Kaja
PRISLAN MIHELIČ

Maja
MODIC

Branko
LOBNIKAR

Boštjan
SLAK

Anže
MIHELIČ

Ko se srečata znanje in odločanje

Pristopi k ocenjevanju varnostnih tveganj

Univerzitetna založba
Univerze v Mariboru

Univerza v Mariboru

Fakulteta za varnostne vede

Ko se srečata znanje in odločanje

Pristopi k ocenjevanju varnostnih tveganj

Avtorji

Kaja Prislan Mihelič

Maja Modic

Branko Lobnikar

Boštjan Slak

Anže Mihelič

Januar 2024

Naslov **Ko se srečata znanje in odločanje**
Title *When Knowledge and Decision-making Meet*

Podnaslov **Pristopi k ocenjevanju varnostnih tveganj**
Subtitle *Approaches to Security Risk Assessment*

Avtorji Kaja Prislan Mihelič
Authors (Univerza v Mariboru, Fakulteta za varnostne vede)

Maja Modic
(Univerza v Mariboru, Fakulteta za varnostne vede)

Branko Lobnikar
(Univerza v Mariboru, Fakulteta za varnostne vede)

Boštjan Slak
(Univerza v Mariboru, Fakulteta za varnostne vede)

Anže Mihelič
(Univerza v Mariboru, Fakulteta za varnostne vede)

Recenzija Iztok Podbregar
Review (Univerza v Mariboru, Fakulteta za organizacijske vede)

Andrej Benedejčič
(Kabinet predsednika vlade Republike Slovenije)

Jezikovni pregled Barbara Erjavec
Language editing (Univerza v Mariboru, Fakulteta za varnostne vede)

Tehnični urednik Jan Perša
Technical editor (Univerza v Mariboru, Univerzitetna založba)

Oblikovanje ovitka Jan Perša
Cover designer (Univerza v Mariboru, Univerzitetna založba)

Grafika na ovitku Ozadje Flowers beside yellow wall, avtorica: Mona Eendra,
Cover graphic unsplash.com, CC 0, 2017

Grafične priloge Viri so lastni, razen če ni navedeno drugače.
Graphic material Prislan Mihelič, Modic, Lobnikar, Slak, Mihelič, 2023

Založnik **Univerza v Mariboru**
Published by **Univerzitetna založba**
Slomškov trg 15, 2000 Maribor, Slovenija
https://press.um.si, zalozba@um.si

Izdajatelj **Univerza v Mariboru**
Issued by **Fakulteta za varnostne vede**
Kotnikova ulica 8, 1000 Ljubljana, Slovenija
https://www.fvv.um.si, fvv@um.si

Izdaja
Edition Prva izdaja

Vrsta publikacije
Publication type E-knjiga

Dostopno na
Available at http://press.um.si/index.php/ump/catalog/book/825

Izdano
Published at Maribor, januar 2024

Naslov projekta: Razvoj celovitih modelov ocenjevanja nacionalnovarnostne ogroženosti in merjenja uspešnosti, učinkovitosti ter kakovosti policijskega dela: pregled tujih pristopov, dobrih praks in njihova aplikacija za Slovenijo.

Šifra projekta: V5-2148.

Financer projekta: Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije in Ministrstvo za notranje zadeve Republike Slovenije.

CIP – Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

355.2(082)(0.034.2)

KO se srečata znanje in odločanje [Elektronski vir] : pristopi k ocenjevanju varnostnih tveganj / avtorji Kaja Prislan Mihelič ... [et al.]. - 1. izd. - E-publikacija. - Maribor : Univerza v Mariboru, Univerzitetna založba, 2023

Način dostopa (URL): https://press.um.si/index.php/ump/catalog/book/825
ISBN 978-961-286-802-4
doi: 10.18690/um.fvv.1.2024
COBISS.SI-ID 177486339

ISBN 978-961-286-802-4 (pdf)
978-961-286-803-1 (trda vezava)

DOI https://doi.org/10.18690/um.fvv.1.2024

Cena
Price Brezplačni izvod

Odgovorna oseba založnika
For publisher prof. dr. Zdravko Kačič,
rektor Univerze v Mariboru

Citiranje
Attribution Prislan Mihelič, K., Modic, M., Lobnikar, B., Slak, B. in Mihelič, A. (2024). *Ko se srečata znanje in odločanje: Pristopi k ocenjevanju varnostnih tveganj*. Univerza v Mariboru, Univerzitetna založba. doi: 10.18690/um.fvv.1.2024

Univerzitetna založba
Univerze v Mariboru

Kazalo

Univerzitetna založba
Univerze v Mariboru

1 Uvod

Temeljna naloga in odgovornost vsake države je poskrbeti za varnost njenih prebivalcev skozi urejen sistem zagotavljanja nacionalne varnosti. Država se mora s svojimi organi, regulatornimi in izvršilnimi mehanizmi ter odzivnimi službami ustrezno pripraviti na potencialne dogodke, ki bi lahko ogrozili prebivalce in njihovo imetje, gospodarstvo, suverenost ali družbeno ureditev. Pri tem morajo omenjeni subjekti delovati preventivno in poskušati v čim večji meri preprečiti pojav varnostnih incidentov. Ker pa ni možno preprečiti vseh nevarnosti in groženj, morajo biti zagotovljeni tudi ustrezni načrti, sposobnosti in viri za odzivanje v primeru njihove uresničitve (OECD, 2018).

Med pomembne izzive sodobnega časa, ki vplivajo na učinkovitost družbenega upravljanja, in zagotavljanja varnosti sodijo spremembe, ki smo jim priča na področju (varnostnih) groženj. V zadnjih letih se namreč države Evropske unije (EU) soočajo s spremembami varnostnih razmer, pojavom novih, bolj kompleksnih, nepredvidljivih, organiziranih in hibridnih groženj (European Commission, 2016, 2020), posledično pa se spreminjajo tudi pristopi k zagotavljanju varnosti (Prislan in Lobnikar, 2019; Van Den Born idr., 2013). Vpliv družbenih sprememb na varnostne razmere, procese in ukrepe zagotavljanja varnosti ter legitimnost ključnih deležnikov nacionalnovarnostnega sistema je bil še posebej opazen v času epidemije covida-19. Ker se varnostne razmere neprestano spreminjajo, se lahko države in njihove

varnostne organizacije uspešno prilagajajo spremembam le, če pridobijo temeljit vpogled v razmere v okolju, v katerem delujejo.

Da bi se učinkovito soočali z omenjenimi spremembami, Slovenija v svoji razvojni strategiji med temeljne cilje umešča spodbujanje zaupanja vrednega pravnega sistema ter varne in globalne odgovorne družbe, skozi izboljšanje zaupanja državljanov v pravni sistem in javne institucije, ohranjanje nizke stopnje kriminalitete in visoke umeščenosti Slovenije na globalni indeks miru. Pri tem med ključne sodijo ukrepi, ki prispevajo k večji produktivnosti, učinkovitosti in usposobljenosti na področju upravljanja varnosti ter proaktivno naslavljanje in ocenjevanje varnostnih groženj (Strategija razvoja Slovenije 2030 (Šooš idr., 2017)). Tovrstne razvojne usmeritve na področju varnosti so skladne s cilji evropske razvojne politike (United Nations Department of Economic and Social Affairs, 2015) in skupno evropsko varnostno strategijo, v kateri je med drugim kot pomemben ukrep za usklajeno odzivanje na grožnje in zmanjševanje razdrobljenosti med državami določeno, da je treba izvajati skrbno oceno (varnostnih) groženj in tveganj (European Commission, 2020). Tudi v »Resoluciji o nacionalnem programu zatiranja in preprečevanja kriminalitete za obdobje 2019–2023 (»ReNPPZK19–23)« (2019) so opredeljeni podobni ukrepi za spodbujanje večje varnosti v slovenski družbi, ki vključujejo nadgradnjo enotne metodologije za izdelavo ocene tveganj in ranljivosti, ugotavljanje varnostnih problemov, ter iskanje rešitev, metod in oblik dela, ki so potrebni za rešitev varnostnih problemov ter prepoznavanje dobrih praks.

Dejavno spremljanje sodobnih trendov, uvajanje najboljših praks in prepoznavanje priložnosti za razvoj so torej temeljni predpogoji, da se bosta varnostni sistem in varnostna dejavnost v prihodnje razvijala v kar najboljši smeri (Prislan in Lobnikar, 2019). Kot je razvidno iz aktualnih razvojnih usmeritev in prioritet, si EU in države članice prizadevajo za izboljševanje sistema upravljanja kakovosti, kar med drugim vključuje tudi posodobitev in razvoj mehanizmov ocenjevanja varnostnih razmer oz. ogroženosti.

Nacionalna ocena tveganj (ang. *national risk assesment* – NRA) predstavlja pomemben mehanizem za izvajanje integriranega upravljanja tveganj na nacionalni ravni. Ima pomembno vlogo pri obvladovanju tveganj naravnih nesreč (ang. *disaster risk management* – DRM) skozi zagotavljanje kakovostne informacijske podpore v odločitvenih procesih, v katerih sodeluje širok krog deležnikov, in pomembno

prispeva k ocenjevanju sposobnosti za upravljanje tveganj (ang. *risk management capability assessment* – RMCA) na nacionalni ravni. NRA skupaj z RMCA omogoča vzpostavitev urejene strukture za upravljanje tveganj, ki vključuje procese ocenjevanja tveganj, načrtovanja sposobnosti in ukrepov preprečevanja ter odzivanja. NRA in RMCA morata biti prilagojena okoliščinam države in nacionalnim ciljem, temeljni namen pa je zmanjšati število incidentov, obseg škode in zagotoviti večjo odpornost na tveganja (Poljansek idr., 2019). Da bi lahko zagotovili ustrezen in celosten pristop k upravljanju tveganj na nacionalni ravni, je treba razumeti, kakšni so možni in najbolj učinkoviti mehanizmi ocenjevanja in obvladovanja različnih vrst groženj ter tveganj.

Univerzitetna založba
Univerze v Mariboru

2 Proces upravljanja in ocenjevanja tveganj

Proaktivno delovanje pri obvladovanju oz. upravljanju nacionalnovarnostne ogroženosti[1] je močno odvisno od ustreznega pristopa k ocenjevanju tveganj, ki je sestavni del procesa upravljanja tveganj. Cilj upravljanja tveganj je zagotoviti pripravljenost (organizacije, države ali nekega subjekta) na potencialne nevarnosti in pravilno odzivanje oz. nemoteno delovanje tudi ob morebitni uresničitvi groženj. V tem delu je smiselno poudariti, da je koncept upravljanja tveganj (ang. *risk management*) nekoliko širši kot DRM.[2] V nadaljevanju na splošno opisujemo, kako poteka proces upravljanja in ocenjevanja tveganj, ki je aplikativen tudi na področju nacionalnih ocen tveganj in obvladovanju tveganj naravnih nesreč.

Upravljanje tveganj je proces načrtovanja obravnavanja tveganj[3] in vključuje postopke, povezane z ugotavljanjem (identificiranjem) in analiziranjem (ocenjevanjem oz. vrednotenjem) dejavnikov, ki vplivajo na tveganja, ter

[1] Ocena nacionalnovarnostne ogroženosti je izraz, ki se nanaša na nacionalno oceno tveganj. V tej monografiji za ta koncept uporabljamo oba izraza, ki tako predstavljata sinonima.
[2] Obvladovanje tveganj naravnih nesreč je področje, ki se ukvarja z upravljanjem specifičnih tveganj, navadno na nacionalni ravni, pri čemer proces sledi enakim zakonitostim kot splošen proces upravljanja tveganj, ki ima široko aplikativnost.
[3] Z odzivanjem na krizne razmere in situacije se ukvarja posebno področje/disciplina krizni management oz. krizno upravljanje (ang. *crisis management*), ki je tesno povezano s področjem upravljanja tveganj.

sprejemanjem odločitev glede njihove obravnave. Takšen proces je podlaga za zagotovitev učinkovitega pristopa k zagotavljanju varnosti, tj. izbira najboljših možnih ukrepov in sprejem pravih odločitev o ukrepih glede na potrebe in zmogljivosti. Pri obravnavanju tveganj je namreč treba zagotoviti tudi racionalnost in gospodarnost – pomembno je, da se odkrijejo najvplivnejši dejavniki tveganj ter da se čas in denar namenita za bistvene grožnje in razvoj najučinkovitejših ukrepov (Meško in Sotlar, 2012).

