poročilo prekratko, obstaja nevarnost, da je izločil tudi pomembne informacije, če je preobsežno, pa tvega, da uporabnik njegovih informacij sploh ne bo prebral oziroma vsaj ne v celoti.

Prav tako je lahko njegovo poročilo posredovano bodisi prezgodaj bodisi prepozno. Določeno težavo predstavljajo tudi izdelki, namenjeni širšemu krogu, saj naslovniki, katerih obravnavana problematika ni primarni interes, najverjetneje te informacije ne bodo prebrali, prav tako pa obstaja možnost, da bodo tudi vse nadaljnje podobne izdelke obravnavali zelo površno. Podobno velja tudi za izdelke, ki so namenjeni le ozkemu krogu. Pri slednjih obstaja nevarnost, da z njihovo vsebino ne bodo seznanjeni tisti, ki so za to problematiko pristojni. Problem je tudi odločitev, kako pogosto obveščati naslovnika o novih oziroma dodatnih ugotovitvah o obravnavani problematiki. Če je dodatnih informacij veliko, lahko naslovnika zasujemo z njimi, kar zmanjšuje njihovo učinkovitost. Skratka, v sedanjem načinu posredovanja obveščevalnih izdelkov je kar nekaj slabosti, ki lahko negativno vplivajo na njihovo učinkovitost in verodostojnost.

Pri novem načinu posredovanja pa naj bi bila odločitev o izboru podatkov, stopnji njihove podrobnosti, obliki in času (timing) prepuščena kar uporabniku. V bistvu bi analitik še naprej oblikoval enake vrste izdelkov kot doslej, ki pa bi bili uvrščeni v skupno bazo obveščevalnih izdelkov, med katerimi bi uporabniki izbirali zase najustreznejše.

Prva predpostavka takšnega načina pa je, da so vsi uporabniki usposobljeni za delo z bazami ozlroma iskanje po parametrih. Hkrati pa bodo morali analitiki v nekem smislu spremeniti dosedanjo obliko svojih izdelkov oziroma jo strukturirati tako, da bo omogočala iskanje (glavni parametri oziroma ključne besede, povzetki itn.). Pomisleki, ki se že sedaj pojavljajo glede novega načina, so povezani zlasti s strahom, da se bo povečalo predvsem povpraševanje po surovih podatkih, dejstvih, oblikovanje zaključkov in ocen pa bo vse bolj prepuščeno uporabnikom. Po najbolj črnogledem scenariju naj bi uporabniki vse bolj postajali tudi »obveščevalni analitiki« in bodo zato dosedanji profesionalni analitiki vse manj potrebni.

Seveda pa je slednje skoraj neverjetno, saj so uporabniki zelo obremenjeni, jim kronično primanjkuje časa, zato bodo gotovo tudi v prihodnje

dobre analize oziroma mnenja ekspertov še kako pomembna. Analize namreč poleg golih dejstev dajejo tudi informacije o zanesljivosti podatkov, opozarjajo na različne možnosti razvoja dogajanja in tako preprečujejo morebitna neprijetna presenečenja

Pričakovati je, da se bo tudi s predvidenim uveljavljanjem modela »deskanja po bazah« še povečala potreba tako po kratkih, ažurnih in zelo skoncentriranih informacijah (le najnovejša dejstva), ki bodo kar najhitreje dostopne v bazi, hkrati pa tudi po informacijah oziroma analizah, ki bodo uporabnikom pomagale razumeti ozadje in predvsem pomen novih dejstev ter dogodkov. Zahteva po čim hitreje dostopnih informacijah ima tudi negativne strani. Krajšanje časa za vrednotenje in analiziranje podatkov in stalni časovni pritisk bosta analitikom najverjetneje preprečevala podrobnejšo proučitev vseh novih dejstev oziroma uporabo zahtevnejših metodoloških pristopov (npr. analizo alternativnih hipotez).

Ne glede na vse možne slabosti in pomanjkljivosti pa je osnovni cilj opisanega trenda: **več informacij, boljše informacije, njihovo hitrejše posredovanje ter predvsem - bolj uporabne informacije.**

Informacije morajo zadostiti naslednjim kriterijem:

- novost vsebine,
- pomembnost, uporabnost in koristnost za uporabnika,
- aktualnost,
- pravočasnost in ažurnost,
- resničnost oziroma preverjenost podatkov,
- točnost in natančnost podatkov,
- objektivnost in nepristranskost,
- jasna razmejitev med podatki in mnenji,
- navajanje vira podatkov,
- ustreznost in
- drugo.

Uporabnik obveščevalnih izdelkov mora biti vsebinsko kompetenten, strokovno usposobljen in socialno uravnotežen ter mora v osnovnih okvirih poznati celoten obveščevalni proces, da bi lahko kakovostno podal usmeritve, izrazil jasne zahteve in popolnoma uporabil dobljene obveščevalne informacije. Prav tako zelo koristi miselna odprtost, intelektualna rado-

vednost, intuicija, ustvarjalnost, sistematičnost, metodičnost, načrtnost, intelektualna poštenost in pogum, kritičnost in samokritičnost, prilagodljivost oziroma fleksibilnost.

To je še posebej pomembno v obdobju, ko v roke prevzema vajeti nova Vlada RS, kjer so ministrske in ostale vodilne vloge prevzeli povsem novi ljudje, ki se prvič srečujejo z vlogo uporabnika obveščevalnih informacij in podatkov. Takšne situacije postavljajo pred vodstva naših obveščevalno-varnostnih subjektov precej pomembno delo usposabljanja in harmonizacije delovanja.

PERCEPCIJA UPORABNIKOV OBVEŠČEVALNIH INFORMACIJ

Uporabniki dojemajo realnost na podlagi sprejetih informacijah. Poleg **individualne ravni dojemanja** pa je treba upoštevati še t.i. **organizacijsko oziroma skupinsko raven**, saj uporabnik ne deluje v zaprtem okolju, temveč v okviru manjše organizacijske skupine, enote in ne nazadnje večje organizacije, ki s svojim ustaljenim organizacijskim procesom v nekem smislu prav tako vpliva na uporabnikovo percepcijo.

Dejstvo je, da točna obveščevalna analiza zahteva tudi točno in natančno dojemanje realnosti.

Ponavadi pa o sami percepciji niti ne razmišljamo, saj jo dojemamo kot povsem pasivno dejanje, čeprav je resnica povsem drugačna. Gre za zelo aktivno dejanje, saj skupaj z dojemanjem oblikujemo tudi svoje videnje realnosti. Skratka, tudi na osnovi enakih informacij si ljudje oblikujejo različne oziroma svoje razlage njihovega pomena. Poleg tega obstajajo v vsakem dojemanju tudi negativne tendence, ki so slabost in omejitev tudi za analitično razmišljanje.

Predstavili smo različna možna tveganja, pasti in napake v dojemanju uporabnika, vendar še zdaleč ne vseh. Človeški miselni proces je le eden od virov napak. Naše sicer nepristransko ravnanje oziroma reševanje problema pa lahko spremenijo tudi potrebe, želje ali pričakovanja itd.

Praksa oziroma izkušnje pri delu na analitičnem področju kažejo, da so najpogostejše napake povezane predvsem z naslednjimi pomanjkljivostmi in nedoslednostmi, skratka slabostmi v procesu vrednotenja in analiziranja podatkov, te slabosti pa vplivajo na dojemanje uporabnika obveščevalnih informacij:

Mnenja, ki jih ne podpirajo dejstva. Mnenja analitikov ali uporabnikov o tem, kaj bi bilo dobro oziroma kaj bi želeli, da se zgodi, lahko negativno vplivajo na izbor podatkov ter metod in načinov njihovega vrednotenja in analiziranja.

Zrcalna prevara. Gre za zmotno mišljenje, da morajo različne osebe, ki analizirajo iste dogodke, priti tudi do istih zaključkov. Nevarnost je torej v zmotnem prepričanju analitika, da obstaja ena sama možna interpretacija podatkov, pri čemer zanemarja številne druge okoliščine (različne kulture, vrednote, miselne vzorce itn.), ki prav tako vplivajo na vrednotenje podatkov.

Breme navajenosti je pravzaprav vrsta poenostavitve, pri kateri analitik uporabi le del zbranega informacijskega materiala in na osnovi tega izpelje zaključke, ki jih nato posploši (uporaba enostavnih miselnih vzorcev in posploševanja). Napaka je v tem, da pri takšnem načinu analitik izbere le nekaj podatkov in med njimi vzpostavi povezave na osnovi domnev, ne pa objektivnih dejstev.

Zloraba analogije se zgodi, ko analitik gradi konstrukcijo problema na podobnosti. Napaka je v tem, da podobni dogodki ne morejo biti argument pri dokazovanju, temveč le pomoč pri pojasnjevanju.

Enačenje namena in sposobnosti pomeni nerazlikovanje med dejanskim namenom oziroma interesi države, organizacije ali posameznika za izvršitev kakega dejanja ter dejansko sposobnostjo za njegovo uresničitev. Namen namreč še ne pomeni tudi sposobnosti in obratno. Analitik mora upoštevati, da pomeni realno grožnjo in nevarnost predvsem tisti, ki ima namen in sposobnosti, da ta namen uresniči.

V bistvu gre za **enačenje možnosti in verjetnosti.** Dogodek je možen takrat, ko je z vidika objektivnosti mogoče sklepati, da se res lahko zgodi. Nasprotno, verjeten pa je takrat, ko je zaradi razumljivih vzrokov razumno

pričakovati (ne sklepati), da se bo zgodil. Vse stvari, ki so verjetne, so tudi možne, medtem ko obratno ne velja – če so možne, še niso verjetne. Pri verjetnosti je poleg sposobnosti pomemben tudi namen.

Nepazljivost se običajno zgodi zaradi nasičenosti s podatki ali nenehne izpostavljenosti kriznim razmeram. V takih situacijah se lahko zniža prag analitikove pozornosti, saj je tako zatopljen v problem, da ne opazi, da se je medtem ko ga proučuje, že spremenil.

Predsodki, ki jih največkrat ne moremo spremeniti ali odpraviti, moramo pa se jih zavedati in si prizadevati, da ne bi vplivali na naše vrednotenje. Človeški element je namreč pri analitični dejavnosti odločilen. Učinkovitost metod in tehnik je odvisna prav od ljudi, ki jih uporabljajo.

NADZOR OBVEŠČEVALNO-VARNOSTNE DEJAVNOSTI

Vprašanje nadzora nad delom obveščevalnih in varnostnih služb je v neposredni zvezi z zaupanjem javnosti v njihovo delo. Delovanje služb, ki izvajajo obveščevalno varnostno dejavnost, velikokrat zbuja dvome o zakonitosti in tudi strokovnosti njihovega dela.

Republika Slovenija je zato uvedla različne oblike nadzora nad njimi, saj le-ta povečuje raven njihove legitimnosti ter zagotavlja varstvo človekovih pravic.

V Sloveniji imamo razvejan model nadzora obveščevalno-varnostne dejavnosti, ki ga izvajajo institucije različnih vej oblasti:

- Vlada Republike Slovenije, kot celota in prek različnih vladnih organov in inšpekcij;
- Parlament prek Parlamentarne komisije za nadzor nad obveščevalno-varnostnimi službami;
- sodni nadzor prek Vrhovnega sodišča RS, ki izdaja na predlog predstojnika službe sodne odredbe za posege v človekove pravice;
- Računsko sodišče, ki izvaja nadzor nad porabo proračunskih finančnih sredstev;

– Varuh človekovih pravic, ki na podlagi zahtev državljanov preverja zakonitost in potrebnost posegov v človekove pravice;
– Informacijska pooblaščenka, ki izvaja nadzor v zvezi z informacijskimi posegi v zasebnost;
– javnost, ki prek medijev izvaja določen nadzor;
– notranji nadzor v službah;
– drugi.

Za izvajanje nadzora imajo praviloma vse naštete nadzorne institucije jasno določena zakonska pooblastila, ki jih, po mojem mnenju, tudi izvajajo. O učinkih izvajanja vseh vrst nadzora pa lahko navedem nekaj lastnih izkušenj in pogledov.

Moje osebno mnenje je, da uravnoteženega in stalnega nadzora ni nikoli dovolj ali celo preveč. Postavlja pa se vprašanje, kaj je uravnotežen in odmerjen nadzor. Zame je to nadzor, ki na eni strani zagotavlja kvalitetno izvedbo nadzora posameznim nadzornim institucijam, hkrati pa zagotovi kvalitetno izvajanje zakonitih nalog nadzorovani obveščevalno-varnostni službi ali agenciji.

KAKO GRADITI OBVEŠČEVALNO DEJAVNOST V SLOVENIJI Z ORGANIZACIJSKEGA VIDIKA

Najprej je potrebno nekaj stavkov nameniti organizaciji in delovanju Sveta za nacionalno varnost Republike Slovenije (SNAV), ki je posvetovalno telo Vlade RS za vsebine nacionalne varnosti.

Že nekaj časa se pojavljajo v javnosti razprave, da je to, sicer koordinativno telo, potrebno podpreti z določeno profesionalno organizacijsko strukturo. Prav gotovo slovenski SNAV potrebuje boljšo strokovno podporo za učinkovito delovanje. Ponavadi je tako, da čim ustanoviš novo organizacijsko strukturo s sistemizacijo za stalno zaposlene uslužbence javne uprave, se le ta postopoma, vendar vedno, razbohoti in postane neučinkovita.

Več let sem bil sekretar SNAV in menim, da bi zadostovalo že to, da bi na vsakem ministrstvu določili že zaposleni osebi nekje blizu ministra, da bi večji del delovnega časa namenila podpori svojega ministrstva za SNAV. Na ta način bi dosegli izjemne učinke brez novih organizacijskih struktur.

Vsake morebitne večje spremembe na tem področju pa bi pred uveljavitvijo dobro preveril z simulacijsko vajo.

V Sloveniji smo tako v SOVA, kot v OVS MORS gradili hibridno organizacijo za izvajanje obveščevalno-varnostne dejavnosti. Torej, ena organizacijska struktura izvaja obveščevalne in varnostne ter protiobveščevalne naloge.

V EU so uveljavljeni različni modeli in moram povedati, da je tudi pri nas ves čas po letu 1991 prisotna razprava med poznavalci o tem, da je treba sedanji hibridni model spremeniti. Z vidika virov - kadrovskih, finančnih, infrastrukturnih, kot tudi z vidika groženj nacionalni varnosti, se mi zdi takšna struktura sprejemljivejša. Ne nazadnje je lahko tudi zelo učinkovita glede na vse krajši čas, ki je odmerjen izvedbi obveščevalno-varnostnih nalog.

V zadnjih letih se morda pojavlja podvajanje zakonsko predpisanih obveščevalnih nalog med SOVO in OVS MO, kar pa je nujno potrebno urediti.

Nasploh je potrebno med SOVO in OVS MO doseči veliko večjo sinergijo. Bilo bi pa zelo napačno, da bi preambiciozni posamezniki z določenimi, premalo premišljenimi idejami, uspeli pri političnih avtoritetah doseči odločitve za hitre spremembe v OVS MO in SOVI, kar bi verjetno povzročilo samo še kakšno dodatno afero.

Če je za spremembe SNAV in njegovega delovanja, pri čemer pa je potrebna odmerjena postopnost, ki še posebej velja za vse spremembe obveščevalno varnostne dejavnosti in njene specifične naloge. Najboljše so premišljene, s simulacijo preverjene in postopne spremembe. Imam izkušnjo iz leta 2002, ko smo SOVO selili iz ene lokacije na drugo in nekoliko spremenili način delovanja, pa nam je uspelo to narediti brez pretresov, ker smo se dalj časa temeljito in motivirano pripravljali.

Hiti počasi, je najboljši recept.

V.

Utrjevanje tarč

Napotek 28: Ocenite ranljivost tarče: uporabite IVIL UZBL (angl. EVIL DONE – narejeno zlo op. prev.)

Kot sva že izpostavila, je z analizo dveh bistvenih lastnosti mogoče identificirati tarče, ki so za teroriste bolj atraktivne: ranljivost in pričakovana izguba. V tem napotku predstavljava način, kako oceniti ranljivost tarč z uporabo IVIL UZBL, akronima, ki povzema pomembne vidike ranljivosti. Zapomnite si, da se ranljivost nanaša na značilnost tarče, ki lahko privabi teroristični napad, medtem ko se pričakovana izguba nanaša na predvidene poškodbe ali škodo, do katere lahko pride, če je tarča napadena. O določanju pričakovane izgube bomo govorili v naslednjem napotku.

Elementi IVIL UZBL (angl. EVIL DONE)

Izpostavljenost (**E**xposed): tarča izstopa iz mestnega obrisa (na primer Dvojčka ali Kip svobode) ali na kak drug način: edina večnadstropna zgradba v majhnem mestecu; zgradba zvezne oblasti; velik nakupovalni kompleks; nuklearna elektrarna.

Vitalnost (**V**ital): tarča igra osrednjo vlogo v vsakdanjem življenju. Oskrba z vodo, električno omrežje, prehrambena veriga in transportni sistem so vitalni za katerokoli mesto, majhno ali veliko. Če teroristi menijo, da bo njihovo uničenje povzročilo zmedo, bodo morda izbrali te tarče.

Ikoničnost (**I**conic): tarče, ki imajo visoko simbolično vrednost, tudi lahko pritegnejo teroriste. Kip svobode, na primer, je predvsem ikona New York Cityja in Združenih držav na splošno. Tim McVeigh pa je izbral Zvezno stavbo Alfreda P. Murraha v Oklahoma Cityju, ker je predstavljala zvezno oblasti, ki jo je preziral. Čeprav ne tako ikonična kot Kip svobode, je predstavljala nekaj abstraktnega in pomembnega: zvezno oblast.

Legitimnost (**L**egitimate): pomemben dejavnik pri odločitvi za napad tarče je, kako bodo napad dojemali drugi teroristi, njihovi podporniki in namišljeni podporniki. Če bodo napad dojeli kot nelegitimen – kot je bil IRIN umor lorda Mountbattena leta 1979 – bo teroristična skupina morda izgubila javno podporo. Hamas v Palestini izvaja pogoste raziskave javnega mnenja, da bi ugotovil, ali njihovi podporniki izbrane tarče dojemajo kot legitimne.

Uničljivost (**D**estructible): tarča mora biti uničena ali izbrani posamezniki ubiti, da se teroristično dejanje oceni kot uspešno. Nekatere stavbe so težko uničljive in nekateri ljudje so preveč dobro varovani, da bi jih lahko ubili. Teroristi zato na tarčo morda za nekaj časa odložijo napad, ker menijo, da je neuničljiva. Kot taka sta veljala tudi Dvojčka, dokler Al Kaida v drugem napadu ni izumila načina za njuno uničenje.

Zasedenost (**O**ccupied): z redkimi izjemami teroristi poskušajo ubiti čim več ljudi, ker je to tisto, kar najbolj straši njihove sovražnike. Prednost imajo tarče, katerih uničenje ustvarja množične žrtve; to so lahko bodisi prostorna zbirališča z veliko ljudmi ali pa manjše, gosto nagnetene tarče, kot so kavarne ali vlaki.

Bližina (Near): razdalja je vitalnega pomena pri razumevanju terorizma, tako kot pri pojasnjevanju kriminala. Študije kažejo, da kršitelji običajno izberejo bližnje tarče in pogosto prežijo na svoje lastne soseske in skupnosti. Če teroristi živijo tesno skupaj s tistimi, katere sovražijo, je njihova naloga močno poenostavljena; ne le da je logistika napada veliko lažja, temveč je možnost pobega veliko večja, če se storilec lahko zlije z okoliško skupnostjo. Primer irske republikanske armade (IRA) to potrjuje: od 1970 do 1994 je IRA pripravila na desettisoče napadov na Severnem Irskem, vendar le peščico v Angliji. Razdalja je zelo važna, ko gre za domače teroriste v zelo velikem okolišu. Ko gre za tuje teroriste, so vse tarče v vašem okolišu enako oddaljene – razen če teroristi delujejo iz priseljenske soseske, kot npr. odgovorni za prvi napad na Dvojčka, ki so prišli iz bližnjega Jersey Cityja v New Jerseyju.

Lahkost (**E**asy): Kako lahko je dostopna tarča? Za Timothya McVeigha je bila prelahko dostopna: uspel je parkirati svoj tovornjak samo 8 čevljev od stavbe Murrah. Kako lahko se je Al Kaida prebila do Svetovnega trgovinskega centra? Pri prvem napadu je bilo to zaradi pomanjkljive varnosti v podzemni parkirni garaži relativno lahko. Drugi napad pa je zahteval zapletene priprave, vključno z urjenjem pilotov, da so usmerili komercialna letala v Dvojčka.

Uporabite model IVIL UZBL

Tabela ponazarja uporabo IVIL UZBL za nekatere razpoznavne lokacije v Washingtonu, D.C. z vidika tujih teroristov, ki načrtujejo napad z uporabo letal ali tovornjakov bomb. (»Bližina« ima manjšo vlogo pri izbiri, ker je vsaka lokacija enako oddaljena od tuje operacijske baze.) Ocenam v tabeli je mogoče oporekati, pa tudi vse teroristične skupine nimajo istih prioritet. Namen tabele je le pokazati, da je v bistvu mogoče oceniti ranljivost tarč vsakega mesta. Narišete lahko podobno mrežo in jo uporabite za identifikacijo in oceno tarč v vaši skupnosti. Vprašajte se, kako se njihove značilnosti spreminjajo glede na metodo (uporaba strelnega orožja, požig) in vrsto terorističnega napada (domač, enoproblemski). To je prvi korak v pripravi sistematičnega načrta za zaščito tarč. V naslednjih napotkih bova predstavila metodo ocenjevanja pričakovane izgube, če je tarča zadeta.

Lestvica privlačnosti tarč, Washington, D.C. (simulirani primer)

1=majhna privlačnost; *5*=velika privlačnost

Značilnosti tarče	Bela hiša	Kongres Združenih držav	Pentagon	Washingtonski spomenik	Žel. postaja	Wasingtonska nacionalna katedrala	Stara pošta	Univerza Georgetown	Narodni živalski vrt
Izpostavljenost	4	*5*	*5*	*5*	3	4	0	2	1
Vitalnost	3	3	4	0	4	0	0	1	0
Ikoničnost	*5*	*5*	5	2	0	1	0	0	0
Legitimnost	*5*	*5*	5	*5*	3	1	2	1	0
Uničljivost	4	3	2	4	4	4	4	1	1
Zasedenost	4	4	3	2	4	1	2	3	3
Bližina	1	1	1	1	1	1	1	1	1
Lahkost	2	3	3	2	*5*	*5*	4	4	4
SKUPAJ TOČK	28	29	28	21	24	17	13	13	10

Vir: Clarke, Ronald V. in Graeme R. Newman, Outsmarting The Terrorists. Westport, Connecticut: Praeger Security International, 2006.

Napotek 29: Predvidite stranske učinke napada – uporabite KDORUP (angl. CARVER – veliki nož op.prev.)

Prejšnji napotek je opisoval oceno ranljivosti – verjetnosti, da bo določena tarča napadena – z uporabo IVIL UZBL. V tem napotku sva opisala KDORUP (angl. CARVER), metodo za ocenjevanje pričakovane izgube zaradi napada na kakršnokoli posebno tarčo. Upoštevajte, da ranljivost in pričakovana izguba nista nujno soodnosni; torej, **četudi je tarča močno ranljiva, ni nujno, da bo pričakovanja izguba ob napadu zelo velika.** Na primer, napad na električno omrežje morda ne bo zahteval človeških življenj ali poškodb – kljub temu pa bo velikemu številu ljudi povzročil nevšečnosti – torej potencialna izguba življenja ne bo tako velika kakor v primeru uničenja velike, zasedene poslovne stavbe.

Predstavitev KDORUP (angl. CARVER)

KDORUP je protokol, ki ga uporabljajo posebne operacijske enote Združenih držav (U.S. Special Operations Forces) za ocenjevanje in izbor nasprotnikovih postavitev. Obstaja veliko različic tega protokola, ki je bil prilagojen številnim lokacijam, tarčam in okoliščinam. Nekaj podobnosti ima z IVIL UZBL, vendar pa ta tarče obravnava z vidika lastnika in ne z vidika terorista, kar je primarni zorni kot v okviru IVIL UZBL.

KDORUP in IVIL UZBL na različna načina ocenjujeta ranljivosti tarče; vendar pa KDORUP vključuje tudi oceno pričakovane izgube ob napadu. Pričakovana izguba pomeni poškodbe in škodo, ki so lahko posledica napada, medtem ko ranljivost pomeni verjetnost, da bo tarča napadena (kar ocenjuje IVIL UZBL). Pričakovana izguba in ranljivost združena nudita oceno tveganja:

TVEGANJE = RANLJIVOST + PRIČAKOVANA IZGUBA

Lahko se zgodi, da zaradi praktičnih ali celo proračunskih razlogov določene tarče ni mogoče popolnoma zaščititi. Na primer, električno omrežje je precej izpostavljeno in pokriva obsežno geografsko področje, kljub temu pa je mogoče zavarovati njegove najbolj kritične točke in vzpostavi rezervni sistem za zagotovitev nemotenega obratovanja omrežja, četudi je ena kritična točka onesposobljena. Čeprav omrežje ostane ranljivo, je

pričakovana izguba zmanjšana, ker je škoda, ki jo utegne povzročiti napad, minimalizirana.

Elementi KDORUP (angl. CARVER)

Kritičnost (**C**riticality): Bo uspešen napad pomembno vplival na delovanje in storilnost objekta? (Pričakovana izguba)

Dostopnost (**A**ccessibility): Kako napadalec doseže tarčo? Bo potreboval posebno orodje ali orožje? So bili sprejeti ukrepi za zavarovanje tarče? (Ranljivost)

Obnovljivost (**R**ecuperability): Koliko časa bodo trajali zamenjava, obhod ali popravilo tarče? (Pričakovana izguba)

Ranljivost (Vulnerability): Je tarča grajena tako, da bo kos napadu? Vsebuje vnetljive snovi, ki bodo stopnjevale udarnost napada? (Ranljivost)

Učinek (**E**ffect): Kakšen učinek bo imel napad? Bo šokiral lokalno prebivalstvo? Bo prišlo do verižnega učinka na druge kritične tarče? Uničenje Svetovnega trgovinskega centra je na primer vplivalo na borzno trgovanje in ekonomsko sposobnost letalskih družb. (Pričakovana izguba)

Prepoznavnost (**R**ecognizability): Je tarča izrazita ali ikonična (npr. Pentagon, Empire State Building)? Je varovana s poostrenimi varnostnimi ukrepi (kot je jekleni obroč okoli Bele hiše), ki poudarjajo njeno pomembnost? (Ranljivost)

Ti kriteriji so osnova ocenjevalne lestvice, ki jo lahko uporabite za strukture in objekte v vašem okolišu. Ocene so lahko popolnoma subjektivne, kljub temu bi bile pri ocenjevanju vsake komponente koristne nekakšne smernice. Zato sva pripravila skrajšan model, ki ga boste lahko prilagodili svojim lastnim lokalnim potrebam. Seveda je KDORUP le okvirno vodilo. Lahko je bolj ali manj uporabno, odvisno od lokalnih okoliščin. V vsakem primeru bo uporaba KDORUP in IVIL UZBL zadostovala za začetek vaših lastnih sistematičnih ocen tveganja.

