VARSTVOSLOVJE,
letn. 21
št. 1
str. 73–86

Predlog modela ocen ogroženosti in ocen tveganj za področje obveščevalno-varnostne dejavnosti v Republiki Sloveniji

Jaroš Britovšek

Namen prispevka:

Cilj prispevka je pokazati razliko med oceno ogroženosti in oceno tveganj ter razviti predlog modela izdelave teh ocen za področje obveščevalno-varnostne dejavnosti v Republiki Sloveniji in hkrati spodbuditi praktike k uporabi enotne metodologije in terminologije na tem področju.

Metode:

Prispevek je strokovne narave in temelji na analizi procesa izdelave ocen ogroženosti in ocen tveganj za področje obveščevalno-varnostnih dejavnosti.

Ugotovitve:

Pri obravnavani tematiki obstajajo nekatere nejasnosti, ki se nanašajo na trenutno uporabo terminov grožnja in tveganje, ter posledično ocene ogroženosti in ocene tveganj. Avtor izhaja iz ideje, da so ocene ogroženosti del ocene tveganj, ki poleg ogroženosti vsebuje še pomembnost in ranljivost tarče. Nadalje je opredeljena terminologija, predstavljene pa so tudi nekatere hevristične rešitve ter predlog modela izdelave ocene ogroženosti in ocene tveganj primernih za področje obveščevalno-varnostne dejavnosti v Republiki Sloveniji. Obveščevalno-varnostna dejavnost se odvija v kompleksnem okolju z visoko stopnjo negotovosti, kjer je zaželena preprostejša in bolj prilagodljiva metodologija. Avtor priporoča uporabo hevristike, kar pri oceni ogroženosti pomeni, da več, kot je potrjenih indikatorjev, večja je verjetnost uresničitve grožnje, pri oceni tveganj pa, da se tveganje poviša ob povečani ogroženosti, ranljivosti ter pomembnosti tarče, in obratno.

Praktična uporabnost in pomembnost prispevka:

Prispevek se ukvarja z izdelavo ocen ogroženosti in ocen tveganj, z namenom poskusa poenotenja procesov izdelave in terminologije ter razumevanja omenjenih ocen za področje obveščevalno-varnostne dejavnosti.

UDK: 351.746.1(497.4)

Ključne besede: obveščevalno-varnostna dejavnost, tarče, grožnje, tveganja, ranljivosti, ocene ogroženosti, ocene tveganj, Slovenija

A Threat Assessment and Risk Assessment Model Proposal for Intelligence and Security Purposes in the Republic of Slovenia

Purpose:

The aim of the paper is to point out the differences between threat assessment and risk assessment, and to develop a proposal for an assessment model for intelligence and security purposes in the Republic of Slovenia. The purpose is also to encourage practitioners to use common methodology and terminology in this field.

Design/Methods/Approach:

The paper is of a professional nature and it is based on analysis of the process of threat assessment and risk assessment that is developed for intelligence and security area.

Findings:

The paper points out some confusing aspects regarding current usage of the term threat and risk, and consequently threat assessments and risk assessments. The paper is based on the idea that the threat assessment is a part of a risk assessment that additionally to the threat includes also the importance and vulnerability of the targets. The terminology is also defined, some heuristic solutions are put forward, and a proposal of threat and risk assessment model suitable for intelligence and security purposes in the Republic of Slovenia is made. Intelligence and security are taking place in a complex environment with high level of uncertainty. This fact demands the methodology that is simple and adaptable. The usage of heuristics is recommended, since more confirmed indicators by the threat assessment assume the increased likelihood of the achievement of the objectives set. In risk assessment the elevated risk depends on elevated threat, vulnerability and criticality of the target, and vice versa.

Practical Implications and Value:

The paper deals with threat and risk assessment, and it attempts to unify methodology, terminology and understandings of these assessments in the area of intelligence and security.

UDC: 351.746.1(497.4)

Keywords: intelligence, security, targets, threats, risks, vulnerabilities, threat assessment, risk assessment, Slovenia

1 UVOD

Ocene ogroženosti in ocene tveganj na obveščevalno-varnostnem področju so razmeroma skromno obdelana tematika v Republiki Sloveniji, kar lahko tudi vodi do nekaterih nejasnosti v praksi. Slednje lahko izhaja tudi iz nerazumevanja pojmov, kot so grožnje in tveganja ter posledično ocene ogroženosti in ocene tveganj. O tem oziroma o kognitivni zmedi na terminološkem varnostnem področju je govoril že Prezelj (2001), nejasnosti pa se lahko izražajo tudi v

zakonodaji. V Zakonu o organiziranosti in delu v policiji (2013) se na primer za potrebe varovanja objektov in okolišev posebnega pomena uporablja izraz ocena tveganj, medtem ko se v Pravilih službe Slovenske vojske (2009) in Uredbi o določitvi objektov in okolišev objektov, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje (1999) uporablja izraz ocena ogroženosti.

V prispevku izhajamo iz sicer redkih standardov, ki govorijo o ocenah ogroženosti in ocenah tveganj na področju obveščevalno-varnostne dejavnosti. Eden izmed teh je standard zveze NATO o zaščiti sil (Allied joint doctrine for force protection (AJP 3.14), 2015), kjer je ocena ogroženosti razumljena kot del ocene tveganj, ki poleg ogroženosti vsebuje tudi elementa pomembnosti (nakazuje na posledice) in ranljivosti. Pri tem je zanimivo, da so takšnemu razumevanju v Republiki Sloveniji še najbolj podobne ocene tveganj na področju zasebnega varstva, kjer sta v Uredbi o obveznem organiziranju varovanja (2012) kot obvezna elementa ocene tveganja navedena tudi ranljivost in ogroženost.

Nejasnosti lahko nastanejo tudi zaradi prevajanja določenih pojmov, predvsem iz angleščine v slovenščino. Kot primer si lahko pogledamo primer prevajanja v zaključnih nalogah pripadnikov Slovenske vojske. Angleški pojem ‚threat assessment' iz AJP 3.14 (2015) tako nekateri v slovenščino prevajajo kot ocena groženj (Gregorič, 2008), drugi pa kot ocena ogroženosti (Žeželj, 2011). Lahko bi sicer zagovarjali, da gre za sinonima, vendar vseeno menimo, da je pojem ogroženosti bolj ustrezen, saj ogroženost že nakazuje na element ocene, in sicer na stopnje ogroženosti, ki izhajajo iz groženj.