Gre torej za analitičen in sistematično zasnovan proces, v katerem se odločevalcem zagotovi ustrezna informacijska podpora – ugotavlja se, katera tveganja ogrožajo analiziran sistem, katera tveganja so bolj ali manj pogosta in nevarna, kar omogoča sprejem odločitev, kako se nanje pripraviti. S tem se ustvari podlaga za odločanje, katere ukrepe (če sploh) je treba sprejeti, da se zmanjša verjetnost pojava dogodkov in potencialna škoda (Deng, 2015).

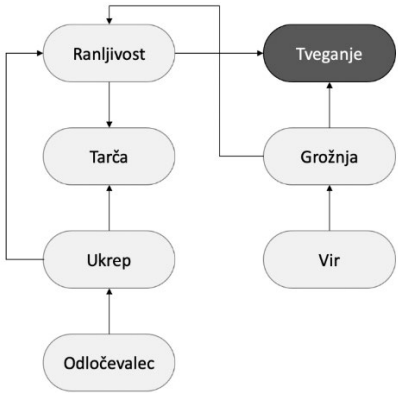
Glede na splošno opredelitev se tveganje nanaša na stopnjo verjetnosti, da bo prišlo do škodnega dogodka, natančneje pa se nanaša na verjetnost, da bo določena grožnja izkoristila določeno ranljivost na ravni določenega vira/tarče. Pri tem je stopnja tveganja odvisna od stopnje ogroženosti in stopnje ranljivosti – pri tem je stopnja ogroženosti odvisna od verjetnosti pojava groženj in resnosti možnih posledic, stopnja ranljivosti pa od izvedenih ukrepov. Manjša, kot je pogostost oz. pojavnost groženj in njihova resnost (posledice), ter več, kot je izvedenih ukrepov za zmanjševanje ranljivosti, manjša je tudi stopnja tveganja (Prislan in Bernik, 2019). Model z dejavniki, ki opredeljujejo tveganja, je predstavljen na sliki 1.

Ključna faza procesa upravljanja tveganj je ocena (varnostnih) tveganj (ang. *risk assessment*), ki je sestavljena iz več korakov in med drugim vključuje identifikacijo in oceno tveganj (ang. *risk analysis*), kar zajema:

a) Identifikacijo in oceno (vrednosti) ogroženih virov/dobrin/vrednot.
b) Identifikacijo in oceno (verjetnosti in nevarnosti) groženj.

Upravljanje tveganj je torej celovit proces (makro raven) obravnave tveganj, ocena tveganj pa je proces, ki je del tega (mezo raven) in se nanaša na vrednotenje tveganj, medtem ko je analiza tveganj (mikro raven) ožji del tega in vključuje postopke zagotavljanja informacij – identifikacija in vrednotenje posameznih dimenzij tveganj.

Ko je opravljena analiza tveganj, se v okviru ocenjevanja izvajajo še nekateri drugi koraki (npr. ocena ranljivosti oz. primernosti izvedenih ukrepov), ki omogočajo pripravo načrta obravnave v procesu upravljanja.



Slika 1: Model in dejavniki tveganj

Varnostno tveganje lahko torej razumemo kot produkt vseh elementov (dobrin, verjetnosti in nevarnosti groženj ter ranljivosti) – situacija, ki ogroža varnost nekega sistema (vira/dobrine/vrednote) in pred katero je le-ta ranljiv tako zaradi visoke verjetnosti uresničitve, nevarnosti posledic kot tudi pomanjkljivih ukrepov (Cox, Jr, 2008). V tem procesu vrednotenja se uporabi vnaprej predpisana metodologija, ki omogoča oceno posameznih elementov tveganja in izračun višine tveganja v kvantitativni obliki.

Države pri načrtovanju in upravljanju sistema nacionalne varnosti uporabljajo t. i. modele nacionalnovarnostne ogroženosti, ki pomagajo pri sprejemanju odločitev glede proaktivnega delovanja in odzivanja v primeru izrednih razmer. Modeli podpirajo celoten proces upravljanja varnostnih tveganj (od analize ogroženosti in pripravljenosti do obveščanja prebivalstva) in so zato pomemben varnostni instrument države (OECD, 2018).

Ocena tveganj v državi lahko poteka na več ravneh (lokalni, regionalni, nacionalni), vendar je za nas relevantna na nacionalni ravni, ki je pravzaprav proces, ki zahteva sodelovanje različnih državnih organov, subjektov s področja temeljnih družbenih funkcij (npr. kritične infrastrukture) in strokovnjakov z različnih področij. Pri izdelavi ocene ogroženosti v praksi države uporabljajo različne metode, kjer gre

lahko le za krajši opis možnih scenarijev ali pa uporabo kompleksnejših modelov. Ključna tveganja pa so praviloma opredeljena v nacionalnih strateških dokumentih.

V osnovi se najprej definirajo najpomembnejši dogodki, ki bi lahko ogrozili nacionalno varnost in družbeno stabilnost – npr. možne nesreče, izredne razmere in krize in nato za vsako izmed njih opredeli več scenarijev, ki vsebujejo njihove glavne značilnosti in potencialne izvore. V večini držav se analize tveganj nanašajo na naravne nesreče, izbruhe bolezni, industrijske nesreče, teroristične napade, kibernetske napade oz. obsežne pojave, ki lahko ogrozijo varnost in stabilnost družbe (Office of the Director of National Intelligence, 2021). Tovrstni scenariji se nato analizirajo z dveh vidikov: resnosti posledic in verjetnosti uresničitve. Navadno se pri ocenah uporabljajo večstopenjske lestvice (npr. od 1 do 5, pri čemer najnižja ocena pomeni nizko verjetnost ali lahke posledice, najvišja ocena pa visoko verjetnost ali katastrofalne posledice). Pri takšnem analiziranju scenarijev je treba identificirati konkretne grožnje, ki jih lahko povzročijo in so pomembne za družbo. Pri tem je glavni cilj ustvariti seznam groženj, jih kategorizirati po skupinah/scenarijih in določiti, katere grožnje ustvarjajo potrebo po obravnavi. Najboljša praksa je ta, da se analizirajo vsi možni dogodki oz. grožnje, ki bi lahko državo prizadele, od naravnih nesreč do dogodkov, ki jih lahko stori človek in ne le grožnje na specifičnih področjih. Tudi posledice lahko razdelimo na več področij, in sicer posledice za zdravje in blaginjo prebivalstva, ekonomske posledice, motnje v izvozu in uvozu v in iz države, okoljska škoda in politični ter socialni vpliv. Nekatere države te posledice razčlenijo še na več podkategorij, kar se je tudi izkazalo kot dobra praksa, saj to omogoči še bolj natančno oceno ogroženosti (OECD, 2018). Pri vsem tem je pomembno, da končni rezultat omogoča sprejem odločitev glede izvajanja nujno potrebnih ukrepov in situacijsko zavedanje, katere grožnje je treba konstantno spremljati in nadzirati.

Kot omenjeno, je v izdelavi ocene nacionalnovarnostne ogroženosti ključnega pomena, da sodelujejo različne organizacije – tako nacionalne, regionalne kot tudi lokalne organizacije; državne in javne organizacije kot tudi organizacije zasebnega sektorja. Seveda pa bi v ta proces morali biti vključeni strokovnjaki z določenih področij (kriznega managementa in komunikacije, varnosti, organizacije, napovedne analitike ipd.). Bistveno je tudi, da se ocene nadzirajo in redno posodabljajo. Civilna zaščita EU priporoča, da se ocena posodablja vsaj vsake tri leta, saj so razmere v sodobnem, hitro spreminjajočem se svetu zelo nepredvidljive (European Parliament,

2019). Zaradi tega je pomembno tudi, da se ob pripravi ocene ne gleda zgolj na pretekle primere in zgodovino, temveč se sestavljajo scenariji primerov, ki se še niso zgodili, a bi se v prihodnosti lahko (Lin, 2018).

Ocenjevanje nacionalnovarnostne ogroženosti je v praksi sicer povezano s številnimi izzivi. Poleg tega, da to zahteva dobro sodelovanje in koordinacijo med različnimi subjekti, temeljno težavo predstavlja kompleksnost in nepredvidljivost tveganj; nepoenotenost metodologij; pomanjkanje kakovostnih podatkov in nepreglednost dobrih praks.

V sodobnem času zagotovo enega največjih izzivov za države in njihove sisteme zagotavljanja nacionalne varnosti predstavlja dejstvo, da so tveganja po naravi kompleksna, zato je njihovo ocenjevanje zahtevna naloga. Varnost države je namreč odvisna od izjemno raznolikih tveganj, ki jih lahko kategoriziramo v različne skupine, kot so splošna kriminaliteta, napadi na državno suverenost, tveganja za gospodarsko in socialno stabilnost, nesreče, izbruhi izrednih razmer in množičnih pojavov ipd. Pri tem pa je treba upoštevati tudi, da so grožnje vedno bolj hibridne, se stalno razvijajo, zaradi medsebojne povezanosti pa lahko pride celo do součinkovanja in stopnjevanja posledic (Office of the Director of National Intelligence, 2021).

Pomemben izziv predstavlja tudi sama metodologija ocenjevanja ogroženosti. Primarno težavo predstavlja nepoenotenost pristopov za ocenjevanje, konkretno pa težavo predstavlja tudi pomanjkanje kakovostnih podatkov, izkušenj oz. dobrih praks, kar ovira zanesljivost vrednotenja tveganj (European Commission, 2020; Hirsch Ballin idr., 2020; Poljansek idr., 2019b). Pogosto se zgodi tudi, da so zaradi pomanjkanja časa, sredstev in potrebnega strokovnega znanja take ocene napisane v naglici in ne zajemajo podrobne analize verjetnosti in posledic (OECD, 2018). Zaradi omenjenih različnih pristopov in praks med državami si EU z zakonodajo in smernicami ter priporočili prizadeva za poenotenje in harmonizacijo metodoloških okvirov (podrobneje predstavljeno v poglavju 3.1).

Kot je razvidno iz splošnega pregleda procesa ocenjevanja in analiziranja tveganj, je priporočen večfazen in večdeležniški pristop ter ocenjevanje na različnih vsebinskih področjih. V naslednjem poglavju predstavljamo ključne evropske strategije in usmeritve k izvajanju ocenjevanja (varnostne) ogroženosti na nacionalni ali širši teritorialni ravni.

Univerzitetna založba
Univerze v Mariboru

3 Strategije, usmeritve in strokovni viri na področju ocenjevanja in obvladovanja tveganj

3.1 Strateška in zakonodajna podlaga Evropske unije

Na območju EU živi približno 500 milijonov ljudi v 27 državah, ki tvorijo unijo. Gospodarska rast in povečana mobilnost, skupaj s priložnostmi, ki jih ponuja svobodna in demokratična družba, ki temelji na pravni državi, ustvarjata blaginjo med evropskimi državljani. Toda s takšnimi razvojnimi trendi in priložnostmi prihajajo tudi najrazličnejša tveganja. Pri tem nevarnosti za blaginjo predstavljajo tako naravne nesreče kot škodljiva vedenja, ki so po svoji naravi kriminalna in izvirajo iz človeške dejavnosti.

Področje ocenjevanja tveganj je znotraj koncepta obvladovanja tveganj naravnih nesreč (DRM) v EU pridobilo večji pomen že leta 2009, ko je bilo sklenjeno, da mora Evropska komisija spodbuditi približevanje (harmonizacijo) ocen tveganj po posameznih državah članicah in na podlagi primerjave nacionalnih pristopov primerjati rezultate ter se osredotočiti na skupen (evropski) pristop za določitev metodologij ocene tveganj. Takšen pristop naj bi vodil k obvladovanju in upravljanju tveganj zaradi naravnih nesreč na ravni celotne EU, zlasti v smislu dajanja

prednostnih nalog skupnim naložbam in dejavnostim. Za pripravo primerljivih rezultatov nacionalnih pristopov ocenjevanja tveganj je bilo predvideno približevanje konceptov in metodologij. Do danes je bila ta praksa izvedena dvakrat (2012, 2019), v tretjem krogu pa je bilo pričakovano, da bodo do konca leta 2020 posodobljeni nacionalni regulativni organi. Tretji pregled naj bi Evropska komisija tako izdelala leta 2021 (Pursiainen in Rød, 2021).