Primer KDORUP protokola

KRITIČNOST (Criticality)
(izid uspešnega napada)

Takojšnje zaprtje objekta za nedoločen čas, gospodarska motnja, nevarnost za lokalno skupnost..... *5*

Takojšnje zaprtje, ponovno obratovanje po več mesecih, nevarnost za lokalno skupnost 4

Ponovno obratovanje po več tednih, nekaj gospodarskih motenj 3

Ponovno obratovanje po 2 tednih, nevšečnosti za skupnost 2

Objekt ni bistven za skupnost, minimalen razdor..... 1

DOSTOPNOST (Accessibility)

Varnost okolice, neobstoječe vhodne točke..... *5*

Okolica je ograjena, vendar so številne vhodne točke nevarovane..... 4

Video nadzor, neizurjeno varnostno osebje..... 3

Uporabljen je PKPOM* (angl. CPTED), izurjeno varnostno osebje..... 2

PKPOM, zračen nadzor, visoko tehnološka identifikacija za vstop, blažilna cona..... 1

OBNOVLJIVOST (Recuperability)

Ni dodatnih sistemov, opreme ali materialov..... *5*

Omejena rezervna oprema ali materiali 4

Dodatni sistemi so nameščeni, ni načrta za nujne primere..... 3

Obnovitvena oprema in sistemi na varni lokaciji, načrt za nujne primere 2

Obsežni dodatni sistemi, načrt za nune primere je usklajen z lokalnim načrtom za odziv v nujnih primerih.....1

**Preprečevanje kriminala prek okoljskega modela*

RANLJIVOST (Vulnerability)

Vsebuje kemikalije ali druge materiale, ki lahko stopnjujejo uničenje, nahaja se na gosto poseljenem območju *5*

Ni grajena, da bi bila kos zmernim eksplozijam, nahaja se na gosto poseljenem območju 4

Vsebuje steklo ali druge materiale, ki lahko povečajo poškodbe, nahaja se v predmestnem industrijskem parku..... 3

Zgrajena, da prenese večje eksplozije, nahaja se na podeželju 2

Zgrajena, da prenese večje eksplozije in zračni napad, nahaja se na podeželju..... 1

UČINEK (Effect)

Panika prebivalstva na lokalni in državni ravni, resne državne in mednarodne gospodarske motnje..... *5*

Stranski negativni učinki na druge sestavne dele industrije ali storitev..... 4

Preobremenjene skupine za nujne primere in bolnišnice..... 3

Lokalno in nacionalno medijsko pokrivanje 2

Reden odziv organov kazenskega pregona, lokalna skupnost..... 1

PREPOZNAVNOST (Recognizability)

Tarča je izrazito izpostavljena v medijih; nacionalna ikona..... *5*

Tarča je izpostavljena ogledom..... 4

Pomen tarče in lokacije je znan predvsem lokalni skupnosti..... 3

Načrti objekta so dostopni na spletu, v knjižnici..... 2

Ciljne točke lokalnim prebivalcem niso nepoznane, potrebno je poznavanje od znotraj..... 1

Večina različic protokola KDORUP obravnava tveganje za fizične strukture in postavitve, vendar ker so te različnih velikosti, oblik in organiziranosti, bi morali ocenjevalno lestvico prilagoditi, da bo ustrezala vašim lokalnim potrebam. Železniški sistem, na primer, pomeni izrazito drugačna tveganja kot poslovna zgradba ali industrijska cona.

In končno, ta verzija KDORUP pove le malo o pomembni značilnosti vseh tarč, ki privlači teroriste: to so ljudje, ki so pogosto glavna tarča.

Ta vidik ocene tveganja obravnavava v naslednjem napotku.

Napotek 30: Zavarujte življenja preden zavarujete zgradbe

Teroristi pogosto izberejo za tarče ljudi, bodisi tiste, ki delajo v poslovni zgradbi, bodisi zbrane v restavracijah in tržnicah ali nagnetene v javnem transportnem sistemu. Najljubše tarče samomorilskih bombnih napadalcev v Izraelu so avtobusi, avtobusne postaje, tržnice in restavracije. Uničenje zgradb je v teh primerih sekundarnega pomena: ljudje so tisti, ki jih teroristi želijo ubiti ali poškodovati. Da bi jim to uspelo, izdelujejo posebne bombe, ki razstrelijo granatne delce, da poškodujejo čim več ljudi. Kombinacija uničenja in krvi zagotavlja veliko medijsko pozornost.

Zato namenite posebno pozornost dvema značilnostima v IVIL UZBL in KDORUP, ki se osredotočata na ranljivost ljudi kot tarč; teroristi raje napadejo močno obljudene stavbe in lokacije (Zasedenost pri IVIL UZBL); teroristi imajo rajši napade, ki bodo povzročili strah in paniko v skupnosti (Učinek pri KDORUP).

Kjerkoli so ljudje. Izvedite predhodno raziskavo, da boste ugotovili, katere zgradbe in objekti bodo najbolj verjetno privabili teroristične napade, bodisi zato, ker je v njih veliko ljudi, ali zato, ker bo njihovo uničenje povzročilo velik strah, poškodbe ali smrt ljudi v lokalni skupnosti. V primeru Svetovnega trgovinskega centra sta bili izpolnjeni obe merili izbiranja tarč. Številni, ki so bili v času napada v Dvojčkih, so umrli v neposrednem napadu; številni člani nujnega odzivnega osebja so umrli med reševalnimi operacijami. In tudi kasnejši učinek napada – tako čiščenje kot tudi onesnaženost zaradi sesutja stolpnic – še dandanes terjata žrtve.

Gosto obljudeni zaprti prostori. Zaprti prostori, v katerih se zadržuje veliko ljudi, kot so avtobusi, železniški vagoni, nakupovalni centri, podzemne postaje, gledališča, hoteli, konferenčni centri in stadioni so priljubljene teroristične tarče: veliko ljudi na majhnem prostoru pomeni, da lahko že razmeroma majhna bomba povzroči veliko število žrtev. Na srečo pa imajo tovrstne zgradbe in vpzila majhno število vhodov in izhodov, ki jih lahko nadzoruje usposobljeno varnostno osebje ali moderna tehnologija, kakršna je videonadzorna oprema.

Močno obljudeni odprti prostori. Odprti prostori brez nadzorovanih vhodov, kot so avtobusne postaje, nakupovalna četrt v središču mesta, odprte tržnice in javni parki.

Gosto obljudeni objekti za posebne priložnosti. Stavbni kompleksi, v katerih se gibljejo delavci, študentje, kupci in stranke, kot so bolnišnice, šole, poslovne zgradbe, veleblagovnice in stadioni.

Stanovanjska področja ob možnih tarčah. Katastrofi v Bhopalu (v Indiji) in Černobilu (v Ukrajini) sta povzročali še dolgo po dogodku poškodbe in smrt med tistimi, ki so živeli blizu krajev katastrof ali v smeri pihanja vetra. V vašem območju so objekti, katerih uničenje bi lahko povzročilo poškodbe okoliških stanovalcev še dneve in leta po napadu, kot so kemične tovarne in drugi obrati, ki proizvajajo toksične materiale, vključno z nuklearnimi elektrarnami in naftnimi rafinerijami.

Panika. V preteklosti je Al Kaida izvajala napade na več različnih lokacijah hkrati, da bi povzročila paniko med ljudskimi množicami in preobremenila nujne odzivne skupine. Kadar so pogoji temu naklonjeni, teroristi celo pripravijo napade na ekipe za nujno pomoč. Take vrste napadi so malo verjetni v Združenih državah, vsaj s strani terorističnih skupin z oporiščem v tujini, ker so za to potrebne okoliščine, ki omogočajo rutinski terorizem. Pripravljenost ekip za nujno pomoč je odločilnega pomena za zmanjševanje panike in poškodb, ki jih je povzročil napad, ker pomagajo nevtralizirati cilj teroristov: ubiti in pohabiti čim več ljudi.

Časovni okvir	Mrtvi (točka = 3 na primer)	Večje poškodbe (urgentna nega; točka = 2 na primer)	Resne poškodbe (dolgoročna nega; točka = 1na primer)	SKUPEN REZULTAT POŠKODB
Neposredno				
Naslednji dan/teden				
Številni meseci				
Številna leta				
SKUPAJ				

Najprej ljudje. Da bi zagotovili, da boste na vašem varnostnem seznamu ljudi postavili na prvo mesto, izvedite začetno raziskavo o svojem mestu: identificirajte močno obljudene objekte, potem jih ocenite v skladu s presojo o tem, koliko ljudi bi lahko bilo ubitih ali poškodovanih, vključno z osebjem za nujno prvo pomoč. Rezultate te raziskave uporabite v vaših KDORUP in IVIL UZBL ocenah. Končna ocena bo morda videti kot orodje za splošno oceno tveganja (Comprehensive Risk Assessment - CRA instrument), ki sva ga pripravila spodaj. Priredite ga, da bo ustrezalo lokalnim

potrebam, informacijam, ki ste jih pridobili, in zbirki možnih scenarijev, ki ste si jih predstavljali.

IVIL UZBL, KDORUP in podobni programi zahtevajo natančne informacije, ki zadevajo strukturo in funkcijo različnih tarč, storitve, ki jih nudijo, vodstvene in organizacijske strukture in kakršnekoli varnostne postopke, ki so že v veljavi. Za pridobitev teh podatkov, boste morali vzpostaviti dober delovni odnos z lastniki in direktorji teh lokacij (napotek 16); za uporabo programov in izdelavo ocen boste rabili tudi usposobljeno osebje. Če med osebjem nimate izurjenega analitika za tveganje, boste morali poiskati strokoven nasvet zunaj postaje ali pa si ga boste morali priskrbeti z usposabljanjem lastnih policistov. Zlasti ocene poškodb lahko zahtevajo znanje strokovnjakov, ker se bodo razlikovale glede na vrsto napada (biološki, nuklearni, konvencionalen) in posamezno tarčo. Dognanja teh posameznikov se lahko prenesejo tudi na druge zgradbe, lokacije in postavitve. Prosite jih za pomoč.

Splošna ocena tveganja (Comprehensive Risk Assessment - CRA) Scenarij napada (čas dneva, orožje ipd.)				
Opis tarče in lokacije	IVIL UZBL ocena	KDORUP	Rezultat poškodb	*Skupaj CRA
Predmestni nakupovalni center Nakupovalna četrt v središču mesta Železniška postaja v središču mesta Avtobusna postaja pred tržnico Električno omrežje Kongresni center Magistrat Bolnišnica Srednja šola Fakulteta Osnovna šola Srednja šola Avtobusi Železniški vagoni Gledališče Športna dvorana Kemična tovarna Naftna rafinerija Shranjevalni tanki za zemeljski plin Tovarna barv blizu stanovanjskega predmestja Železniška proga v mestnem jedru Odlagališče strupenih odpadkov blizu šole Drugo				
*CRA = (IVIL UZBL + KDORUP) X Rezultat poškodb				

Napotek 31: Naj vas ne zavedejo napovedi premestitev tarč

Nekateri skeptiki trdijo, da so varnostni ukrepi pri teroristični grožnji neučinkoviti, ker teroristi lahko preprosto preusmerijo pozornost z utrjenih tarč na tiste manj varne; to pomeni, da čeprav je morda mogoče izboljšati varnost ikoničnih struktur, kot je Empire State Building, do stopnje, da bo napad skoraj nemogoče izvesti, bodo druge lokacije, kot so npr. povsod zelo razširjeni nakupovalni centri in restavracije, vedno mehke tarče. Ko načrtujejo napad, morajo teroristi upoštevati številne dejavnike. Dva sta verjetno najpomembnejša: neposredna bližina tarče operacijski bazi in lahek dostop do tarče. Nakupovalni center, zavarovan s standardnimi varnostnimi postopki, je verjetno dovolj utrjen, da odvrača morebitne napade. Po drugi strani pa je visoka poslovna zgradba brez osnovne varnosti – kjer na primer lahko tovornjak bomba parkira v podzemni garaži – zagotovo mehka tarča. Čeprav je ranljivost tarče odvisna od primernih varnostnih ukrepov, je v končni fazi vendarle odvisna od tega, kako teroristi zaznavajo stopnjo varnosti. In dejstvo je, da vsaka trda tarča, ne glede na to, kako dobro je varovana, lahko postane mehka tarča, če napadalci uspejo pridobiti orodje ali orožje, potrebno za premagovanje obrambe.

Premestitev. Bodo teroristi preprosto prešli na mehkejšo, manj pomembno tarčo, če večino tarč utrdite v skladu z IVIL UZBL in KDORUP? Če poostrite varnost v vašem okolišu – in o tem vse obvestite – bodo teroristi preprosto šli naprej v naslednji okoliš? Kriminologi pravijo temu premiku kriminala z enega območja v drugo - premestitev.

Študije o situacijskem preprečevanju kriminala ugotavljajo, da premestitev ni nujna. Lahko se zgodi, vendar ne v večini primerov. Dejstvo je, da kršitelji, ki jih odvrnejo varnostni postopki, preprosto nadaljujejo z načrtovanim kaznivim dejanjem. Vsekakor se varnostni postopki za preprečevanje kriminala na eni lokaciji včasih odražajo v razširitvi koristi: zmanjšanje kriminala na lokacijah, ki sicer niso bile določene v okviru varnostnih procedur.

Vemo tudi, da premestitev ni, kadar so priložnosti za terorizem omejene, posebno v primerih ugrabitev letal. Tabela spodaj kaže število ugrabitev, ki so se zgodile med letoma 1961 in 1972. Med letoma 1968 in 1972 je prišlo do večjega števila ugrabitev letal (med Združenimi državami in Kubo), zaradi česar so na letališčih uvedli pregledovanje potnikov in prtljage, Zdru-

žene države in Kuba pa sta podpisali pakt, da bosta vračali ugrabitelje njihovim državam. Po letu 1973 je število ugrabitev občutno padlo. Je ta povečana varnost povzročila, da so ugrabitelji šli v druge države izvajati tovrstne zločine? Očitno ne: podatki ne govorijo o povečanju ugrabitev v drugih državah; dejansko se je stopnja ugrabitev znižala tudi v tujini. So kršitelji prešli na drugo obliko terorizma, kot je sabotažno bombardiranje, ko je ugrabljanje postalo preveč težavno? Nikakor ne. Kot je razvidno iz tabele, se bombardiranje letal po uvedbi varnostnih ukrepov ni povečalo, temveč je celo upadlo.

	Število let	Povprečje ugrabitev na leto		Povprečje sabotažnih bombardiranj na leto
		ZDA	Tujina	Po svetu
1961-1967	7	1.6	3.0	1.0
1968	1	20.0	15.0	1.0
1969-1979	2	30.5	58.0	4.5
1971-1972	2	27.0	33.0	4.5
1973-1985	13	9.4	22.7	2.3
1986-1989	4	2.8	9.0	2.0
1990-2000	11	0.3	18.5	0.3
2001-2003	3	1.3	5.7	0.0
1961-2003	43	6.7	17.9	1.6
Vir: Clarke, Ronald V. in Graeme R. Newman. Outsmarting the Terrorists. Westport, Connecticut: Praeger Security International, 2006.				

Naj vas od vaših namer ne odvrnejo napovedovalci premestitev. Utrditev tarč v skladu z IVIL UZBL in KDORUP bo pripomogla k preprečevanju terorističnih napadov. Teroristom bo zagrenila življenje, ko se bodo odločali kdaj, kje in kaj napasti, tehtati bodo morali številne dejavnike. Morda bo to zanje taka ovira, da ne bodo več poskušali.

Podrobnejši vidiki premestitve

Prilagoditev. Le malo kdo dvomi o tem, da bodo ob uvedbi novih varnostnih ukrepov teroristi in drugi kriminalci sčasoma ustrezno prilagodili svoje vedenje. Ne gre toliko za premestitev kakor za prilagoditev. Ta proces

smo spoznali pri tatvinah avtomobilov. V Združenih državah in drugje so v 1970. ugotovili, da volanske protivlomne ključavnice učinkovito zmanjšujejo tatvine avtomobilov. Ko so tatovi ugotovili, kako onesposobiti te ključavnice, so bile uvedene nove tehnologije, kot so posebni alarmi, sledilne naprave in električni imobilizatorji. Posledica tega je, da tatovi zdaj raje zaobidejo te tehnologije in vlamljajo v hiše, da bi ukradli ključe, ali se osredotočajo na izposojevalnice avtomobilov (gre za izposojo avtomobilov z uporabo ponarejenih osebnih dokumentov). Ta proces – nekakšna tekma v oboroževanju med »njimi« in »nami« – se imenuje prilagoditev. Načrt, da se na letalih, namenjenih v Združene države, uporabi tekoči eksploziv, je primer take prilagoditve. Teroristi so ob soočenju z poostrenimi varnostnimi postopki na letališčih izrabili dejstvo, da se lahko tekočino prosto nese na letalo.

Alternativne tarče. Nekateri samomorilski bombni napadalci načrtujejo alternativne tarče, če je pot do prve tarče ovirana. Ob načrtovanju več hkratnih bombnih eksplozij izberejo teroristi alternativne tarče, navadno v bližini primarne tarče. Mohamed Atta, vodja teroristične skupine 11. septembra je med vadbenim poletom v New York City z zadovoljstvom opazoval jedrsko elektrarno na Three Mile Island. Kolikor ne bi bil zmožen doseči Dvojčka, bi morda poskusil uničiti to alternativno tarčo. Zagotovite, da bodo tudi tovrstne alternativne tarče zaščitene.

Drugačno orožje, ista tarča. Ko je postalo jasno, da Dvojčkov ni mogoče uničiti s tovornjakom bombo, teroristi niso zamenjali tarče, temveč so raje izumili nekonvencionalno orožje in nekonvencionalno sredstvo za njegovo dostavo do tarče. Zakaj niso prešli na tarčo, ki bi jo bilo lažje zadeti in uničiti? O tem lahko le ugibamo, vendar bi bil lahko eden od razlogov skoraj edinstveni ikonični pomen Svetovnega trgovinskega centra. Drugi je zagotovo dejstvo, da so storilci vložili veliko časa in sredstev v preučevanje Svetovnega trgovinskega centra. Če bi prešli na drugo tarčo, v drugem mestu, bi nastala množica logističnih težav.

Če povzamemo, čeprav morate biti pozorni na izbor alternativne tarče in na možnost, da se bodo teroristi prilagodili vaši obrambi, je malo verjetno, da bodo zaradi vaših varnostnih ukrepov premestili svoje dejavnosti. Vendar pa je prilagoditev treba jemati zelo resno, ker morate zaradi nove možne tarče nenehno preverjati obrambo, da predvidite, kje in kako jo bodo teroristi poskušali premagati.

Napotek 32: Izboljšajte osnovno varnost vseh tarč

Vsi se zavedamo, da vseh potencialnih tarč ne moremo zaščititi do enake stopnje, toda ali jih lahko zavarujemo vsaj do neke mere? Za to obstajajo številni načini, vendar najprej kratka zgodovina napada neznanih storilcev na državljane Združenih držav s strupom, ki se je zaključil s sedmimi smrtnimi žrtvami.

Leta 1982 se je sedem ljudi, od katerih so bili trije iz iste družine, na območju Chicaga naenkrat zgrudilo in umrlo. Ugotovljeno je bilo, da so umrli po zaužitju kapsul Tylenol®, ki so jih kupili v lokalni lekarni. Neznani morilci, katerih identitete so še danes neznane, so tablete namazali s cianidom. Prijetje storilcev se je izkazalo za nemogoče; njihovih motivov niso nikoli razkrili. Danes bi to dejanje poimenovali terorizem, ker je šlo za naključen kemični napad neznanih napadalcev, ki so izbrali lekarno za kraj napada. (Upoštevati moramo, da tako izbira določene lekarne kakor tudi metoda izvedbe nista bili naključni.) Johnson & Johnson, proizvajalec Tylenola, je sprejel ukrepe, da se taki umori ne bi nikoli več zgodili. V sodelovanju s skupino strank in z vladnimi regulatorskimi agencijami so uvedli pakiranje, odporno na vdore. Z enim ukrepom se je pakiranje proizvodov v Združenih državah spremenilo za vedno. Danes so vsa zdravila, potrošni proizvodi in katerikoli osebni predmet v maloprodaji pakirani odporno na vdore ali tako, da je morebiten vdor viden. S preprosto inovacijo je prišlo do bistvenega izboljšanja varnosti proizvodov in javne varnosti na nacionalni in vsekakor tudi na mednarodni ravni. In do preprečitve skrajno redke oblike umora.

Ne pričakujeva, da bo vodja lokalne policije uvedel preventivne tehnike tako mogočnih razsežnosti. To izredno zgodbo omenjava ne le kot dokaz, da ustvarjalno mišljenje lahko reši navidezno nerešljive probleme, temveč zato, da bi poudarila, da ima lahko varnostno posredovanje izrazito pozitivne verižne učinke. Uvedba odpornosti na vdore velja za neverjetno veliko število proizvodov in je zavarovala ljudi pred številnimi možnimi napadi.

Osnovna varnost ščiti pred terorizmom in kriminalom. V manjšem obsegu se lahko veliko stori za zagotavljanje osnovnih varnostnih standardov v vseh vladnih, javnih in komercialnih objektih. Osnovna stopnja varnosti bi se konec koncev morala vzdrževati za zaščito pred kriminalnimi dejanji in ne le pred terorizmom. Kot sva izpostavila v napotku 7, zelo po-

maga, če o terorizmu razmišljamo kot o obliki kriminalitete in če k njegovemu preprečevanju pristopamo na zelo podoben način: prek sodelovanja z državljani, trgovci in vladnimi uradniki. Dejansko, **osnovni varnostni ukrepi, ki lahko preprečijo vlom v trgovsko ustanovo, ščitijo ustanovo tudi pred terorističnimi napadi**: okolica bi morala biti zavarovana, nameščena naj bi bila ustrezna razsvetljava in tako dalje. Sodelovati morate z lokalnimi uradniki in trgovci, da jih ozavestite o temeljnih varnostnih postopkih, vključno s preprečevanjem kriminalitete z uporabo okoljskega modela (Crime Prevention Through Environmental Design CPTED; glej okvir). Ne glede na to, ali se pričakuje teroristični napad ali ne, imajo vse zgradbe in lokacije koristi od vzdrževanja osnovne stopnje varnosti. V takih primerih je zaščita pred kriminalom tudi zaščita pred terorizmom.

Osnove preprečevanja kriminalitete z uporabo okoljskega modela (CPTED)

CPTED analizira okoljske razmere in priložnosti, ki omogočajo kriminaliteto ali drugo nedobronamerno ali nezaželeno vedenje. Poskuša zmanjšati ali odpraviti te priložnosti z uporabo okoljskih elementov za (1) nadzor dostopov; (2) zagotovitev priložnosti, da bi videli in bili videni ter (3) določitev lastništva in spodbujanje vzdrževanja urejenega ozemlja.

CPTED vrednoti načine, na katere različne značilnosti določenega okolja dajejo priložnost kriminalu in drugemu nezaželenemu vedenju. CPTED poskuša odpraviti ali zmanjšati priložnosti s spremembo različnih vidikov fizičnega in družbenega okolja, vključno z naslednjim:

- načrt zgradbe
- tloris in značilnosti lokacije, kot so osvetlitev in usklajenost gradnje s pokrajino
- lokacija objekta in vpliv okoliške uporabe zemljišč
- utrjevanje tarč in varnostni ukrepi (ali pomanjkanje tega)
- redna uporaba zgradbe in urniki dejavnosti
- pravila in politike, ki urejajo uporabo in vedenje.

Za pravilno delovanje zahteva CPTED strokovno mnenje in analize. Če vaša postaja nima tovrstnih strokovnjakov, boste morali zadolžiti svetovalca ali usposobiti svoje lastne policiste. Uporaba CPTED pogosto zahteva vključe-

nost lokalnih sosedskih organizacij, zato bi morali poiskati mesta in velemesta, kjer redno uporabljajo CPTED. Tak primer je soseska Seattla (Seattle Neighborhood Group) (http://www.sngi.org), ki je CPTED sprejela kot svoj osrednji pristop za reševanje varnostnih težav v skupnosti.

Splošna fizična varnost. Odvisno od tega, kje živite, boste morda potrebovali strokovno pomoč v zvezi s številnimi posebnimi vprašanji, vključno z zasebnim varovanjem, varnostniki in patruljami, preprečevanjem izgube, izvršnim varovanjem in CPTED. Informacije o usposabljanju in strokovni pomoči lahko pridobite pri naslednjih organizacijah.

- Mednarodno združenje za CPTED (The international CPTED Association) je organizacija, ki se ukvarja s preprečevanjem kriminalitete s pomočjo okoljskega modela. Publikacije so dostopne pri CPTED virih: http://www.cpted.net/.
- ASIS International (nekdanja American Society of Industrial Security) nudi vrsto tečajev usposabljanja iz varnostnih raziskav, CPTED in ocenjevanje tveganja. ASIS nudi tudi potrdila za številna varnostna področja in posreduje zainteresiranim sezname strokovnjakov, ki lahko izvajajo ocene tveganja in raziskave objektov. ASIS najdete na: https://www.asisonline.org. Morda obstaja tudi lokalna podružnica ASIS-a v ali blizu vašega mesta.

Več o tem: Zahm, Diane. Using Crime Prevention through Environmental Design in Problem-Solving, Problem-Solving Tools Series No. 8. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2007. http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=440

Napotek 33: Spoprimite se z izzivom zaščite infrastrukture

Na tarče gledamo kot na posebne kraje, zgradbe ali ljudi. Infrastrukture so nekaj drugega: so kompleksni sistemi, ki zasedejo tako prostor kot tudi čas in vsebujejo številne trdne in gibljive tarče. O njih je torej bolje razmišljati kot o sistemih. Obstajajo številni različni načini klasifikacije infrastruktur, vključno z naslednjo:

- transportna: letalski, morski, cestni, železniški, podzemni, pristaniški promet, mostovi, tuneli;
- prehrambna in kmetijska: kmetije, predelovalni obrati, distribucijski centri;
- komunikacijska: telekomunikacijska omrežja, poštne storitve, radijske in televizijske postaje, ponudniki spletnih storitev;
- vodovodna: zbiralniki, vodne cevi, čistilni sistemi;
- energetska: rafinerije, generatorske postaje, jedrske elektrarne, električna omrežja, naftni ali plinski cevovodi;
- industrijska in proizvodna: tovarne, skladišča, trgovine in blagovni trg na drobno;
- javni objekti: nakupovalni centri, restavracije, hoteli, stadioni, kinodvorane;
- bančna in finančna: podružnice, računalniški sistemi, uradi;
- javnozdravstvena in varnostna: javne evidence, zdravstveni, varnostni in socialnovarnostni sistemi.

Ker so infrastrukture kompleksne, jih teroristi ne izberejo pogosto za tarče, čeprav so zagotovo tudi izjeme, kot so naftovodi v Iraku. Teroristom je zelo težko uničiti specifično infrastrukturo, ker ima večina rezervne sisteme in sisteme, ki varujejo pred izpadi delovanja sistema. Čeprav je napad na infrastrukturo lahko razdiralen, je z njim težko doseči večjo stopnjo poškodb ali uničenje. Četudi teroristi napadejo vlak ali avtobus, tega ne naredijo, da bi zaustavili transportni sistem, temveč zato, da bi z enim napadom ubili čim več ljudi. Napadi na avtobuse, vlake in letala so redko napadi na infrastrukturo, temveč prej napadi na privlačne tarče, ki so slučajno del infrastrukture.