Kotnik-Dvojmoč (2000/2001) je pojme, kot so negotovost, izzivi, tveganja, grožnje ter nevarnosti, opredeljeval skozi dvoje dimenzij: verjetnosti (trenutne prisotnosti/odsotnosti varnostno zanimivih pojavov/procesov) in intenzivnosti (stika med pojavom/procesom in subjektom, ki se z njim lahko sooča). Pri tem je izpostavil grožnje in tveganja kot najbolj pogosto uporabljana pojma za opredeljevanje varnostnih problemov prihodnosti, kar je tudi glavno delovno področje obveščevalno-varnostne dejavnosti. Prezelj (2001) je grožnjo opredelil kot pojav, ki povzroča ogrožanje varnosti referenčnega objekta oziroma stanje, v katerem ni zagotovljen njegov obstoj in uravnotežen razvoj. Nevarnost pa je opredelil kot prehod grožnje iz latentne v manifestno fazo. Govorimo lahko tudi o uresničitvi grožnje. Tveganje pa je omenjal kot verjetnost nevarnosti, ki mu je subjekt izpostavljen. Podobno je ugotavljal tudi Rupnik (2018), ki je varnostna tveganja opredelil kot verjetnost varnostnih incidentov ter sposobnost preprečitve, preiskovanja in odpornosti na varnostne incidente.

V prispevku bomo nadgradili in opredelili omenjene pojmovne razlike ter predstavili predlog modela izdelave ocen ogroženosti in ocen tveganj za potrebe obveščevalno-varnostne dejavnosti. Slednje pomeni tudi osredotočenje predvsem na varnostne grožnje in tveganja. Glavni namen prispevka je spodbuditi praktike na obveščevalno-varnostnem področju k uporabi in razvoju enotnejše metodologije in terminologije ocen ogroženosti in ocen tveganj na obveščevalno-varnostnem področju, ki deluje v kompleksnem, negotovem in pogosto nepredvidljivem okolju. Slednje zato zahteva mero previdnosti in preprostosti v pristopu do metodologije na tem področju.[1]

1 *Todd in Gigerenzer (2012) trdita, da so v okolju visoke negotovosti in nizke predvidljivosti bolj kot kompleksni statistični modeli primerne preprostejše kognitivne strategije (hevristike).*

2 TARČE, GROŽNJE IN TVEGANJA

Kadar gre za konkretno stvar, ki jo želimo obvarovati oziroma zaščititi, te ni težko opredeliti. Splošno poimenovanje tistega, kar varujemo, ščitimo oziroma je predmet zaščite, pa že predstavlja določen izziv. Kotnik-Dvojmoč (2000/2001) je na primer govoril o subjektu, Prezelj (2001) pa o referenčnem objektu. V angleško govorečem svetu govorijo o ‚*assets*', ki jih slovar Merriam-Webster (2019) opredeli kot nekaj vrednega oziroma nekaj, kar cenimo. Eden od prevodov v slovenščino je lahko ‚dobrina', ki jo Slovar slovenskega knjižnega jezika opredeli kot tisto, »kar je namenjeno za zadovoljitev človekovih potreb« (Fran, 2018), nekaj, kar cenimo in posledično tudi želimo zaščititi in obvarovati pred škodo ali izgubo. Ker ljudje pri besedi ‚dobrine' razumemo predvsem materialni vidik tistega, kar želimo zavarovati, velja dodati še nematerialni vidik, ki ga prav tako želimo obvarovati. To vrzel po naši oceni najbolje dopolni beseda ‚vrednota', kot nekaj vrednega, nekaj »čemur priznava kdo veliko načelno vrednost in mu zato daje prednost« (Fran, 2018). Ker so tako dobrine kot vrednote cilji posameznih groženj in, da se izognemo dvobesednem poimenovanju, bomo za potrebe opredelitve tistega, kar varujemo ali želimo obvarovati (ljudi, objekte, podatke, opremo, območja, državo, interese, cilje …), v nadaljevanju prispevka uporabljali pojem ‚**tarče'**.

Da bi lahko pravočasno zavarovali tarče pred nezaželenimi posledicami, moramo najprej ugotoviti, kaj in v kolikšni meri jih ogroža. Tega natančno ni mogoče storiti, zato govorimo o oceni groženj oziroma ogroženosti (angl. *threat assessment*), kar že po opisu nakazuje, da gre za bolj subjektivno in približno presojanje. Pri tem se poraja vprašanje, kaj sploh so grožnje? Slovar slovenskega knjižnega jezika ponuja dokaj skromno opredelitev, ki pravi, da je grožnja »*obljuba, napoved komu česa neprijetnega, hudega*« (Fran, 2018). Merriam-Webster (2019) grožnjo opredeli kot namen povzročitve škode; kot vir ogrožanja ter kot indikator nečesa, kar se pripravlja. Gre torej za nekaj potencialnega, nekaj, kar se lahko zgodi, nekaj, kar lahko povzroči škodo, in ki izhaja iz nečesa. Če upoštevamo naštete elemente, lahko **grožnje** razumemo kot

‚vire ogrožanj in dejavnosti, ki bi lahko ogrozile tarčo'.

V takšno opredelitev je tako vključen vir ogrožanj in dejavnosti, ki jih vir izvaja ali pa bi jih lahko izvajal ter s tem ogrozil varnost tarč. Na področju obveščevalno-varnostne dejavnosti nas zanimajo predvsem varnostne grožnje, torej namerne oziroma zlonamerne grožnje (Jore, 2019). Tipične kategorije takšnih groženj so tuje oborožene sile (vir) in vojaški napad (aktivnosti); teroristične skupine (vir) in teroristični napad (aktivnosti); tuje obveščevalne službe (vir) in vohunjenje ter vplivanje (aktivnosti); kriminalne skupine in/ali posamezniki (vir) in kriminaliteta (aktivnosti). Posebna kategorija groženj za obveščevalno-varnostno področje predstavljajo notranje grožnje (znotraj institucij), ki so lahko namerne ali nenamerne in/ali povezane z drugimi grožnjami (Kont, Pihelgas, Wojtkowiak, Trinberg in Osula, 2015). Zaradi globaliziranosti, kompleksnosti in prepletenosti sodobnega okolja je grožnje vedno težje popolnoma kategorizirati, zato so opisne razlage nujne.