Evropska komisija pri pripravi skupnega pristopa in določitev standardov za ocenjevanje tveganj ni izhajala iz začetka. Področje proučevanja tveganj in njihovega ocenjevanja je raziskano z več zornih kotov (za pregled glej Kuipers idr., 2018). Proučevanje ocenjevanja tveganj je pravzaprav uveljavljeno multidisciplinarno akademsko področje, z objavami v številnih recenziranih revijah in učbenikih (Aven, 2015, 2016; Coleman, 2012; Ostrom in Wilhelmsen, 2012; Pritchard, 2014). Vse to znanje je vodilo k razvoju skupnih standardov na področju ocenjevanja tveganj. Najpomembnejši izmed standardov je standard Mednarodne organizacije za standardizacijo (ISO) 31000 za upravljanje tveganja. Evropska komisija je standard ISO 31000 določila kot osnovo za nacionalne regulativne organe v svojih prvih smernicah (European Commission, 2010) in je nadaljevala z uveljavljanjem standarda v svojih priporočilih ES/JRC (European Commission, 2019) tako kot številne druge mednarodne organizacije (OECD, 2018; United Nations Office for Disaster Risk Reduction, 2017).

Pristop, ki ga uveljavlja Evropska komisija, je pristop ocenjevanja vseh nevarnosti (ang. *all-hazard approach*). Iz smernic Evropske komisije (Commission notice: Reporting guidelines on disaster risk management, Art. 6(1)d of Decision No 1313/2013/EU, 2019; Poljansek idr., 2019) izhaja, da bodo nacionalni regulativni organi svoje dejavnosti izvajali na pristopu (ocene) vseh nevarnosti, namesto da bi se osredotočali zgolj na določene vrste nevarnosti, kot so terorizem ali naravne nesreče. Ta pristop je formaliziran v Strategiji notranje varnosti (Council of the European Union. General Secretariat of the Council, 2010), kjer je bila naloga ocenjevanja tveganj na evropski ravni opredeljena kot dejavnost, ki zajema tako naravne nesreče kot nesreče, ki jih povzroči človek. V podrobnejših definicijah običajno ločimo med neškodljivimi in zlonamernimi nevarnostmi, ki jih povzroči človek, tehnološke nevarnosti pa se pogosto razumejo kot ločena kategorija tveganj.

Strategije in konkretnejše usmeritve EU glede pristopov k zagotavljanju varnosti in na področju izvajanja ocenjevanja tveganj so sicer zajete v različnih dokumentih, ki jih podrobneje opisujemo v naslednjih podpoglavjih.

3.1.1 Evropska varnostna strategija

Evropski svet je decembra 2003 sprejel Evropsko varnostno strategijo. Evropska varnostna strategija je dokument, ki temelji na vrednotah EU in v katerem je EU prvič določila jasne cilje in načela za napredovanje varnostnih interesov. V hitro spreminjajočem se svetu EU sicer velja za enega najvarnejših delov sveta, vendar tega ne smemo jemati kot samoumevno, saj se krajina varnostnih groženj v Evropi hitro spreminja. Evropska varnostna strategija temelji na principu, da je varnost skupna odgovornost. 24. julija 2020 je bila objavljena nova strategija za naslednjih 5 let (2020–2025), s poudarkom na podpori članic k spodbujanju varnosti za vse tiste, ki živijo v Evropi (European Commission, 2020).

Strategija opredeljuje strateške prednostne naloge in ustrezna orodja ter ključne ukrepe za celostno obravnavo digitalnih in fizičnih tveganj v celotnem ekosistemu varnostne unije. Med ključne varnostne grožnje EU umešča kibernetsko kriminaliteto, hibridne napade, teroristične napade in dejavnosti organiziranih kriminalnih združb.

Med temeljne skupne cilje strategija umešča:

- Krepitev zmogljivosti za zgodnje odkrivanje in preprečevanje kriz ter hitro odzivanje nanje, kar med drugim zajema vzpostavitev zmogljivosti za zgodnje odkrivanje varnostnih kriz in hitro odzivanje nanje s celostnim in usklajenim pristopom, na podlagi obstoječih pobud in orodij (tudi s področja civilne zaščite). Skladno s tem bo Evropska komisija podala predloge za obsežen sistem kriznega upravljanja, ki bi bil lahko pomemben tudi za varnost.
- Osredotočenost na rezultate: uspešnost in učinkovitost strategije temelji na skrbni oceni groženj in tveganj in kakovostni informacijski podpori.
- Povezovanje vseh akterjev v javnem in zasebnem sektorju z namenom sodelovanja. Odpraviti je treba nenaklonjenost deležnikov k izmenjavi

> informacij in zagotoviti tesnejše sodelovanje med državami članicami, vključno z organi kazenskega pregona, pravosodnimi in drugimi javnimi organi, institucijami in agencijami EU (npr. Eurojust, Europol), da bi dosegli razumevanje in izmenjavo, ki sta potrebna za skupne rešitve. Ključnega pomena je tudi sodelovanje z zasebnim sektorjem, saj ima v lasti ključno infrastrukturo, ki je potrebna za učinkovit boj proti kriminaliteti in terorizmu ter drugimi deležniki na področju izobraževanja in ozaveščanja.

Med glavne strateške prednostne naloge pa strategija umešča razvoj varnostnega okolja, primernega za prihodnost (krepitev zaščite in odpornosti kritične infrastrukture, kibernetske varnosti, varovanje javnih prostorov); obravnavanje spreminjajočih se groženj (razvoj kapacitet na področju kibernetske kriminalitete, sodobnih pristopov h kazenskemu pregonu, hibridnih groženj); zaščita državljanov EU pred terorizmom in organizirano kriminaliteto (s poudarkom na agendi in akcijskih načrtih za boj proti terorizmu, radikalizaciji, organizirani kriminaliteti, drogam, trgovini s strelnim orožjem, okoljski kriminaliteti in tihotapljenju migrantov); trden evropski varnostni ekosistem (sodelovanje in izmenjava informacij, krepitev raziskav in inovacij na področju varnosti, krepitev varnosti zunanjih meja, razvoj znanj, spretnosti in ozaveščanje).

3.1.2 Strategija zagotavljanja notranje varnosti

Področje zagotavljanja notranje varnosti je treba razumeti kot širok in celovit sistem, ki sega na več področij in obsega več sektorjev, namen pa je zagotoviti učinkovito spopadanje z velikimi grožnjami in grožnjami, ki neposredno vplivajo na življenja, varnost in dobro počutje državljanov, vključno z naravnimi (npr. potresi, poplave, požari, neurja) in drugimi nesrečami ter tveganji, ki jih lahko povzroči človek. Pri zagotavljanju notranje varnosti EU je bistvenega pomena predvsem sodelovanje organov pregona in mejnih organov, pravosodnih organov in drugih služb (npr. v zdravstvenem, socialnem in civilnem sektorju).

Evropska strategija notranje varnosti (*Internal security strategy for the European Union*) izhaja iz predpostavke, da je treba zagotoviti in izkoristiti potencialne sinergije, ki izhajajo iz sodelovanja na področju kazenskega pregona, integriranega upravljanja meja, kazenskega pravosodja in civilne zaščite. V bistvu so dejavnosti, ki spadajo na

področje zagotavljanja pravic, svobode in varnosti, neločljive: strategija notranje varnosti mora zagotoviti, da se dejavnosti na različnih področjih dopolnjujejo in medsebojno krepijo. EU stremi k razvoju varnostnega modela, ki temelji na načelih in vrednotah EU: spoštovanju človekovih pravic in temeljnih svoboščin, pravne države, demokracije, dialoga, strpnosti, preglednosti in solidarnosti (Council of the European Union. General Secretariat of the Council, 2010).

Skupne grožnje in tveganja (terorizem, resna in organizirana kriminaliteta, kibernetska kriminaliteta, čezmejna kriminaliteta, množično nasilje, naravne in s strani človeka povzročene nesreče) je treba obravnavati s celostnim pristopom, kar predstavlja glavni cilj strategije notranje varnosti. Vse to se lahko aplicira preko varnostnega modela, katerega temeljna načela so:

1. pravica, svoboda in varnostna politika, ki se medsebojno krepijo ob spoštovanju temeljnih pravic, mednarodne zaščite, pravne države in zasebnosti;
2. zaščita vseh državljanov, zlasti najbolj ranljivih skupin, kot so žrtve kaznivih dejanj (trgovina z ljudmi, spolno nasilje, žrtve terorizma);
3. preglednost in odgovornost v varnostnih politikah, ki jih državljani dobro razumejo;
4. dialog kot sredstvo za reševanje razlik v skladu z načelom strpnosti, spoštovanja in svobode izražanja;
5. integracija, socialna vključenost in boj proti diskriminaciji, ki predstavlja ključni element notranje varnosti EU;
6. solidarnost med državami članicami pred izzivi, s katerimi se ne morejo soočiti, še posebno če delujejo same, in
7. medsebojno zaupanje kot ključno načelo za uspešno sodelovanje.

Na podlagi teh načel je bilo določenih deset smernic za oblikovanje evropskega varnostnega modela, da bi zagotovili notranjo varnost EU:

1. Širok in celovit pristop k notranji varnosti.

Notranja varnost zajema ukrepe tako na horizontalni kot vertikalni dimenziji, in sicer:

- Horizontalna dimenzija: da se doseže ustrezna raven notranje varnosti v zapletenem globalnem okolju, je potrebno sodelovanje organov pregona, pravosodnih organov, agencij za civilno zaščito, političnega, gospodarskega, finančnega, socialnega in zasebnega sektorja ter nevladnih organizacij.
- Vertikalna dimenzija: nanaša se predvsem na mednarodno sodelovanje, varnostne politike na ravni EU, pobude, regionalno sodelovanje med državami članicami ter nacionalne, regionalne in lokalne politike znotraj držav članic.

2. Zagotavljanje učinkovitega demokratičnega in sodnega nadzora varnostnih dejavnosti.

Lizbonska pogodba je privedla do povečanega sodelovanja Evropskega parlamenta pri razvoju varnostnih politik. Nacionalni parlamenti imajo prav tako večjo vlogo pri spremljanju uporabe načela subsidiarnosti, prav tako pa ocenjujejo izvajanje politik s področja zagotavljanja pravic, svobode in varnosti. Na tem področju postane sodišče EU v celoti pristojno, izjemo predstavlja notranja zakonodaja in pravni red držav članic in njihove varnostne odgovornosti. Zavezanost EU k Evropski konvenciji o varovanju človekovih pravic prav tako prispeva k boljši zaščiti za pravice ljudi v Evropi.

3. Preprečevanje in predvidevanje: proaktiven pristop na podlagi zbranih informacij.

Med glavnimi cilji notranje varnostne strategije so preprečevanje in predvidevanje kriminalitete, naravnih nesreč in nesreč, ki jih povzroči človek, ter ublažitev njihovega negativnega vpliva. Bistvenega pomena pa je predvsem učinkovit pregon storilcev kaznivih dejanj poleg tega pa tudi osredotočenost na preprečevanje kriminalnih dejanj in terorističnih napadov, preden se zgodijo. Strategija poudarja preprečevanje in predvidevanje, ki temelji na proaktivnem pristopu na podlagi zbranih informacij ter dokazov, potrebnih za pregon. Treba je razviti strateški pristop k preprečevanju in predvidevanju nesreč ter nadaljevati z izboljšanjem

pripravljenosti in odzivnosti, razvojem smernic za metode, ocene in analize nevarnosti ter tveganj. Pri tem pa je ključnega pomena, da se identificirajo nove grožnje.

V tem kontekstu je treba izboljšati tudi mehanizme preprečevanja, kot so analitična orodja ali sistemi zgodnjega opozarjanja.[4] Preventivne varnostne politike morajo poleg organov pregona vključiti tudi druge institucije in strokovnjake na nacionalni in lokalni ravni. Potrebno je sodelovanje s šolami, univerzami in izvajati morebitna druga izobraževanja ter usposabljanja, ki bi preprečevala, da bi se mladi zatekali h kriminaliteti. Zasebni sektor, ki je vključen v finančne dejavnosti, lahko prispeva k razvoju in učinkovitemu izvajanju mehanizmov za preprečevanje goljufivih dejavnosti ali pranja denarja. Pri tem so izrednega pomena tudi civilne družbe pri izvajanju kampanj za ozaveščanje javnosti.

4. Razvoj celovitega modela za izmenjavo informacij.

Notranja varnostna politika mora biti podprta z izmenjavo informacij na podlagi medsebojnega oz. vzajemnega zaupanja. To pomeni, da če želijo organi pregona pravočasno ukrepati, morajo imeti dostop do vseh podatkov o kaznivih dejanjih, morebitnih storilcih, načinu delovanja, žrtvah in podobno. Zato je pomembno krepiti in izboljšati mehanizme, ki gradijo medsebojno zaupanje med organi, ki so pristojni za zagotavljanje notranje varnosti v EU. Model bi moral vključevati različne baze podatkov EU, ki so pomembne za zagotavljanje varnosti v EU, če je to potrebno in dovoljeno za namen zagotavljanja učinkovite izmenjave informacij po vsej EU. Pri tem je pomembno, da model izmenjave informacij v celoti spoštuje pravico do zasebnosti in varstva osebnih podatkov.