Ker je večji del infrastrukture in njeno upravljanje v Združenih državah v zasebni lasti, bo tesno sodelovanje z lokalnimi podjetji ključnega pome-

na za vaša varnostna prizadevanja. Ne predpostavljajte, da bodo zasebne družbe in podjetja razumeli varnostne potrebe: podjetja se močno razlikujejo po stopnji, do katere varnost obravnavajo kot del svojih rednih podjetniških dejavnosti. Številne fizične elemente infrastrukture (zgradbe, stolpnice, žice, zbiralnike) je mogoče dobro zaščititi z osnovnimi CPTED postopki (glej predhodni napotek). Kjer je to potrebno, pokličite na pomoč strokovnjake za zaščito posebne infrastrukture. Spodaj sva sestavila seznam nekaterih virov za zavarovanje transportnih sistemov, stadionov in javnih prireditev. Strokovni viri za druge vrste infrastrukture so navedeni v napotku 36, ker njihova kompleksnost izziva teroriste k uporabi nekonvencionalnih sredstev napada, vključno s biološkimi in jedrskimi metodologijami.

Stadioni in prireditve

Čeprav strogo gledano ti niso del pomembne infrastrukture, je njihovo ščitenje kritično povezano z varnostjo druge lokalne infrastrukture, ker množično uničenje lahko preobremeni sicer ustrezen sistem komunikacij, transporta ali javnega zdravstva.

- Posebna prireditev, imenovana Nacionalni varnostni dogodek (National Security Event), je upravičena do posebne zvezne zaščite in postopkov pod vodstvom tajnih služb Združenih držav. http://www.secretservice.gov/nsse.shtml. Več o varnosti posebnih prireditev boste zvedeli v publikaciji COPS urada *Načrtovanje in obvladovanje varnosti ob večjih posebnih dogodkih: smernice za kazenski pregon.* http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=441.
- Direktorat za analizo informacij in zaščito infrastrukture DHS-ja (The information Analysis and Infrastructure Protection Directorate of the DHS) http://www.llnl.gov/hso/iaip.html)

Transportni sistemi

Največji zvezni naslov za transportno varnost je Transportna varnostna administracija (Transportation Security Administration – TSA). Njena spletna stran (http://www.tsa.gov) vsebuje obilo informacij, vključno s povezavami do številnih strokovnjakov za transportno varnost. Drugi splošni naslov je neprofitno, nestrankarsko Ameriško združenje avtocestnih in

transportnih delavcev (angl. American Association of Highway and Transportation Officials). Najdete ga na http://www.transportation.org.

Za posebne transportne sektorje, začnite z naslednjim:

1. **Železnica** – običajna železniška varnost vključujejo naslednje:
- varnost postaj
- odprto arhitekturo
- preiskovalne metode in pravila za potnike in prtljago
- varnost železniškega tovornega prometa in preiskave železniških motornih vagonov in zabojnikov.

2. Za začetek pojdite na spletno stran skupine železniških potnikov TSA (TSA passenger rail group) na TSA-jini spletni strani. Ta spletna stran nudi povezave na železniška potovanja ter številne koristne namige. http://www.tsa.gov
3. Za koristen pregled varnostnih problemov potnikov poglejte Varnost železniških potnikov: Pregled vprašanja (angl. Passenger Rail Security: Overview of Issues), Davida Randalla Petermana, Congressional Research Service, Maj 2005. http://www.fas.org/sgp/crs/homesec//RL32625.pdf.
4. Za pregled posebnih tveganj in načinov za njihovo preprečevanja preglejte Varnost železniških potnikov: Ocena tujih varnostnih postopkov ter Tveganje lahko pomaga voditi varnostna prizadevanja (Passenger Rail Security: Evaluating Foreign Security Practices ter Risk Can Help Guide Security Efforts). Urad za odgovornost vlade (angl. Government Accountability Office), poročilo št. GAO-06-557T. http://www.gao.gov/new.items/d06557t.pdf
5. **Avtobus** - za pregled vprašanj v zvezi z avtobusnim transportom prenesite program varnostnega usposabljanja voznikov šolskih avtobusov, ki ga je razvila programska skupina Sigurnost iz New Mexica (Mew Mexico Surety Task Force). Čeprav je namenjena voznikom šolskih avtobusov, so številne točke in postopki uporabni za katerokoli vrsto avtobusov. http://www.nasdpts.org/documents/SecurityNewMexicoCourseTrainingGuide.pdf
   Poleg tega Nacionalno združenje državnih direktorjev služb za prevoz učencev (National Association of State Directors of Pupil Transportation Services) nudi številne koristne povezave in članke. http://nasdpts.org
6. **Tovornjak** – če vaše mesto leži ob prometni avtocesti, je cestna varnost pomembna. Za namige o varnosti, zaščiti in mejnih vprašanjih se obr-

nite na Zvezno administracijo za varnost prevoznikov (Federal Motor Carrier Safety Administration). http://www.fmcsa.dot.gov

7. **Zračni promet** – obiščite TSA Center za raziskave in razvoj transportne varnosti (TSA's Transportation Security Research and Development Center) na http://www.tsa.gov/research/index.shtm.
8. **Morski promet** – kolikor je vaše mesto blizu morskega pristanišča, boste verjetno rabili posebno pomoč, zlasti zaradi prekrivanja pristojnosti med zveznimi, državnimi in lokalnimi agencijami. Za več informacij poglejte *Pristaniška varnost: Država se sooča s pomembnimi izzivi v prizadevanjih za uspešnost novih iniciativ (Port Security: Nation Faces Formidable Challenges in Making New Initiatives Successful).* Urad za odgovornost vlade (angl. Government Accountability Office). Poročilo št. GAO-02-993T. http://www.gao.gov/new.items/d02993t.pdf

Napotek 34: Poznajte VNPUUZDNV (angl. MURDEROUS) orožja

Kljub grozljivim scenarijem, ki jih omogoča orožje za množično uničevanje, se to orožje redko uporabi v terorističnem napadu iz razlogov, ki jih bomo obravnavali v prihodnjem napotku. Večino terorističnih napadov izpeljejo z uporabo strelnega orožja in eksploziva. Med številnimi vrstami konvencionalnega orožja so majhne razlike, zato je vsako bolj ali manj primerno za različne vrste napadov. Da bi ustrezno zaščitili tarče, morate določiti, katere vrste orožja bodo najverjetneje uporabili za vsako posamezno tarčo. V tem procesu vam ponujamo v pomoč VNPUUZDNV (angl. MURDEROUS), ki povzema lastnosti orožja, ki ga teroristi dozdevno cenijo. Tako orožje je:

Večnamensko (angl. **M**ultipurpose). Večina strelnega orožja se uporablja za prav posebne namene. Na primer, puška visoke zmogljivosti se na splošno uporablja za streljanje na tarčo, ki je daleč od strelca; po drugi strani pa šibrovka zagotovi široko strelno polje, vendar se uporablja samo, kadar je tarča v bližini strelca. Eksplozivi so uporabni veliko širše: avto bomba se lahko npr. uporabi za umor posameznika, medtem ko se tovornjak bomba lahko uporabi za uničenje velike poslovne zgradbe. Jasno je, da se eksplozivov ne more ponovno uporabiti, zato je zalogo treba obnoviti. Kljub temu pa je z uporabo manjšega orožja, ki lahko izstreli eksplozivno strelivo, kot so dum-dum izstrelki in granate na raketni pogon, mogoče doseči uničevalni učinek.

Nezaznavno (angl. **U**ndetectable). Zaradi poostrene varnosti na letališčih in drugih verjetnih tarčah morajo teroristi na splošno uporabljati orožje, ki se ga da skriti in ga ni mogoče zaznati. To razloži priljubljenost semtexa, lahkega, večinoma nezaznavnega eksploziva. Za zrušenje letala PanAm 103 nad Lockerbiem na Škotskem je zadostovalo le 11 unč semtexa, spravljenega v majhnem magnetofonu. Ker ga je lahko skriti, je idealno orožje samomorilskih bombnih napadalcev, ki morajo, da bi se prebili do tarče, pogosto prodreti mimo številnih varnostnih ovir.

Prenosljivo (angl. **R**emovable). Orožje teroristov mora biti prenosno, kar pomeni, da mora biti dovolj lahko in majhno, da ga lahko dvigne in nese en ali dva človeka. Zaradi te lastnosti in dimenzije je tako orožje tudi eno-

stavno ukrasti. Iz študij o zanimivih proizvodih vemo, da je med tatovi prenosljivost predmeta visoko cenjena. Na primer, ko je bila visoko kakovostna avdiooprema zelo draga, je bila priljubljena tarča vlomilcev, ker so jo lahko z lahkoto odnesli in preprodali. Čeprav teroristov ne zanima preprodajna vrednost ukradenih stvari, velja isto načelo , saj je orožje cenjeno, ker je uničevalno, ne pa estetsko.

Uničevalno (angl. **D**estructive). Strelno orožje je najbolj primerno za uboj določenega posameznika. Ker teroristi na splošno želijo ubiti čim več ljudi in to čim hitreje, je pogosto eksploziv orožje po njihovi izbiri. V Iraku, na primer, so uporniki z uporabo improviziranih eksplozivnih naprav (angl. improvised explosive devices – IED) ubili veliko več ameriških vojakov kot z uporabo izstrelkov. Glej tabelo s povzetkom smrtonosnosti različnih vrst orožja.

Uživaško (angl. **E**njoyable). Teroristi uživajo v orožju in so dozdevno zelo navdušeni in zadovoljni ob njegovi uporabi. Seveda v orožju ne uživajo samo teroristi: številni običajni ljudje prav tako uživajo v njem.

Zanesljivo (angl. **R**eliable). Da bi bilo uporabno, mora biti strelno orožje zanesljivo, zaradi česar vojaške rekrute temeljito urijo za vzdrževanje in uporabo orožja. Civilni uporabniki ugotovijo z nenehno uporabo, ali je orožje zanesljivo. Če so navajeni na določeno orožje (ali na podobno), bodo verjetno bolj naklonjeni temu orožju kakor drugemu. To pomeni, da se bodo teroristi verjetno izogibali nekonvencionalnemu ali nepoznanemu orožju, razen če svoje naloge ne morejo izpeljati na noben drugi način. Zato je verjetno, da se bodo rutinski teroristični napadi dogajali z uporabo znanega, konvencionalnega orožja.

Dosegljivo (angl. **O**btainable). Razpoložljivost je nemara najbolj pomembna od vseh lastnosti orožja. Kako lahko je dobiti orožje? Se ga da enostavno kupiti ali ukrasti? Se ga da izdelati doma? Svet je preplavljen z lahkim orožjem, ki je najbolj pogosto uporabljano teroristično orožje. In ker ga je tako veliko, obstajajo številni kraji, kjer ga je mogoče dobiti; tatvina je verjetno najbolj običajen način, na katerega teroristi pridobijo orožje.

Nezapleteno (angl. **U**ncomplicated). Ali je orožje uporabniku »prijazno«, določa, koliko urjenja je potrebno za njegovo uspešno uporabo. Celo na videz preprosto orožje, kot so pištole, zahteva vajo in urjenje. Zapleteno

orožje, ki zahteva precejšnje strokovno znanje, kot so prosto leteči izstrelki za prebijanje oklepov, bo redko uporabljano. Dejansko se je dogajalo, da kadar so uporabili tovrstno orožje, so napadi pogosto spodleteli, ravno zato, ker so orožje uporabili nepravilno. Leta 1972, na primer, je gibanje Črni september z uporabo granatnega metalca RPG-7 poskusilo zrušiti letalo El Al; strel je zgrešil smer in zrušil letalo jugoslovanske letalske družbe.

Varno (angl. **S**afe). Bombe so same po sebi bolj nevarne od strelnega orožja. Številne člane začasne irske republikanske armade je raznesla prezgodnja detonacija eksploziva.

Do VNPUUZDNV (angl. MURDEROUS, kar pomeni - ubijalsko) smo prišli tako, da smo poskušali razmišljati kot teroristi; nedvomno bi shemo lahko izboljšali z empirično raziskavo. Vendar pa take raziskave verjetno ne bi ovrgle osnovnega načela, da imajo teroristi raje orožje s specifičnimi značilnostmi, ki ustrezajo nameravanim napadom. Razumevanje teh značilnosti nam lahko pomaga ugotoviti načine preprečevanja napadov in nadzorovanja dostopa do orožja, ki ga imajo teroristi najraje.

Smrtonosnost orožja

Uničevalna zmogljivost orožja se pogosto ocenjuje v skladu z naslednjimi dejavniki:

- prodornost: kako globoko v tarčo prodre orožje (npr. oklepna prodornost proti zadeni in ubij);
- ustvarjanje drobcev, granatnih delcev in ruševin;
- razstrelitev in sunek: stopnja, na kateri se struktura tarče zruši; verižni učinek udarca;
- proizvajanje ognja in dima;
- natančnost: eksplozije povzročajo uničenje na široko; puška visoke zmogljivosti je ozko usmerjena;
- količina žrtev: število ljudi, ki jih je mogoče ubiti z enim napadom.

Posvetujete se in sledite smernicam ministrstva za obrambo o primernih razdaljah za konvencionalne eksplozivne naprave za vse zgradbe, ki ste jih v vaši primerjalni analizi tveganja ocenili visoko (glej napotek 30).

Več o tem: U.S. Department of Defense, Unified Facilities Criteria (UFC): DoD Minimum Antiterrorism Standards of Buildings, UFB 4-010-01. Washington, D.C.: U.S. Department of Defense, 2003.

Več o tem: Clarke, Ronald V. in Graeme R. Newman, Outsmarting the Terrorists. Westport, Connecticut: Praeger Security International, 2006.

	Lahko orožje	**Eksplozivne naprave**	**Biološko/ kemično orožje**	**Jedrsko orožje**
Prodornost	Omejena	Omejena	Zmerna	Visoka
Ruševine	Omejeno	Visoko	Neobstoječe	Visoko
Razstrelitev	Omejena	Visoka	Neobstoječa	Visoka
Ogenj in dim	Omejen	Visoko	Visoko	Visoko
Natančnost/ točnost	Visoka	Zmerna	Nizka	Nizka
Količina žrtev	Nizko	Zmerno	Zmerno/Visoko	Visoko

Napotek 35: Ne bojte se pretirano orožja za množično uničevanje

Veliko nas živi v strahu, da bodo teroristi napadli z biološkim, kemičnim ali jedrskim orožjem, to je z orožjem za množično uničevanje (OMU). Čeprav je to morda vaša najhujša nočna mora, je bilo do danes zelo malo napadov s tovrstnim orožjem. Leta 1995 so teroristi Aum Shinrikyo na tokijski podzemni železnici spustili plin sarin in z njim ubili 12 ljudi, na tisoče pa je bilo poškodovanih. Istega leta so v moskovskem parku odkrili neeksplodirano umazano bombo (napravo, namenjeno disperziji radiološkega materiala s konvencionalnim eksplozivom), ki so jo podtaknili čečenski separatisti. Vendar pa tem osamljenim primerom ni sledil izbruh napadov z orožjem za množično uničevanje, verjetno zato, ker tovrstno orožje ustreza le malo pogojem VNPUUZDNV (Večnamensko, Nezaznavno, Prenosljivo, Uničevalno, Uživaško, Zanesljivo, Dosegljivo, Nezapleteno, Varno; (glej napotek 34). Dejansko OMU ni zelo primerno za teroriste, ker so njegovi učinki nepredvidljivi in pogosto temeljijo na letečih kemikalijah ali bioloških povzročiteljih, ki bi lahko škodili samim teroristom ali njihovim podpornikom. Poleg tega OMU ni takoj na voljo, njegova izdelava in uporaba je zahtevna in včasih ga je težko prevažati in zakriti. In čeprav je lahko zelo uničevalno, si vsaka teroristična skupina ne želi povzročiti tako obsežnega uničenja. Ekoteroristi, na primer, izvajajo majhne, vendar natančno izbrane tarče, ki so skrbno prilagojene njihovim političnim ciljem; druge skupine bi morda raje izsilile koncesije, zato zajemajo talce ali okupirajo ambasade in druge uradne zgradbe. Uporaba OMU bi se teroristom lahko celo maščevala z izgubo podpore.

Teroristi redko uporabljajo nekonvencionalno orožje, celo tisto, ki ga je relativno lahko dobiti, kot so izstrelki zemlja-zrak, in ki lahko sestrelijo letalo. Ocenjuje se, da je bilo od 1970. let po svetu proizvedeno 700.000 tovrstnih izstrelkov, znanih kot zračni obrambni sistemi, ki jih lahko prenaša človek (man-portable air defense systems – MANPADS). Na črnem trgu jih ni težko dobiti in so razmeroma poceni: po nekaterih ocenah je cena starejših modelov nekaj sto dolarjev. Za številne se domneva, da so že v rokah teroristov, ki so sovražni do Združenih držav, vendar doslej ni bil kakšen uporabljen proti letalu ZDA. Iz tega lahko sklepamo, da bodo teroristi verjetno še naprej raje uporabljali strelno orožje in eksploziv, razen v zelo nenavadnih okoliščinah, ali kjer so tarče izrazito težko dostopne.

Verjetnost, da bo manjše mesto napadeno z OMU, je še posebej majhna, ker mesta s številčnejšim in bolj koncentriranim prebivalstvom omogočajo veliko večje uničenje - da ne govorimo o verižnem učinku, ki bi ga povzročil tak napad. V vsakem primeru lahko na lokalni ravni naredite le malo, da bi preprečili tak napad, kljub temu pa morate imeti pripravljen načrt za tovrsten scenarij. Ta vprašanja bova obravnavala v zadnjem delu tega priročnika. Uporabite lahko, in morali bi, znanje tistih, ki so usposobljeni za spoprijemanje s tveganji in zapletenostjo nekonvencionalnega orožja. Nekateri od teh strokovnih virov so navedeni spodaj.

Biološka in kemična tveganja

- Medicinski raziskovalni inštitut kemične obrambe ameriške vojske (U.S. Army Medical Research Institute of Chemical Defense): razvija medicinske protiukrepe za kemične vojne povzročitelje in usposabljajo medicinsko osebje v medicinskem obvladovanju kemičnih žrtev. http://chemdef.apgea.army.mil/
- UCLA center za javno zdravstvo in katastrofe (UCLA Center for Public Health and Disasters): spodbuja interdisciplinarna prizadevanja za zmanjšanje vpliva naravnih nesreč in katastrof, ki jih je povzročil človek, na zdravje. http://www.cphd.ucla.edu
- Agencija za zaščito okolja (angl. Environmental Protection Agency): s pomočjo državnim in lokalnim odzivnim ekipam pri načrtovanju odzivov v nujnih primerih, z usklajevanjem s ključnimi partnerji, usposabljanjem prvih odzivnih ekip in z nudenjem sredstev v primeru terorističnega napada podpirajo zvezni protiteroristični program. http://www.epa.gov/ebtpages/emercounter-terrorism.html
- Center za raziskavo in ustrezno ravnanje v primeru infekcijskih bolezni (Center for Infectious Disease Research & Policy): njegova naloga je preprečevanje bolezni in smrti zaradi infekcij z pidemiološkimi raziskavami in hitro pretvoroe znanstvenih informacij v praktične ukrepe in rešitve. http://cidrap.umn.edu/cidrap
- Centri za nadzor in preprečevanje bolezni (Centers for Disease Control and Prevention – CDC): priznan je doma in v tujini kot vodilna zvezna agencija za varovanje zdravja in varnosti ljudi v Združenih državah; CDC nudi verodostojne informacije za izboljšanje zdravstvenih ukrepov in promovira zdravje prek močnih nacionalnih in mednarodnih partnerstev. http://www.cdc.gov
- DHS: nudi informacije o blažitvi tveganj. http://www.dhs.gov/xprepresp

Ščitenje infrastrukture

V napotku 33 sva predstavila strokovne vire s področja transportne varnosti. Tu je kratek seznam pomembnejših organizacij, povezanih z infrastrukturami, ki bi lahko bile napadene z nekonvencionalnim orožjem, zlasti jedrskim ali biološkim. Za natančne informacije in vire pomoči navežite stik z njimi.

Živila in kmetijstvo

- Ministrstvo za kmetijstvo Združenih držav (United States Department of Agriculture): nudi smernice za uničenje mednarodno oporečnih proizvodov. http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/index.asp
- Nacionalno združenje ministrstev za kmetijstvo (National Association of State Departments of Agriculture – NASDA): kot del njegove naloge razvoja in implementacije programov, namenjenih podpori in spodbujanju kmetijske industrije ZDA vsebuje spletna stran NASDA model živilskega načrta za nujne primere za zvezno in državno partnerstvo. http://www.fsis.usda.gov/Food_Defense_&_Emergency_Responske/Model_Food_Emergency_plan/index.asp
- Center za varnost živil in uporabno prehrano (Center for Food Safety and Applied Nutrition): kot Administracija za živila in zdravila ZDA (Food and Drug Administration) je center oblikoval navodila za pomoč živilskim trgovinam na drobno in ustanovam s prehrambnimi storitvami pri uporabi osnovnih varnostnih postopkov v živilstvu; Živilske trgovine na drobno in ustanove s prehrambnimi storitvami: vodič po živilskih preventivnih varnostnih ukrepih (angl. Retail Food Stores and Food Service Establishments: Food Securtiy Preventive Measures Guidance), http://www.cfsan.fda.gov/~dms/secgui18.html

Komunikacije

- Državni telekomunikacijski sistem (National Telecommunications System): poiščite direktive in priročnike na http://www.ncs.gov/.
- Zvezna komunikacijska komisija (Federal Communications Commission): nudi smernice za oblikovanje prednostnih nalog pri obnovi telekomunikacijskih objektov in sistemov ter oskrbi nadomestnih sistemov. http://www.fcc.gov/cgb/consumerfacts/homelandtsp.html

- Komisija za varnost in zasebnost informacij (Information Security and Privacy Board): nudi nasvete vladnim uslužbencem glede varnosti in zasebnosti informacij, ki pripadajo zveznim vladnim informacijskim sistemom.
- Skupina za računalniško pripravljenost v nujnih primerih ZDA (U.S. Computer Emergency Readiness Team)
- Nacionalno partnerstvo za spletno varnost (National Cyber Security Partnership)

Voda

- Center za izmenjavo in analizo informacij o vodi (The Water Information Sharing And Analysis Center) v sodelovanju z Agencijo za varovanje okolja in DHS nudijo štiri podatkovne baze o onesnaževalcih, bele knjige (white papers) o številnih varnostnih temah s področja vode in dostop do orodja za ocenjevanje ranljivosti. http://www.waterisac.org

Energetika

- Administracija za energetske informacije (Energy Information Administration): nudi informacije o motnjah in ranljivosti rafinerij po celotnih Združenih državah; ladijskih prehodnih točkah in razlitjih; in ščitenju naftnih rafinerij, skladiščenju in transportu. http://www.eia.doe.gov/emeu/sucurity/Oil/index.html
- Ministrstvo za energijo ZDA (U.S. Department of Energy): nadzira program infrastrukturne varnosti in energetske obnove (Infrastructure Security and Energy Restoration program). Nudi izobraževanje in podporo na državni in lokalni vladni ravni. http://www.oe.energy.gov/our_organization/isei.htm
- Energetska in infrastrukturna zagotovila (Sandia državni laboratoriji) (Energy and Infrastructure Assurance – Sandia National Laboratories): njihova primarna naloga je izboljšanje varnosti, zaščite in zanesljivosti energetike ter druge pomembne infrastrukture. http://www.sandia.gov/mission/energy

Ogroženost in zaščita kritične infrastrukture v Sloveniji

Teodora Ivanuša

Komisija EU je kritično infrastrukturo opredelila kot »obrate, omrežja in premoženje fizične in informacijske tehnologije, katerih okvara ali uničenje bi resno vplivalo na *zdravje, varnost, zaščito, gospodarsko in družbeno blaginjo* državljanov oziroma *učinkovito* delovanje vlad držav članic. Po mnenju Komisije kritično infrastrukturo predstavljajo številni sektorji gospodarstva, tudi bančništvo in finance, promet in infrastruktura, *zdravstvo, oskrba s hrano in komunikacijami,* kot tudi ključne državne službe. Nekateri kritični elementi v teh sektorjih niso v strogem pomenu »infrastruktura«, ampak so dejansko omrežja ali dobavne verige, ki podpirajo oskrbo s ključnimi proizvodi ali storitvami, kakor tudi samo delovanje sektorjev.« (Sporočilo Komisije, 2004: 1).

Evropski svet je junija 2004 zaprosil Komisijo, da pripravi celovito strategijo varovanja ključne infrastrukture (KI). Komisija je 20. oktobra 2004 sprejela sporočilo »Varovanje kritične infrastrukture v boju proti terorizmu«, v katerem je dala jasne predloge o tem, kaj bi okrepilo preprečevanje terorističnih napadov na ključno infrastrukturo, pripravljenost in odziv nanje v Evropi.

Svet je v sklepih o »preprečevanju pripravljenosti in odzivu na teroristične napade« in »solidarnostnem programu Evropske Unije (EU) o posledicah terorističnih groženj in napadov«, ki jih je sprejel decembra 2004, podprl namero Komisije, da predlaga Evropski program za varovanje ključne infrastrukture (EPCIP), in se strinjal z vzpostavitvijo informacijskega omrežja za opozarjanje o ključni infrastrukturi (CIWIN) pri Komisiji.

Rezultat usklajevanja članic EU je Zelena knjiga (2005), katere »osrednji cilj je pridobivanje povratnih informacij o možnih politikah EPCIP, tako da se pritegne širok krog interesnih skupin.

Za učinkovito varovanje ključne infrastrukture so pomembni:

– komunikacija,
– koordinacija in
– sodelovanje

med vsemi zainteresiranimi skupinami – lastniki in upravljavci infrastrukture, zakonodajalci, strokovnimi telesi in gospodarskimi združenji, v sodelovanju z vsemi upravnimi ravnmi in javnostjo« (Zelena knjiga, 2005: 2).

Ključna infrastruktura (KI) se lahko »poškoduje, uniči ali okvari zaradi namernih terorističnih napadov, naravnih nesreč, malomarnosti, nesreč ali vdorov hekerjev, kriminalnih dejavnosti in zlonamernega vedenja. Da bi življenja in premoženje ogroženih ljudi v EU zavarovali pred terorizmom, naravnimi in drugimi nesrečami, bi morale biti motnje ali manipulacije ključne infrastrukture čim krajše, čim manj pogoste, čim bolj obvladljive, zemljepisno omejene in kar najmanj škodljive za blaginjo držav članic, njihovih državljanov in EU.« (Zelena knjiga, 2005: 1).

Evropska obrambna agencija (European Defense Agency (EDA)) je 2006 objavila povzetek: »The executive summary of EU Chemical, Biological, Radiological, Nuclear, Explosive Ordnance Disposal (CBRN EOD)", v katerem predvideva zaščito osebja, materiala, infrastrukture in okolja z namenom ohranjanja operativnih sposobnosti. Tveganja, ki izhajajo iz možne ofenzivne uporabe jedrskih, radioloških, kemičnih, bioloških agensov in tekoči eksplozivov (JRKB/E) bi lahko prizadela in kontaminirala večja območja EU, prebivalstvo, infrastrukturo, okolje in zmanjšala operativne sposobnosti delovanja. Zaradi kompleksnosti tovrstnih dogodkov/okolij EDA nedvoumno odsvetuje avtonomne/izolirane odzive posameznih članic EU, predlaga soodvisnost. Glede na nacionalno alokacijo pooblastil pa EDA kot imperativ nalaga posameznim članicam visoko stopnjo odgovornosti in absolutno odsotnost individualnih in enostranskih odzivov ter solitarnemu delovanju.