Tveganja so za razliko od groženj osredotočena bolj na izpostavljenost tarč posameznim nevarnostnim (Prezelj, 2001) in njihovi zmogljivosti pri

zoperstavljanju posameznim grožnjam (Rupnik, 2018). Slovar slovenskega knjižnega jezika opredeljuje tveganje zelo skopo, in sicer kot »glagolnik od tvegati«, ki pa pomeni »da se doživi kaj nezaželenega, slabega« (Fran, 2018). Gre torej za potencialno škodo, nekaj, kar lahko izgubiš (tvegaš življenje, premoženje, ugled, suverenost …). Tveganja poleg same izpostavljenosti pomenijo tudi verjetnost nezaželenega rezultata (potencialno škodo), ki izhaja iz groženj in ranljivosti tarče (Risk Steering Committee, 2010). Ne gre toliko za verjetnost uresničitve grožnje, temveč za verjetnost, da bo uresničena grožnja uspešna (International Civil Aviation Organization [ICAO], 2011; SANS glossary of security terms, 2019). Z drugimi besedami, ali bo uresničena grožnja uspešna, je poleg same grožnje odvisno tudi od zmogljivosti in zmožnosti tarče, da se zaščiti pred grožnjami. Glede na navedeno lahko **tveganja** razumemo kot

‚izpostavljenost tarče posameznim grožnjam, verjetnost uspešne uresničitve groženj ter škoda, ki lahko ob tem nastane'.

Izpostavljenost tarče kaže na to, kako zelo je tarča oddaljena in zaščitena od posameznih groženj. Verjetnost uspešne uresničitve je poleg samih groženj odvisna tudi od ranljivosti in drugih okoliščin, ki jih lahko viri ogrožanj izkoristijo, ter od zmogljivosti tarče, da se zoperstavi posameznim grožnjam. Tveganja prav tako pomenijo potencialno škodo, torej škodo ali izgubo, ki lahko nastane ob uresničitvi groženj. Kako velika je potencialna škoda, pa je povezano oziroma odvisno od same pomembnosti tarče. Za potrebe obveščevalno-varnostne dejavnosti velja razumeti predvsem to, da tveganja vključujejo in so odvisna od ogroženosti, ranljivosti in pomembnosti tarč.

3 OCENA OGROŽENOSTI

Obveščevalna (protiobveščevalna) dejavnost se ukvarja z zaznavo in analizo groženj (Center for Development of Security Excellence [CDSE], 2014), zato ji je bližji koncept ocen ogroženosti, čeprav je veliko bolj skromno razdelan kot koncept ocen tveganj (Vandepeer, 2011). Ocena ogroženosti se ukvarja z grožnjami in ocenjuje verjetnost, da bo prišlo do napada na neko tarčo v nekem obdobju (ICAO, 2011). Ocena ogroženosti se opredeljuje tudi kot produkt ali proces identifikacije entitet, dejavnosti in dogodkov (grožnje), ki bi lahko ogrozile življenje, informacije, operacije in lastnino (tarče) (Risk Steering Committee, 2010). Opredelitev ocene ogroženosti tako vsebuje naslednje elemente:

- tarčo;
- identificirane grožnje;
- ocene verjetnosti, da se bodo te grožnje uresničile; ter
- časovno obdobje morebitne uresničitve groženj.

Če se torej upoštevajo ti elementi (tarča, grožnje, verjetnost in čas), lahko **oceno ogroženosti** razumemo kot

‚oceno verjetnosti, da bo prišlo v določenem obdobju do uresničitve določenih groženj zoper določeno tarčo'.

Takšna opredelitev vključuje identifikacijo tarče, virov ogrožanj in dejavnosti, verjetnost uresničitve groženj ter časovnega obdobja. Ocena ogroženosti vsebuje nabor kategorij groženj ter stopnjo verjetnosti, da bi se te realizirale zoper tarčo v določenem obdobju. Ta obdobja so različna, govorimo lahko o kratkoročnem, srednjeročnem in dolgoročnem obdobju, kakšen interval zajemajo, pa je navadno odvisno od dogovora. Pomembno je predvsem, da je dogovor dosleden in ga razumeta tako izdelovalec kot uporabnik ocene ali odločevalec (Gallagher, MacKenzie, Blum in Boerman, 2016).

Posebnost pri ocenah na področju obveščevalno-varnostne dejavnosti so besedni opisi verjetnosti (angl. *words of estimative probability*) ali verjetnostni jezik (angl. *language of probability*). Heuer (1999) je ugotavljal, da se besedno izražanje verjetnosti pogosteje uporablja na področju obveščevalno-varnostne dejavnosti kot na drugih področjih. Obveščevalno-varnostno področje namreč deluje v kompleksnem, negotovem in pogosto nepredvidljivem okolju, kjer se izvajajo stalni napori zavajanja in prikrivanja in kjer je popolne ter resnične podatke težje pridobiti in zbrati. Besedni opis verjetnosti (na primer: manj verjetno, verjetno in zelo verjetno) je zato pogostejši. Težava nastane, ker ljudje pogosto različno dojemamo, kaj določene besede pomenijo.

Na težave v komunikaciji med obveščevalno-varnostnimi delavci in odločevalci je opozarjal že Kent (1964), ki je kot eden prvih poskušal na področju obveščevalno-varnostne dejavnosti uvajati enoten sistem besednega opisa verjetnosti. Spoznal je, da ljudje, ko uporabljajo različne besedne zveze pri komuniciranju verjetnosti, tudi precej drugače pripisujejo številčne oziroma odstotne verjetnosti posameznim besednim zvezam. Besedna zveza ‚zelo verjetno' je tako lahko enačena z besedno zvezo ‚obstaja velika možnost', beseda ‚verjetno' pa je lahko razumljena kot ‚možno', ni pa seveda nujno, in to je tisto, kar lahko povzroči zmedo. Ker bo med ljudmi vedno prihajalo do razhajanj pri razumevanju določenih verjetnostnih besed, je pomembno, da se pri ocenah vzpostavi legenda, lahko tudi kot konsenz strokovnjakov na tem področju, ki vsaj okvirno obrazloži, kaj določena beseda oziroma besedna zveza predstavlja.