5. Operativno sodelovanje.

Z Lizbonsko pogodbo je bil ustanovljen stalni odbor za operativno sodelovanje na področju notranje varnosti za zagotovitev učinkovitega usklajevanja in sodelovanja med organi pregona in organi za upravljanje meja (*Standing Committee on Operational Cooperation on Internal Security* – COSI). COSI mora zagotoviti sodelovanje med

[4] Primer tega je evidenca imen letalskih potnikov *European passenger names record* (PNR), ki zagotavlja visoko raven zaščite podatkov za namen preprečevanja, odkrivanja, preiskovanja in pregona terorističnih kaznivih dejanj in hudih kaznivih dejanj.

agencijami EU in organi, vključenimi v notranjo varnost EU, da bi zagotovil usklajeno, integrirano in učinkovito delovanje. Naloga EU bi med drugim morala biti spodbujanje celostnega pristopa pri preprečevanju morebitnih kriz – izvajanje evropske medsebojne pomoči in solidarnosti.

6. Pravosodno sodelovanje v kazenskih zadevah.

Izrednega pomena je sodelovanje med pravosodnimi organi držav članic, poleg tega pa tudi to, da agencija oz. urad za evropsko pravosodno sodelovanje (Eurojust) doseže potencial v okviru veljavne zakonodaje. Na ravni EU je za uspešne kriminalistične preiskave treba uresničiti in zagotoviti sinergijo med organi pregona in mejnimi agencijami ter pravosodnimi organi.

7. Integrirano upravljanje meja.

Treba je okrepiti mehanizem integriranega upravljanja meja, da bi se tako razširila najboljša praksa med mejnimi policisti. Poseben poudarek je treba nameniti nadaljnjemu razvoju evropskega sistema za nadzor meja (Eurosur). Ključna vprašanja za uspeh predstavlja sodelovanje in usklajevanje Evropske agencije za mejno in obalno stražo (Frontex) z drugimi agencijami EU in organi kazenskega pregona držav članic. Pomembno vlogo pri upravljanju meja predstavljajo nove tehnologije, kar pomeni, da lahko državljani lažje prehajajo zunanje mejne prehode skozi avtomatizirane sisteme in predhodne registracije. Vse to izboljša varnost, saj uvedba nadzora omeji ljudem ali blagu, da bodisi prečkajo mejo ali vstopijo v EU. V tem primeru je bistvenega pomena sodelovanje med organi pregona in organi mejne kontrole. Vizumski protokoli, razvoj schengenskega informacijskega sistema, elektronski sistemi mejne kontrole bodo prispevali k integriranemu upravljanju meja. Pomembno vlogo imata tudi ureditev sodelovanja s tretjimi državami in tranzita – izgradnja zmogljivosti za kontrolo meja.

8. Zavezanost k inovacijam in usposabljanju.

Ključnega pomena je sodelovanje pri spodbujanju in razvoju novih tehnologij s skupnim pristopom, zmanjšanje stroškov ter s tem povečanje učinkovitosti. EU bi morala na podlagi rezultatov raziskav in razvojnih projektov razvijati tehnološke standarde, prilagojene njenim varnostnim potrebam. Izrednega pomena je strateški

pristop k strokovnemu usposabljanju v Evropi, predvsem pri organih pregona in organih za upravljanje meja, ki imajo opravka z napredno tehnologijo. Treba je omogočiti usposabljanje evropskih organov, saj se na ta način pospeši nadnacionalno sodelovanje. Vse to se lahko doseže preko nacionalnega usposabljanja in programov izmenjave, kot je Erasmus. Ključno vlogo pri tem imajo evropske agencije, zlasti Agencija EU za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (CEPOL).

9. Zunanja dimenzija notranje varnosti/sodelovanje s tretjimi državami.

Sistem notranje varnosti ne more obstajati brez zunanje dimenzije, saj je notranja varnost vedno bolj odvisna od zunanje varnosti. Mednarodno sodelovanje EU in njenih držav članic je pomembno za zagotavljanje varnosti in zaščit pravic državljanov ter spodbujanje varnosti in spoštovanja pravic v tujini. Politike EU, ki se nanašajo na tretje države, morajo upoštevati varnost kot ključni dejavnik in razviti mehanizme za usklajevanje med varnostnimi in zunanjimi politikami. Varnostna vprašanja morajo biti upoštevana v integriranem in proaktivnem pristopu.

EU se z vidika zunanje varnosti ne sme omejiti le na sodelovanje med organi pregona držav članic. Treba je graditi odnose tudi z drugimi državami preko globalnega pristopa k varnosti in sodelovanja z njimi. Nujno je izboljšati sodelovanje in usklajevanje z mednarodno organizacijo kriminalistične policije (Interpol) in razviti dvostranski in večstranski pristop med državami članicami. Pomembna so tudi prizadevanja za boj proti transnacionalni kriminaliteti zunaj EU in krepitvi spoštovanja pravne države. Treba je okrepiti sodelovanje med organi pregona ter organi za pravosodje, svobodo in varnost v vseh fazah civilnega kriznega upravljanja. Posebno pozornost potrebujejo šibke oz. slabo razvite države, da ne postanejo središče organizirane kriminalitete ali terorizma.

10. Prilagodljivost za prilagajanje prihodnjim izzivom.

V razvoju notranje varnosti EU se je treba osredotočiti na razvoj prožnega in realističnega pristopa, ki se je zmožen prilagajati realnosti oz. situacijam, ob upoštevanju tveganj in groženj, ki bi lahko vplivale na državljane. Treba je ustvariti varnost v širšem kontekstu, prav tako pa je pomembno prilagajanje spreminjajočim se okoliščinam in zagotavljanju najvišje ravni varnosti za prebivalce Evrope.

3.2 Ureditev Evropske unije o izvajanju nacionalnih ocen tveganja

Svet Evropske unije (v nadaljevanju Svet) si prizadeva za vzpostavitev sistematičnega ocenjevanja nacionalnovarnostne ogroženosti in poenotenost metodologij med državami članicami. V nadaljevanju predstavljamo Sklepe Sveta s tega področja iz let 2011 in 2013.

3.2.1 Sklepi Sveta o nadaljnjem razvoju ocene tveganja na področju obvladovanja nesreč v Evropski uniji

Sklepi Sveta o nadaljnjem razvoju ocene tveganja na področju obvladovanja nesreč v Evropski uniji (*Council Conclusions on Further Developing Risk Assessment for Disaster Management within the European Union* (Council of the European Union, 2011), sprejeti na srečanju Sveta v Luxembourgu, poudarjajo pomembnost sistematičnega pristopa k ocenjevanju nacionalnovarnostne ogroženosti, ki vključuje metode identificiranja groženj, ocenjevanja posledic in tveganj, mapiranja tveganj in razvoja scenarijev. Države članice se spodbuja k nadaljnjemu razvoju metodologij, ki naj vključujejo večje naravne in človeško povzročene nesreče ter upoštevajo vplive podnebnih sprememb. Ocene morajo biti utemeljene na dokazih, države pa naj se osredotočijo na vrednotenje ranljivosti, verjetnosti in vplivov. Prizadevati si je treba za poenotenost metodologij med državami članicami, kar bo omogočilo primerljivost rezultatov in skupen odziv EU na skupne grožnje. Komisijo EU se povabi k prevzetju aktivne vloge v spodbujanju razvoja nacionalne ocene tveganj v državah članicah, iskanju dobrih praks, razvoju smernic in informiranju držav članice.

Državam članicam pa so bile podane naslednje usmeritve:

a) Države naj določijo enotno kontaktno točko za usklajevanje dela v izdelavi nacionalnih ocen tveganj.
b) Zagotoviti je treba usklajenosti med ključnimi deležniki pri različnih tveganjih, da bi se spodbudilo enotno razumevanje terminologije tveganj in opredelilo metodologijo ter oceno scenarijev tveganja.
c) Širši javnosti in zainteresiranim stranem je treba zagotoviti ustrezne neobčutljive informacije – rezultate ocen tveganja, da bi se povečale ozaveščenost, preventiva in pripravljenost.

d) Države naj identificirajo in analizirajo scenarije na področju posameznega tveganja in si prizadevajo za upoštevanje možnosti scenarijev, ki vključujejo več tveganj (ang. *multi-risk*).
e) V izvajanju nacionalne ocene tveganj naj države upoštevajo dobre prakse in vodila, ki jih razvija Evropska komisija.
f) Kjer je to mogoče, naj se uporabijo kvalitativne in kvantitativne metode pri ocenjevanju tveganj.
g) Rezultati nacionalnih ocen tveganj naj se upoštevajo pri načrtovanju zmogljivosti, preventivnih ukrepov in pripravljenosti, kot načina spodbujanja nadaljnjega razvoja nacionalne politike obvladovanja tveganj, povezanih z nesrečami (ob spoštovanju obstoječe sektorske zakonodaje EU).
h) Da bi razvili tesnejše sodelovanje na področju upravljanja tveganj, je potrebna izmenjava informacij in dobrih praks z drugimi državami članicami in Komisijo, zlasti glede podobnih in skupnih tveganj.

Do konca leta 2011 naj države članice Komisiji posredujejo informacije glede napredka in metod, ki se uporabljajo za izvajanje nacionalne ocene tveganj; nezaupne informacije glede scenarijev in rezultatov ocen; opis vplivov scenarijev na različna področja (okoljski, človeški, gospodarski vplivi); seznam scenarijev tveganj in ostale potencialno pomembne informacije.

3.2.2 Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite iz leta 2013

Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance) iz leta 2013 (s spremembo Sklepa EU 2019/420 in Uredbe EU 2021/836)[5] je namenjen krepitvi sodelovanja med EU

[5] V letih 2019 in 2021 je bil omenjeni sklep spremenjen z Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism (Sklep (EU) 2019/420 Evropskega parlamenta in Sveta z dne 13. marca 2019 o spremembi Sklepa št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite) in Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection

in državami članicami na področju civilne zaščite ter olajšanju usklajevanja. Z njim se uvaja kakovosten, celovit in stroškovno učinkovit pristop k upravljanju nesreč. Sklep se uporablja za sodelovanje na področju civilne zaščite, kar vključuje dejavnosti na področju preventive in pripravljenosti Unije in dejavnosti pomoči pri odzivanju na nesreče.

Posebni cilji mehanizma so:

- Visoka raven zaščite pred nesrečami:
  - s preprečevanjem ali zmanjševanjem njihovih morebitnih posledic,
  - s spodbujanjem preventivne kulture in
  - z izboljšanjem sodelovanja med službami civilne zaščite in drugimi pristojnimi službami.
- Dvig pripravljenosti na nacionalni ravni in na ravni EU za odziv na nesreče.
- Lajšanje hitrega in učinkovitega odziva ob nesrečah ali grožnjah nesreč, tudi s sprejetjem ukrepov za blažitev neposrednih posledic nesreč.
- Povečanje ozaveščenosti javnosti o nesrečah in njene pripravljenosti nanje.
- Povečanje razpoložljivosti in uporabe znanstvenih spoznanj o nesrečah.
- Okrepitev sodelovanja in usklajevanja na čezmejni ravni in med državami članicami, ki so izpostavljene enakim vrstam nesreč.

Mehanizem določa tudi, da države članice spodbujajo usklajen in učinkovit pristop k preventivi pred nesrečami in pripravljenosti nanje skozi izmenjavo informacij, ki niso občutljive narave, in v ta namen pripravijo ocene tveganj na nacionalni ravni ter osnovne informacije glede tega vsake tri leta sporočijo Komisiji, ki ji prav tako vsake tri leta predložijo oceno svojih zmogljivosti obvladovanja tveganj. Mehanizem za potrebe zagotavljanja pripravljenosti ustanovi tudi Center za usklajevanje nujnega odziva (ERCC), ki neprekinjeno zagotavlja operativne zmogljivosti.

Mechanism (Uredba (EU) 2021/836 o spremembi Sklepa št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite).