Zveza NATO (North Atlantic Treaty Organization) je 2007 ratificirala AJP-3.14 (Allied Joint Publication, Ratification Draft) Force Protection (FP): Zaščita sile, ki pomeni: »merila in sredstva z zmanjšanje ranljivosti osebja, zvez, materiala, operativne sposobnosti in delovanja pred tveganji in nevarnostmi za zagotavljanje ter ohranjanje operativne učinkovitosti ter uspešnosti poslanstva« (AJP-3.14, 2007: 1-1). NATO priznava, da je sila najbolj ranljiva med razmeščanjem, sprejemanjem, nameščanjem, premikanjem, izvedbo in ponovnim razmeščanjem v različnih fazah operativnega delovanja, predvsem pa dokler infrastruktura ni določena in so informacije o tem nepopolne. Za Zvezo NATO je kritična infrastruktura tista, ki »predstavlja tiste fizične in informacijske tehnologije, omrežja, storitve in

premoženje, katerih okvara bi resno vplivala na zdravje, varnost, varstvo ali gospodarsko stanje (CIP v Garb, 2009: 28).

Leta 2006 je bila v Republiki Sloveniji (RS) ustanovljena medresorska skupina za usklajevanje priprav za zaščito kritične infrastrukture z naslednjimi nalogami:

– »priprava pregleda organiziranosti in normativne urejenosti zaščite kritične infrastrukture po posameznih dejavnostih oziroma podsistemih nacionalne varnosti;
– proučitev organizacije postopkov ter smeri razvoja zaščite kritične infrastrukture na vzorcu članic Nata in EU;
– priprava ocene varnostnih razmer, tveganj in virov ogrožanja državne infrastrukture, tudi ocene možnega obsega posledic na prebivalstvo, ekonomijo in okolje:
– določitev enotne označitve vitalne infrastrukture države;
– oblikovanje predloga ustreznih ukrepov in postopkov za zaščito kritične infrastrukture z upoštevanjem usmeritev in stališč Nata in EU;
– priprava predloga organov in organizacij, ki bi morali načrtovati ukrepe za zaščito kritične infrastrukture« (Prezelj, 2007, Garb, 2009: 30).

V RS poteka raziskava z naslovom »Definicija in zaščita kritične infrastrukture v RS«, vendar pojmovanja oziroma definicije kritične infrastrukture v RS še vedno nimamo.

Zanimiva je definicija Garba (2009: 31), ki meni, da »kritično infrastrukturo predstavlja razvejana mreža neodvisnih, večinoma v zasebni lasti, sistemov, zmogljivosti in procesov, ki s sinergijskim delovanjem zagotavljajo neprekinjeno proizvodnjo in distribucijo osnovnih dobrin in storitev in katerih uničenje ali okvara lahko povzroči hude posledice na javno zdravstvo, varnost, gospodarsko stanje, socialno blaginjo prebivalcev in delovanje javnega sektorja.«

Garbova definicija (2009) se (z izjemo koncentracije na zasebno lastnino, ki ni popolnoma razumljiva in s tem korektna) približuje definiciji kritične infrastrukture v Zvezi Nato in v Združenih državah Amerike (ZDA), (tudi v Kanadi, na Finskem, v Veliki Britaniji ter v Organizaciji za gospodarsko sodelovanje in razvoj (OECD), ki kot posledico poškodovanja ali uničenja kritične infrastrukture navajajo neposredni negativni vpliv na javno zdravstvo.

Definiranje (ključne/kritične) infrastrukture je v ZDA je daleč najobširnejše, sklicevanje posameznih članic EU (vključno z RS), da so vzrok temu dejanski dogodki v ZDA (industrijske nesreče, izpad elektroenergetskih sistemov širših razsežnosti, naravne nesreče, ekološke nesreče, terorizem idr.) pa ni povsem prepričljivo. ZDA pojmujejo (ključno/kritično) infrastrukturo (Murray, 2007, Garb, 2009: 29,30) po naslednjih segmentih:

»A. gospodarski sektor:

– poljedelstvo, kmetijstvo in prehrana;
– voda in vodovodni sistemi;
– javno zdravstvo z urgenco;
– sistem zaščite in reševanja:
– obrambna industrija;
– telekomunikacije;
– energetski sistemi;
– transport;
– bančništvo in finance;
– kemikalije in nevarne snovi;
– pošta, pristanišča in pomorski promet.

B. javni in državni sektor:

– spomeniki nacionalnega pomena;
– jezovi, pregrade in nasipi;
– skladišča, deponije in ravnanje z radioaktivnimi snovmi;
– pomembne poslovne zgradbe.«

Sam pojem zaščite kritične infrastrukture v ZDA pa je definiran kot »strategija, politika, pripravljenost varnostnih sil, preventiva in odzivanje na napade na kritično infrastrukturo« (Lewis v Vršec, 2008: 3077 in Garb, 2009: 30).

Ni povsem jasno, še manj razumljivo, zakaj Republika Slovenija kot članica EU in Zveze Nato še vedno, od leta 2006 zavlačuje z definicijo ključne/kritične infrastrukture. Razumljivo ni tudi to, da bi Republika Slovenija lahko v tem vmesnem času, ko se ključna/kritična infrastruktura definira, uporabila znane definicije iz drugih držav članic EU, Zveze Nato, OECD ali ZDA. Krizno načrtovanje pri katerem nacionalna ključna/kritična infrastruktura ni jasno določena, je najmanj slučajno, slučaji pa so lahko nevarni.

Glavna načela Zelene knjige (2005: 4) so:

– Subsidiarnost
– Povezljivost
– Zaupnost
– Sodelovanje zainteresiranih skupin
– Sorazmernost.

Subsidiarnost je v središču EPCIP, saj bi bilo varovanje ključne infrastrukture predvsem v nacionalni pristojnosti. Glavno odgovornost zanj bi prevzeli države članice in lastniki/upravljavci, ki bi delovali znotraj skupnega okvira. Obveznost in odgovornost lastnikov in upravljavcev za sprejemanje lastnih odločitev in načrtov za varovanje lastnih zmogljivosti morata ostati nespremenjeni.

Povezljivost pomeni, da skupni okvir EPCIP ostaja povezljiv z obstoječimi ukrepi.

Zaupnost in zaupanje pri izmenjavi informacij o varovanju ključne infrastrukture, kar je nujno tudi zaradi tega, da je mogoče določene informacije o ključni infrastrukturi uporabiti in zlorabiti za povzročitev izpada ali nesprejemljivih posledic pri ključni infrastrukturnih objektih. Dostop do informacij na ravni EU in na ravni članic je omogočen izključno po potrebi.

Sodelovanje zainteresiranih skupin sodelujejo in prispevajo k razvoju in izvajanju EPCIP v skladu s svojo vlogo in pristojnostmi. Oblast članic zagotavljajo vodstvo in koordinacijo pri razvoju in izvajanju doslednega nacionalnega pristopa k varovanju ključne infrastrukture znotraj svoje pristojnosti. Lastniki, upravljavci in uporabniki so dejavno vključeni tako na ravni države kot EU. Kadar ne obstajajo sektorski standardi ali še niso vzpostavljene mednarodne norme, lahko organizacije s področja standardizacije sprejmejo enotne standarde, kadar je to ustrezno.

Sorazmernost varnostnih strategij in ukrepov s stopnjo tveganja, saj vseh infrastruktur ni mogoče zavarovati pred vsemi grožnjami. Z uporabo ustreznih metod obvladovanja tveganja, ob upoštevanju grožnje, pomembnosti, razmerja med stroški in koristmi, obstoječe stopnje varovanja ter učinkovitosti razpoložljivih strategij za ublažitev (Zelena knjiga, 2005: 4)

Dejstvo je, da lahko okvara ali uničenje ključne infrastrukture v eni državi članici negativno vpliva na številne druge in evropsko gospodarstvo v ce-

loti. Varnostni ukrepi so učinkoviti le toliko kot njihov najšibkejši člen, kar pomeni, da je potrebna enotna stopnja varnosti. Za učinkovito varovanje so ključni komunikacija, koordinacija in sodelovanje med vsemi zainteresiranimi stranmi na ravni države, EU ter na mednarodni ravni. Zato je potreben skupni okvir EU za varovanje ključne infrastrukture v Evropi, ki naj vsebuje horizontalne ukrepe, ki določajo pristojnosti vseh zainteresiranih skupin pri varovanju ključne infrastrukture in opredeli temelje za pristop v posameznih sektorjih. Skupni okvir bi dopolnil obstoječe ukrepe v posameznih sektorjih, s čimer bi se dosegla najvišja možna raven varovanja kritične infrastrukture v EU. Prednostna naloga je usklajevanje enotnega seznama opredelitev in sektorjev ključne infrastrukture (Zelena knjiga, 2005: 5).

Ključna infrastrukture se z vzpostavitvijo skupnega okvira EPCIP krepi izmenjavo najboljših praks in mehanizmov za zagotavljanje ustreznosti. Med sestavinami skupnega okvira so:

– skupna načela varovanja ključne infrastrukture;
– vzajemno sprejeta pravila ravnanja/standardi;
– enotne opredelitve, na podlagi katerih se lahko sprejmejo opredelitve po posameznih sektorjih;
– enotni seznam sektorjev ključne infrastrukture;
– prednostna področja varovanja ključne infrastrukture;
– opis pristojnosti zainteresiranih strank;
– dogovorjena merila uspešnosti;
– metodologije za primerjavo in opredelitev prednosti infrastrukture v različnih sektorjih.

Tak skupni okvir lahko omeji tudi morebitne škodljive učinke na notranjem trgu. Skupni okvir je lahko prostovoljen ali obvezen – ali pa deljeno, odvisno od zadeve. Oba okvira lahko dopolnjujeta obstoječe sektorske in horizontalne ukrepe, vendar pa bi samo pravni okvir vzpostavil trdno in izvršljivo pravno podlago za usklajeno in enotno izvajanje ukrepov za varovanje evropske ključne infrastrukture. Ne zavezujoči prostovoljni ukrepi so sicer prilagodljivi, vendar posameznih vlog ne opredeljujejo dovolj jasno (Zelena knjiga, 2005: 5,6).

Opredelitev ključne/kritične infrastrukture je določena »z čezmejnim vplivom, ki kaže, ali bi lahko nesreča imela resne posledice zunaj ozemlja države članice, kjer leži objekt. Pri tem je treba upoštevati dejstvo,

da so mednarodni načrti za sodelovanje pri varovanju ključne infrastrukture že uveljavljen in učinkovit način za ravnanje s ključno infrastrukturo med mejami držav članic. Tako sodelovanje lahko dopolni EPCIP. Evropska ključna infrastruktura lahko obsega tudi tiste materialne vire, storitve, infrastrukturo informacijske tehnologije, omrežja in infrastrukturne zmogljivosti, katerih okvara ali uničenje bi resno vplivala na zdravje, varnost, gospodarstvo ali družbeno blaginjo:

– dveh ali več držav članic – to vključuje določeno dvostransko ključno infrastrukturo;
– bi zadevalo tri ali več članic – to bi izključevalo določeno dvostransko ključno infrastrukturo. « (Zelena knjiga, 2005: 6)

Zelena knjiga (2005: 7) posebno pozornost namenja soodvisnosti znotraj podjetij, gospodarskih sektorjev, krajevnih pristojnosti in organov držav članic ter med njimi, zlasti tistih, ki jih omogočajo informacijske in komunikacijske tehnologije.

Koraki za izvajanje evropske ključne infrastrukture (EKI):

1. Komisija skupaj z državami članicami izoblikuje merila, ki se naj uporabljajo za opredeljevanje EKI v posameznih sektorjih.
2. Države članice in Komisija opredelijo in potrdijo EKI po sektorjih. Zaradi čezmejne narave zadevne infrastrukture se sklep o imenovanju določene ključne infrastrukture za evropsko ključno infrastrukturo sprejme na evropski ravni.
3. Države članice in Komisija analizirajo obstoječe varnostne pomanjkljivosti v povezavi z EKI po posameznih sektorjih.
4. Države članice in Komisija se ob upoštevanju soodvisnosti sporazumejo o prednostnih sektorjih/infrastrukturi pri ukrepanju.
5. Kadar je to ustrezno, se za vsak sektor Komisija in ključne zainteresirane strani držav članic sporazumejo o predlogih za minimalne varnostne ukrepe, ki bil lahko vključevali standarde.
6. Potem, ko predlog sprejme Svet, se ti ukrepi začnejo izvajati.
7. Države članice in Komisija zagotovijo reden nadzor. Revizije (ukrepov in opredeljevanja ključne infrastrukture) se sprejmejo, kadar in kjer so potrebne. (Zelena knjiga, 2005: 7,8).

Nacionalna ključna infrastruktura (NKI) v EPCIP: številna evropska podjetja poslujejo prek meja in zato zanje veljajo različne obveznosti za NKI.

V interesu držav članic in EU kot celote se zato predlaga, da vsaka članica zavaruje svojo NKI znotraj skupnega okvira, tako da se lastnikom in upravljavcem po vsej Evropi ni potrebno ukvarjati z nepregledno množico okvirov, iz katerih izhaja nešteto metodologij in dodatnih stroškov. Zato je Komisija predlagala, da EPCIP ne mor povsem izpustiti NKI, vseeno pa se lahko predvidijo tri možnosti:

1. NKI je popolnoma vključena v EPCIP.
2. NKI je zunaj področja delovanja EPCIP in
3. države članice lahko dele EPCIP v povezavi z NKI uporabijo po želji, vendar k temu niso zavezane (Zelena knjigam, 2005: 8, 9).

Na podlagi skupnega okvira EPCIP lahko posamezne države članice razvijejo nacionalne programe varovanja ključne infrastrukture za svojo NKI in lahko pri tem uporabijo celo strožje ukrepe kot jih določa EPCIP.

Potreba po učinkovitosti in usklajenosti ter interoperabilnosti narekuje, da vsaka država članica imenuje en sam nadzorni organ, ki se ukvarja s splošnim izvajanjem EPCIP. Predvideni sta dve možnosti:

1. enoten organ za nadzor varovanja ključne infrastrukture in
2. nacionalna kontaktna točka brez pristojnosti, ki državam članicam prepušča lastno organiziranje (Zelena knjiga, 2005: 9).

Ta organ je lahko podlaga za nacionalno predstavništvo v strokovnih skupinah, ki se ukvarjajo z zadevami varovanja ključne infrastrukture, in bi bil lahko povezan z informacijskim omrežjem za opozarjanje o ključni infrastrukturi (CIWIN). Nacionalni organ za koordinacijo varovanja ključne infrastrukture (NOKK) bi lahko usklajeval nacionalne zadeve na področju varovanja ključne infrastrukture ne glede na to, da so vanje že vključeni drugi organi ali subjekti v državi članici. Postopno opredelitev NKI bi bilo mogoče doseči z zahtevo, da morajo lastniki in upravljavci infrastrukture nacionalnemu koordinacijskemu organu priglasiti vsako poslovanje, povezano z varovanjem ključne infrastrukture (Zelena knjiga, 2005: 9, 10). NOKK bi lahko bil odgovoren tudi za zakonsko odločanje o imenovanju infrastrukture v svoji pristojnosti za NKI, te informacije pa bi bile na razpolago izključno zadevni državi članici.

Republika Slovenija ima na razpolago različne vzore, vzorce in dokumente, po katerih bi lahko določila nacionalno ključno infrastrukturo in se s

tem aktivno ter učinkovito vključila v skupni okvir EPCIP. Pomanjkanje definirane ključne/kritične infrastrukture predstavlja kompleksnejši izziv in zadrego pri kriznem načrtovanju, upravljanju in odzivanju kot se zdi oziroma razume. Brez definicije ključne/kritične infrastrukture se povečuje in predvsem podcenjuje ambivalentnost definicije same, saj je ključno/kritično infrastrukturo potrebno (kljub znani definiciji) vedno znova definirati oziroma določiti prednost glede na varnostna tveganja, ki lahko preidejo v grožnjo in kasnejšo uporabo sile. Zanimivo je, da se kot ključna/kritična infrastruktura navajajo le objekti v posameznih sektorjih, pri čemer pa lahko npr. pri nalezljivi bolezni na meji EU ali znotraj EU postane državna meja. Pomemben je pristop; za zadostno in potrebno celovitost (Mulej in soavtorji, 2003) se avtorji opredelitve ključne/kritične infrastrukture morajo in smejo odločiti kaj bo vključeno v njihov sistem vidikov in kaj bo puščeno ob strani, vendar bo še vedno obstajalo in vplivalo. Zgodovinarji so odkrili, da niso tehnološke najdbe tiste, ki so se prve pojavile in privedle do nove kakovosti življenja/obrambe/varnosti, temveč je bila inovacija v družbi prevladujoče kulture in zavesti tista, ki je ustvarila prostor za svobodno razmišljanje, govorjenje in tveganje kot smiselni dejavnik pri podrobnih kriznih in strateških načrtih. Vizijo moramo razumeti kot »preživetje« na podlagi zaščite kot ključne/kritične infrastrukture s celovitim ustvarjalnim delom in sodelovanjem z inovacijo, usmerjeno k sistemski kakovosti, ki je v skladu z novim pojmovanjem varnostnih/oboroženih sil. Poslanstvo (npr.) » navdušiti sile z izvrstno sistemsko kakovostjo in jih privabiti kot stalne in motivirane uslužbence«. Politika (npr.) »uvaja inovativno izobraževanje in strategije kot vir trajne sistemske in varnostne/obrambne kakovosti na vseh področjih varnostnega/obrambnega delovanja, v vseh enotah«. Taktike za izvajanje takih inovacijskih strategij vključujejo (npr.) »organizirano kritiko, ki ji sledijo skupine in namenske sile, usmerjene v reševanje izbranih problemov in vprašanj – (npr). definiciji ključne/kritične infrastrukture«. (Ivanuša, Mulej, 2009 v pripravi).

Znanje, izkušnje, predanost in možnosti govora ter ugovora, kot odziva na sodobno varnostno okolje, so spremenjene. Ljudje ne poslušajo in ne želijo slišati. Zaznavanje nekega stanja in realnost dejanskega stanja sta dva različna pojma, med katerima je čas ključni/kritični dejavnik pravočasnega odzivanja, zmanjševanja posledic in skrajševanja prehoda v fazo obnove, vzpostavljanja prvotnega stanja ali celo njegove nadgradnje. Ni novost (na žalost), da ljudje so in živijo samozadostno. V vakuumu vse večje brezbrižnosti do sočloveka, do okolja, nacionalne varnosti, zbledelih vrednot

in vedno manjše osebne varnosti iščemo nove poti, a stare resnice, ki jih čas ne spreminja in jih razkrivajo protislovja. Sodobno življenjsko in varnostno okolje je kompleksno, tveganja in dogodki izrazito nepredvidljivi. Zato krizno upravljanje in ustvarjalnost ter sporočilo v tem niso le dogodek, ampak stil. Sogovorniki se zatekajo k ustvarjanju nasprotnih mnenj, s katerimi govorijo in ugovarjajo in znašli smo se v vmesnem prostoru, ki ni ne srednji, ne zadosten in potreben, ampak nevaren. Tveganja se vse kompleksnejša, krizno upravljanje pa ostaja priložnostna domena kompetenc in manj kompetentnosti. Sodobno krizno upravljanje vključuje obvladovanje, pri čemer je obvladovanje nadgradnja, ki čas v vmesnem prostoru bistveno skrajša, zmanjša presenečenja - saj so presenečenja lahko nevarna – in omogoča učinkovit odziv ter učinkovito delovanje. Zmanjševanje razkoraka med realnostjo in njenim zaznavanjem je ključno za zmanjševanje krize, ublažitev njenih posledic in povečevanje/zagotavljanje osebne varnosti, ki je predpogoj za kolektivno varnost. Krizno načrtovanje, upravljanje in obvladovanje krize zahteva interdisciplinarni in interspektralni pristop, odnos in brezhibno uporabo uma, razuma, izkušenj in čustev. S tem ustvarimo utemeljene, ne le želene izide in poti, da jih uresničimo v procesu kriznega upravljanja in obvladovanja. Krizno upravljanje in obvladovanje ima svoje vrednote in smoter, ki so trajni, če je poslanstvo preživetje in je pomemben tako posameznik kot skupina oziroma celota. Definicija ključne/kritične infrastrukture je kompleksna naloga, ki v procesu kriznega načrtovanja, upravljanja in obvladovanja zahteva trajnostno določanje, revizijo, ponovno določanje in mora upoštevati ambivalentnost ključne/kritične infrastrukture

Izdelana vizija, premišljeni načrti, predanost,profesionalnost in zdrava pamet nezmotljivo vodijo k cilju.

Literatura in viri:

- *EDA CBRN EOD Project Team. (2006). EU Chemical Biological Radiological Nuclear Explosives Ordnance Disposal Doctrine for Multinational Operations. Brussels, Belgium.*
- *Garb, G. (2009). Varnostno upravljanje kritične infrastrukture. Magistrsko delo, Fakulteta za logistiko, Celje*
- *Ivanuša, T., Mulej, M. (2009). Toward requisite holism of content of the term critical infrastructure. (v pripravi)*

- *Komisija evropskih skupnosti. (2005). Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture. Bruselj.*
- *Mulej, M., Ženko, Z., Knez-Riedl, J., Potočan, V. (2003). Upravljanje – kdaj je razmišljanje o njem in v njem sistemsko/celovito. Organizacija, Vol. 36, Št. 7, str. 443-445.*
- *Murray, A. (2007). Critical Infrastructure: Reliability and Vulnerability (Advances in Spatial Science). Springer, New York.*
- *NATO Standardization Agency. (2007). Allied Joint Doctrine for Force Protection: AJ-3.14.- Ratification Draft. NSA, Brussels, Belgium.*
- *Prezelj, I. (2007). Nujnost medresorskega in koordiniranja v boju proti terorizmu: nekateri primeri iz Republike Slovenije. Bilten Slovenske vojske, Št. 2/9. GŠSV, Ljubljana.*
- *Vršec, M. (2008). Zaščita kritične infrastrukture v slovenskih organizacijah po evropskih merilih. 27. mednarodna konferenca o razvoju organizacijskih varnosti, Portorož, str. 3075-3083.*

VI.

Ob napadu bodite pripravljeni

Napotek 36: Vedite, da so vse katastrofe lokalne

Za prve odzivne enote ni važno, ali teroristi prihajajo iz Afganistana ali Alabame. V mnogih pogledih so teroristični napadi podobni naravnim katastrofam, kot je npr. potres - čeprav je nekaj očitnih in pomembnih razlik (glej napotek 37). Ker **so učinki** takih **dogodkov lokalni**, so lokalne razmere tiste, ki narekujejo, kako se odzvati na napad.

Prvih nekaj ur napada ste sami. Potreben je čas – veliko časa – da pride pomoč oblasti. Lokalna policija se mora odzvati na terorističen napad, ko se ta dogaja. Ob začetku napada to pomeni uporabo izključno lokalnih virov. Če ste naredili domačo nalogo, boste že imeli vpeljane komunikacijske kanale, ki vam bodo omogočili določitev in vzpostavitev stika s pomembnimi akterji v vaši in sosednih skupnostih. Da se je zgodil napad, boste seveda obvestili tudi zvezne in državne oblasti, vendar se glede takojšnje podpore ne smete zanašati nanje. Pravzaprav vam bodo verjetno najbolj v pomoč šele kasneje, v fazi obnove.

Teroristični napad je kraj zločina. Kot je omenjeno v napotku 9, bi morali na terorizem gledati kot na kriminaliteto. Glede na to, da bo vaša glavna skrb blažitev povzročene škode žrtvam na prizorišču dogodka, bi morali lokacijo napada obravnavati kot kraj kaznivega dejanja. Postopki zbiranja in shranjevanja dokazov bi morali biti nekoliko drugačni od tistih, ki jih izvajajo na kraju vsakega resnega kaznivega dejanja, kljub temu pa boste za zbiranje in shranjevanje dokazov morda rabili strokovno pomoč.

Pregon teroristov. Morebitna povezanost hudodelcev s teroristično skupino bo malo pomembna za vaše dolžnosti kot člana prvih odzivnih enot: vaša neposredna naloga bo spoprijeti se z uničenjem in žrtvami na prizorišču dogodka. Iskanje teroristov bi morali prepustiti FBI in drugim zveznim agencijam. Lahko jim pomagate z ohranitvijo kraja zločina, z nudenjem informacij, ki ste jih že zbrali (napotki 28, 29 in 30), in sistematičnim zbiranjem ustreznih informacij po napadu.

Delajte, kar najbolje znate. Lokalne skupnosti so že zdaj pripravljene na odziv na številne morebitne katastrofe. Policija se redno sooča z nesrečami, katerih posledica so osebne poškodbe in materialna škoda, z manjšimi trčenji kot tudi nesrečami, kjer je udeleženih več avtomobilov. Take nesreče grozijo, da bodo preobremenile zmožnosti odzivnih enot za nujne primere. Večina skupnosti ima pripravljene načrte za primere naravnih ujm, kot so snežne nevihte, potresi, poplave in orkani. Od šolske tragedije v Columbine naprej se lokalne skupnosti pripravljajo na možnost nasilnih napadov v svojih izobraževalnih institucijah; v številnih šolskih okrožjih bombne grožnje in druge oblike nasilja niso bile redke celo pred Columbine. In v zadnjih letih je strah pred gripo in drugimi epidemičnimi boleznimi dvignil lokalno zavest o problemih, ki jih pomenijo virusne in bakterijske nevarnosti. Verjetno že poznate večino tistih, ki so vključeni v načrtovanje odziva na te in druge vrste katastrof. Ena od pomembnih vlog, ki jo lahko imate, je razvoj načrta za usklajevaje teh virov v primeru, da se zgodi katastrofa.

Bodite pripravljeni. V napotku 13 svetujeva, da zamenjate »kaj če« s »kako verjetno.« Ker smo tveganje in ranljivost ocenjevali z vidika preprečevanja, je bilo smiselno določiti tarče, ki so najbolj ranljive. Pripravljenost na katastrofo je zelo drugačna, kadar jo gledamo z vidika prvega odziva nanjo. Član prvih odzivnih enot na teroristični napad mora biti pripravljen na »kaj če«: kaj se bo zgodilo, če se uresniči vaša najhujša mora, ne glede na verjetnost, da se bo to res zgodilo. Vaša naloga v tem primeru ni onesposobitev teroristov, temveč blažitev razmer, ki so jih teroristi pustili za sabo: razdejanje, poškodbe in uničenje. Ko se zgodi teroristični napad, se bo od policije kot prve, ki se odzove na kriminalna dejanja, pričakovalo, da se bo odzvala takoj. Zato se morate vprašati naslednje:

- Je vaša postaja pripravljena na napad?
- Čigava je še odgovornost poleg policije, da usklajuje odzivne enote postaj?
- Kako se policijska postaja pripravi na večje katastrofe?

Vzpostavite ravnotežje. Ker so prve odzivne enote pogosto tiste, ki se jih najprej obtožuje, če gre kaj narobe, je razumljivo, da vodjo policije morda mika pretiran odziv bodisi tako, da bi naredil preveč, ali pa se poskusil izogniti vlogi tistega, ki se odzove prvi. Primer prvega je načelnik v majhnem mestu, ki zapravlja denar ministrstva za domovinsko varnost za dekontaminacijsko komoro, ne da bi prej ocenil tveganje kemičnega

napada. Primer drugega je vodja policije, ki zavzame stališče, da so prej kot policija tisti, ki se prvi odzovejo, v resnici žrtve, gasilci in nujno medicinsko osebje. V takem primeru bo policija prevzela stransko vlogo pri razvijanju načrtov za prvi odziv; in čeprav je takšno stališče pravzaprav pravilno, zanemarja verjetnost, da bo policija javno odgovorna, zaradi svoje tradicionalne vloge pri odzivanju na težave v skupnosti.