Metodologije so različne in so odvisne od konsenza znotraj obveščevalno-varnostnih skupnosti. Na primer, v usmeritvah obveščevalno-varnostni skupnosti ZDA se priporoča uporabo sedem besednih zvez verjetnostnega jezika z opredeljenimi okvirnimi odstotki verjetnosti (Intelligence Community Directive 203, 2015). V nasprotju s tem naš predlog za izdelavo ocene ogroženosti na področju obveščevalno-varnostne dejavnosti uporablja preproste 3-stopenjske besedne opise verjetnosti (verjetnostni jezik): manj verjetno, verjetno ter zelo verjetno. V tabeli 1 je prikazana okvirna verjetnost v odstotkih, ki naj bi dešifrirala tisto, kar okvirno opisujemo s posamezno besedno zvezo. Če uporabljamo besedno zvezo ‚manj verjetno', potem s tem uporabniku sporočamo, da ocenjujemo, da je verjetnost uresničitve grožnje manj kot 40-odstotna. Če govorimo o ‚verjetni', potem ocenjujemo, da je verjetnost med 40 in 59 odstotki. ‚Zelo verjetno' pa pomeni med 60 in 99 odstotkov verjetnosti uresničitve groženj. Tu ne gre za nekakšen znanstveni ali legalističen pristop, temveč za okviren prikaz verjetnosti, katere namen je boljša komunikacija med izdelovalcem ocene ogroženosti in uporabnikom oziroma odločevalcem. Pomembno je predvsem, da

izdelovalec in uporabnik enako razumeta, kaj določena ocena oziroma besedni opis verjetnosti ali jezik verjetnosti pomeni.

Za oceno posameznih groženj si pomagamo z indikatorji. Indikatorji pomenijo indice oziroma ugotovljena dejstva ali ocene, ki namigujejo na to, da se nekaj pripravlja. V primeru ocen ogroženosti namigujejo na to, da se neka grožnja pripravlja ali uresničuje. Največkrat gre za indikatorje, ki se nanašajo na zmogljivosti in namene virov ogrožanj (Cid, 2012; Schuurman in Eijkman, 2015). Ti indikatorji so pogosto kompleksnejši, vendar je priporočljivo, da velja neka načelna preprostost, ki bo razumljiva tako izdelovalcu kot tudi uporabniku oziroma odločevalcu (Gallagher et al., 2016). Obstaja tudi tveganje, da se obveščevalno-varnostnim službam ob kompleksnejših metodologijah zgodi napad, preden ti zberejo vse zahtevane podatke, ki so potrebne za dvig ogroženosti. Zato naš predlog ocene ogroženosti vsebuje samo tri preproste indikatorje (glej tabelo 1): prisotnost potencialnih virov ogrožanj, povečane aktivnosti teh virov in konkreten namen. Prisotnost potencialnih virov pomeni zaznavo posameznikov, skupin ali organizacij, ki nakazujejo namen po izvajanju določenih aktivnosti, ki bi lahko ogrozile varnost. Povečane aktivnosti pomenijo zaznave priprav, ki lahko vodijo v konkretizacijo namenov. Slednji pa pomenijo že zaznano lokacijo in čas napada. Hevristično gledano lahko ocene ogroženosti razumemo v smislu; več, kot je potrjenih indikatorjev, višja je ocena verjetnosti uresničitve grožnje.

Tabela 1: Predlog ocene ogroženosti

Ocena ogroženosti	Verjetnostni jezik	Okvirno	Indikatorji
NIZKA	Manj verjetno	1–39 %	- Prisotnost potencialnih virov ogrožanj - Brez zaznanih povečanih aktivnosti - Brez zaznanega konkretnega namena
SREDNJA	Verjetno	40–59 %	- Prisotnost potencialnih virov ogrožanj - Zaznane povečane aktivnosti - Brez zaznanega konkretnega namena
VISOKA	Zelo verjetno	60–99 %	- Prisotnost potencialnih virov ogrožanj - Zaznane povečane aktivnosti - Zaznan konkreten namen

Katere grožnje se vključi v določene ocene ogroženosti, je ponovno odvisno od dogovora, okoliščin ter zaznave oziroma ocene, ali je neka grožnja sploh prisotna. Ocene ogroženosti lahko vsebujejo različne kategorije ali vrste groženj, lahko pa so osredotočene samo na eno kategorijo. Pogost primer ene same kategorije je ocena ogroženosti zaradi terorizma. Ocene ogroženosti posameznih držav zaradi terorizma se med seboj razlikujejo glede na število stopenj (verjetnost uresničitve groženj). Velika Britanija ima na primer 5-stopenjsko lestvico ocene ogroženosti zaradi terorizma (Security Service MI5, 2019), Francija je imela od 2003 4-stopenjsko barvno lestvico, vendar jo je leta 2014 opustila in prešla na 2-stopenjsko, ki pa ji je leta 2015 dodala še eno stopnjo ogroženosti (Wicky, 2016). Nemčija nacionalne stopenjske ocene ogroženosti zaradi terorizma sploh nima, ker meni, da je takšna lestvica nesmiselna, še posebej za celotno državo, saj so razmere po regijah lahko različne. Ocena naj bi dajala tudi lažen občutek, da je grožnja povsod enaka, in bi s tem povečevala nepotreben občutek nevarnosti med ljudmi (Das Bundesministerium des Innern, für Bau und Heimat, 2019).