Dodatna orodja v okviru mehanizma so še:

- skupni komunikacijski in informacijski sistem za nujne primere, orodje IT za takojšnje obveščanje med državami članicami mehanizma Unije v nujnih primerih;
- vaje in program usposabljanja za povečanje zmogljivosti držav članic za odzivanje na nesreče in boljšo usklajenost pomoči civilne zaščite;
- moduli civilne zaščite, tj. enote osebja in opreme, ki jih je mogoče hitro aktivirati;
- evropski nabor civilne zaščite, tj. prostovoljni nabor predhodno odrejenih odzivnih zmogljivosti držav članic za pomoč ob nesrečah, pripravljenih za aktiviranje v primeru evropskih operacij civilne zaščite – to vključuje zelo kakovostne module s skupinami za pomoč, strokovnjake in opremo ter višje stopnje sofinanciranja EU.

S spremembo sklepa iz leta 2019 se uvajajo spremembe, ki dodatno krepijo skupno zmogljivost EU za preprečevanje naravnih nesreč ter pripravo in odzivanje nanje. Od držav članic se denimo zahteva, da nadalje razvijajo ocenjevanje zmožnosti obvladovanja tveganj na nacionalni ali ustrezni podnacionalni ravni; Evropski komisiji vsaka tri leta zagotovijo povzetek pomembnih elementov ocen s poudarkom na ključnih tveganjih; prostovoljno sodelujejo pri medsebojnih pregledih ocenjevanja zmožnosti obvladovanja tveganj. Spremembe od Komisije zahtevajo, da vzpostavi mrežo ustreznih akterjev in ustanov na področju civilne zaščite in obvladovanja nesreč, vključno s centri odličnosti, univerzami in raziskovalci, za izboljšanje usposabljanja in izmenjave znanja. Ti skupaj s Komisijo tvorijo mrežo znanja Unije na področju civilne zaščite. S spremembo se vzpostavi tudi »*rescEU*«, dodatni nabor zmogljivosti za zagotavljanje pomoči v razmerah, v katerih celotne obstoječe zmogljivosti na nacionalni ravni in zmogljivosti, ki so jih države članice predhodno dodelile evropskemu naboru civilne zaščite, ne zadostujejo za zagotavljanje učinkovitega odziva.

Z uredbo iz leta 2021 se je sklep spremenil v smeri krepitve mehanizma, ki državam članicam omogoča, da se bolje pripravijo in hitreje ter učinkoviteje odzivajo na prihodnje krize s čezmejnimi posledicami (kot je kriza, povezana s covidom-19). S

to spremembo so ERCC dodeljene tudi okrepljene operativne, analitične, spremljevalne in komunikacijske možnosti.

3.3 Strateške usmeritve v Republiki Sloveniji

Nacionalnovarnostna politika Republike Slovenije (RS) je celota vizije, strategij, programov, načrtov in dejavnosti države, potrebna za načrtovano odzivanje na vse vrste kriz, vire ogrožanja in tveganja za njeno nacionalno varnost ter uresničevanje njenih nacionalnovarnostnih ciljev, usmerjenih k zaščiti slovenskih nacionalnih interesov. Temeljni strateški dokument, ki ureja ureditev, cilje, ukrepe in usmeritve na področju zagotavljanja nacionalne varnosti v Sloveniji, je »Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-2)« (2019). Poleg te pa varnost v Sloveniji na nacionalni ravni urejajo še druge resolucije in strategije, npr. s področij naravnih nesreč, kriminalitete, prometa. Namen resolucij je predvsem v tem, da »spodbujajo številne državne, zasebne in vse druge oblike institucionalnega delovanja družbe ter vsakega posameznika k povezovanju, sodelovanju, razmišljanju in uresničevanju zagotavljanja varnosti na vseh ravneh z ukrepi, ki v največji mogoči meri izhajajo iz realno zaznanih in ovrednotenih virov ogrožanja« (Anželj, 2011).

V nadaljevanju so podrobneje opisane tovrstne strateške usmeritve v Sloveniji s poudarkom na ciljih, ukrepih in ključnih deležnikih.

3.3.1 Resolucija o strategiji nacionalne varnosti Republike Slovenije

Državni zbor RS je 20. decembra 1993 sprejel »Resolucijo o izhodiščih zasnove nacionalne varnosti Republike Slovenije« (1993). Dokument je bil podlaga za »Resolucijo o strategiji nacionalne varnosti Republike Slovenije (ReSNV)«, ki je bila sprejeta 2001 in nato posodobljena leta 2010 (»ReSNV-1«, 2010) in leta 2019 (»ReSNV-2«, 2019). V »ReSNV-2« (2019) so opisani in opredeljeni:

- nacionalni interesi in nacionalnovarnostni cilji RS,
- viri ogrožanja varnosti in varnostna tveganja države,
- varnostno okolje,
- izhodišča politike odzivanja RS na posamezne varnostne grožnje in tveganja,
- najširše sistemsko-organizacijske rešitve celovitega delovanja države pri zagotavljanju nacionalne varnosti.

Slovenija ima za zagotavljanje nacionalne varnosti oblikovan sistem nacionalne varnosti, ki temelji na političnih, pravnih, gospodarskih, socialno-zdravstvenih, informacijskih, infrastrukturnih, znanstveno-tehnoloških, izobraževalnih ter drugih temeljih in zmogljivostih države. Zaradi prepletenosti in kompleksnosti groženj ter tveganj je v tem sistemu zahtevano povezovanje in sodelovanje več organizacij in akterjev.

Zagotavljanje nacionalne varnosti RS temelji na delovanju:

1. obrambnega sistema, ki ga tvorita vojaška (Slovenska vojska (SV)) in civilna obramba (organi lokalnih skupnosti, državljani in civilnodružbene organizacije, katerih dejavnosti so posebnega pomena za obrambo)
2. sistema notranje varnosti, ki ga tvorijo slovenska policija, državno tožilstvo in sodstvo, inšpekcijski in nadzorni organi, obveščevalno-varnostne službe, drugi državni organi in organizacije z javnimi pooblastili, zasebne varnostne družbe in druge organizacije zasebnega prava ter organi lokalne samouprave.
3. sistema varstva pred naravnimi in drugimi nesrečami, ki ga tvorijo prebivalci RS, bodisi kot posamezniki bodisi prostovoljno organizirani v društva, strokovna združenja ter druge nevladne organizacije, ki opravljajo dejavnost, pomembno za varstvo pred naravnimi in drugimi nesrečami, javne reševalne službe, gospodarske družbe, zavodi in druge organizacije ter lokalne skupnosti in država.

Poleg tega vključuje tudi podsisteme sistema nacionalne varnosti in zunanjepolitične, gospodarske, informacijske ter druge dejavnosti, ki neposredno vplivajo na nacionalno varnost.

V Sloveniji so v upravljanje in vodenje sistema nacionalne varnosti vključeni organi zakonodajne in izvršilne veje oblasti, in sicer:

- Državni zbor, ki določa zakonske okvire in dolgoročne smernice razvoja nacionalnovarnostne politike in sistema nacionalne varnosti ter sprejema državni proračun, s pomočjo katerega se uresničuje nacionalna varnost.
- Predsednik republike, ki je vrhovni poveljnik obrambnih sil RS.

- Vlada RS, ki predstavlja politično-izvršilno raven upravljanja in vodenja sistema nacionalne varnosti. Usmerja in usklajuje izvajanje nacionalnovarnostne politike, delovanje sistema nacionalne varnosti na vseh ravneh in v ta namen sprejema potrebne politične, pravne, organizacijske, finančne in druge ukrepe.
- Svet za nacionalno varnost (SNaV), ki usklajuje nacionalnovarnostno politiko ter usmerja in usklajuje dejavnosti, ki se izvajajo zaradi uresničevanja interesov in ciljev nacionalne varnosti RS. Je vladni svetovalni in usklajevalni organ za področje nacionalne varnosti. Dejavnosti za delovanje SNaV operativno usklajuje njegov sekretariat. Analitično in strokovno podporo sekretariatu opravlja operativna skupina sekretariata. SNaV je med drugim pristojen za sprejemanje ukrepov in aktov s področja nacionalne varnosti, svetovanje ministrstvom, usklajuje mnenja in dejavnosti ugotavlja in ocenjuje varnostna tveganja, ogrožanje države ter ukrepe in usmeritve za zagotavljanje nacionalne varnosti. Sestavljajo ga predsednik vlade, podpredsednik vlade, ministri, pristojni za notranje zadeve, zunanje zadeve in finance.
- Nacionalni center za krizno upravljanje (notranja organizacijska enota Direktorata za obrambne zadeve na Ministrstvu za obrambo Republike Slovenije) je osrednji nacionalni organ za spremljanje in posredovanje v primeru uveljavitve ukrepov kriznega odzivanja na obrambnem področju v miru, izrednem in vojnem stanju ter za zagotavljanje prostorskih, tehničnih, informacijskih in telekomunikacijskih pogojev za delovanje vlade in teles kriznega upravljanja v krizah, pojavih in izrednih dogodkih, ki lahko pomembno ogrozijo nacionalno varnost. Zagotavlja informacijske in telekomunikacijske povezave za izmenjavo podatkov in informacij med državnimi organi in subjekti, vključenimi v krizno upravljanje, ter povezave za izmenjavo podatkov in informacij, skladno z mednarodnimi obveznostmi države. Opravlja naloge na področju upravnih zvez ter naloge zbiranja, obdelave in hrambe podatkov odgovornih oseb na področju kritične infrastrukture.

Nacionalni interesi RS se delijo na življenjske in strateške:

- Med življenjske interese sodijo: ohranitev neodvisnosti, suverenosti in ozemeljske celovitosti države ter ohranitev nacionalne identitete, kulture in samobitnosti slovenskega naroda.
- Med strateške interese sodijo: priznavanje in spoštovanje nedotakljivosti njenih mednarodno priznanih meja in državnega območja, delovanje demokratičnega parlamentarnega političnega sistema, spoštovanje človekovih pravic in temeljnih svoboščin, krepitev pravne in socialne države, blaginja prebivalcev in celovit razvoj družbe, zaščita življenja in visoka stopnja vseh oblik varnosti prebivalcev, zaščita pravic in razvoj slovenske avtohtone narodne skupnosti v sosednjih državah, mir, varnost in stabilnost v svetu ter ohranitev okolja in naravnih virov RS.

Slovenija svoje življenjske in strateške interese zagotavlja z uresničevanjem nacionalnovarnostnih ciljev preko delovanja vseh subjektov ter jasno določenih pristojnosti in procesov posameznih nosilcev in mehanizmov na področju nacionalne varnosti.

Nacionalnovarnostni cilji Slovenije so:

- zagotovitev visoke stopnje varnosti in blaginje RS ter njenih državljank in državljanov;
- zaščita in krepitev ustavnih načel, nacionalne identitete, kulture in samobitnosti slovenskega naroda;
- učinkovito delovanje pravne in socialne države;
- varovanje okolja;
- trajnostni razvoj gospodarstva;
- krepitev mednarodnega ugleda, politično-varnostnega položaja Slovenije;
- zagotavljanje strateških virov za krepitev vseh struktur nacionalnovarnostnega sistema;
- krepitev dobrih odnosov s sosednjimi in z drugimi državami;
- obramba Slovenije in sodelovanje pri odvračanju groženj.

Glavne grožnje, ki ogrožajo nacionalno varnost RS, so:

- hibridne grožnje;
- informacijsko-kibernetske grožnje;
- obveščevalna dejavnost tujih akterjev;
- vojaške grožnje;
- krizna žarišča;
- terorizem in nasilni ekstremizem;
- nedovoljene dejavnosti na področju konvencionalnega orožja, orožij za množično uničevanje ter jedrskih in raketnih tehnologij;
- hude in organizirane oblike kriminalitete;
- nezakonite migracije;
- podnebne spremembe;
- globalna finančna, gospodarska, tehnološka in socialna tveganja;
- ogrožanje javne varnosti;
- naravne in druge nesreče;
- omejenost naravnih virov in degradacija življenjskega okolja; ter
- zdravstveno-epidemiološke grožnje.

Odzivanje na tveganja in grožnje nacionalni varnosti poteka skozi uresničevanje nacionalnovarnostne politike, ki jo sestavljajo zunanja politika, obrambna politika, politika zagotavljanja notranje varnosti, migracijska politika ter politika varstva pred naravnimi in drugimi nesrečami.

V »ReSNV-2« (2019) je pri vsaki vrsti grožnje podana tudi opredelitev grožnje, pri nekaterih so navedeni tudi akterji, ki vplivajo na njen nastanek. Zatem je za vsako izmed groženj določeno, kako se nanjo odzvati, natančneje, kako se soočiti z grožnjo, kdo so pristojni organi (npr. obveščevalno-varnostne službe, vladne službe, policija, vojska, sistem zaščite in reševanja itd.) in kritična infrastruktura. V večini izmed odzivov je omenjeno tudi mednarodno sodelovanje (ponekod so poimensko navedene nekatere izmed mednarodnih organizacij, s katerimi bi v primeru uresničitve grožnje Slovenija sodelovala ali se povezovala, npr. EU, Nato, OZN, Interpol, Europol, Eurojust).