Ne dovolite, da ukvarjanje s problemi terorizma preobremeni druge naloge vaše postaje. Stremite k vzpostavitvi ravnotežja med pripravljenostjo in vsakodnevno policijsko dejavnostjo, kar vam bo pomagalo izogniti se čezmernemu odzivu. Analizirajte, kako lahko priprava na teroristični napad koristi vsakodnevni policijski dejavnosti in kritično ovrednotite ukrepe, ki koristijo obema področjema. Številni koraki v tem priročniku bodo ustvarili tovrstne dvojne koristi; na primer, ko boste popisovali ranljive tarče, bo vaša postaja vzpostavila tesne odnose s podjetji in skupnostnimi organizacijami. Taka družabništva so lahko zelo koristna pri preprečevanju običajne in ponavljajoče se kriminalitete. Zaradi zaščite stavb pred teroristi so te bolj varne tudi pred običajnim kriminalom. Poostritev postopkov preverjanja identitete v prodajalnah na drobno ne otežuje le dela teroristom, temveč pomaga tudi pri preprečevanju tatvin. Vaje za pripravljenost v nujnih primerih bodo policijo pripravile tudi na soočenje z njeno vlogo enote za prvi odziv na teroristični napad.

Napotek 37: Vedite, da vse katastrofe niso enake

Katastrofe zahtevajo izjemno veliko od prvih odzivnih enot. Teroristični napadi lahko ustvarijo razmere, ki so podobne katastrofam, kot na primer:

- veliko število mrtvih ali poškodovanih ljudi
- prizadetost obsežnega geografskega območja in številnih okolišev
- številne in različne vrste tveganj
- zahteve po virih in sposobnostih, ki presegajo zmožnosti lokalnih odzivnih organizacij
- obsežen dotok prostovoljcev in sredstev
- poškodbe vitalne transportne, komunikacijske in druge infrastrukture
- veliko število tistih, ki se odzovejo iz tako javnih kot tudi zasebnih virov
- nevarnost za življenja članov odzivnih enot

Čeprav je le nekaj terorističnih napadov doseglo stopnjo katastrofe, številni priročniki in učbeniki za odziv na terorizem temeljijo na priročnikih za naravne katastrofe; zato ti priročniki glede pripravljenosti zagovarjajo pristop »vseh tveganj.«

Do katere stopnje so večji teroristični napadi podobni tovrstnim katastrofam? V tabeli 1 primerjamo zgoraj navedene kriterije z značilnostmi večje naravne katastrofe (orkan Katrina) in velikega terorističnega napada (11/9 – Svetovni trgovinski center).

Napad brez opozorila, kar je verjetno najbolj izrazita značilnost terorističnega napada, ima važne načrtovalne posledice. Od naravnih katastrof jih loči trajanje in geografska osredotočenost. Običajni teroristični napadi so natančno usmerjeni: izberejo bodisi posamezno lokacijo – kakor je bilo v primeru Oklahoma Cityja – ali pa izberejo več lokacij v ozkem žarišču, kakor je bilo v primeru napada 11. septembra. Z lokalnega vidika to omogoča odzivnim enotam, da hitro ocenijo obseg škode in nevarnosti. Napad 11. septembra na Svetovni trgovinski center je bil natančno usmerjen na specifični tarči. V nasprotju s tem je orkan Katrina zajel širok pas ozemlja. Prve odzivne enote, ki so prispele na kraj opustošenja v mestu New Orleans, so se soočile tudi s širokim razponom težav po vsej Louisiani in Mississipiju. Poleg tega je orkan trajal več dni, medtem ko je napad 11. septembra trajal zgolj 102 minuti: minilo je maj kot 2 uri od takrat, ko se je prvo letalo zaletelo v severno stolpnico, do takrat, ko sta se obe stolpnici zrušili.

Tabela 1. Primerjava med orkanom Katrina in napadom 11/9

Značilnosti katastrofe	11/9	Orkan Katrina
Predhodno opozorilo	Nobeno	Napovedovalci vremena za več dni so svarili, da se približuje orkan
Ubitih ljudi	Približno 2.750	1500 mrtvih v Louisiani, vključno s približno 600 v New Orleansu: 300 v Mississipiju
Geografsko področje in okoliši	Vsaj pet okolišev, omejeno geografsko področje	Številni okoliši, obsežno geografsko področje
Trajanje katastrofe	1-2 dni	Več dni preden so vode upadle
Čas obnove	Še poteka	Še poteka
Število tveganj	Številna zdravstvena tveganja in tveganja zaradi onesnaženosti, druga še odkrivajo	Onesnaženost iz rafinerij in umazana voda, vendar ne tako resno, kot se je sprva domnevalo
Ustreznost lokalnih virov	Dobra oskrba s stani lokalnih agencij, vendar so dobile veliko zunanje pomoči	Popolnoma neprimerna sredstva; potrebna je bila zunanja pomoč, z večjim delom pomoči se je zavlačevalo
Obsežna nacionalna medijska pokritost	Da	Da
Poškodovana infrastruktura in komunikacije	Da, na lokalnem prizorišču, vendar ne v celotnem mestu, razen nekaj telefonskih motenj	V celotnem New Orleansu ni bilo komunikacije, elektrike in vode
Število in raznolikost odzivnih agencij	Tri javne agencije, številni odzivi zasebnikov	Na začetku le policijska postaja New Orleans in obalna straža; kasneje številne zvezne, državne, lokalne, mestne in zasebne agencije
Ogroženost življenj članov odzivnih enot	Izguba številnih življenj članov odzivnih enot	Nekaj nevarnosti, vendar ni bilo izgubljeno nobeno življenje članov odzivnih enot

Teroristični napadi, ki so najbolj podobni naravnim katastrofam, so tisti, ki se jih najbolj bojimo: bodisi napad z orožjem za množično uničevanje (OMU), ki uniči veliko geografsko področje, ali biološki napad, ki razširi strup na obsežnem področju. Tovrstni napadi ne bi bili usmerjeni na določeno tarčo, kot je Svetovni trgovinski center, temveč na celotno mesto, tako kot se je zgodilo z orkanom Katrina. Biološko in kemično orožje je težko omejiti na specifično tarčo – zaradi njune smrtonosnosti je malo potrebe za takšno usmeritev – zato se ju lahko uporabi za poškodovanje zelo obsežnega dela prebivalstva ali geografskega področja.

Z upoštevanjem teh razlik predstavlja tabela 2 kontrolni seznam, ki se lahko uporabi pri ocenjevanju stopnje potrebnega odziva na teroristični napad. Čeprav gre za zelo splošno vodilo, ga je mogoče uporabiti kot začetno oceno obsega odziva, ki bi bil morda potreben. Protokol se lahko uporabi ali oblikuje v povezavi z ocenjevalno raziskavo ranljivosti, ki naj bi jo izvedli že pred dogodkom kot del vaše pripravljenosti na teroristično katastrofo (glej napotke 28-33).

V zgodnjih fazah terorističnega napada ali naravne katastrofe je težko pridobiti zanesljive informacije. Med dogodkom se razmere nenehno spreminjajo, tako kot v prvih 17 minutah napada na Svetovni trgovinski center. Brez informacij je nemogoče izpolniti protokol, kakršen je predstavljen tukaj. S pridobivanjem novih informacij ga je treba tudi ponovno pregledati in popraviti. Za vajo smo izpolnili protokol, kakor bi lahko bil uporabljen ob napadu 11. septembra. Če se postavimo v kožo članov prvih odzivnih enot v prvih 17 minutah napada na Svetovni trgovinski center, vidimo, da bi številne dele protokola težko izpolnili. Dejansko je na napake pri obvladovanju prizorišča in ravnanju na njem vplivalo pomanjkanje zanesljivih informacij.

Tabela 2. Kontrolni seznam pripravljenosti na terorizem

Predmet	Merila ocenjevanja	STC 11/9 Točke
Uporabljeno orožje (izberi uporabljeno vrsto orožja)	1. Lahko orožje, strelno orožje 2. Majhne eksplozivne naprave 3. Velike eksplozivne naprave 4. Zelo velike eksplozivne naprave 5. Nekonvencionalno orožje	5
	Pomnoži oceno s številom orožij =	10

Predmet	Merila ocenjevanja		STC 11/9 Točke
Tarča/prizorišče (označite vse, ki ustrezajo)	Zasedene zgradbe Visoke zgradbe Odprti prostori Več tarč na različnih lokacijah Nediferencirano območje Gosto naseljeno območje **Skupaj označenih =**		*5*
Škoda na infrastrukturi (3=najbolj resna)	Električno omrežje Vodovod Transportne smeri komunikacije	1 2 3 1 2 3 1 2 3 1 2 3 **Skupaj =**	**4**
Teroristi	1 – Napadalci mrtvi/zapustili prizorišče 2 – En napadalec še vedno na prizorišču 3 – Več napadalcev še vedno na prizorišču **Skupaj =**		**1**
Tveganja (uporabite raziskavo o ranljivosti, ki ste jo izvedli kot del pripravljenosti na katastrofe)	• Toksičnost zaradi ognja/eksploziva • Jedrski objekt na ali v bližini prizorišča • Kemična tovarna na ali v bližini prizorišča • Biološki objekt na ali v bližini prizorišča • Druge znana tveganja na ali v bližini prizorišča **Skupaj označenih =**		**1**
Požarna ocena (ocenite uporabo gasilskih radijskih kod)	1 – Nizka 2 – Srednja 3 – Visoko **Skupaj =**		**3**
Potrebno osebje in oprema (označite potrebno)	• Gasilci • Medicinsko osebje • Ustrezno biološko/kemično osebje • Policija – nadzor prometa • Policija – nadzor prizorišča • Policija – preiskovalci na prizorišču • Policija – specialne enota • Strokovnjaki za komunikacije • Transport – osebje in oprema **Skupaj označenih =**		**8**
			32

Napotek 38: Uporabite pristop 3-na-3

Glede na to, da bo lokalna policija v središču odziva na večje teroristične napade – in bo nosila odgovornost kot prva odzivna enota – se prepričajte, da lahko odgovorite na šest vprašanj od VUSZHU (angl. SECURE).

1. Varno (angl. Safe): Ste zagotovili varnosti svojih policistov?
2. Učinkovito (angl. Effective): Kaj bodo vaši policisti naredili, ko pridejo na prizorišče?
3. Sposobno (angl. Capable): So bili vaši policisti ustrezno izurjeni v odzivanju na katastrofe?
4. Združeno (angl. United): Kako dobro je vaša postaja usklajena z drugimi enotami za prvi odziv?
5. Hitro (angl. Rapid): Kako hitro lahko vaši policisti pridejo na prizorišče?
6. Učinkovito (angl. Efficient): Bodo policijske naloge, ki niso povezane z napadom, zapostavljene?

Ta splošna vprašanja vam bodo pomagala ostati na pravi poti. Toda, če ne boste sistematično pristopili k zagotavljanju vseh pomembnih vidikov, ki jih izpostavlja VUSZHU, ne boste mogli odgovoriti na vsa vprašanja zadovoljivo. Ta napotek predstavlja pristop 3-na-3, ki ga sestavljajo tri faze upravljalnega cikla prvih odzivnih enot in tri faze terorističnega katastrofe.

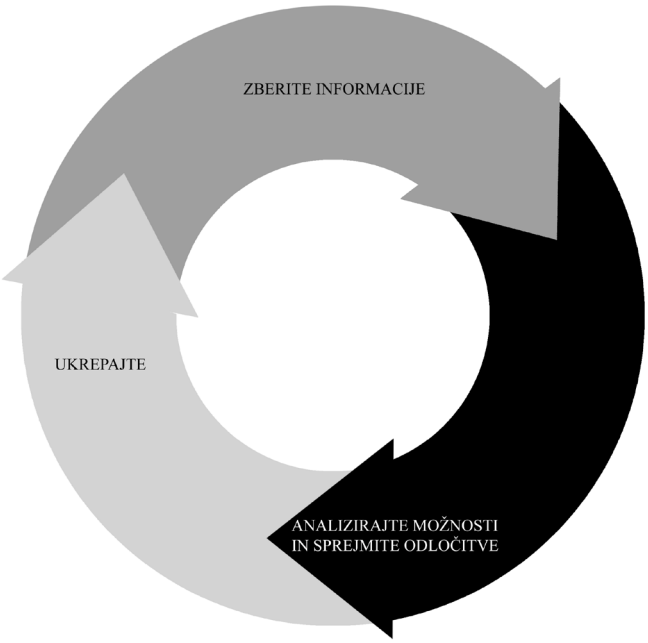
Upravljalni cikel prvih odzivnih enot. Upravljalni cikel prvih odzivnih enot, ki ga je razvila korporacija RAND (glej skico), vam bo pomagal delovati sistematično, s tem da boste naredili tri zaporedne korake: (1) zbrali vse informacije, ki jih potrebujete; (2) analizirali možnosti; in (3) ukrepali. Z uporabo te metode v okviru vseh treh stopenj katastrofe (glej spodaj) boste zagotovili, da bodo vaše odzivne enote vedele, kaj počnejo in zakaj to počnejo. To je seveda daljši proces, saj boste po ukrepanju hoteli ponovno oceniti informacije, ki ste jih zbrali. Upajmo, da se boste lahko učili iz lastnih napak - in uspehov. (Če poznate problemsko naravnano policijsko dejavnost, boste opazili, da je ta proces zelo podoben modelu SAOO (angl. SARA): Skeniranje, Analizira, Odziv in Ocena). (angl. Scanning, Analysis, Response in Assessment.)

Ta upravljalni cikel informacij bi morali vključiti v vsakodnevne operacije svoje postaje. Da bi to dosegli, boste morali narediti naslednje:

- z uporabo preprostih kontrolnih seznamov, obrazcev in predvsem elektronskih pripomočkov, kot so prenosni računalniki, poenostavite zbiranje in beleženje informacij;
- izobrazite svoje policiste, da bodo razumeli pomen zbiranja informacij pri razreševanju policijskih problemov;
- shranite informacije tako, da bodo lahko dostopne in posodobljene;
- ustvarite bazo podatkov, ki jo lahko policisti uporabljajo v okviru svojih vsakodnevnih operacij;
- bazo podatkov strukturirajte tako, da jo je mogoče analizirati pri reševanju velikih in tudi majhnih ponavljajočih se policijskih problemov;
- določite in usposobite posebne policiste za analizo informacij.

Informacije so ključne pri reševanju vseh policijskih problemov, vključno s terorizmom. Pomanjkanje informacij ima lahko velikanske posledice. Med napadom 11. septembra se je izkazalo, da ni bilo nenehnega posodabljanja in dopolnjevanja informacij, vitalnih za reševalske operacije.

Upravljalni cikel prvih odzivnih enot.



Vir: Prirejen od: RAND Corporation. Protecting Emergency Responders. Volume 3: Safety Management in Disaster and Terrorism Response, 2004, p.xvii.

Tri faze večjega terorističnega napada. Večja katastrofa oz. teroristični napad ima tri faze: pred, med in po napadu. Skrbna priprava na vsako fazo bo občutno ublažila težave, s katerimi se boste soočali v vsaki naslednji fazi. To pomeni, če vložite veliko truda v fazo pred napadom, se boste pri odzivu na dejanski napad soočali z manj težavami. In če prizorišču napada posvetite natančno pozornost, boste ublažili učinke napada in s tem zmanjšati probleme, s katerimi se boste soočali po napadu. Prve odzivne enote in mediji namenjajo največ pozornosti sredinski fazi, napadu, zaradi očitne travme in uničenja, ki ga ta povzroči; večji teroristični napad traja zelo kratek čas, kar predstavlja le majhen delež vseh učinkov katastrofe in odzivov, ki so potrebni za njihovo ublažitev.

Čeprav se zdi očitno, da je trenutek napada drugačen od časa pred in potem, se strokovnjaki za katastrofe ne strinjajo o tem, kdaj se vsaka faza začne in konča. Nekateri na primer trdijo, da je bilo zaradi neustreznega uradnega odziva čutiti najhujše učinke orkana Katrina v New Orleansu šele nekaj dno po tem, ko je orkan udaril. Razmere v louisianskem večnamenskem prostoru, kamor so ljudi napotili, so ustvarile svojevrstno katastrofo. Odvisno od vrste katastrofe in vrste odziva se posamezne faze precej prekrivajo. Kot sva navedla, bo delo, ki ga opravite v vsaki fazi, ublažilo učinke vsake naslednje faze. Razumljivo je, da ob razvoju katastrofe različne vladne agencije igrajo različne vloge, ki so različnega pomena in so izvajane ob različnem času. Primer tega si oglejte v tabeli v napotku 48, ki prikazuje, kako se v okviru manjše naravne katastrofe vloge prvih odzivnih enot s časom spreminjajo.

3-na-3 pristop obvladovanja teroristične katastrofe

	1. Zbiranje informacij.	2. Analiziranje možnosti.	3. Ukrepaj.
Pred	Naredi sezname	Nariši zemljevide	Razvij odzivne načrte
Med	Imejte učinkovito komunikacijo	Uskladite prizadevanja	Razvrstite osebe in opremo
Potem	Nadzorujte tveganja in zdravje žrtev in prvih odzivnih enot	Ocenite potrebe po oskrbi, ocenite preventivne potrebe	Podpirajte okrevanje; ponovno preglejte načrte v primeru katastrofe

Napotek 39: Bodite pripravljeni pred napadom

Pripravljajte sezname in to veliko seznamov. Da bi bili pripravljeni na teroristični napad, boste morali oceniti vse svoje odzivne zmožnosti. V podporo tem prizadevanjem pripravite sezname naslednjega:

- odzivnih organizacij in njihovih podružnic - zveznih, državnih ali lokalnih; osebja v vsaki organizaciji in njihovih veščin, področij strokovnosti in stopnje usposobljenosti;
- podjetij, ki bi bila lahko vključena med prve odzivne enote, kot so bolnišnice in transportna ter telekomunikacijska podjetja;.
- opreme na vaši postaji in v drugih odzivnih enotah, kot so obleke, maske, orožje in vozila;
- denarja, ki je na voljo za podporo vašemu odzivu, vključno z možnimi viri dolgoročnega financiranja, kot so državne in zvezne subvencije domovinske varnosti (glej napotek 19);
- zaloge opreme in oskrbe;
- nujnih predmetov za opremljanje vaših policistov ob soočenju z izrednimi razmerami (kar zadeva tveganja, glej spodaj). Za to boste rabili strokovni nasvet. Začnite pri RAND bazi znanja za prve odzivne enote (glej napotek 38).

Spoznajte tveganja. Ko boste izpeljali raziskavo ranljivosti (napotki 28-30), boste dobro poznali tveganja, s katerimi se sooča vaša skupnost. Večji teroristični napadi so lahko različni: kemični, biološki, jedrski, visoko eksplozivni in tako naprej. Odvisno od vrste in lokacije napada se boste morda soočali s sekundarnimi tveganji; na primer, posebne lokacije morda vsebujejo proizvode, ki lahko pomenijo dodatno nevarnost, če jih poškoduje eksplozija, vročina, ogenj ali voda. Zato bi morali pripraviti seznam vseh tveganj v lokalnih podjetjih, proizvodnih obratih in skladiščih. Pri ocenjevanju ogroženosti, ki jih ta tveganja pomenijo, vključno s tem, ali so kateri kemični, biološki ali radiološki povzročitelji tako smrtonosni, da bodo nevarni prvim odzivnim enotam, boste najverjetneje rabili strokovno pomoč. Morda obstajajo načini, kako minimalizirati morebitna tveganja za prve odzivne enote in žrtve vključno z uporabo varovalne opreme za korozivne kemikalije ali uporabo protistrupov v primeru bioloških tveganj. Glede izvedljivosti in potrebe po nakupu tovrstnih materialov ter ob upoštevanju možnosti tveganja zaprosite za strokovni nasvet.

Narišite zemljevid. Ko boste zbrali vse ustrezne informacije, nadaljujte z drugo fazo upravljanja prvih odzivnih enot: analizirajte svoje možnosti. Na seznamih boste imeli ogromno količino informacij. Čas je, da te informacije pretvorite v obliko, ki vam bo pomagala oceniti svoje možnosti. Uporaben način za vizualizacijo možnosti je oblikovanje zemljevida, ki vključuje naslednje informacije:

- lokacije tveganj in njihovih stopenj toksičnosti in ranljivosti;
- lokacije potencialnih tarč in njihovih stopenj ranljivosti;
- lokacije odzivnih organizacij; če je vaša skupnost majhna, označite dejanska prebivališča osebja;
- razpoložljivost prostovoljcev, njihove stopnje strokovnosti in kako lahko z njimi vzpostavite zvezo;
- transportne poti, vključno s tistimi, po katerih bi se člani prvih odzivnih enot lahko peljali do potencialnih tarč;
- lokacije posebne opreme, ki jo bodo rabile prve odzivne enote;
- lokacije bolnišnic in drugih centrov za oskrbo, kamor se lahko odpelje žrtve;
- lokacije transportnih virov, kot so avtobusi in vlaki..

Na podlagi zemljevida boste lahko določili naslednje:

- preferenčne točke srečanja prvih odzivnih enot;
- preferenčne poti do posameznih tarč in od njih do centrov za oskrbo;
- poti za množično evakuacijo;
- problematične lokacije, ki za ublažitev posledic napada zahtevajo več pozornosti pred napadom;
- potencialne težave pri večkratnem prevozu članov odzivnih enot na prizorišče katastrofe in z njega.

Oblikujte odzivni načrt za izredne razmere. Za oblikovanje učinkovitega načrta boste morali sodelovati z večjimi odzivnimi organizacijami tako v svojem okolišu kot tudi v sosednjih. Opremljeni z informacijami, ki ste jih zbrali v prvih dveh fazah upravljalnega cikla odzivnih enot, oblikujte načrt za usklajevanje vseh različnih odzivnih skupin. To bo zahtevalo tesno sodelovanje z drugimi odzivnimi organizacijami, saj so pogosti sestanki pomembni za ustvarjanje zaupanja in določitev vlog ter odgovornosti vsake organizacije. Natančen načrt za odzivanje na napade bi moral vključevati naslednje:

- enoto za odziv na kritične dogodke (Critical Incident Response Team – CIRT); enota naj bi bila sestavljena iz predstavnikov prvih odzivnih organizacij, podjetij in javnih servisnih služb;
- sporazum med prvimi odzivnimi organizacijami glede vloge in odgovornosti, vključno s podrobnostmi o tem, kako bo uporabljena njihova specifična strokovnost in oprema;
- jasen opis poveljniške strukture v primeru večjega napada ali katastrofe, vključno z imenovanjem vsesplošnega poveljujočega častnika (glej napotek 44);
- časovnico dejavnosti v okviru pripravljenosti na katastrofo;
- načrt za aktiviranje prvih odzivnih enot v primeru napada;
- evakuacijski načrt, če je to potrebno;
- protokol, ki meri resnost katastrofe ali napada, tako da se lahko v skladu s stanjem prilagodi odziv. Kot je navedeno v napotku 37, niso vse katastrofe enake: število žrtev in obseg uničenja infrastrukture se od napada do napada razlikujeta. Na primer, morda ne boste potrebovali strokovnjakov za biološko vojskovanje, če bo neka lokacija napadena s konvencionalnim eksplozivom;
- kriterije za odločanje, ali in kdaj poklicati zvezno ali državno pomoč (nacionalno gardo, inženirski korpus ameriške vojske itd.) in opis, kako se bodo ti subjekti vključili v CIRT poveljniško strukturo;
- komunikacijski protokol, ki omogoča komunikacijo med okoliši in prvimi odzivnimi enotamii;
- urnik usposabljanja prvih odzivnih enot pred napadom in testiranje poveljniške strukture in komunikacije;
- določitev stikov in sklenitev uradnih sporazumov z zveznimi, državnimi in regionalnimi oblastmi, ki so morda potrebni zaradi pravnih ali operativnih postopkov;
- oceno oskrbe in storitev za spoprijemanje s katastrofo (npr. medicinska oskrba, objekti za izredne razmere); če oskrba ni na voljo takoj, načrt za pridobitev in transport tovrstnega materiala;
- načrt, da se članom prvih odzivnih enot omogoči, da poleg svojih uradnih dolžnosti poskrbijo tudi za svoje družine.

Veliko nadzora imate nad tem, kaj lahko naredite v fazi pred katastrofo. Če ste prizadevni, se bo delo, ki ga boste opravili v tej fazi, obrestovalo v naslednji, saj je **pridobivanje informacij in njihova pravilna razlaga zdaleč najtežji izziv, s katerim se spoprijema ekipa za upravljanje prvega odziva** ob soočenju s terorističnim napadom.

Napotek 40: Vlagajte v usposabljanje

Policijsko usposabljanje je nujno zlasti, ko se soočamo z moro obsežnega terorističnega napada. Vendar pa, preden sploh začnete razmišljati o protiterorističnemu usposabljanju, morate najprej vedeti, katera izobraževanja so vaši policisti že opravili v okviru rednih policijskih dolžnosti.

Osnovno usposabljanje. Vsi vaši policisti morajo biti izurjeni v zbiranju in upravljanju s podatki. Čeprav se nekaterim zdi upravljanje s podatki nepomembno za vsakodnevno policijsko delo, bi do zdaj že moralo biti popolnoma jasno, da vaša postaja ne more biti pripravljena na spoprijemanje s terorističnim napadom, ne da bi zbrala obsežno količino informacij o preprečevanju terorizma (tarče, teroristične priložnosti in tveganja) ter odzivu na terorizem (viri skupnostne podpore, oprema in oskrba).

Idealno bi bilo, če bi seminar zbiranja podatkov potekal na postaji, tako da bi ga neposredno povezali s sistemom, ki ga vaša postaja uporablja za zapisovanje dnevnih dogodkov, klicev na pomoč ter situacij in informacij, ki se nanašajo na preprečevanje in odziv na terorizem. Vsi policisti ne potrebujejo podrobnega usposabljanja za ocenjevanj ranljivosti, vsi pa morajo razumeti pomemben vpliv zbiranja podatkov na to, kako se bo vaša postaja odzvala na teroristični napad – in seveda na kakršnokoli vrsto kriminaitete ali nezakonitega vedenja. Usposabljanje na policijski postaji o postopkih in sistemih zbiranja podatkov je torej nujno. Čeprav bo to osnovno usposabljanje zadostovalo za večino vaših policistov, je prepoznavanje pomena zbiranja podatkov le prvi korak. Da bi v celoti izrabili svoje zbiranje obveščevalnih podatkov, morate imeti tudi posameznike, ki so izurjeni v analizi in razlagi informacij, tako da jih lahko uporabite pri občutljivih odločitvah. Za to boste rabili kriminalističnega analitika. Seminarji iz kriminalistične analize potekajo na številnih univerzah. Če tovrstnih tečaj na vašem območju ni, se pozanimajte na katedri za družbene vede ali oddelku za kazensko pravosodje svoje lokalne univerze in preverite, če so pripravljeni organizirati tak tečaj. Priročnik *Kriminalistična analiza za reševalce problemov v 60 kratkih korakih (Crime Analysis for Problem Solvers in 60 Small Steps)* bo izkušenim kriminalističnim analitikom pomagal nadgraditi znanje in njihovo vključevanje v vlogo ključnega člana ekipe za reševanje problemov.

http://www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=47.

Kako se lahko poleg omenjenega še prepričate, da bodo vaši policisti pripravljeni na vlogo sodelovanja v prvih odzivnih enotah ob terorističnem napadu? Za začetek se morate odločiti glede naslednjega:

- Katere teme bodo obravnavane?
- Kakšna bo oblika usposabljanja (predavanje, video posnetki, delavnice, terenske vaje)?
- Kateri policisti se bodo udeležili katerih seminarjev?
- Kdo bo izobraževal?
- Kako boste plačali usposabljanje?