Zanimiv primer so tudi ZDA, ki so imele 5-stopenjsko barvno lestvico ocene ogroženosti zaradi terorizma, vendar so jo opustile oziroma preoblikovale. Kritiki so namreč stopenjskemu sistemu z barvnimi lestvicami očitali, da je presplošen, da povzroča samo nepotreben strah in da ne prinaša nobene dodane vrednosti, še posebej na področju priprav na morebiten napad. Dvig stopenj ogroženosti naj bi bil po mnenju kritikov tudi precej bolj odvisen od političnih interesov kot od dejanske ogroženosti (Color-coded threat system to be replaced in April, 2011). ZDA so zato leta 2011 spremenile in uvedle nov, bolj preprost, sistem ocen ogroženosti, kjer se ob povišani ogroženosti konkretne informacije objavijo na spletni strani ministrstva za domovinsko varnost (angl. *Homeland Security*). Dejansko gre še vedno za nekakšne stopnje ogroženosti zaradi terorizma, ki pa temeljijo na večji vsebinski konkretizaciji groženj. Mesečni bilten redno objavlja splošne trende na področju terorizma. Če obstajajo specifične informacije o grožnji, govorijo o povišani ogroženosti (angl. *elevated threat*), če pa obstajajo podatki o konkretnejši lokaciji in tudi času pričakovanega napada, pa govorijo o pričakovani ogroženosti (angl. *impending threat*) (Homeland Security, 2011). Ravno obratno je Republika Slovenija, ki je imela od leta 2004 3-stopenjsko lestvico, leta 2016 prešla na 5-stopenjsko barvno lestvico ocene ogroženosti zaradi terorizma (Vlada RS, 2019).

Kadar se izdeluje ocena ogroženosti, ki vključuje več kategorij groženj, se poraja dilema, kako določiti končno stopnjo ocene ogroženosti. Posamezne kategorije groženj imajo namreč različen vpliv na varnost tarč, oziroma z drugimi besedami, njihova uspešna uresničitev bi tarči povzročila različno škodo. Imela bi torej drugačne posledice. Navadno je težko predvideti, kakšne vse posledice lahko imajo posamezne uresničene grožnje. Eden od možnih kriterijev je takojšnja fizična oziroma kinetična škoda, ki jo uresničena grožnja lahko povzroči. Na podlagi tega ima lahko na primer uresničena vojaška grožnja hujše posledice kot teroristična grožnja, slednja pa večje kot obveščevalna grožnja in tako naprej. Zato se države pogosto ob končnih ocenah ogroženosti nanašajo predvsem na stopnjo ocene ogroženosti zaradi terorizma, ostale varnostne grožnje pa obravnavajo predvsem opisno in z uporabo verjetnostnega jezika.[2]

4 OCENA TVEGANJ

Ocena tveganj (angl. *risk assessment*) se ukvarja z analizo tveganj in pomeni oceno verjetnosti, da bo napad oziroma uresničena grožnja uspešna (ICAO, 2011). Omenili smo, da lahko tveganja razumemo kot izpostavljenost tarče posameznim grožnjam, verjetnost uspešne uresničitve groženj ter potencialno škodo, ki ob tem nastane. Ocena tveganj pa ugotavlja, v kolikšni meri je neka tarča izpostavljena določeni grožnji, torej kakšna je stopnja verjetnosti uspešne uresničitve groženj. Hkrati pa nakaže, kako zelo nujno je treba vzpostaviti in okrepiti zmogljivosti varovanja in zoperstavljanja grožnjam (Risk Steering Committee, 2010). Ocene

2 *Litvanska nacionalna ocena ogroženosti na primer vsebuje opredeljeno ocenjevalno obdobje in oceno ogroženosti zaradi terorizma (nizka), za ostale grožnje pa uporablja opredeljen 4-stopenjski verjetnostni jezik (National threat assessment 2019, 2019).*

tveganj niso tako pogost koncept v obveščevalno-varnostni dejavnosti kot ocene ogroženosti, kljub temu pa se delno srečujejo z njimi, predvsem na varnostnem področju (zaznava ranljivosti). **Ocena tveganj** je v primerjavi z oceno ogroženosti bolj osredotočena na posamezne tarče in jo lahko razumemo kot

‚oceno verjetnosti uspešne uresničitve groženj, ki je poleg ogroženosti odvisna od pomembnosti in ranljivosti tarče'.

ISO 31010 navaja okoli 40 metod ocenjevanja tveganj (Cross, 2017). Te pogosto temeljijo na verjetnostnih modelih ali modelih frekvenčnih modelov, ki pa ne obstajajo sami po sebi in so smiselni samo v določenih situacijah s ponavljajočimi se elementi (Aven, 2017). Primer takšne metodologije je matrica verjetnosti in posledic, kjer se na podlagi preteklih izkušenj ugotavlja verjetnost nezaželenih dogodkov in se jih primerja s posledicami (Cross, 2017). Slednje predstavlja določeno težavo za obveščevalno-varnostno področje, ki deluje v kompleksnem varnostnem okolju s težko predvidljivimi nezaželenimi dogodki. V takšnem okolju se je bolje kot na napovedovanje dogodkov, ki veljajo za manj verjetne in imajo lahko hude posledice, osredotočati na zmanjševanje ranljivosti ob morebitni uresničitvi groženj (Taleb, Goldstein in Spitznagel, 2009). Dodatno težavo predstavljajo stohastične grožnje, kot so teroristični napadi ‚samotnih volkov', ki jih je pogosto nemogoče konkretno napovedati (Hamm in Spaaij, 2017). Lahko pa iščemo in prepoznavamo ranljivosti, kar je delo predvsem varnostnega dela obveščevalno-varnostne dejavnosti (CDSE, 2014). Obveščevalno-varnostno področje pa zahteva preproste in prilagodljive rešitve, ki ne obljubljajo preveč, a lahko vseeno uspešno zaznajo povišana tveganja.

V ta namen smo razvili svoj predlog matrike ocene tveganj (tabela 2). Matrika vsebuje podobne elemente in načela, kot jih uporablja metodologija ocen tveganj ameriške Zvezne agencije za krizno upravljanje (Federal Emergency Management Agency, 2005), vendar ne vsebuje točkovnega sistema in je na splošno manj kompleksna. Predlog matrike ocene tveganj vključuje: oceno ogroženosti tarče, oceno ranljivosti in oceno pomembnosti tarče (posledice). Za ugotavljanje ocene tveganj je treba oceno ogroženosti (verjetnost uresničitve groženj) primerjati z ranljivostjo (zaščito) in pomembnostjo tarče (privlačnostjo). Zaradi boljše komunikacije in razumevanja med izdelovalcem ocene in uporabnikom je načeloma zaželena preprostejša matrika, zato smo se omejili na tri spremenljivke tudi pri ocenah ranljivosti in pomembnosti tarče.