V resoluciji je zapisano tudi, da bo z namenom učinkovitega spremljanja in odzivanja na hitro spreminjajoče se varnostno okolje, letno izdelana nacionalna ocena varnostnih tveganj in groženj.

3.3.2 Resolucija o nacionalnem programu varstva pred naravnimi in drugimi nesrečami

Nacionalni program varstva pred naravnimi in drugimi nesrečami temelji na »ReSNV-2« (2019) in upošteva vse nevarnosti naravnih in drugih nesreč, ki ogrožajo ljudi, živali, premoženje, kulturno dediščino in okolje. Upošteva tudi naravne in druge danosti, ki vplivajo na nesreče in varstvo pred njimi, ter človeške in materialne vire, ki jih je mogoče uporabiti pri obvladovanju nevarnosti in varstvu ogroženih. Poleg nacionalnih interesov so upoštevane tudi obveznosti Slovenije, ki izhajajo iz sprejetih mednarodnih in regionalnih pogodb, konvencij in sporazumov ter sklenjenih dvostranskih sporazumov s področja varstva pred nesrečami (»Resolucija o nacionalnem programu varstva pred naravnimi in drugimi nesrečami v letih od 2016 do 2022 (ReNPVNDN16–22)«, 2016).

Program sledi splošnemu cilju varstva pred naravnimi in drugimi nesrečami, ki je: zmanjšati število nesreč ter preprečiti oz. ublažiti njihove posledice, da bi bilo življenje varnejše in bolj kakovostno. Usmerjen je v preventivo in zagotavljanje ustrezne pripravljenosti, ki omogoča hitro in učinkovito ukrepanje ob nesrečah.

Temeljni cilji varstva pred naravnimi in drugimi nesrečami (skupaj 17 ciljev, npr. prednostno preventivno ravnanje; usklajevanje ocen tveganj; povečevanje zmogljivosti opazovalnih omrežij; reorganizacija sil za zaščito, reševanje in pomoč na vseh ravneh; dograjevanje informacijsko-komunikacijske infrastrukture; reorganiziranje službe nujne medicinske pomoči; posodabljanje programov usposabljanja; dograjevanje reševalnih sestav SV itd.) so zastavljeni na podlagi ocen ogroženosti (tveganja), ki jih RS pripravlja v skladu z (»Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite«, 2014a). Državne ocene tveganja so tudi izhodišče za izdelavo načrtov zaščite in reševanja – priprava teh je natančneje opredeljena v Uredbi o vsebini in izdelavi načrtov zaščite in reševanja (2012), ki zavezuje Upravo RS za zaščito in reševanje, da na spletni strani objavi povzetke ocen z osnovnimi zaključki o možnosti nastanka nesreč.

V »ReNPVNDN16–22« (2016) so opredeljene tudi dejavnosti in ukrepi, ki jih bo Slovenija izvajala na šestih področjih: razvoj opazovalnih, informacijskih, komunikacijskih, logističnih in drugih sistemov za zaščito, reševanje in pomoč; razvoj preventivnih dejavnosti razvoj zmogljivosti ter sil za zaščito, reševanje in pomoč; usmeritve za izobraževanje in usposabljanje; raziskovalno-razvojno delo; odpravljanje posledic nesreč ter zagotavljanje finančnih in drugih sredstev za varstvo pred naravnimi in drugimi nesrečami; mednarodno sodelovanje.

Leta 2016 je Slovenija sprejela tudi Strateški okvir prilagajanja podnebnim spremembam, ki vključuje tudi oceno podnebnih sprememb do konca 21. stoletja, ki vključuje opredelitev vizije, ciljev, ukrepe za dosego ciljev, mednarodno primerjavo procesov prilagajanja in kazalce ranljivosti Slovenije.

3.3.3 Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2019–2023

Temeljni cilj »ReNPPZK19–23« (2019) je učinkovito oblikovanje in izvajanje politike preprečevanja in zatiranja kriminalitete oz. zagotavljanje takšnega družbenega okolja, ki bo dolgoročno vplivalo na zmanjšanje kriminalitete, zagotavljalo varnost, prebivanje in delo v varnem okolju, ter na podlagi predlaganih ukrepov doseči tako družbeno stanje, da bi se ljudje počutili varne.

Za ustrezno odzivanje na ogrožanje varnosti je odgovorna predvsem policija, ki naj bi s preostalimi subjekti (ministrstva, lokalna skupnost, nevladne organizacije in organizacije civilne družbe), pa tudi s partnerstvom med javnim in zasebnim (varnostnimi službami), ustvarjala razmere za uspešno spopadanje s kriminaliteto. Policija deli kriminaliteto na splošno in gospodarsko. Pri odkrivanju in preiskovanju kaznivih dejanj je ena od prednostnih nalog policije odkrivanje in preiskovanje gospodarskih kaznivih dejanj z veliko premoženjsko škodo, kaznivih dejanj v škodo slovenskega bančnega sistema, kriminalitete, ki posledično ogroža finančne interese slovenske države in EU, ter organiziranih oblik korupcije tam, kjer so korupcijska tveganja največja. Velik poudarek je tudi na izvajanju finančnih preiskav. Pri tem se je treba zavedati, da policija ni edina, ki se ukvarja s preprečevanjem in zatiranjem kriminalitete. Zelo pomembno vlogo pri zagotavljanju varnosti oz. varovanju ljudi in premoženja, v okviru svojih pristojnosti, imajo tudi družbe za zasebno varovanje ter občinska redarstva, organizirana v samoupravnih lokalnih skupnostih. Za

uspešno zatiranje in preprečevanje kriminalitete je ključno sodelovanje lokalnih, državnih in tudi mednarodnih organov, kajti kriminaliteta v sodobnem svetu je redko kdaj omejena le na eno državo.

Za pripravo resolucije je bila ustanovljena medresorska delovna skupina, v kateri so bili predstavniki z vseh ministrstev in predstavnik Fakultete za varnostne vede Univerze v Mariboru. Ob izdelavi resolucije je bila upoštevana tudi njena vključitev v že obstoječe strateške in razvojne cilje RS, čemur je bila prilagojena tudi metodologija. Sočasno je bila upoštevana tudi vključenost v strateške programe na mednarodni ravni in trajnost dejavnosti pri preprečevanju in zatiranju kriminalitete.

Podlaga za pripravo resolucije so področni resorni programi ter načrti in drugi akti, ki določajo ukrepe in naloge, ki lahko vplivajo na preprečevanje kriminalitete. Upoštevani so bili različni resorni strateški dokumenti in programi dela, povezani s preprečevanjem kriminalitete. Na mednarodni ravni so bili upoštevani akti in dokumenti Organizacije združenih narodov, EU, Organizacije za varnost in sodelovanje v Evropi ter Sveta Evrope. V resoluciji je navedeno še, da je bila posebna pozornost namenjena objektivnosti pripravljenih vsebin, natančni določitvi obsega obravnavanih problemov in sistematičnemu pristopu, ki za vsak identificiran problem navaja opis konkretnega problema, ugotavlja vzroke za takšno stanje in nakaže možne rešitve.

V resoluciji je skupaj opredeljenih 27 temeljnih ciljev (npr. ugotavljanje vzrokov in rešitev za kriminaliteto; več partnerskega sodelovanja; učinkovitejše sodelovanje z lokalnimi skupnostmi; ozaveščanje javnosti o nasilju, pravicah in možnih oblikah pomoči; vzpostaviti skupin kriminalistov za identifikacijo mladoletnih oseb, ki so žrtev spolnih zlorab in storilcev; kakovostnejše zbiranje dokazil v predkazenskih postopkih; krepitev mednarodnega sodelovanja in povezovanja na nacionalni ravni ter zagotoviti pravočasno izmenjavo informacij; izboljšate ukrepanje na področju organizirane kriminalitete, sovražnega govora, zlorab pri gospodarskem poslovanju, medicinskih ponaredkov, kibernetske varnosti itd.) in devet področij preprečevanja in zatiranja kriminalitete s specifičnimi cilji. Med ključna področja sodijo: varnost v lokalnih skupnostih (skupaj pet ciljev); nasilje nad ženskami, nasilje v družini, medvrstniško nasilje, nasilje na športnih prireditvah, nasilje nad otroki na svetovnem spletu (skupaj 15 ciljev); javno spodbujanje sovraštva in nestrpnosti – sovražni govor (dva cilja); gospodarska kriminaliteta pri varovanju finančnih interesov v RS in EU

(osem ciljev); korupcija in zaščita javnih sredstev (pet ciljev); ogrožanje javnega zdravja (sedem ciljev); informacijska varnost (štirje cilji); radikalizacija, ekstremno nasilje in terorizem (13 ciljev); hude in organizirane oblike kriminalitete (18 ciljev). Za vsako posamezno področje so poleg ciljev določeni tudi vzroki in rešitve ter strategije/programi, ki opisujejo ključne dejavnosti in ukrepe, nosilce načrtovanih dejavnosti in sodelujoče, roke za izvedbo strategije oz. programa in indikatorje za merjenje uspešnosti izvedenih nalog. Med nosilce sodijo predvsem policija in Ministrstvo za notranje zadeve (MNZ) ter druga ministrstva, med sodelujoče pa najrazličnejši deležniki (npr. Skupnost občin Slovenije, Združenje občin Slovenije, občine, civilna družba, ministrstva, centri za socialno delo, univerze in raziskovalne institucije, Nevladne organizacije, javne agencije, zbornice, skladi, Slovenski državni holding, inšpektorati, tožilstvo, odvetništvo, olimpijski komite, Varuh človekovih pravic Republike Slovenije, Urad Republike Slovenije za preprečevanje pranja denarja (URSPPD), Finančna uprava Republike Slovenije, Računsko sodišče, Urad Republike Slovenije za nadzor proračuna, vladne službe in vladni uradi, Komisija za preprečevanje korupcije, Zavod za zdravstveno zavarovanje Slovenije, Uradni list Republike Slovenije, Slovenska obveščevalno-varnostna agencija (SOVA), Obveščevalno-varnostna služba Ministrstva za obrambo idr.).

3.3.4 Resolucija o nacionalnem programu varnosti cestnega prometa

V tem strateškem dokumentu je opredeljen nacionalni program, ki vključuje opis stanja, ciljev in ukrepov za zagotavljanje trajnostnega in celostnega razvoja na področju varnosti cestnega prometa. Temelji na analizi obstoječega stanja varnosti cestnega prometa ter na vlogi in pomenu varnosti za gospodarski in družbeni razvoj (»ReNPVCP13–22«, 2013). Nacionalni program je usklajen s slovensko prometno politiko in politiko ter strategijo EU na področju varnosti v cestnem prometu. Temeljna vizija, zapisana v programu, je vizija nič – nič smrtnih žrtev in nič hudo telesno poškodovanih oseb zaradi prometnih nesreč v Sloveniji. Med glavna načela sodijo: uveljavljanje najboljših standardov varnosti, celovit pristop do varnosti, subsidiarnost, sorazmernost, uresničljivost, usklajenost, sledljivost, primerljivost, merljivost idr.

Skupni cilj držav članic EU je, da se do leta 2020 v cestnem prometu ohrani čim več življenj in prepolovi število žrtev in hudo telesno poškodovanih oseb. Temu cilju sledi tudi slovenski nacionalni program, katerega izvajanje mora zagotoviti, da na

slovenskih cestah konec leta 2022 ne bo umrlo več kot 70 oseb in se ne bo hudo telesno poškodovalo več kot 460 oseb.

Nacionalni program prav tako zelo natančno opredeli splošna in parcialna področja varnosti cestnega prometa (splošna: cestna infrastruktura; vozila; prometna vzgoja in vseživljenjsko učenje; zdravstvena oskrba ponesrečencev; nadzor; varnost in zdravje pri delu; pomoč žrtvam in svojcem žrtev prometnih nesreč. Parcialna: hitrost; alkohol, prepovedane droge in druge psihoaktivne snovi; vozniki motornih dvokoles; kolesarji; vozniki traktorjev; pešci; varnostni pas in otroški varnostni sedeži; mladi vozniki; starejši vozniki; prehodi cest preko železnice) za vsako področje pa so podrobno opredeljeni temeljni cilji, specifični cilji, dejavnosti in nosilci dejavnosti (npr. vrtci, starši, učitelji, mediji, Agencija za varnost prometa, občinski organi, ministrstva, zbornice, zveze, zdravstveni delavci, Nevladne organizacije, fakultete, policija, Slovenske železnice, Skupnost občin Slovenije, Združenje občin Slovenije, Avto-moto zveza Slovenije, Družba za avtoceste v Republiki Sloveniji itd.) po posameznih specifičnih ciljih.