Katere teme? Zvezna agencija za obvladovanje izrednih razmer (Federal Emergency Management Agency – FEMA, ki je zdaj del ministrstva za domovinsko varnost – DHS) nudi številne koristne spletne tečaje, najbolj ustrezni so navedeni v tabeli spodaj. Vsi vaši policisti bi se morali udeležiti uvodnih in splošnih tečajev; morda obstajajo tudi drugi, ki ustrezajo vašim posebnim potrebam ali odgovornostim. Jasno je, da bo širina tem odvisna od vaše vloge v strukturi Nacionalnega sistema obvladovanja napadov (National Incident Management System – NIMS; glej napotek 44 in stopnje, do katere boste vi in vaši policisti sodelovali v dejavnostih NIMS-a. Ni presenetljivo, da je najbolj priljubljen tečaj skladnosti z NIMS, ki je obvezen za vse postaje, ki prejemajo denar od DHS. Spletni tečaji so verjetno najbolj priročna alternativa, še posebej, če jih vaši policisti lahko opravljajo ob določenem času na računalnikih postaje. Potrdila o usposobljenosti izdajajo po opravljenem tečaju.

Vaje na podlagi scenarijev. Čeprav naj bi bile vaje, ki temeljijo na resničnih dogodkih, koristne, zahtevajo veliko časa in sredstev. Scenariji iz resničnega življenja, v katerih vaditelji uprizarjajo izredne razmere, na katere se odzivajo vse ustrezne agencije – zahtevajo veliko priprav in usklajevanja. Zahtevajo tudi izurjeno osebje ali svetovalce za razvoj scenarija in nadzor operacije. Osnovni scenariji lahko vključujejo naslednje:

- napad z umazano bombo na naseljeni lokaciji
- bombardiranje kemičnega obrata ali jedrske postavitve
- napad nakupovalnega centra s tovornjakom bomba
- izpust biološkega orožja v sistem podzemne železnice

Pri odločanju, ali boste potrošili sredstva za tovrstne vadbene operacije, morate razmisliti, kakšna je verjetnost, da se takšni napadi zgodijo na va-

šem območju. V pomoč so vam lahko merila, izpostavljena v napotkih 8 in 28-30. Čeprav lahko take operacije po nepotrebnem povečajo lokalne strahove, ni boljšega načina za zagotovitev, da so vse agencije za obvladovanje izrednih razmer pripravljene na napad. Take vaje so lahko zares edini zanesljivi način za odkrivanje napak in mrtvih točk v operacijah, kjer sodeluje več agencij in več okolišev. FEMA ponuja spletne tečaje usposabljanja na podlagi virtualnih ali simuliranih scenarijev, na katere se odzove osebje NIMS-a in drugih agencij.

Kdo bo usposabljal? Nekateri od vaših policistov so se morda že udeležiti usposabljanja za odzivanje v izrednih razmerah. Ti policisti so lahko pomemben vir in z nekaj dodatnega usposabljanja »treniraj trenerja«, bi lahko vodili usposabljanje na podlagi scenarija za ostale vaše policiste. Tečaji »treniraj trenerja« so na voljo na Inštitutu za obvladovanje izrednih razmer (Emergency Management Institute – EMI), na oddelku FEMA. EMI nudi tudi bolj intenzivno usposabljanje iz večine teh tem. In nazadnje, uporabite Skupnostno enoto za odziv v sili (Community Emergency Response Team – CERT), dostopno na https://www.citizencorps.gov/cert. Ta spletna stran ima programe v vsaki državi in na njej boste zvedeli, kako vzpostaviti lokalni CERT program.

Kdo plača? Spletni tečaji usposabljanja so brezplačni, potrebujete le računalnik in dobro internetno povezavo. EMI tečaji so tudi brezplačni, poleg tega nudijo tudi nekaj potovalnih štipendij. Odvisno od vaše lokacije in okoliščin vam morda za usposabljanje ne bo treba plačati. Največji strošek bo delovna sila, saj bo usposabljanje vzelo čas, ki bi ga vaši policisti sicer porabili za opravljanje rednih policijskih nalog. Da bi povečali učinkovitost takih operacij, poskušajte kombinirati ta specializirana usposabljanja z izobraževanjem, ki lahko pomaga vašim policistom pri izpolnjevanju njihovih rednih policijskih zadolžitev.

Izbor certificiranih FEMA tečajev, dostopnih prek spleta. Najnovejši seznam si oglejte na http://training.fema.gov/IS/crslist.asp.

Uvodni in splošni

- Obvladovanje izrednih razmer: umerjenost na položaj
- Uvod v sistem nezgodnega vodenja za kazenski pregon
- Osnove katastrof
- Uvod v nevarne materiale
- Živali in katastrofe: skupnostno načrtovanje
- Razvoj in upravljanje s prostovoljci
- Usmeritve za vaje skupnostnih katastrof
- Uvod v nepretrganost operacij
- Uvod v proces javne pomoči
- Načrtovanje ukrepov ob nepredvidljivih dogodkih v okviru posebnih prireditev za agencije javne varnosti

Obvladovanje izrednih razmer in katastrof

- Uvod v poveljniški sistem v primeru nezgod (angl. Incident Command System – ICS)
- Uvod v poveljniški sistem v primeru nezgod, 1-100, za osebje javnih del
- Nacionalni sistem obvladovanja nesreč (National Incident Management System – NIMS), uvod
- Nacionalni sistem obvladovanja nesreč (NIMS), Javni informacijski sistemi
- NIMS upravljanje z viri
- Uvod v blažitev razmer
- Nacionalni odzivni načrt (National Response Plan – NRP), uvod
- Posamezna sredstva začetnega ukrepanja
- Obvladovanje državnih katastrof
- Načela obvladovanja izrednih razmer
- Načrtovanje v izrednih razmer
- Načrtovanje v izrednih razmer z več tveganji za šole
- Uvod v ruševinske operacije
- Operacije javne pomoči

Posebne veščine

- Vodstvo in vpliv
- Odločanje in reševanje problemov
- Učinkovita komunikacija
- Izgradnja sodelovanja s lokalnimi vladami

Posebna področja

- Obvladovanje radioloških izrednih razmer
- Odziv na radiološke izredne razmere
- Usposabljanje za prevažanje v okviru odziva na radiološke izredne razmere
- Gradnja za jutrišnje potrese: izpolnjevanje izvršne odredbe 12699
- Živina in katastrofe
- Usklajevanje okoljskih in zgodovinskih varstvenih predpisov
- Predvidevanje nevarnega vremena & skupnostnih groženj
- Vloga operativnega centra v izrednih razmerah (angl. Emergency Operations Center – EOC) v skupnostnih dejavnostih pripravljenosti, odziva in obnove
- Principi inženirstva in vaje za stanovanjske strukture, ki so v nevarnosti ob poplavah
- Ravnanje z nevarnimi materiali za medicinsko osebje
- Uvod v obalne stanovanjske gradnje.

Napotek 41: Poznajte prizorišče katastrofe

Raziskave kažejo, da žrtve nenadnih katastrof na splošno ne zajame panika – in tudi če jih, je ta kratkotrajna. Na splošno žrtve poskušajo pomagati ena drugi. Kaos in panika, ki sta tako pogosto prikazana kot posledici katastrofe, sta v veliki meri stvaritvi medijev. Katastrofi običajno ne sledita takšno vsesplošno ropanje in brezzakonje, kot so poročali mediji v New Orleansu po pustošenju orkana Katrina. Dejstvo je, da si je velika večina ljudi v New Orleansu pomagala sama. In lahko bi rekli, da je vsaj nekaj začetnega kaosa in hrupa, ki je sledil orkanu (npr. dogajanje v louisianskem večnamenskem prostoru), prej povzročila nesposobnost državnih in lokalnih policistov kakor meščani sami.

Čeprav dokončne študije ni na voljo, ni videti, da bi stopnja kriminalitete v času večjih katastrof praviloma porasla. Dejansko obstajajo dobri razlogi za sodelovanje javnost na prizorišču katastrofe. Vendar pa pri odpravljanju posledicah katastrofe včasih pride do porasta nekaterih vrst goljufij (goljufije pri gradnji stanovanj, posojilne sleparije, zavarovalniške goljufije).

Preučimo postopek vzdrževanja prizorišča katastrofe s primeri ob napadih 11. septembra:

Pridobivanje informacij. Dogodki 11. septembra so bili skrajno zapleteni: dogajalo se je več stvari na več krajih in vsak je potekal v skladu s svojim lastnim časovnim razporedom. Kot je zaključila komisija 11/9, je h kaotičnosti operacij prvih odzivnih enot pripomoglo neuspešno: (a) pridobivanje točnih informacij; (b) interpretiranje podatkov; in (c) posredovanje informacij tistim, katerih vloga je bila obvladovanje prizorišča katastrofe. Za to je bilo več razlogov.

- Številne konkurenčne prve odzivne organizacije so neusklajeno posredovale informacije in izdajale neusklajene ukaze, vključno s Severnoameriškim letalskim in vesoljskim obrambnim poveljništvom (North American Aerospace Defense Command – NORAD), Zvezno letalsko administracijo (angl. Federal Aviation Administration – FAA) in njihovimi podružnicami, Zvezno protiteroristično projektno skupino (Federal counterterrorism task force), Tajno službo ZDA (U.S. Secret Service), različnimi vojaškimi oddelki, lokalno policijo, gasilci in nujnim medicinskim osebjem in različnimi zveznimi akterji ter vključno z uradom podpredsednika.

- Ekipe za izredne razmere ali načrt za obvladovanje napada niso bili pripravljeni – oziroma, če je načrt bil, se mu ni sledilo – čeprav so številni člani prvih odzivnih enot nedavno opravili urjenje za primer terorističnega napada, vključno s scenarijem na podlagi resničnega dogodka, v okviru katerega je komercialno letalo trčilo v zgradbo.
- Kompleksnost napada je bila preobremenjujoča. Ena od časovnic napada 11. septembra je vsebovala 425 ločenih komunikacijskih dogodkov – in to je zagotovo podcenjeno, če upoštevamo na tisoče klicev – verjetno javnosti - na številko 911.

Na lokalni ravni je nezmožnost jasnega in učinkovitega komuniciranja resno vplivala na aktivnosti na terenu, kot je razvidno iz tabele, ki povzema komunikacije, ki so v prvih 17 minutah napada na Svetovni trgovinski center vplivale na prve odzivne enote v New York Cityju.

Interpretacija informacij. Iz tabele je razvidno, da so 11. septembra prve odzivne enote skrajno težko razumele razsežnost katastrofe. To je morda največji izziv za prve odzivne skupine: ocena resnosti napada. Brez nekaj vedenja o resnosti katastrofe, bo za prve odzivne enote težka naloga učinkovito razporediti osebje in opremo ter oceniti stopnjo nevarnosti. Odzivni čas newyorške policijske postaje (New York City Police Department - NYPD) in newyorške gasilske postaje (Fire Department of New York - FDNY) na napad na Svetovni trgovinski center je bil izjemno kratek – nekaj članov osebja policijske postaje pristaniške oblasti (Port Authority Police Department - PAPD) je bilo že na prizorišču, ko je prišlo do napada. Vendar pa hiter prihod na prizorišče le malo koristi, če ni pravilne ocene narave katastrofe, obsega škode ter potrebnega števila reševalnega osebja. Potreben je triažni protokol, tako da ima ekipa za usmerjanje prvih odzivnih enot nekaj kriterijev za ovrednotenje informacij, ki jih prejme, in oblikovanje ocene resnosti dogodka.

Tako NYPD kot FDNY sta imeli dejansko različne stopnje alarmnega poziva, vendar sta se poziva izkazala za preveč splošna in še posebej v primeru FDNY se je to zaključilo z zbiranjem številnih članov osebja na prizorišču brez jasne predstave o tem, kako se učinkovito razporediti. Rezultat tega je bil, da so se zaradi slabe organiziranosti številni člani prvih odzivnih enot izčrpali ob vzpenjanju po stopnicah v stolpnici in so ostali ujeti, ko sta se stolpnici zrušili.

11/9 Časovnica prvih odzivnih enot na napad na Svetovni trgovinski center:
prvih 17 minut.

(Bilanca povzeta iz poročila komisije 11/9

Po dogodku je lahko navajati pomanjkljivosti. Natančna analiza prvih 17 minut napada poudarja napake v odzivu, ki jih je ugotovila komisija 11/9 in drugi. V celoti je bilo potrebnih le 17 minut, da so prve odzivne enote uvidele, da je šlo za reševalno akcijo in ne za gasilsko akcijo. Devetintrideset minut kasneje se je zrušila južna stolpnica, 29 minut za tem pa še severna stolpnica. Upoštevajte, da je Newyorški urad za obvladovanje izrednih razmer (New York City Office of Emergency Management – OEM) izvzet iz časovnice: igral je omejeno vlogo pri usmerjanju operacij, čeprav je usklajevanje prvih odzivnih agencij sestavni del njegove naloge. Na začetku je OEM klicala FEMA in zahtevala reševalne enote ter Večje bolnišnično združenje (Greater Hospital association). Usodno je bilo, da je bil njihov sedež v 23. nadstropju zgradbe Svetovnega trgovinskega centra.

Čas	Dogodek	Newyorška gasilska postaja	Newyorška policijska postaja	Policijska postaja pristaniške oblasti
8:46 dop. do 9:03 dop.	Letalo 11 je trčilo v severno stolpnico. 911 preplavijo klici; 911 operaterji svetujejo tistim, ki so se nahajali v severni stolpnici, naj ostanejo na mestu in počakajo na reševalce, kar je standardni operativni postopek. Večina tistih, ki so se nahajali v stolpnici, so začeli evakuacijo ne glede na navodila.	FDNY je prišla na prizorišče ob 8:52 dop. Dispečerji niso imeli informacij o lokaciji ali obsegu območja udara. Vodje FDNY v avli so določili, da morajo vsi zapustiti zgradbo. Ta informacija ni bila posredovanja operaterjem 911 ali razpečevalcem FDNY. Enotam je bilo ukazano, da se vzpnejo v stolpnico do območja udara. FDNY je sporočila, da se zgradba verjetno ne bo zrušila. Vodje so govorili z PAPD in OEM.	Ob 8:50 dop. je NYPD odposlala helikopterje za pregled škode. V skladu s standardnimi operativnimi postopki v helikopterjih ni bilo članov FDNY. NYPD je ugotovila, da reševanje s strehe ni možno. Informacije ni posredovala FDNY. Policisti NYPD so bili na prizorišču ob 9:00 dop.	PAPD sporočila FDNY, da je prek sistema javnega naslavljanja bil izdan ukaz za popolno evakuacijo, vendar da sistem ni popolnoma funkcionalen. Policisti PAPD na prizorišču so pomagali v reševalnih operacijah v nižjih nadstropjih, vendar vsi policisti niso imeli poveljniških radiev Svetovnega trgovinskega centra.

Čas	Dogodek	Newyorška gasilska postaja	Newyorška policijska postaja	Policijska postaja pristaniške oblasti
8:49 dop. do 8:57 dop.	Namestnik direktorja gasilcev v južni stolpnici je ljudi v stavbi obvestil, da je stavba varna in jih pozval, naj ostanejo v pisarnah.	FDNY je izdala ukaz za evakuacijo južne stolpnice. Bili so nezmožni slediti različnim reševalnim operacijam in razvrstitvi osebja.	NYPD je počistila večje prehode in v sodelovanju s PAPD evakuirala trg Svetovnega trgovinskega centra.	Ob 9:00 dop. je poveljujoči častnik PAPD ukazal evakuacijo vseh civilistov iz Svetovnega trgovinskega kompleksa.
9:03 dop.	Let 175 je trčil v južno stolpnico. Operaterji 911, preobremenjeni s klici, so ljudem v zgradbi naročili naj ostanejo na mestu.	FDNY analogni radii so slabo delovali, ker telefonski ojačevalec STC ni bil vključen.	NYPD je poslala manjše reševalne enote v stolpnici. Združene reševalne operacije NYPD in PAPD.	PAPD policisti so se odzvali posamezno; PAPD ni vedela, koliko policistov se je odzvalo ali kam gredo.

Napotek 42: Prevzemite nadzor – razumno

Ob soočenju s katastrofo ali terorističnim napadom je najpomembnejša naloga lokalne policije čisto preprosto vzdrževanje reda. Za obvladovanje prizorišča terorističnega napada bodo bolj verjetno poklicali policijo kakor katerokoli drugo odzivno agencijo za izredne razmere, preprosto zato, ker je tradicionalna vloga policije vzdrževanje reda. Kljub temu pa se je treba zavedati, da obstajajo tudi druge prve odzivne agencije, kot so nacionalna garda in različne vojaške enote (npr. Inženirski korpus ameriške vojske - U.S. Army Corps of Engineers), katerih naloge tudi vključujejo vzdrževanje reda; zato je pri oblikovanja načrta pripravljenosti na terorizem ali katastrofo bistveno določiti vlogo, ki jo ima vsaka agencija pri vzdrževanju družbenega reda. V času po orkanu Katrina je bila nezmožnost sodelovanja med policijo in vojaškimi organizacijam pri vzdrževanju reda na splošno videti kot resen zlom vodstva; v veliki meri se je za to obtoževalo lokalne policije. **Ker so lokalne policije pogosto prve, ki se jih obtožuje, bi morali zagotoviti, da boste pripravljeni** narediti naslednje:

1. **Upravljati vhode in izhode s prizorišča napada.** Ko se napad enkrat zgodi, bi morala biti ena vaših primernih nalog vzdrževanje prehodnosti večjih poti, tako da lahko reševalna vozila prihajajo in odhajajo s prizorišča in da se z območja katastrofe lahko evakuira žrtve. Tudi če je napad hitro zaključen, bodo njegovi najhujši učinki morda šele nastopili, kot se je zgodilo, ko se je zrušil Svetovni trgovinski center. Odgovornost za oceno, ali so take nevarnosti verjetne, ima navadno gasilska postaja ali mestni inženir.
2. **Vztrajajte pri policijski dejavnosti v skupnosti, kadar je ta najbolj potrebna.** Ko skupnost prizadene velika katastrofa, pričakujte, da boste naleteli na skoraj idealne razmere za skupnostno policijsko dejavnost. Eno od doslednih (in opogumljajočih) odkritij glede večjih katastrof je, da se žrtve v stiski povezujejo in so si vzajemno v podporo in tolažbo. Vaši policisti za delo v skupnosti lahko prevzamejo vodstvo pri usklajevanju teh prizadevanj in lahko pomagajo preprečevati državljanom, da bi vzeli zakon v svoje roke, kot se je zgodil po orkanu Andrew, kjer so ponekod izobesili obvestila »Če plenite, mi streljamo.«
3. **Bodite pozorni na sleparstvo.** Le nekaj dni po orkanu Andrew so prišli iz sosednjih lokacij na prizadeto območje brezvestni posamezniki, ki so ponujali svoje storitve in prodajali predmete, kot so generatorji in

led, po nezaslišanih cenah. Prevare v zvezi s storitvami in cenami so se izkazale kot velik kriminalni problem.

4. **Upravljajte informacije in dajajte točna navodila.** Posledica neustreznih informacij in slabe komunikacije v obeh stolpnicah Svetovnega trgovinskega centra med napadom 11. septembra so bila napačna evakuacijska navodila. Na srečo se je veliko tistih, ki so bili v stolpnicah, še posebej tistih v drugi stolpnici, samih odločilo, da zapustijo stavbi, zato je bilo veliko manj smrtnih žrtev, kot bi jih bilo sicer. Ključ do odpravljanja tovrstnih napak je učinkovita komunikacijska tehnologija in jasen sistem izmenjave informacij med štirimi vrstami prvih odzivnih agencij – policijo, gasilci, vojsko in zdravstvom – ki se običajno nahajajo na prizorišču katastrofe (glej napotek 46).
5. **Opozorite žrtve in potencialne žrtve.** Napovedovanje poti orkana je možno z znano stopnjo odstopanja (približno 300 km); čas njegovega prihoda pa je mogoče napovedati s še večjo natančnostjo. Napovedati natančno, kdaj ali kje se bo zgodil teroristični napad, je skrajno težko – in verjetno nemogoče – četudi je možno identificirati določene tarče, ki bodo bolj verjetno napadene. Dnevna stopnja ogroženosti, ki je bila ustanovljena po napadih 11. septembra, je zato skoraj nekoristna. Ker je presenečenje zaščitni znak vsakega terorističnega napada, bodo vsakršna nedoločena opozorila ali navodila, dana pred dejanskim napadom, verjetno povzročile le paniko. Če imate protokol (v okviru svoje načrtovalne faze), kateremu lahko sledite pri odločanju, katere okoliščine zahtevajo opozorilo in katera stopnja urgentnosti naj bi spremljala ta opozorila, bo vaše sprejemanje odločitev veliko lažje.
6. **Premikanje opreme in oskrbe.** Načrt odziva na teroristično katastrofo bo določil dobavitelje in poti za prevoz opreme, ki bo morda nujna za spoprijemanje z napadom kakor tudi oskrbo za potrebe prvih odzivnih enot in žrtev. Policija bo morala vzdrževati proste oskrbovalne poti, da pomanjkanje opreme ali oskrbe ne bi poslabšalo razmer. Poleg tega, če je ekipa za prvi odziv opravila svoje delo pravilno, bo dobavljena oskrba in oprema ključna za blažitev dolgoročnih poškodb tako žrtev kot tudi prvih odzivnih enot.
7. **Bodite prilagodljivi.** Kljub temu, da je treba načrtu odzivanja na katastrofe slediti, se zavedajte, da je to samo načrt in vsi vemo, da lahko še najbolje pripravljeni načrti zgrešijo smer. Ko je v visoki stavbi požar, je standardni postopek za tiste, ki so v zgradbi, da ostanejo na svojih mestih in počakajo navodila bodisi gasilcev, policije ali lastnih varnostih uslužbencev. Če bi vsi posamezniki v Svetovnem trgovinskem centru

naredili tako, bi le redki preživeli. Premislite: je bilo smiselno, da so se prve odzivne enote začele vzpenjati v stolpnice z namenom, da bi dosegle območje požara in ocenile škodo? To je bilo vsekakor junaško, vendar, gledano nazaj, se zdi tudi nepremišljeno – čeprav plezanje po stopnicah, da bi pomagali tistim, ki so bili potrebni pomoči, to ni. Veliko odločitev je bilo sprejetih na podlagi predpostavke, da se stolpnici ne bosta ali ne moreta zrušiti. Izkušnje s Svetovnim trgovinskim centrom kažejo, da se je težko prilagoditi novim okoliščinam med katastrofo, razen če obstaja nekdo, ki lahko naredi korak nazaj in poskuša razumeti celotno dogajanje. Prilagodimo se lahko samo, če je na voljo več možnosti, med katerimi se lahko odločimo. Informacije, ki so se nanašale na območje požara, so bile ključne; piloti helikopterjev NYPD so bili verjetno edini, ki bi lahko narediti tako oceno. Žal pa je bila očitno njihova osrednja naloga oceniti možnosti za reševanje s strehe. Niso imeli navodil, naj ocenijo resnost požara in med njimi ni bilo članov gasilske postaje, ki bi jim lahko pomagali.

Napotek 43: Blažite škodo, vendar se ne odzivajte pretirano

Postopek blaženja se začne v okviru faz pripravljenosti in pričakovanja. Bolj ko je skupnost pripravljena na teroristični napad, več možnosti ima za ublažitev nastale škode. Na primer, **boljša ko je zaščita privlačnih tarč, večje možnosti so za zmanjšanje učinkov napada.** Če so bili nameščeni pomožni generatorji in komunikacijska oprema, je mogoče minimalizirati sekundarne učinke napada. Če so bile prve odzivne enote dobro usposobljene in je bil pripravljen učinkovit načrt za izredne razmere, obstaja večja možnost za ublažitev škode, ki jo povzroči napad. Boljša komunikacija 11. septembra med prvimi odzivnimi enotami bi najverjetneje pomagala evakuirati še več posameznikov iz Dvojčkov. Nepovedana zgodba – verjetno največja uganka katastrofe Svetovnega trgovinskega centra – je, zakaj je bilo mrtvih sorazmerno malo ljudi, če upoštevamo zmedena in nasprotujoča si navodila, ki so prihajala v privih 17 minutah katastrofe. Prvotne ocene, ki so temeljile na znani zasedenosti stolpnic, so bile okoli 12.000 mrtvih. Kot smo omenili v prejšnjem napotku, bo razumno obvladovanje prizorišča katastrofe pomagalo ublažiti škodo, ker bo več možnosti za pobeg žrtev s kraja katastrofe in bo delavcem za izredne razmere omogočilo boljši dostop do prizorišča. Vseeno pa se je pri obvladovanju prizorišča katastrofe in njenih posledic mogoče odzvati tudi pretirano.

Ne odzovite se pretirano. Ob napadu 11. septembra je bil ves letalski promet prekinjen veliko prepozno, verjetno šele takrat, ko to ni bilo več potrebno, kar je prej prispevalo h krizi kot pa jo blažilo. Očitno ni bilo nikakršne ocene učinka, ki naj bi jih te dejavnosti imele na potnike ali letalsko panogo. Številni varnostni odzivi po napadu so kazali znamenja panike. Načelnika policije ali gasilcev lahko močno mika, da bi se na nek dogodek pretirano odzval, ker bo verjetno nosil odgovornost, če bi šlo kaj narobe; kljub temu lahko pretiran odziv povzroči paniko in poveča učinke terorističnega napada. Ko se zgodi kaj hudega, je najboljša obramba pred kritikami to, da lahko pokažete, da ste bili tako dobro pripravljeni, kot je bilo mogoče, da ste ravnali na sistematičen in racionalen način in da ste pridobili najboljši strokovni nasvet in mu sledili. Nekateri pretirani odzivi, do katerih je prišlo po napadu 11. septembra, so navedeni v tabeli.