Ocena ranljivosti se ukvarja z ranljivostmi, pri čemer se analizira značilnosti in okoliščine tarč, ter prepoznava ranljivosti, ki bi jih lahko izkoristili viri ogrožanj (ICAO, 2011). Oceno ranljivosti ugotavljamo z analizo varnostnih ukrepov in zmogljivosti tarče pri zoperstavljanju grožnjam ter drugih okoliščin, ki bi lahko vplivali na lažjo uresničitev groženj. V predlogu govorimo o treh spremenljivkah ocene ranljivosti, kjer ugotavljamo, ali je tarča zaščitena, delno zaščitena ali ranljiva. Ocena pomembnosti kot tretji element ocene tveganj se posredno nanaša tudi na posledice, ki lahko nastanejo ob uresničitvi grožnje, torej izguba ali poškodba tarče ter njen pomen. V predlogu smo se podobno kot pri ranljivostih omejili na tri spremenljivke, ki tarčo ocenjujejo kot manj pomembno, pomembno ali zelo pomembno.

Tabela 2: Predlog matrike ocene tveganj

Ocena ogroženosti →	NIZKA	SREDNJA	VISOKA	**Pomembnost tarče/ posledice ↓**
Ustrezno zaščitena	Nizko	Nizko	Povišano	Manj pomembna
Delno zaščitena	Nizko	Nizko	Povišano	Manj pomembna
Ustrezno zaščitena	Nizko	Povišano	Povišano	Pomembna
Ustrezno zaščitena	Nizko	Povišano	Povišano	Zelo pomembna
Ranljiva	Povišano	Povišano	Povišano	Manj pomembna
Delno zaščitena	Povišano	Povišano	Visoko	Pomembna
Ranljiva	Povišano	Povišano	Visoko	Pomembna
Delno zaščitena	Povišano	Visoko	Visoko	Zelo pomembna
Ranljiva	Povišano	Visoko	Visoko	Zelo pomembna
↑ Ocena ranljivosti	**↑ Ocena tveganj**			

Če je ranljivost manj pomembne tarče ocenjena kot zaščitena in je ocena ogroženosti, torej verjetnost, da se bodo grožnje uresničile, NIZKA, potem tveganje ocenjujemo kot nizko. Če pa je ranljivost zelo pomembne tarče ocenjena kot ranljiva in je ocena ogroženosti VISOKA, ocenjujemo tveganje kot visoko. Hevristično gledano lahko ocene tveganj razumemo v smislu; tveganje se poviša/ zmanjša, če:

- se poveča/zmanjša verjetnost uresničitve groženj;
- se dodajo/umaknejo pomembnejše tarče;
- se poveča/zmanjša ranljivost.

Predvsem pa je eden glavnih ciljev ocene tveganj podpora odločevalcem pri prepoznavanju nujnosti ukrepanja za primerno zaščito in razvoj zmogljivosti pri zoperstavljanju grožnjam. Povišano tveganje, na primer, še ne pomeni, da je ukrepanje nujno, je pa indic, medtem ko daje visoka ocena tveganja jasen znak za nujnost ukrepanja.

Poglejmo si še hipotetičen primer. Obveščevalno-varnostna služba dobi nalogo za izdelavo ocene tveganja za določen objekt, posebnega pomena za obrambo. Ta objekt je sedež ministrstva, kar pomeni, da gre za zelo pomembno tarčo, čemur primerne so tudi posledice ob morebitni uspešni uresničeni grožnji. Obveščevalno-varnostna služba (njen obveščevalni/protiobveščevalni del) ocenjuje ogroženosti države s stopnjo NIZKO, kar pomeni, da so sicer zaznani viri ogroženosti, vendar službe niso zaznale nobenih povečanih aktivnosti in konkretnega namena za uresničitev grožnje. Obveščevalno-varnostna služba (njen varnostni del) mora za ustrezno oceno tveganja izdelati še oceno ranljivosti, kjer pregleda ustreznost varnostnih ukrepov objekta glede na potencialne grožnje in morebitne okoliščine, ki bi lahko omogočile lažjo uresničitev groženj. Pri tem oceni, da je objekt zaradi določenih pomanjkljivosti samo delno zaščiten. Zato je tveganje glede na predstavljeno matriko ocenjeno kot povišano, kar odločevalcem daje znak, da je treba ukrepati. Če bi služba ocenila, da je objekt ranljiv, bi bilo tveganje ocenjeno kot visoko, kar pa pomeni nujno ukrepanje. Tveganje bi bilo ocenjeno visoko tudi, če se oceno ogroženosti države dvigne na SREDNJO.

5 ZAKLJUČEK

Namen prispevka je bil razložiti razliko med oceno ogroženosti in oceno tveganj ter razviti predlog modela izdelave za področje obveščevalno-varnostne dejavnosti v Republiki Sloveniji in hkrati spodbuditi praktike k uporabi enotne metodologije in terminologije na tem področju. Izhajali smo iz predpostavke, da so ocene ogroženosti del ocene tveganj, ki poleg ogroženosti vsebuje še pomembnost in ranljivost tarč. Pojem tarče smo uporabljali za dobrine in vrednote oziroma za tisto, kar želimo zavarovati in obvarovati. Grožnje lahko razumemo kot vire ogrožanj in dejavnosti, ki bi lahko ogrozile tarče. Tveganja lahko razumemo kot kombinacijo izpostavljenosti tarč posameznim grožnjam, verjetnosti uspešne uresničitve groženj ter škode, ki lahko ob tem nastane. Oceno ogroženosti lahko razumemo kot oceno verjetnosti, da bo v določenem obdobju prišlo do uresničitve določenih groženj zoper določeno tarčo. Oceno tveganj pa lahko razumemo kot oceno verjetnosti uspešne uresničitve groženj, ki je poleg ogroženosti odvisna od pomembnosti in ranljivosti tarče.