Temeljne strateške usmeritve za zagotavljanje večje varnosti cestnega prometa v Sloveniji se opirajo na grobe analize prometnovarnostnih razmer in na izbor t. i. »uspešnih strategij in ukrepov«, ki jih priporočajo države članice EU z zadovoljivo prometno varnostjo. Po drugi stani pa nepredvidljive spremembe prometnih razmer zahtevajo vzpostavitev orodja, ki omogoča:

a) merjenje negativnih posledic cestnega prometa in primerjanje razvoja prometne varnosti znotraj EU; in
b) spremljanje doseganja ciljev in učinkovitosti zastavljene strategije in ukrepov.

V ta namen nacionalni program uvaja kazalce prometne varnosti, ki jih za uporabo na nacionalni ravni predlagajo evropske institucije in so osnova spremljanja razvoja prometne varnosti v EU. V nadaljevanju (tabela 1) predstavljamo kazalce uspešnosti oz. učinkovitosti zagotavljanja prometne varnosti. Ti kazalci tvorijo temeljno platformo za analitično spremljanje razmer prometne varnosti na strateški ravni.

Tabela 1: Kazalci uspešnosti oz. učinkovitosti zagotavljanja prometne varnosti (povzeto po »ReNPVCP13–22«, 2013)

SPLOŠNI KAZALCI	
Tveganje v cestnem prometu	Umrli na milijon prebivalcev. Umrli na 100.000 prebivalcev. Mrtvi na milijon prevoženih km.
POSEBNI KAZALCI	
Tveganje mladih v cestnem prometu	Delež umrlih in hudo telesno poškodovanih v cestnem prometu v populaciji med 15 in 24 letom.
Tveganje voznikov enoslednih motornih vozil: vozniki motornih koles, vozniki koles z motorji in mopedov	Delež umrlih in hudo telesno poškodovanih voznikov motornih koles v prometu motornih koles. Delež umrlih in hudo telesno poškodovanih voznikov koles z motorjem in mopedov. Delež umrlih potnikov na motornih kolesih, kolesih z motorjem ter mopedov. Delež uporabe zaščitne čelade za vse voznike enoslednih motornih vozil.
Tveganje pešcev	Delež umrlih in hudo telesno poškodovanih pešcev v prometnih nesrečah. Delež uporabe odsevnih materialov med pešci. Pešci po starostnih skupinah in spolu.
Tveganje kolesarjev	Delež umrlih in hudo telesno poškodovanih kolesarjev v prometu kolesarjev. Delež uporabe kolesarske čelade.
Tveganje starejših v cestnem prometu	Delež umrlih in hudo telesno poškodovanih v cestnem prometu v populaciji starostnikov nad 64 let.
VEDENJSKI KAZALCI PROMETNIH UDELEŽENCEV	
Hitrost	Delež umrlih in hudo telesno poškodovanih v prometnih nesrečah z alkoholom kot sekundarnim vzrokom. Povprečna hitrost. Varianca hitrosti. Delež vozil, ki prekoračujejo omejitev hitrosti (za 10 km/h). Vrsta ceste in vozila. Dan v tednu in ura.
Alkohol in droge	Delež umrlih in hudo telesno poškodovanih v prometnih nesrečah z alkoholom kot vzrokom. Delež poškodovanih v prometnih nesrečah z alkoholom kot vzrokom. Delež alkoholiziranih voznikov v cestnem prometu. Delež umrlih in poškodovanih v prometnih nesrečah z prepovedanimi drogami kot vzrokom.
Pripetost z varnostnim pasom	Delež pripetosti v vozilu spredaj / zadaj. Delež pripetosti glede na spol. Delež pripetosti glede na vrsto ceste. Delež pripetosti glede na regijo.
Pripetost otrok z varnostnim pasom	Delež pripetosti otrok v vozilu. Uporaba zadrževalnih sistemov.
Nujna medicinska pomoč	Število urgentnih oddelkov. Število kadrov, usposobljenih za dajanje nujne medicinske pomoči na urgentnih oddelkih. Število reševalnih vozil. Povprečni reakcijski čas.

Izvajanje nacionalnega programa je razdeljeno na pet časovnih obdobij, v katerih se pripravljajo dvoletni obdobni načrti po enotno izdelani metodologiji. Aktualno je peto obdobje (leti 2021 in 2022), v katerem sta načrtovana nadaljevanje izvajanja prometnovarnostnih ukrepov in primerjava rezultatov z rezultati predhodnih akcijskih načrtov. Za pripravo obdobnih načrtov so v sodelovanju s civilno pobudo (nevladne organizacije, civilna združenja, strokovne organizacije, gospodarske družbe, združenja) odgovorne strokovne službe Javne agencije za varnost prometa in državnih organov. Nadzor nad izvajanjem teh načrtov opravlja Državni zbor RS in Odbor direktorjev za spremljanje, vodenje in nadziranje nacionalnega programa, ki ga vodi Ministrstvo za infrastrukturo.

Za strokovno izvajanje nacionalnega programa je Vlada RS konec leta 2013 ustanovila medresorsko delovno skupino za spremljanje in izvajanje programa, in sicer iz skupine strokovnjakov, tako da sodelujejo v njem vsi organi in organizacije, ki med svojimi pristojnostmi in nalogami skrbijo za varnost cestnega prometa, strokovne organizacije in posamezni strokovnjaki, organizacije civilne družbe, podjetja, vseslovensko zavarovalniško združenje in samoupravne lokalne skupnosti (Ministrstvo za infrastrukturo, 2013).

3.3.5 Strategija kibernetske varnosti

Ker je v sodobnih družbah uporaba informacijsko-komunikacijskih sistemov za vsakodnevno delovanje postala skoraj neizogibna, je pomembno nasloviti tudi s tem povezane varnostne vidike. V zadnjih letih je namreč vedno več varnostnih incidentov, naprednih ciljanih napadov in zlorab informacijsko-komunikacijske infrastrukture. Glavna tveganja predstavljajo predvsem tehnološki razvoj, internet, kibernetski kriminal, obveščevalna dejavnost, spreminjanje varnostnega okolja in vdori v zasebnost. Skladno s tem je Slovenija sprejela Strategijo kibernetske varnosti (Republika Slovenija, 2016).

Pri izdelavi strategije so sodelovale naslednje organizacije: Agencija za energijo, Agencija za komunikacijska omrežja in storitve, Ministrstvo za finance, Ministrstvo za gospodarski razvoj in tehnologijo, Ministrstvo za infrastrukturo, Ministrstvo za izobraževanje, znanost in šport, Ministrstvo za javno upravo, policija, MNZ, Ministrstvo za obrambo, Ministrstvo za zdravje, Ministrstvo za zunanje zadeve, Nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih

omrežij in informacij (SI-CERT), SOVA, Svet za nacionalno varnost in Urad za varovanje tajnih podatkov.

Namen strategije je opredeliti ukrepe za vzpostavitev celovitega nacionalnega sistema kibernetske varnosti, okrepiti sistem zagotavljanja kibernetske varnosti in to področje tudi sistemsko urediti. Temeljni cilj je zagotoviti odprt, varen in varovan kibernetski prostor. V strategiji so opredeljeni tudi natančnejši podcilji (skupaj osem) in ukrepi za njihovo uresničevanje, ki so predstavljeni v tabeli 2 in naj bi bili izvedeni v štiriletnem časovnem obdobju (do leta 2020).

Tabela 2: Strateški cilji in ukrepi na področju kibernetske varnosti (Republika Slovenija, 2016)

CILJI	UKREPI
Okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti	– vzpostavitev osrednje koordinacije nacionalnega sistema zagotavljanja kibernetske varnosti; – kadrovska in tehnološka okrepitev organov na operativni ravni sistema zagotavljanja kibernetske varnosti skupaj z vzpostavitvijo SIGOV-CERT; – redna udeležba na mednarodnih vajah s področja kibernetske varnosti ter izvedba nacionalnih vaj; – postopna nadgradnja omrežja državnih organov HKOM z opremo, ki so jo ustrezno potrdili slovenski organi kot varno in primerno za uporabo; – vzpostavitev kompetentnega preverjanja varnosti in funkcionalnosti informacijske opreme v okviru obstoječih in novo vzpostavljenih organov.
Varnost državljanov v kibernetskem prostoru	– redno izvajanje programov ozaveščanja na področju kibernetske varnosti; – uvedba vsebin s področja kibernetske varnosti v sistem izobraževanja in usposabljanja.
Kibernetska varnost v gospodarstvu	– spodbujanje razvoja in vpeljave novih tehnologij na področju kibernetske varnosti; – redno izvajanje programov ozaveščanja na področju kibernetske varnosti za gospodarske subjekte.
Zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore	– redno ocenjevanje tveganj za delovanje kritične infrastrukture sektorja informacijsko-komunikacijske podpore, načrtovanje ustreznih ukrepov za zaščito ter posodabljanje ocene tveganj na tem področju.

CILJI	UKREPI
Zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetske kriminalitete	– implementacija ustreznih kibernetskih zmogljivosti za varovanje informacijskih in komunikacijskih sistemov policije; – redno usposabljanje s področja kibernetske varnosti za organe pregona, ki sodelujejo pri razvoju kibernetskih zmogljivosti za področje javne varnosti in pri zatiranju kibernetske kriminalitete; – redno posodabljanje zakonodaje in postopkov skladno z razvojem informacijsko-komunikacijskih tehnologij.
Razvoj obrambnih kibernetskih zmogljivosti	– razvoj ustreznih kibernetskih zmogljivosti za varovanje obrambnih komunikacijskih in informacijskih sistemov.
Zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah	– zagotovitev pogojev za nemoteno delovanje ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah.
Krepitev nacionalne kibernetske varnostiz mednarodnim sodelovanjem	– zagotovitev pogojev za sodelovanje slovenskih strokovnjakov v relevantnih mednarodnih delovnih telesih in združenjih s področja kibernetske varnosti.

Udejanjenje strategije je pri tem prioritetno osredotočeno na:

1. Preprečevanje varnostnih incidentov: to obsega vse od tehnične zasnove komponent informacijskih sistemov do zagotavljanja zakonskih okvirov in predpisov, ki pripomorejo k razvoju varnejših aplikacij in infrastrukture.
2. Odzivanje na varnostne incidente: na podlagi izkušenj ter analiz incidentov in tveganj se postopki odzivanja stalno posodabljajo in izboljšujejo.
3. Ozaveščanje ciljnih skupin o pomenu kibernetske varnosti: z ozaveščanjem in izobraževanjem se lahko zmanjšujejo tveganja in zagotavlja varnejša uporaba tehnologije. Uporabijo se izkušnje iz faz preprečevanja in odzivanja.

V strategiji je poleg ciljev in ukrepov opredeljena tudi struktura sistema zagotavljanja in upravljanja kibernetske varnosti, ki je sestavljena iz strateške ravni, operativne ravni in širšega kroga deležnikov po posameznih področjih delovanja. Na strateški ravni Vlada RS vzpostavi osrednji koordinacijski organ, ki koordinira dejavnosti na

operativni ravni ter predstavlja enotno kontaktno točko pri mednarodnem sodelovanju (Urad Vlade RS za informacijsko varnost). Na operativni ravni s svojimi zmogljivostmi delujejo SI-CERT, Ministrstvo za obrambo na področju obrambe in varstva pred naravnimi in drugimi nesrečami, policija na področju zagotavljanja kibernetske varnosti v okviru javne varnosti in zatiranja kibernetske kriminalitete, SOVA na področju protiobveščevalnega delovanja in SIGOV-CERT na področju javne uprave. Širše deležnike v sistemu zagotavljanja kibernetske varnosti predstavljajo predvsem organizacije iz javnega in zasebnega sektorja, kot so Agencija za komunikacijska omrežja in storitve (AKOS), telekomunikacijski operaterji in upravljavci telekomunikacijske infrastrukture, ponudniki storitev informacijske družbe, akademsko-raziskovalna sfera, stanovska in strokovna združenja ter proizvajalci programske opreme, ki nudijo podporo državnim organom. V širšem pomenu se kot deležniki štejejo tudi organizacije s tega področja v tujini, predvsem pomembni so partnerji v okviru EU in Nato.