Pretiran odziv?	
Incident	**Razmislek**
Benamarja Benatta, državljana Alžirije in muslimana, so 11/9 aretirali in pridržali v ameriškem zaporu več kot 3 leta »ne da bi (vlada) dejansko izvedla kakršnekoli sodni postopek zaradi kaznivega dejanja, za katerega je (bil) obtožen.« Zaprt je bil v strogo varovanih zaporih in kasneje oproščen vseh obtožb, ki sta jih sprožila FBI in INS. Na koncu so ga izpustili v Kanadi julija 2006, kjer je zaprosil za politični azil.	Prevelik poudarek na obveščevalnih podatkih kot sredstvu za uničenje domnevne teroristične mreže lahko vodi v pretirano vnete odzive. Primer Benatta je eden od številnih, ko posamezni deli kriminalističnega pravosodnega sistema – kazenski pregon, tožilstvo, agentje INS – določijo posameznike za krive na podlagi neustreznih ali nepopolnih informacij, ki temeljijo na predpostavki, da se lahko nadaljnje obremenilne informacije (to je izdaja imen sodelavcev) iz njih iztisne, ko bodo enkrat aretirani. V tem primeru so bili redki viri zapravljeni za neproduktivno nalogo.
17. oktobra 2001 so na podlagi prijave o sumljivem belem prahu v Južno osnovno in srednjo šolo poslali gasilske tovornjake, policijo in enoto za nevarne materiale Orange Cunty. Šolo so kasneje zaprli.	Je bilo to res potrebno? Ali ni v šoli, kjer se vsak dan uporablja bela kreda, pričakovati bel prah? Vendar, kaj če bi bil antraks? Če bi prve odzivne enote na lokalni ravni opravile raziskavo o vseh tveganjih in razvile načrt za odziv v izrednih razmerah, ki bi temeljil na oceni ranljivosti tarč in možnosti biološkega napada na šolo, bi se verjetno odzvali bolj zmerno.
12. avgusta 2005 se je odkritje sumljive naprave za čiščenje zob v zobozdravnikovi prtljagi zaključilo s triurnim zaprtjem regionalnega letališča za reaktivna letala Kinston v Severni Karolini.	Je imelo vodstvo letališke varnostne službe načrt za odzive na incidente? Čigava odgovornost je bil ukaz za zaprtje? So bila pred drastično odločitvijo, ki je vplivala na tisoče potnikov po celih Združenih državah, potrebna posvetovanja z drugimi enotami za prvi odziv? Na katerih informacijah je temeljila ta odločitev? Je načrt za odzive na kritične incidente vključeval različne stopnje odzivov na različne vrste napadov ali incidentov?
26. maja 2006 v Washingtonu, D.C., je policija, potem ko je neidentificiran klicatelj prijavil streljanje, za kratek čas zapečatila kongresno stavbo in sprožila preiskavo po nadstropjih največje strukture uradov v Capitol Hill. Po več kot 4 urah je policija ponovno odprla stavbo.	Je ekipa za odzive v izrednih razmerah imela načrt za odziv na bombne grožnje ali prijave drugih nasilnih izgredov? So prve odzivne enote ocenile vrsto prijave in izbrale primerno stopnjo odziva? Je bilo zaprtje potrebno? Če je bilo slišati strele, kaj so policisti med zaprtjem iskali?
16. novembra 2001 je bilo mednarodno letališče Hartsfield Atlanta štiri ure zaprto, kar je zelo vplivalo na promet po celih Združenih državah. Razlog? Mladenič je stekel v napačno smer skozi varnostno točko, potem ko je dobil pozabljeno torbico s fotoaparatom.	Na katerih predpostavkah je temeljila odločitev za zaprtje letališča? Se je upoštevalo druge učinke – posebej vpliv na druge potnike? So bile na voljo druge, manj nadležne izbire? Bi se lahko sklicevali na rek »Bolje varni, kot skesani«? To je bila navsezadnje najbolj varna odločitev, čeprav je zanemarila izgubo življenja potnikov – kar je ravno tisto, česar si teroristi želijo. So enote letališke varnosti pred kritičnimi dogodki imele načrt za oceno resnosti ali nevarnosti varnostnih kršitev?

Napotek 44: Vedite, kdo je vodilni: osvojite NIMS

Verjetno je najbolj pomemben sestavni del načrta za izredne razmere predstavljen v napotku 39, to je Odzivna enota za kritične incidente (Critical Incident Response Team – CIRT). Njena prva dolžnost je osnovati poveljniške strukture in načrtovati posebne vloge in naloge različnih prvih odzivnih agencij. Veliko je bilo že napisanega o strukturah poveljevanja v kriznih razmerah, večino tega pa vključuje Nacionalni sistem obvladovanja incidentov (National Incident Management System – NIMS). Model, ki je prikazan spodaj, se na široko uporablja po vseh Združenih državah, da bi se vzpostavil enoten in skupen pristop k prvemu posredovanju. NIMS je nastal v 1970. letih zaradi niza požarov, ki so zahtevali sodelovanje številnih agencij iz različnih okolišev. Gašenje požarov je bilo težavno iz več razlogov, in sicer zaradi:

- nejasne poveljniške strukture
- nesporazumov in slabe komunikacije
- odsotnosti usklajevanja vlog in dolžnosti
- pomanjkanja jasnega vodje
- tekmovanja za vire in njihovo pomanjkanje

Razumen način premagovanja teh težav je osnovanje jasno strukturiranega organizacijskega načrta, s čimer se zagotovi, da vsakdo ve, kdo naj bi kaj naredil. To je tisto, kar dela NIMS. Obstajajo številne različice načrta; najnovejšo verzijo, HPD5, je razvil DHS v poskusu, da bi vzpostavil določeno stopnjo poenotenja raznovrstnih agencij za pripravljenost na katastrofe. Odločiti se boste morali, (a) ali bi vi in vaši namestniki morali biti označeni v shemi in (b) ali bo načrt deloval ob morebitnem terorističnem napadu.

Kdo gre kam? Kje bi morali biti postavljeni vi in vaši namestniki v okviru NIMS sheme? Seveda bi si želeli, da bi imeli povsod nekoga, vendar bi to lahko presegalo meje vaše razpoložljive delovne sile. Lahko bi tudi zameglilo vaše vloge in obveznosti, ker bi bila vsaka drugačna, odvisno od vrste napada in drugih vpletenih agencij. Na primer, prav mogoče je, da med katastrofo različne agencije igrajo večje ali manjše vloge, zato načelniki teh agencij prevzemajo večje ali manjše vodilne obveznosti.

Poveljnik ali vodja? 11. septembra je štab za obvladovanje izrednih razmer župana Rudolpha Giulianija ostal v ozadju. Kolikor se da razbrati

iz poročila, Giuliani ni prevzel nadzora nad operacijo. Kljub temu pa se je tisti dan in dneve, ki so sledili, pokazal kot vodja mestnega odziva na napad. Znano je, da so Giulianijevi javni nastopi in dejanja pomagali ljudem razumeti obsežnost katastrofe ter jih soočiti z izgubami in motnjami v vsakdanjem življenju, ki jih je povzročil napad. Župan Giuliani je bil nedvomno vodja mestnega odziva, vendar ni bil operativni poveljnik, čeprav bi morda moral biti. Vsekakor lahko rečemo, da bi moral županov štab za obvladovanje izrednih razmer igrati pomembnejšo vlogo pri usklajevanju prvih odzivnih enot, čeprav je možno, da bi kakršnokoli povečano prizadevanje še vedno ovirala nezdružljiva komunikacijska tehnologija, ki so jo uporabljale različne agencije. Enoten operativni poveljnik bi lahko ublažil tekmovalnost in pomanjkanja usklajenosti med gasilsko in policijsko postajo, vendar glede na okoliščine na terenu, še posebej v prvih 17 minutah, je to malo verjetno. Težav, ki so ovirale reševanje, verjetno ne bi mogli preseči z enotnim poveljnikom. Je pa mogoče, da bi vsaj nekaj težav, ki so vzniknili tisti dan, lahko odkrili v okviru pripravljenostnega usposabljanja, ki bi ga morali izpeljati veliko prej preden se je zgodila katastrofa. Kakšno vlogo bi si vi želeli? Vodje? Poveljnika? Obe? Preden odgovorite, se zavedajte, da župan Giuliani brez podpore medijev ne bi mogel prevzeti vodstvene vloge.

Poveljniški štab. Načrt za izredne razmere bi moral vključevati poveljniški štab, primeren katastrofi, s katero se soočate. Na primer, če ni dokazov o kemičnem ali biološkem tveganju, ne bo potrebe po vključevanju posameznikov ali agencij, ki se spoprijemajo s tovrstnimi tveganji. Poleg mestnih agencij bi subjekti in oblasti, predstavljene v poveljniškem štabu, lahko vključevale:

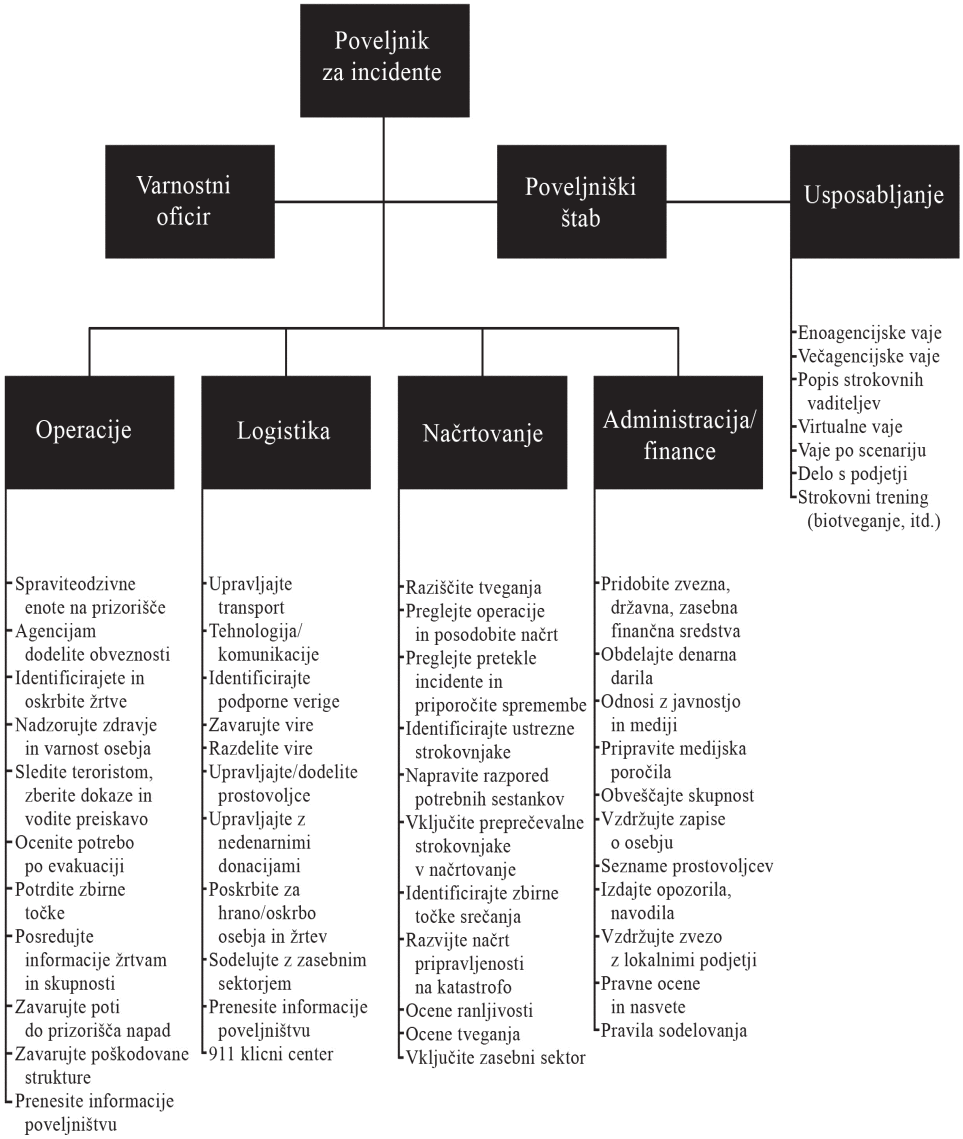
- poslovna združenja
- večja lokalna podjetja
- šolsko okrožje
- združenja bolnišnic
- združenja prostovoljcev
- strokovnjake za nevarne materiale
- osebje subjektov zasebnih varovanj
- prevozno osebje
- večje medijske skupine
- predstavnike domovinske varnosti
- telekomunikacijske in javne službe

Ni treba, da v vsako operacijo vključite vsakega od zgoraj omenjenih subjektov, vendar bi morali biti vsi vključeni v vaje usposabljanja. Ker obsežen poveljniški štab postane okoren, še posebej, če se je treba hitro odločati, bi številne subjekte z zgornjega seznama lahko obdržali na pozivu, če bi bila potreba po specifičnem znanju (na primer, lokacije električnega omrežja, podzemni plinski vodi itd.)

NIMS je rešitev na papirju. NIMS je organizacijska shema in samo to. Uporaben je pri razvoju vaj usposabljanja, ki posameznike učijo njihovih vlog in obveznosti. Čeprav bo ob soočenju s katastrofo včasih treba kršiti poveljniško strukturo, bi moralo usposabljanje razjasniti, da ima to lahko resne posledice še posebej za komunikacijo med številnimi prvimi odzivnimi agencijami. Med napadom se je treba hitro odločati, pogosto na podlagi površnih informacij. V prvih 17 minutah napada 11. septembra smo videli, kako težko so informacije potovale od vodje ene agencije do druge (glej napotek 41) in celo od enega predstojnika k drugemu v okviru iste postaje. Zato je treba dinamično spreminjati te upravljavske strukture v skladu z razmerami na terenu. Sprememba ne more biti učinkovita brez učinkovitega komunikacijskega sistema in tehnologije – ker je bistven del vsake poveljniške strukture zbiranje in pretok informacij s terena do poveljnika in spet nazaj. NIMS shema ne kaže potrebe po dinamičnosti za operativno učinkovitost. Kar potrebujemo, je razumevanje, kako in kje bi morale potekati informacije, kar neizbežno zareže našo organizacijsko shemo. To vprašanje sva naslovila v naslednjem napotku.

Več o tem: Jackson, Brian A. et. al., Protecting Emergency Responders, vol. 3, Safety Management in Disaster and Terrorism Response. RAND Corporation, 2004.

NIMS shema policijskega vodstva



Napotek 45: Vedite, da je informacija ključna

Čeprav organizacijska shema nacionalnega sistema obvladovanja nesreč (National Incident Management System – NIMS), predstavljena v prejšnjem napotku, nima puščic, ki bi kazale tok informacij, se v tovrstnih shemah navadno domneva, da informacije potekajo od zgoraj navzdol. To pomeni, da ukazi prihajajo od poveljnika in se po posrednikih prenašajo v prve vrste. Shema NIMS je v našem primeru bolj slika organov oblasti kakor načrt za reševanje problemov. Dejansko je največji problem v teh organizacijskih ureditvah poveljnik, saj lahko on ali ona brez ustreznih informacij izda napačen ukaz. Vsak učinkovit poveljniški sistem mora vsebovati načine zbiranja podatkov, njihove analize in način posredovanja tistim, ki odločajo, torej, poveljniku za nesreče. Da bi vzpostavili učinkovit tok informacij, morate v NIMS vključiti sistem upravljanja prvih odzivnih enot (First Responder Management System – FRMS) na naslednji način:

- identificirajte vse vire informacij na prizorišču katastrofe
- identificirajte načine nadzora toka informacij
- premagajte ovire učinkovitega pretoka informacij

Viri informacij. Prve odzivne enote na prizorišču katastrofe so potencialni vir informacij, toda ne smete misliti, da bodo te informacije dale točno in celotno sliko dogodkov na terenu. Prve odzivne enote, ki so se pognale v Dvojčka, niso natančno vedele, kakšno je dejansko prizorišče katastrofe. Njihova dejanja so bila omejena na pošiljanje ljudi na območje požara, da bi ocenili škodo. Piloti helikopterjev newyorške policijske postaje (NYPD) so imeli bolj natančne informacije o območju požara, vendar pa niso bili strokovno usposobljeni, da bi ocenili, kar so videli. Razpečevalcem klicnega centra 911 – katerih delo je bilo, teoretično, posredovanje napotkov klicateljem, kaj naj storijo – je primanjkovalo jasnih informacij o prizorišču katastrofe, zaradi česar so dajali nasprotujoče si nasvete in nezavedno pomagali širiti napačne informacije. Neposrednega pretoka informacij od klicnega centra 911 do policije in odzivnih gasilskih enot (glej shemo) ni bilo. Sistem 911 naj bi povečal odzivno učinkovitost na klice na pomoč; ironično je, da je med napadom na Svetovni trgovinski center zelo učinkovito pomagal širiti napačne informacije.

Potrebni so bili tudi strokovnjaki zunaj lokacije, da bi pomagali razlagati dogodke na prizorišču katastrofe. Se lahko stolpnici zrušita? Kakšni sistemi

so nameščeni za preprečevanje širjenja ognja? Gre za gasilsko operacijo ali reševalno operacijo? Ni znano, koliko časa so potrebovali med napadom 11. septembra za izsleditev ustreznih strokovnjakov. Kakorkoli že, nauk je jasen: informacije in strokovno znanje je treba zbirati preden pride do katastrofe.

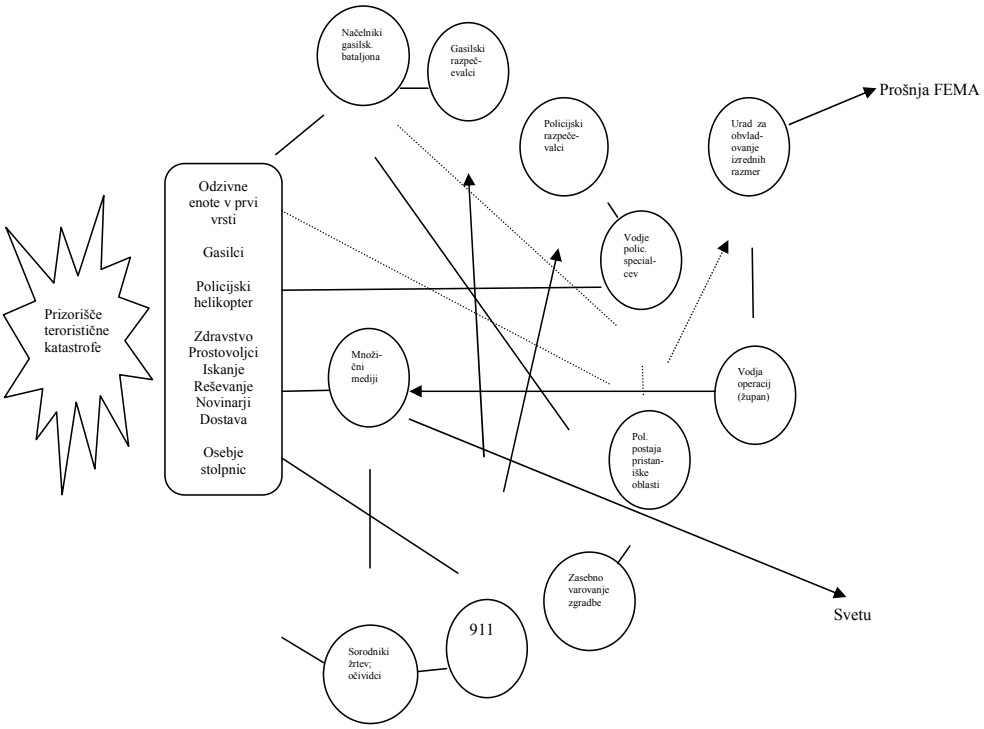
Nadzorujte tok informacij. Napredne komunikacijske tehnologije, kot so mobilni telefoni, okrepljen klicni center 911, različne radijske valovne tehnologije in radijski ter televizijski množični mediji, so povečale naše zmožnosti komuniciranja nad vsa pričakovanja. Težava, ki je neločljivo povezana s tem komunikacijskim obiljem, je dejstvo, da ni mogoče vedeti, ali je informacija resnična ali lažna. Zato večji centri za obvladovanje katastrof vzdržujejo tesne vezi z mediji: da bi se prepričali v točnost poročanja, da ne gra za pretiravanja glede razsežnosti katastrofe in da mediji ne povečujejo težav, s katerimi se soočajo prve odzivne enote. Pogosto je možno, da enota za obvladovanje katastrofe izrabi očitno medijsko strokovno poznavanje; na primer, med orkanom Katrina je večja televizijska mreža poročala o razmerah v New Orleansu bolj natančno in točneje, kot so to počeli zvezna agencija za obvladovanje izrednih razmer (Federal Emergency Management Agency – FEMA) in uradniki lokalnih oblasti.

Ob napadu na Svetovni trgovinski center so mediji igrali dodatno vlogo kanala, prek katerega je župan Giuliani pomirjal in spodbujal skupnost. Kot kaže potek na skici, je bila županova vloga v pretoku informacij primarno vezana na množične medije in sekundarno na newyorški urad za obvladovanje izrednih razmer (New York City Office of Emergency Management – OEM). OEM je bil ustanovljen več mesecev pred 11. septembrom ravno zato, da bi premagali komunikacijske in logistične težave, ki že po tradiciji obstajajo med različnimi mestnimi agencijami za odziv v izrednih razmerah, in je bil namenjen usklajevanju mestne odzivne operacije v primeru katastrof. To je bil NIMS v skladu s pravili. Vendar, kot je jasno pokazalo poročilo 11.9, sta NYPD in FDNY še naprej delovali kot neodvisni agenciji. (To je izpostavljeno v shemi). Med njimi ni bilo radijske zveze – in njihovi uporabniki so to tudi želeli. Prav tako ni nobena od agencij hotela biti podrejena OEM, ki je imel zelo majhno vlogo v okviru operacij. Zdi se, da je bila njegova edina funkcija prošnja FEMA za pomoč. Zato bodite previdni: NIMS je shema na papirju. In potreben bo trud, da bo medoperativnost delovala v praksi.

Upoštevajte, da je shema poenostavljena predstavitev toka informacij in komunikacij. Enajstega septembra so bili prisotni številni viri informacij;

posnetek smo omejili na prvih 17 minut napada na Svetovni trgovinski center. Kot je razvidno iz sheme, so bile neposredne povezave med klicnim centrom 911 in žrtvami ter agencijskimi razpečevalci ključne. Operaterji 911 so bili verjetno najpomembnejši vir informacij, ker so prejemali informacije od žrtev na prizorišču ter posredovali informacije žrtvam in naslednjim klicateljem. Lahko bi tudi posredovali te informacije poveljniškemu centru v izrednih razmerah – v tem primeru OEM – ki bi, če bi deloval pravilno, zbral informacije iz različnih virov in poskrbel, da bi se točne informacije posredovale vzdolž poveljniške verige (to je NYPD in FDNY) ter nazaj do klicnega centra 911. Shema razkriva tudi, kje ni bilo povezave med agencijami. Teh povezav ni bilo zaradi ovir, ki so informacijam ovirale pretok.

Tok informacij na prizorišču katastrofe prvih 17 minut, operacija 11/9 STC



* *Vse črte so dvosmerne, razen, če je drugače označeno*

* *Črtkane črte kažejo na sporadičen tok informacij zaradi slabe komunikacijske tehnologije.*

Napotek 46: Ustvarite medoperativnost

Premagajte ovire. Obstajata dve večji oviri za učinkovit pretok informacij: (1) sodobna tehnologija in (2) zastarelo mišljenje.

Postaje, ki morajo sodelovati, če se zgodi katastrofa, včasih izberejo konkurenčne in nezdružljive komunikacijske tehnologije. To je bila ena od številnih težav, s katero so se soočile prve odzivne enote v New York Cityu 11. septembra. Radijski sistemi NYPD in FDNY med seboj niso bili združljivi. Radijski sistemi FDNY so bili združljivi s komunikacijsko opremo, ki jo je uporabljalo osebje Dvojčkov, vendar le, če je bil telefonski ojačevalec znotraj Dvojčkov vključen – kar pa ni bil. Radijski sistemi policijske postaje pristaniške oblasti (PAPD) so bili tako slabe kakovosti, da so bili PAPD policisti komaj sposobni komunicirati s komerkoli. In čeprav so tisti v stolpnicah uspeli poklicati razpečevalce klicnega centra 911 in jim posredovati informacije s prizorišča, ti informacij niso poslali naprej do vseh razpečevalcev; zato večji del teh, življenjsko pomembnih opažanj s prizorišča, ni bil nikoli posredovan prvim odzivnim enotam.

Vprašanje je: Zakaj sta NYPD in FDNY nabavila nezdružljive radijske sisteme? Odgovor je - zaradi zastarelega mišljenja. Ti dve postaji imata dolgo zgodovino v medsebojni tekmovalnosti in zdi se verjetno, da sta imeli nezdružljivo tehnologijo zato, ker nista želeli govoriti ena z drugo. **Iz tega sledi, da se težav z ovirami pretoka informacij ne da rešiti zgolj s tehnologijo**. (Da ne boste mislili, da se to lahko zgodi le v New Yorku. Med bombnim napadom v londonski podzemeljski železnici, julija 2005, policijski radijski sistemi v podzemeljski železnici niso delovali, tako da pod zemljo policisti med seboj niso mogli komunicirati.) Poveljniški štab nacionalnega sistema obvladovanja incidentov (National Incident Management System – NIMS) bi to vprašanje moral obravnavati kot glavno in verjetno najbolj pomembno. Težave se ne da rešiti z napotki. Župan Giuliani je dolgo pred napadom na Svetovni trgovinski center izdal odredbo, s katero je zahteval sodelovanje med postajami; dejansko, je to usmeritev pospešil prvi napad na Svetovni trgovinski center kakih 8 let prej. Ne le to, Giuliani je ustanovil urad (OEM), katerega naloga je bila zagotavljanje medoperativnosti. Kot znamenje, da smo se nečesa naučili, bi bilo dobro, če bi zagotovili, da bodo imele vse postaje in agencije, ki bi se lahko v vaši skupnosti morda odzvale na napad, medoperativno komunikacijsko opremo.

Ustvarite mostove. Čeprav obstajajo številne tehnike, ki so lahko v pomoč pri razvoju učinkovitih medagencijskih odnosov, so verjetno najbolj pomembni pretekli odnosi med postajami, ki sestavljajo prve odzivne enote v vaši skupnosti.

1. Najdite svoje mesto. Kakšna je vaša vloga policijskega predstojnika pri pospeševanju tesnejših odnosov med agencijami? Imate avtoriteto? Razen če niste izbrani poveljnik NIMS, morda nimate moči za spodbujanje sodelovanja med konkurenčnimi postajami, vključno z vašo. V New York Cityju je župan – ki je na videz imel pooblastilo, da to naredi – poskušal vsiliti medoperativnost z vrha navzdol; jasno je, da je ta poskus spodletel.
2. Ne bodite v celoti odvisni od usposabljanja. Usposabljanje in vaje so zelo pomembne, vendar ne zmorejo vsega. Čeprav lahko izboljšajo specifične operativne veščine, bodo v majhno pomoč pri nevtralizaciji dolgoletne tekmovalnosti med postajami. Nobena usposabljanja ne bodo nevtralizirala naravnega antagonizma, ko dve postaji tekmujeta za ista proračunska sredstva. Gotovo je New York Cityjev OEM pred 11. 9 nadzoroval številna usposabljanja; vendar ta niso zadostovala za preseganje zgodovinske ali kulturne delitve in tekmovalnosti med postajami. Da bi presegli to tekmovalnost, morajo načelniki postaj spremeniti miselnost na policijskih postajah. Če naj bi sprememba trajala, ne sme biti vsiljena od zgoraj, čeprav lahko spreten župan oblikuje spodbude, ki bi načelnikom pomagale to izpeljati.
3. Poskusite z vzajemno pomočjo. Približno polovica posameznikov, ki delajo v okviru kazenskega pregona, pa tudi gasilci, reševalci, nujna medicinska pomoč in z njimi povezane službe, imajo drugo službo v podobni nujni odzivni agenciji. Najbolj resno prizadete so majhne gasilske postaje, ki so močno odvisne od prostovoljskih gasilcev. Številne policijske postaje prav tako doživljajo ta »sindrom dveh klobukov.« Poleg tega so številni člani osebja javne varnosti in osebja za nujno pomoč tudi člani Nacionalne garde; če številne službe pokličejo naenkrat, se bazen razpoložljive delovne sile za odziv v primeru katastrofe drastično zmanjša. Jasno je, da je to bolj zaskrbljujoče v majhnih mestih in vaseh kakor v gosto naseljenih mestih, kot sta Chicago in Los Angeles. Za majne postaje sosednjih mestnih občin je smiselno sprejeti formalni sporazum, v skladu s katerim se vsaka strinja, da bo v primeru izredne zahteve po delovni sili ali drugih sredstvih postaje ob terorističnem napadu ali naravni katastrofi pomagala drugi. Ob priznavanju izrednih izzivov, s

katerimi se lahko sooča majhen ali podeželski okoliš, ministrstvo za domovinsko varnost spodbuja prve odzivne enote na takih območjih, da izpolnijo skupne prijave za subvencije domovinske varnosti. Vodite tudi popis opreme in sredstev v sosednjih okoliših, tako da enota za odziv na kritične dogodke (Critical Incident Response Team – CIRT) natančno ve, katera sredstva so na voljo, kje se nahajajo ter ali kateri nujni materiali niso na razpolago oziroma so zastareli.