Grožnje so spremenljivka, na katere načeloma nimamo toliko vpliva, medtem ko na tveganja lahko lažje vplivamo, predvsem s krepitvijo lastnih zmogljivosti varovanja ter odzivov na grožnje. Slednje lahko razumemo tudi kot izzive. Ocene tveganj izhajajo iz samih tarč (posamezniki, podatki, aktivnosti, objekti …), medtem ko ocene ogroženosti izhajajo iz groženj, ki tarče ogrožajo. So pa ocene ogroženosti del ocene tveganj, ki poleg ocene virov ogrožanj in aktivnosti, ki bi lahko ogrozile tarčo, temeljijo tudi na pomembnosti ter ranljivosti same tarče. Grožnje se lahko uresničijo ali pa ne (ogroženost), v kakšni meri bodo uspešne (tveganje), pa je odvisno od privlačnosti (pomembnost in posledice) in ranljivosti tarč (pomanjkljivi varnostni ukrepi in nezmožnost odzivanja na grožnje). Ocene ogroženosti so pomembne, ker nas opozarjajo na grožnje, ocene tveganj pa so pomembne, ker nas opozarjajo na naše pomanjkljivosti in na nujnost ukrepanja, s katerim lahko zmanjšamo tveganje oziroma izpostavljenost tarč posameznim grožnjam.

V prispevku smo predstavili predlog za izdelavo ocen ogroženosti in ocen tveganj za področje obveščevalno-varnostne dejavnosti. Za lažjo predstavo smo v prispevku uporabili različne besede za določanje stopenj posameznih ocen. Poudariti je treba, da je pretirana kvantifikacija in matematizacija ocen ogroženosti in ocen tveganj lahko nevarna, še posebej na področju obveščevalno-varnostne dejavnosti, ki deluje v kompleksnem, negotovem in pogosto nepredvidljivem varnostnem okolju, kjer so prisotni elementi zavajanja in prikrivanja ter kjer so posledično popolni in resnični podatki težje dosegljivi. Matematizacija namreč lahko daje lažno legitimnost in pomembnost ter posledično preveliko samozavest uporabnikom (odločevalci) takšnih ocen. Zato so pomembne opisne ocene, ki morajo vsebovati tudi tisto, o čemer nismo prepričani, česar enostavno ne vemo ali ne moremo vedeti. S tem lahko ohranjamo bolj realno sliko in ne zavajamo uporabnikov oziroma odločevalcev. Zato naj omenjene tabele služijo kot pomoč pri razumevanju ocen in se uporabljajo le tam, kjer se lahko oziroma je smiselno. Sicer pa se lahko uporablja hevristika, ki smo jo predstavili za ocene ogroženosti (več, kot je potrjenih indikatorjev, večja je verjetnost uresničitve grožnje) in ocene tveganj (tveganje se poviša ob povečani ogroženosti, ranljivosti ter pomembnosti tarče in obratno).

Opredelitve in metodologija, predstavljeni v prispevku, so omejeni in namenjeni predvsem praktikom na področju obveščevalno-varnostne dejavnosti. Ocene ogroženosti so sicer bolj znan koncept na področju obveščevalno-varnostne dejavnosti, medtem ko se ocene tveganj pogosteje uporabljajo in so tudi bolje razdelane na področju informacijske varnosti. Pri tem velja poudariti, da smo se pri razvoju predloga ocene tveganj izognili kopiji kompleksnejših metodologij s področja informacijske varnosti. Obveščevalno-varnostna dejavnost se odvija v kompleksnem okolju z visoko stopnjo negotovosti, kjer je zaželena preprostejša in prilagodljivejša metodologija (Todd in Gigerenzer, 2012), ki tudi ne sme preveč obljubljati. Vseeno menimo, da lahko predlog ocene tveganj nudi določeno pomoč pri opisni analizi ocene ogroženosti, kjer lahko delavci z besedno zvezo ‚povišano tveganje' v svojih izdelkih opisujejo določena dejstva in okoliščine (ranljivosti, zmogljivosti in pomembnost tarče), ki bi lahko omogočale lažjo uresničitev groženj.

Predstavljen predlog in metodologija lahko služita praktikom na obveščevalno-varnostnem področju pri izdelavi ocen ogroženosti in ocen tveganj ali pa kot podlaga za razvoj lastnih metodologij. Kot vodilo predlagamo načeli preprostosti in prilagodljivosti, saj narava dela obveščevalno-varnostnih delavcev zahteva delo v okolju, ki zahteva hitro odzivnost ter jasno in preprosto komuniciranje z uporabniki oziroma odločevalci. Ob zapletenih ocenah in časovnem pritisku se lahko po eni strani zgodi, da praktiki iščejo bližnjice, po drugi strani pa, da odločevalci zaradi impresivnosti nad kompleksnostjo dajejo ocenam preveliko pomembnost. Zato menimo, da morata načeli preprostosti in prilagodljivosti veljati tudi v prihodnjem raziskovanju in razvoju metodologij na področju obveščevalno-varnostne dejavnosti, predvsem na morebitnem raziskovanju in izdelavi metodologij indikatorjev ogroženosti, ocen ranljivosti in pomembnosti tarč za področje obveščevalno-varnostne dejavnosti.

UPORABLJENI VIRI

Allied joint doctrine for force protection (AJP 3.14.). (2015). Brussels: NATO Standardization Office.

Aven, T. (2017). A conceptual foundation for assessing and managing risk, surprises and black swans. V G. Motet in C. Bieder (ur.), *The illusion of risk control* (str. 23–39). Cham: Springer.

Center for Development of Security Excellence [CDSE]. (2014). *The relationship between counterintelligence and security: Student guide*. Pridobljeno na https://www.cdse.edu/documents/student-guides/relationship-between-ci-and-security.pdf

Cid, D. (1. 4. 2012). The next worst thing. *FBI Law Enforcement Bulletin.* Pridobljeno na https://leb.fbi.gov/articles/featured-articles/the-next-worst-thing

Color-coded threat system to be replaced in April. (26. 1. 2011). *CNN*. Pridobljeno na http://edition.cnn.com/2011/POLITICS/01/26/threat.level.system.change/index.html

Cross, J. (2017). *ISO 31010 Risk assessment techniques and open systems.* Tokyo: WOSD. Pridobljeno na http://tc56.iec.ch/action/WOSD2017b.pdf

Das Bundesministerium des Innern, für Bau und Heimat. (2019). *Häufig nachgefragt – Islamistischer Terror*. Pridobljeno na https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/sicherheit/islamismus/islamismus-liste.html