4. Spodbujajte partnerstva. Če so številni vaši policisti v Nacionalni gardi, bi bilo lahko koristno z Gardo sprejeti vzajemni paket pomoči, ki bi se nanašal na objekte za usposabljanje, vaje in opremo. Javna in zasebna partnerstva so lahko pomembna tudi pri razvijanju učinkovite odzivne strategije, ker so podjetja pogosto primarne ali stranske tarče terorističnih napadov. Vzdržujte stike z lastniki in stanovalci možnih tarč in imejte njihove kontaktne podatke pri roki. Poleg tega imajo zasebna podjetja pomembna sredstva, ki se jih lahko uporabi ob katastrofi, kot so komunikacijska oprema, živila, ležišča in prevozna sredstva. Morda imajo tudi dostop do specializirane opreme, kot je material za rušenje, oprema za gradnjo in tako naprej.

Več o tem: Hawkins, Dan M. Law Enforcement Tech Guide for Communications Interoperability: A Guide for Interagency Communications Projects. Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services, 2006. http://www.cops.usdoj.gov/RIC/ResourcesDetail.aspx?RID=238

NAPOTEK 47: **Po napadu ne prenehajte z dejavnostjo**

Obvladovanje prostovoljcev. Ena od vaših težav po napadu bo spoprijemaje s številnimi ponudbami za pomoč. Pričakujte dotok prostovoljcev, vendar bodite previdni, ker bo med številnimi iskrenimi ponudbami brez dvoma nekaj takih, ki ne bodo povsem dobronamerne. Če je vaš okoliš majhen, bo dejstvo, da osebno poznate številne njegove člane, zmanjšalo to težavo. V večjih okoliših pa boste morali v sodelovanju z agencijami, ki vodijo javne evidence, oblikovati sistem vodenja evidence pretoka oseb na in iz območja katastrofe. To bi moralo biti narejeno pred napadom kot del vašega načrta pripravljenosti. Poleg tega je možno, da se bodo nekateri prostovoljci preprosto pojavili, ne da bi vedeli, kam iti, kako pomagati ali kako se česa lotiti. Najlažja rešitev bi verjetno bila usmeritev neizurjenih prostovoljcev k organizacijam, kot je Rdeči križ. Dejansko lahko te organizacije uporabite kot del svojega načrta pripravljenosti. Rdeči križ, na primer, je razvil vrsto tečajev, vključno z nekaj spletnimi, za izobraževanje ljudi o tem, kako delovati prostovoljno po katastrofi (http://www.redcross.org). Nekatere cerkvene organizacije so uvedle podobne izobraževalne tečaje za prostovoljce v primeru katastrofe. Vaša lastna logistična ekipa bi morala opraviti takšne tečaje, tako da bo pripravljena uporabiti prostovoljce in njihovo znanje. Poleg tega se prepričajte, da druge prostovoljske organizacije v vaši skupnosti poznajo možnosti za usposabljanje prostovoljcev.

Najbolj pomembni prostovoljci so zdravstveni delavci. Po napadu 11. septembra v New York Cityu so se številni zdravniki in medicinske sestre preprosto pojavili v območnih bolnišnicah in ponudili svojo pomoč, čeprav številnih niso mogli sprejeti, ker njihovih strokovnih potrdil ni bilo mogoče preveriti. To je zapleten problem, ki vključuje številna pravna in tehnična vprašanja. Na srečo je leta 2002 kongres odobril razvoj Sistema za predhodno registracijo prostovoljnih zdravstvenih strokovnjakov za izredne razmere (Emergency System for the Advanced Registration of Volunteer Health Professionals). Kot del načrtovanja odziva na izredne razmere zagotovite, da bodo lokalne bolnišnice in klinike obveščene o postopku predhodne registracije zdravstvenih delavcev, tako da bodo lahko sprejele prostovoljne zdravstvene strokovnjake, če pride do katastrofe. Za več informacij obiščite spletno stran Administracije zdravstvenih sredstev in storitev (Health Resources and Human Services Administration) http://www.hrsa.gov/esarvhp.

Ocena posledice napada. Po napadu je pomembno, da z zbiranjem in analiziranjem koristnih informacij ocenite škodo in poškodbe, ki jih je utr-

pela vaša skupnost. Brez teh informacij se ni mogoče lotiti obnovitvenega načrta. Informacije v zvezi s tveganji in ranljivostjo, ki ste jih zbrali pred napadom, bodo na tej stopnji zelo uporabne. So se tveganja in ranljivost z napadom povečali? Kateri pomembni objekti so bili prizadeti? Strokovnjaki bodo morali oceniti prizorišče napada in njegovo okolico, da bi ugotovili, ali je napad povzročil nova tveganja in, če je tako, kakšne kratkoročne in dolgoročne zdravstvene posledice bi lahko imela ta tveganja. Na primer, ogromna količina prahu, ki se je dvignila ob napadu na Svetovni trgovinski center, je vsebovala najrazličnejše strupene snovi, vključno s svincem, živim srebrom ter azbestom, kar je povzročilo izčrpavajoče in kronične bolezni, ki zahtevajo dolgotrajno zdravljenje in onemogočajo, da bi posamezniki delali in skrbeli za svoje družine. Tabela kratko povzema dejanske ekonomske in druge učinke napada na Svetovni trgovinski center.

Škoda in poškodbe, ki so posledica napada na Svetovni trgovinski center

Mrtvih ljudi	
Skupaj	pribl. 2.750
Gasilci in bolničarji	343
Policisti NYPD	23
Policisti PAPD	37
Osebne izgube	
Osebe, ki so v napadu izgubile zakonca ali partnerja	1.609
Otroci, ki so izgubili starša	3.051
Poslovne izgube	
Podjetja v STC, ki so izgubila uslužbence	60
Ekonomska izguba za New York v mesecu po napadu	$105 milijard
Izguba delovnih mest v New Yorku zaradi napada	146.100
Dnevi, kolikor je bila zaprta Newyorška borza	6
Škoda	
Uničena vozila FDNY	98
Ton ruševin, odpeljanih s prizorišča	1.506,124
Ocenjena cena čiščenja	$600 milijard
Pomoč	
Enot darovane krvi Krvnemu centru New Yorka	36.000
Enot darovane krvi, ki se jih je dejansko uporabilo	258
Vsota, darovana dobrodelnim ustanovam 11/9	$1.4 milijarde
Zbran denar za družine NYPD in FDNY	$500 milijard
Skupaj denar, ki ga je porabila FEMA za izredno stanje	$970 milijard

Vir: prilagojeno po »9/11 by the numbers,« New York Magazine.
http://www.newyorkmetro.com/news/articles/wtc/1year/numbers.htm

Pripravite se na zagovor svojega odziva. Prehod od blažitve škode na prizorišču katastrofe do daljšega procesa obnove zahteva vztrajnost in vzdržljivost. Ne le, da se boste morali spoprijeti s samimi učinki katastrofe, temveč ta prehod skoraj vedno spremlja boleče ocenjevanje katastrofe in dela prvih odzivnih agencij. Kaj je šlo narobe? Kaj je bilo prav? Kdo je kriv? Čigave so zasluge? Odgovori na ta vprašanja ne bodo zahtevali le ocene tega, kako so se odzvali vaši policisti na prizorišču katastrofe, temveč tudi priprav, ki jih je vaša postaja izvedla v pričakovanju terorističnega napada.

Brez dvoma boste odgovorni za delovanje svoje postaje in policistov. Če ste sledili korakom v priročniku, boste imeli veliko informacij, na katerih bo temeljil pregled, ker boste sposobni dokazati, da ste izpeljali naslednjih 10 ukrepov:

1. Sistematično ocenili teroristično ogroženost svoje skupnosti
2. Sprejeli potrebne ukrepe za zaščito verjetnih tarč v skupnosti.
3. Najeli strokovnjake za podporo, ko ste potrebovali pomoč.
4. Poskrbeli za potrebno usposabljanje policistov.
5. Tesno sodelovali z odzivnimi enotami za izredne razmere
6. Polno sodelovali v vajah usposabljanja.
7. Delili vire z drugimi agencijami.
8. Zagotovili medoperativnost z drugimi agencijami in okoliši.
9. Pripravili predloge za subvencije domovinske varnosti.
10. Zavarovali zdravje in varnost svojih policistov na prizorišču katastrofe.

Učinkovitost teh desetih točk bo odvisna od stopnje, do katere ste izpeljali cikel obvladovanja teroristične katastrofe. Z zbiranjem podatkov o rednih policijskih dejavnostih (podrobnosti o kriminalnih dogodkih, o klicih na pomoč in z opisi težav s ponavljajočimi se nezakonitostmi; s popisi ranljivih tarč, opisi tveganj in pomoči prebivalstvu v nevarnosti; o razvrstitvi in usposabljanjem policistov; nabavi opreme in oskrbe) z vsem tem boste imeli pri roki potrebne dokaze, da je vaša postaja naredila vse, kar je bilo mogoče za preprečitev in ublažitev napada. Seveda boste delali napake, še posebej ob kaosu, do katerega pride v prvih trenutkih katastrofalnega napada. In dejansko bi moral ponoven pregled razkriti te napake, tako da se lahko iz njih učite. Če lahko dokažete, da je vaša postaja naredila vse, kar je bilo mogoče, boste lažje priznali napake in drugi vam bodo zanje lažje oprostili.

Napotek 48: Vzdržujte obnovo

Pravijo, da čas zdravi vse rane. Do mere, da pozabimo strašne dogodke iz preteklosti, je to morda res. Ponovna graditev ali obnova prizorišča katastrofe nam pomagata preboleti travmo ter nam obenem pomagata pozabiti. Številne žrtve – družine, ki so izgubile ljubljene osebe, in tisti, ki morajo živeti s poškodbami – ne morejo pozabiti, ker morajo s posledicami katastrofe živeti vsak dan svojega življenja. Občutna sprememba, ki se zgodi po napadu ali kateri drugi katastrofi, je prehod iz blaženja škode na prizorišču k trajnostnemu dolgoročnemu okrevanju. Časovnica tega prehoda se bo spreminjala z naravo dogodka. Tabela kaže čas obnove področja v izmeri 2 km2, ki jo je uničil manjši ciklon. Kot je razvidno, se je prehod od ublažitve do obnove zgodil med 4. in 5. dnem po dogodku. Časovnica prehoda bo odvisna od vrste katastrofe. V primeru napada na Svetovni trgovinski center se je časovnica razpotegnila na dni, mesece in leta: na prizorišču je gorelo še 99 dni po napadu; čistilne ekipe so odstranjevale ruševine več mesecev. Večji del tega dela je bilo treba opraviti v ruševinah in strupenem prahu. Čeprav je bilo prizorišče manjše od 1 kvadratne 2 km2, ki jo je prizadela spodaj opisana ciklonska katastrofa, je bilo očitno prizorišče Svetovnega trgovinskega centra veliko bolj zgoščeno.

NIMS in trajnostna obnova. Naloga poveljniškega štaba nacionalnega sistema obvladovanja nesreč (National Incident Management System – NIMS) in njegovih podrejenih teles je organizirati pomoč s pozivi zveznim, državnim in lokalnim vladnim agencijam. Kakšna skupnostna pomoč je na voljo? Kakšno finančno podporo rabijo družine? Posebnega pomena bo skrb za dobrobit policistov, ki so služili v privih odzivnih enotah bodisi kot člani postaje ali kot policisti za zvezo z drugimi agencijami. Dolgoročni učinki napada na vaše policiste in njihove družine bodo morda eden od najtežje obvladljivih vidikov.

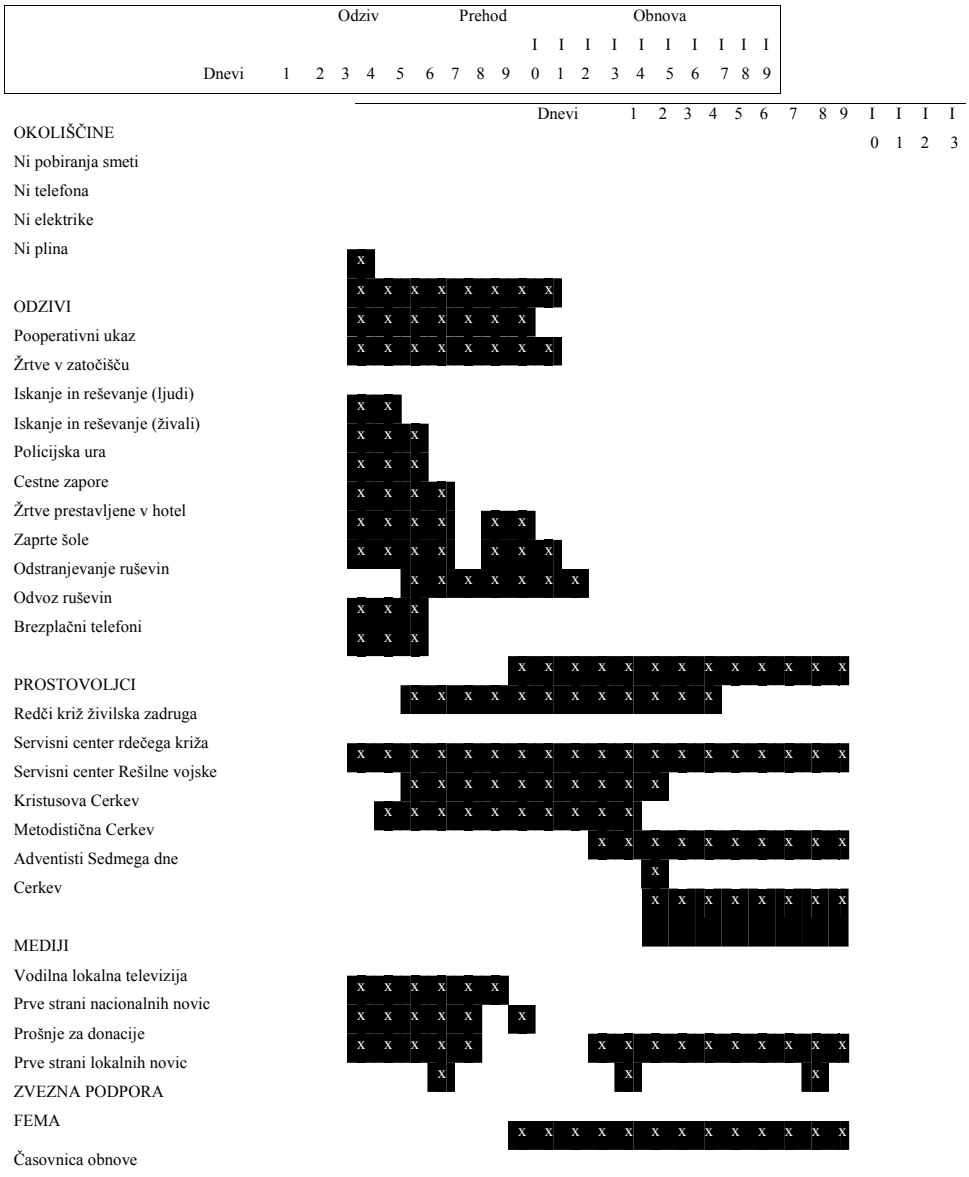
Odvisno od vaše vloge v poveljniški organizaciji NIMS se boste morda želeli sami polno vključiti v dejavnosti, ki so namenjene celostni obnovi. Predvsem boste morali narediti naslednje:

1. Po zaključeni notranji reviziji dela vaše postaje (glej napotek 47), sodelujte pri revizijah drugih agencij in pripravite poakcijsko poročilo.
2. Identificirajte potrebe vaše in drugih agencij v luči katastrofe in njenih posledic. Posebno pozornost namenite zdravju in dobrobiti vaših poli-

cistov, obnovi zalog in opreme ter ugotavljanju usposabljanj in opreme, ki je manjkala.
3. Primerjajte napake med operacijami in poiščite načine za njihovo odpravo, vključno z izboljšanjem usposabljanja.
4. Pripravite načrt za dolgoročno spremljanje zdravja in dobrobiti vaših policistov, tistih iz drugih agencij in ostalih žrtev katastrofe.
5. Povežite se z drugimi agencijami pri iskanju zunanje finančne pomoči za žrtve
6. Prek partnerstev, ki ste jih vzpostavili kot del pripravljenosti na katastrofo, zadolžite trgovski sektor pri zbiranju finančne podpore za zagotovitev dolgotrajnega celostnega procesa obnove.
7. Uporabite svoje zveze s podjetji za pospešitev ekonomske sanacije področji, ki jih je prizadela katastrofa.

Spreminjajoča se vloga policije. Ob velikem napadu se bo vsaka policijska postaja soočila z velikimi neposrednimi zahtevami, vendar pa je obvladovanje stalnih sprememb, ki sledijo napadu, lahko enako zahtevno. Ob katastrofi Svetovnega trgovinskega centra so policijo poklicali k iskanju in reševanju ponesrečencev in žrtev. V času blaženja posledic napada je policija usmerjala promet, upravljala s cestnimi zaporami in nadzorovala varnost v tunelih in na mostovih. Spet drugi so popisovali in razvrščali dele teles, ki so jih našli na prizorišču - delo, ki je trajalo več mesecev. Naknadni učinki napada so bili tako siloviti, da so zahtevali trajno prerazporeditev številnih policistov. Promet v središču Manhattna je bil spremenjen zaradi čiščenja, gradnje in ogledov. Razvrstitev policije za vzdrževanje nadzora nad možnimi tarčami (mostovi, tuneli, podzemnimi železnicami, železniškimi postajami, itd.) je verjetno za vedno spremenila način delovanja newyorške policijske postaje. Za Svetovni trgovinski center se faza obnove nadaljuje in se bo nadaljevala, dokler ne bo postavljen nov Svetovni trgovinski center.

Spreminjajoči se obrazi kriminala. Kot je bilo že omenjeno, neposredno po večji katastrofi se ljudje povežejo in drug drugemu pomagajo premagovati težave, s katerimi se soočajo. Odvisno od narave katastrofe bodo nastopile nove priložnosti za kriminalce, kot so prevare izvajalcev različnih del, cenovne prevare, zavarovalniške goljufije in goljufije z javno pomočjo. Ena od najresnejših težav, ki se lahko pojavi po katastrofi, je uničenje tako zasebnih kot tudi javnih evidenc. Ko se to zgodi, je odstranjena pomembna ovira za izvajanje goljufij in številnih drugih vrst kriminala.



Vir: Prirejen po Neal, David M. Transition from Response to Recovery: A Look at the Lancaster, Texas Tornado. Quick Response Report #79. Denton, Texas: University of North Texas, 1995. http://www.colorado.edu/hazards/qr/qr79.html

Napotek 49: Obveščajte javnost

O prometni nesreči, ki povzroči smrtne žrtve in resne poškodbe, bo zagotovo poročala lokalna televizija, vendar imata policija in osebje za nujne primere običajno čas, da se spoprimeta z nesrečo pred prihodom medijev. Pri večjih katastrofah in terorističnih napadih je precej drugače: mediji pridejo pogosto na prizorišče ob istem času kot prve odzivne enote. Ob soočenju z orkanom Katrina in napadu 11. septembra so mediji igrali pomembno vlogo pri posredovanju informacij o prizorišču katastrof. Odvisno od vaše vloge v okviru poveljniške strukture nacionalnega sistema obvladovanja nesreč (National Incident Management System – NIMS), boste morda zadolženi za odnose z mediji in javnostmi. Skrbno obvladovanje in komunikacija z mediji in javnostmi je bistvena, da ne bi poleg teroristične katastrofe prišlo še do medijske katastrofe.

Pred napadom

Pomagajte medijem povedati svojo zgodbo. Javnosti lahko veliko poveste o prizadevanjih za pripravo ocene ranljivosti in o razvoju sodelovanja, ki viša stopnjo varnosti. Seveda morate biti previdni pri posredovanju podrobnosti o ukrepih za zavarovanje najbolj verjetnih tarč. Čeprav nočete, da bi teroristi izvedeli za specifične podatke o preprečevalnih dejavnostih, ki ste jih izvedli, bi si morali prizadevati, da izvejo, da ste ukrepali tako, da boste otežili njihovo delo, kar jih bo morda odvrnilo od napada v vašem mesu. Poleg tega, več ko javnost ve o zaščitnih ukrepih, bolj boste obvarovani pred obtožbami po napadu.

Vključite predstavnike medijev v NIMS načrtovanje. Medije pritegnite k sodelovanju čim bolj zgodaj in jim dodelite vlogo v okviru NIMS načrtovanja. S tem, da si priskrbite nekaj nadzora nad informacijami, ki jih mediji posredujejo javnosti, se boste izognili napačnim predstavam in nesporazumom glede tega, kaj si prizadeva doseči NIMS. To lahko dosežete z vključitvijo medijev v delo NIMS-a.

Določite uradnika za javno informiranje. Določitev uradnika za javno informiranje in zagotovitev, da ima uradnik tesen, pozitiven odnos z mediji, vam bo omogočilo preprečiti negativno publiciteto. Na primer, 28. avgusta 1992, komaj 6 dni po orkanu Andrew, je zgodba v *Miami Heraldu*

z naslovom »Preobremenjeni metropolicisti (metropolitanski policisti op. prev) obravnavajo le nujne primere« bralcem svetovala: »So vam v času, ko vas ni bilo doma, vlomili v hišo? Ne kličite metropolitanske policije okrožja Dade. Ne morejo priti.« Čeprav je za medije pomembno, da prenašajo informacije javnosti – celo informacije o tem, da so policija in vsi ostali preobremenjena z operacijami iskanja in reševanja – bo pozitiven odnos z mediji zagotovil, da bodo informacije posredovane na pošten in uravnotežen način.

Vzpostavite prostovoljsko komunikacijsko mrežo. Prostovoljska komunikacijska mreža lahko učinkovito sporoča informacije lokalnim skupnostnim organizacijam in prostovoljcem. Radioamaterji so imeli pomembno vlogo pri obvladovanju številnih katastrof. Cerkvene skupine in druge prostovoljske organizacije imajo pogosto komunikacijske mreže, ki lahko dosežejo posameznike, za katere vi ne veste, kot so bolni, starejši in invalidi. Bolj kot zaradi zagotovil in podpore, boste morali poiskati te posameznike zaradi morebitne potrebe po evakuaciji.

Postavite spletno stran policijske postaje. Množični mediji so močno navzoči v katastrofi, vendar splet kot pomemben vir informacij prehiteva tradicionalne medije. Če tega še niste storili, ustvarite spletno stran in z njo ravnaje kot z izložbo svoje postaje. Ustanovite posebno sekcijo za terorizem in pripravljenost na katastrofe ter vključite nasvete o tem, kako se pripraviti na katastrofo in kaj narediti, ko do nje pride. Poleg tega opišite korake, ki jih bo naredila vaša postaja v primeru katastrofe, vse do in vključno s kriteriji, ki bodo uporabljeni pri ocenjevanju potrebe po evakuaciji. Kot enega izmed odličnih primerov si oglejte spletno stran policijske postaje Sacramenta, ki omogoča prenos publikacije *Ste pripravljeni?* regijskega sveta meščanskega korpusa Sacramenta (Sacramento Region Citizen Corps Council) (na voljo v sedmih jezikih). Druga pomembna zadeva so odgovori na pogosto zastavljana vprašanja (PZV), ki se nanašajo na to, kaj bi se lahko zgodilo v primeru terorističnega napada. Tabela kaže PZV spletne strani policijske postaje mesta Mountain View (Kalifornija). Kot najboljši primer lahko vaša spletna stran služi dvojnemu cilju: lahko vam pomaga pri odzivu na terorizem in lahko služi kot pomoč pri rednem delu vaše postaje.

PZV o terorizmu spletne strani policijske postaje Mountain View, Kalifornija	
Kaj lahko pričakujem od policijskih in gasilskih postaj v primeru katastrofe?	Kaj je antraks?
Kako se lahko pripravim na katastrofo?	Kaj naj naredim, če prejmem pismo z belo, prahu podobno snovjo?
Kako bom obveščen o katastrofi?	Kaj so koze?
Kaj naj naredim, če se zgodi katastrofa?	Kako nalezljive so koze in kako se zdravijo?
Kaj naj naredim, če opazim sumljivo vedenje v svoji soseščini?	Se lahko moji otroci ali jaz cepimo proti kozam?
Kako naj se izognem središču terorističnega dejanja?	Me bo zapečatenje oken z lepilnim trakom in plastičnimi ponjavami pomagalo zaščititi pred napadi bioterorizma?
Kaj lahko naredim glede stresa, ki ga čutim? In kako naj to razložim svojim otrokom?	Naj kupim plinsko masko?
Koliko je verjetno, da se bo teroristično dejanje zgodilo v Mountain View?	
Kako lahko pomagam svoji skupnosti, če se zgodi napad?	Več informacij/koristne povezave

Med napadom naredite naslednje.

1. Prek uradnika za javno obveščanje zagotovite, da bodo mediji pripravljeni pomagati čim prej.
2. Zagotovite, da bodo informacije, ki jih posredujete javnosti, v skladu s tem, kar poročajo mediji.
3. Vključite podporo medijev pri izdajanju opozoril in ukazov za evakuacijo.
4. Izrabite medije za komunikacijo s prostovoljci in za nadzorovanje prošenj za pomoč, opremo in donacije.
5. V okviru poveljniškega štaba določite posameznika, ki se spozna na medije in bo medijem dajal sporočila za javnost ter intervjuje.
6. Zagotovite, da bo vaša spletna stran nenehno posodobljena in bo poročala o spremembah razmer in dajala nova navodila za prebivalce.
7. Zagotovite posredovanje doslednih in pravočasnih informacij operaterjem klicnega centra 911, tako da bodo imeli podatke za obveščanje

klicateljev o najnovejših dogodkih. Poleg tega zagotovite snemanje in potrditve informacij, ki se jih prejme od klicateljev, tako da se jih lahko vključi v tok informacij. Oskrba z zasloni, ki prikazujejo spletno stran in lokalne televizijske postaje prav tako pomeni vzdrževanje posodobljenih medijskih virov.

Po napadu

Mediji lahko igrajo pomembno vlogo v obnovitveni fazi po teroristični katastrofi, posebej, če so potrebne donacije in pomoč prostovoljcev. Časovnica obnove v napotku 48 (orig. napotku 49) kaže, da so kljub poznemu prihodu na prizorišče ostale v obnovitveni fazi katastrofe aktivne samo zvezne agencije za obvladovanje izrednih razmer. Lokalni mediji so poročali s prekinitvami, četudi so bile prošnje za donacije objavljene vsak dan. Seveda ob katastrofi večjih razsežnosti, kot je bila 11. septembra, obnova traja leta, ne mesece. V tem času policija ne more veliko storiti, razen morda oskrbovati medije z zgodbami, ki bodo vzdrževale v javnosti podobo obnove. Kljub temu pa morate še naprej ostati pripravljeni na možnost, da pride do ponovnega napada.

O slovenskih avtorjih:

Bojan Dobovšek je doktor politoloških znanosti, izredni profesor za kriminalistiko na Fakulteti za varnostne vede Univerze v Mariboru.

Teodora Ivanuša je doktorica veterinarskih znanosti, specialistka policijskega managementa in docentka varnostnega managementa na Fakulteti za varnostne vede Univerze v Mariboru.

Iztok Podbregar je doktor organizacijskih znanosti, izredni profesor za organizacijo in management na Fakulteti za varnostne vede Univerze v Mariboru.

Andrej Sotlar je doktor obramboslovnih znanosti in docent za varnostni sistem na Fakulteti za varnostne vede Univerze v Mariboru.

Bojan Tičar je doktor pravnih znanosti, izredni profesor za področje prava javnega sektorja na Fakulteti za varnostne vede Univerze v Mariboru ter predavatelj na Fakulteti za management Primorske univerze.

ISBN 978-961-6821-00-1