Federal Emergency Management Agency. (2005). *Risk assessment: A how-to guide to mitigate potential terrorist attacks against buildings* (FEMA 452). Pridobljeno na https://www.wbdg.org/ffc/dhs/criteria/fema-452

Fran: Slovarji Inštituta za slovenski jezik Frana Ramovša ZRC SAZU. (2018). Ljubljana: Inštitut za slovenski jezik Frana Ramovša ZRC SAZU. Pridobljeno na http://www.fran.si/

Gallagher, M., MacKenzie, C., Blum, D. in Boerman, D. (2016). Improving risk assessment communication. *Military Operations Research, 21*(1), 5–20. Pridobljeno na http://www.jstor.org/stable/24838659

Gregorič, B. (2008). *Samomorilski terorizem – opredelitev in dileme v sistemu zaščite sil* (Zaključna naloga). Maribor: Poveljniško-štabna šola. Pridobljeno na http://dk.mors.si/IzpisGradiva.php?id=21&lang=slv

Hamm, M. S. in Spaaij, R. (2017). *The age of lone wolf terrorism*. New York: Columbia University Press

Heuer, R. J. (1999). *Psychology of intelligence analysis.* Washington: Center for the Study of Intelligence. Pridobljeno na https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf

Homeland Security. (2011). *National terrorism advisory system public guide*. Pridobljeno na https://www.dhs.gov/xlibrary/assets/ntas/ntas-public-guide.pdf

Intelligence Community Directive 203: Analytic Standards. (2015). Office of the Director of National Intelligence. Pridobljeno na https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf

International Civil Aviation Organization [ICAO]. (2011). *Manual on threat assessment and risk management methodology*. Montréal: ICAO. Pridobljeno na https://www.icao.int/SAM/Documents/ICAOLACACAVSECRG2/Manual%20on%20Threat%20Assessment%20and%20Risk%20Management%20Methology%20NoLogos.pdf

Jore, S. H. (2019). The conceptual and scientific demarcation of security in contrast to safety. *European Journal for Security Research, 4*(1), 157–174. Pridobljeno na https://link.springer.com/article/10.1007%2Fs41125-017-0021-9

Kent, S. (1964). Words of estimative probability. *Studies in Intelligence 8*(4), 49–65. Pridobljeno na https://www.cia.gov/library/readingroom/docs/CIA-RDP-93T01132R000100020036-3.pdf

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. in Osula, A. (2015). *Insider threat detection study.* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. Pridobljeno na https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

Kotnik-Dvojmoč, I. (2000/2001). Varnostna tveganja in grožnje v sodobnem svetu. *Ujma,* (14/15), 215–223.

Merriam-Webster. (2019). Springfield: Merriam-Webster. Pridobljeno na https://www.merriam-webster.com/dictionary/

National threat assessment 2019. (2019). Vilnius: State Security Department of the Republic of Lithuania, Second Investigation Department under the Ministry of National Defence. Pridobljeno na https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf

Pravila službe v Slovenski vojski. (2009). *Uradni list RS*, (84/09).

Prezelj, I. (2001). Grožnje varnosti, varnostna tveganja in izzivi v sodobni družbi: Razreševanje nekaterih terminoloških dilem. *Teorija in praksa, 28*(1), 127–141.

Risk Steering Committee. (2010). *DHS Risk Lexilon.* Department of Homeland Security. Pridobljeno na https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

Rupnik, A. (14. 12. 2018). *Uporaba intruzivnih metod v obveščevalnem in preiskovalnem procesu* [Predstavitev]. Pridobljeno na https://infosec-seminar.si/arhiv/08_Andrej_Rupnik_Uporaba_intruzivnih_metod_v_obvescevalnem_in_preiskovalnem_procesu.pdf

SANS glossary of security terms. (2019). Swansea: SANS Institute. Pridobljeno na https://www.sans.org/security-resources/glossary-of-terms/

Schuurman, B. in Eijkman, Q. (2015). Indicators of terrorist intent and capability: Tools for threat assessment. *Dynamics of Asymmetric Conflict*, *8*(3), 215–231.

Security Service MI5. (2019). *Threat levels*. Pridobljeno na https://www.mi5.gov.uk/threat-levels

Taleb, N. N, Goldstein, D. D. in Spitznagel M. W. (2009). The six mistakes executives make in risk management. *Harward Business Review,* (Oct.). Pridobljeno na https://hbr.org/2009/10/the-six-mistakes-executives-make-in-risk-management

Todd, P. M. in Gigerenzer, G. (ur.). (2012). *Ecological rationality: Intelligence in the world.* New York: Oxford University Press.

Uredba o določitvi objektov in okolišev objektov, ki so posebnega pomena za obrambo, in ukrepih za njihovo varovanje. (1999, 2003, 2010). *Uradni list RS*, (7/99, 67/03, 26/10).

Uredba o obveznem organiziranju varovanja. (2012). *Uradni list RS*, (80/12).

Vandepeer, C. (2011). *Intelligence analysis and threat assessment: Towards a more comprehensive model of threat.* Prispevek, predstavljen na 4th Australian Security and Intelligence Conference, Edith Cowan University, Perth. Pridobljeno na https://ro.ecu.edu.au/asi/21/

Vlada RS. (19. 3. 2019). *Ocena ogroženosti*. Pridobljeno na http://www.vlada.si/teme_in_projekti/krizno_upravljanje_in_vodenje/ocena_ogrozenosti/

Wicky, L. (20. 12. 2016). En France, le plan Vigipirate et ses trois niveaux d'alerte. *Le Monde*. Pridobljeno na https://www.gouvernement.fr/risques/comprendre-le-plan-vigipirate

Zakon o organiziranosti in delu v policiji (ZODPol). (2013, 2014, 2015, 2016, 2017). *Uradni list RS*, (15/13, 11/14, 86/15, 77/16, 77/17).

Žeželj, D. (2011). *Sodobna zaščita pomorskih pristanišč* (Zaključna naloga). Maribor: Šola za častnike. Pridobljeno na http://dk.mors.si/IzpisGradiva.php?id=506

O avtorju:

Dr. Jaroš Britovšek, zaposlen na Ministrstvu za obrambo Republike Slovenije. E-pošta: jaros.britovsek@mors.si