V zaključnem delu strategije pa je predstavljena tudi analiza SWOT, ki opisuje prednosti, pomanjkljivosti, priložnosti in nevarnosti za udejanjanje strategije. Opisani so potencialni pozitivni učinki in razvojne priložnosti uspešne realizacije strategije kakor tudi obstoječe pomanjkljivosti v ureditvi, ovire, ki zavirajo njeno uresničenje in potencialne nevarnosti, ki bi izvirale iz neustrezne vzpostavitve sistema kibernetske varnosti.

3.3.6 Druge strateške usmeritve v Sloveniji

Na podlagi resolucij, strategij, nacionalnih programov, ki urejajo področje nacionalne varnosti in delovanje posameznih resorjev, so nato sprejete še strategije dela in razvoja posameznih organizacij oz. njihovi razvojnousmerjevalni programi. Na osnovi zakonodaje, mednarodnih načrtov, »ReSNV-2« (2019) in Obrambne strategije RS, (2012) je za usmerjanje delovanja in razvoja Slovenske vojske denimo sprejeta »Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035 (ReDPROSV35)« (2022), Srednjeročni obrambni program Republike Slovenije 2022–2026 (Vlada RS, 2022) in Bela knjiga o obrambi Republike Slovenije (2020). Na podlagi zakonodaje in skladno z »ReSNV-2« (2019) ter »ReNPPZK19–23« (2019) pa je sprejet dolgoročni razvojnousmerjevalni planski dokument, ki zagotavlja platformo in okvir za razvoj policije (tj. Resolucija o dolgoročnem razvojnem programu policije do leta 2025 – »Kakovostna policija za

varno Slovenijo« (ReDRPPol), 2015). Na tej podlagi in skladno z drugimi strategijami (npr. s področja varnosti v prometu) so oblikovane temeljne in letne usmeritve ministrstva, na osnovi katerih se nato pripravi srednjeročni načrt razvoja in dela policije, ter letni načrti dela policije. Ključne razvojnousmerjevalne programe predstavljamo v nadaljevanju.

»Nacionalna strategija za preprečevanje terorizma in nasilnega ekstremizma« (2019): V tej strategiji, ki jo je sprejela Vlada RS, je sprva podana ocena varnostnih razmer, kar vključuje opis trendov, vrst ogrožajočih oblik terorizma in nasilnega ekstremizma ter zunanjih in notranjih elementov ogrožanja varnosti RS. Nato je opredeljenih pet strateških ciljev s podcilji (preprečevanje radikalizacije, ki vodi v nasilni ekstremizem ali terorizem; zaščita pred terorističnimi dejanji in dejanji nasilnega ekstremizma; preprečevanje terorističnih dejanj in dejanj nasilnega ekstremizma; izboljšanje pripravljenosti na ukrepe po terorističnem napadu in pregon storilcev kaznivih dejanj terorizma). Zatem so navedene dejavnosti Slovenije v mednarodnih prizadevanjih za preprečevanje terorizma in nasilnega ekstremizma ter določbe glede uresničevanja strategije in koordinacije dejavnosti (odgovornost je dodeljena Vladi RS, državnim organom in nacionalnima koordinatorjema za preprečevanje terorizma in nasilnega ekstremizma ter radikalizacije).

»Resolucija o nacionalnem programu preprečevanja nasilja v družini 2009–2014 (ReNPPND0914)« (2009): Resolucija je pravzaprav nacionalni program in strateški dokument, ki določa cilje, ukrepe in ključne nosilce politik za preprečevanje in zmanjševanje nasilja v družini v Sloveniji od leta 2009 do 2014. Čeprav je trajanje določeno do 2014, je nacionalni program še vedno veljaven in ni bil posodobljen. Temeljna cilja tega dokumenta sta povezati ukrepe različnih resorjev in zagotoviti učinkovite dejavnosti za zmanjšanje nasilja v družini, in sicer na ravni njegovega prepoznavanja in preprečevanja. Konkretne naloge in dejavnosti za doseganje ciljev in izvajanje posameznih ukrepov morajo biti opredeljene v akcijskih načrtih (po Zakonu o preprečevanju nasilja v družini bi morali biti akcijski načrti, izdelani vsaki dve leti, v njih pa natančno določeni časovni roki in izvedbeni načini – do sedaj sta bila sprejeta dva akcijska načrta, in sicer za obdobji 2010–2011 in 2012–2013). V resoluciji je najprej podan splošen okvir, ki vključuje primerjalno pravno prakso držav članic EU, OZN in Sveta Evrope, ocena stanja z opredelitvijo glavnih težav, pregledom statistik in raziskovalnih ugotovitev. Zatem je opisana strategija politike

proti nasilju v družini, ki vključuje opis načel in izhodišč za delovanje proti nasilju v družini, namen nacionalnega programa in cilje: (1) zmanjšati nasilje v družini in širši družbi nasploh; (2) povečati občutljivost za problematiko nasilja v družini; (3) zagotoviti usklajeno delovanje pristojnih organov in organizacij; (4) spodbujati raznovrstnost, enakomerno dostopnost, razvoj in kakovostno izvajanje programov za pomoč žrtvam; (5) spodbujati raznovrstnost, enakomerno dostopnost, razvoj in kakovostno izvajanje programov dela s povzročitelji nasilja; (6) zagotoviti sistematično ozaveščanje otrok, mladine in odraslih o njihovih temeljnih človekovih pravicah in dolžnostih ter vzgajanje za življenje v družbi brez nasilja, za sožitje med generacijami in spoštovanje vseh ljudi; (7) spodbujati ozaveščanje zlasti tistih, ki so izpostavljeni nasilju v družini, o možnih oblikah pomoči in zagotavljati njihovo dostopnost po vsej državi; in (8) zagotavljati redne vire financiranja programov pomoči. Temu sledi opis konkretnih ciljev, strategij in odgovornih subjektov za izvajanje strategij (Ministrstvo za kulturo; Ministrstvo za okolje in prostor; Ministrstvo za delo, družino in socialne zadeve; MNZ, Ministrstvo za šolstvo in šport; Ministrstvo za zdravje, Ministrstvo za pravosodje; Urad za enake možnosti) na področju preventivnega delovanja, odprave telesnega kaznovanja otrok in ponižujočega ravnanja z njimi, obravnave nasilja v družini, pomoči osebam z izkušnjo nasilja v družini in raziskovanja. V zaključnem delu so podana še določila glede izvajanja nacionalnega programa, in sicer priprave akcijskih načrtov in podatkov ter kazalcev.

»Resolucija o preprečevanju korupcije v Republiki Sloveniji (RePKRS)« (2004): Resolucija teži k realnim, postopnim in premišljenim dolgoročnim ukrepom za odpravo korupcije, njeni osnovni cilji pa so usmerjeni v preventivno, in sicer v dolgoročno in trajno odpravo pogojev za nastanek in razvoj korupcije, vzpostavitev ustreznega pravnega in institucionalnega okolja za preprečevanje korupcije, dosledno uveljavitev odgovornosti za nezakonita dejanja, izgradnjo splošno sprejemljivega sistema ničelne tolerance do vseh korupcijskih ravnanj skozi razne oblike izobraževanj in učinkovito uporabo mednarodno uveljavljenih standardov na tem področju. Resolucijo tvorijo uvod z opredelitvijo namena, opredelitve korupcije, predpostavke oz. načela resolucije, cilji (neposredni, splošni in širši družbeni cilji), opis vrst in obsega korupcije v Sloveniji skozi predstavitev policijskih podatkov in raziskav. Zatem so podrobno opredeljeni zakonodajni, institucionalni in praktični ukrepi na ravni politike, državne uprave, organov odkrivanja, pregona in sojenja, gospodarstva, nevladnih organizacij, medijev in splošne javnosti. Sledi še opis

mednarodnega sodelovanja in odgovornosti za uresničevanje resolucije. Pri tem je določeno, da akcijski načrt za realizacijo sprejme Komisija za preprečevanje korupcije, ki prav tako zbira in ocenjuje podatke o uresničevanju (do sedaj so bili sprejeti trije akcijski načrti, in sicer v letih 2005, 2009 in 2016).

Obrambna strategija Republike Slovenije (2013): Strategija opredeljuje interese in cilje RS na obrambnem področju ter ob upoštevanju sodobnih groženj in tveganj za nacionalno varnost usmerja obrambno politiko države, organiziranost njenega obrambnega sistema ter razvoj njenih vojaških in civilnih zmogljivosti za zagotavljanje nacionalne obrambe v okviru sistema kolektivne obrambe in varnosti, skladno z razpoložljivimi viri. Poleg vprašanj o uveljavljanju sprememb na obrambnem področju izpostavlja tudi tveganja pri uveljavljanju teh sprememb ter s tem pri uveljavljanju oz. uresničevanju obrambnih interesov in ciljev RS. Glavni interesi RS na obrambnem področju so ohranitev neodvisnosti, suverenosti in ozemeljske celovitosti države, nedotakljivosti njenih meja in območja, ustrezna stopnja obrambne sposobnosti države, uresničevanje skupnih obrambnih interesov v okviru Nata in EU, mir, varnost in stabilnost v svetu s poudarkom na območju JV Evrope. Temeljni obrambni cilji RS pa so zagotavljanje obrambne sposobnosti države z razvojem vojaških in drugih obrambnih zmogljivosti za učinkovito uveljavljanje njenih interesov na obrambnem področju ter uporabo obrambnih zmogljivosti za podporo drugim podsistemom nacionalnovarnostnega sistema RS; učinkovito odvračanje vojaških in drugih sodobnih groženj RS; neprekinjeno delovanje obrambnega sistema in drugih družbenih podsistemov, ki so življenjsko pomembni za učinkovito odzivanje države na grožnje in tveganja na obrambnem področju; krepitev dvo- in večstranskega sodelovanja RS na obrambno-vojaškem področju z zavezniškimi, partnerskimi in prijateljskimi državami ter v okviru OZN, Nata, EU in OVSE; sodelovanje v prizadevanjih mednarodne skupnosti za vzpostavljanje in ohranjanje miru ter krepitev varnosti in stabilnosti v svetu, s težiščem na območju JV Evrope, s sodelovanjem RS v mednarodnih operacijah in na misijah; povečanje ozaveščenosti družbe o pomenu nacionalnega obrambnega sistema ter krepitev njegovega ugleda med. Med drugim so v strategiji predstavljene tudi ključne grožnje in tveganja na obrambnem področju, dejavnosti obrambne politike pri uresničevanju ciljev, opis obrambnega sistema RS, ki ga tvorita SV in nevojaški del ter načrtovanje kadrovskih, finančnih, materialnih in infrastrukturnih virov.

Strategija Vlade RS na področju migracij (2019): Strategija, ki jo je pripravila medresorska skupina (državni sekretarji vseh ministrstev, predstavniki Kabineta predsednika Vlade RS, SOVE, policije, Urada za oskrbo in integracijo migrantov, Urada Vlade RS za komuniciranje, Urada Vlade RS za makroekonomske analize in razvoj ter URSZR), temelji na medresorskem povezovanju in migracije obravnava na večplasten, celovit in dolgoročen način ter v ospredje postavlja boljše razumevanje vseh vidikov migracij in izboljšanje ukrepov za njihovo upravljanje. Strategijo sestavlja šest horizontalnih stebrov, povezanih s posameznimi vidiki migracij (mednarodni vidik migracij; ekonomske migracije kot del zakonitih migracij; mednarodna zaščita; integracija; nezakonite migracije in vračanje; varnostna komponenta). V strategiji so predstavljeni temelji in načela imigracijske politike, trendi na področju migracij, nato pa akcijski načrti za posamezne stebre, kar vključuje opredelitev stanja, ciljev, dejavnosti oz. ukrepov, rokov in odgovornih subjektov. Med cilje denimo sodijo spodbujanje priseljevanja tuje delovne sile; zagotavljanje hitrih in učinkovitih postopkov za ugotavljanje upravičenosti do mednarodne zaščite; odkrivanje in preprečevanje nezakonitih migracij tako na zunanjih kot tudi na notranjih schengenskih mejah RS; učinkovito izvajanje sporazumov o vračanju oseb; odpravljanje in omejitev tveganj za nacionalno varnost, ki izhajajo iz migracijskih gibanj; zagotavljanje sinergijskih učinkov različnih akterjev na področju oblikovanja in izvajanja integracijske politike; obravnavanje vzrokov migracij ter zaščita življenj, dostojanstva in osnovnih človekovih pravic migrantov. Med odgovorne subjekte pa sodijo Ministrstvo za zunanje zadeve; Ministrstvo za delo, družino, socialne zadeve in enake možnosti; Vlada RS; MNZ; Ministrstvo za šolstvo, izobraževanje in šport; Urad za oskrbo in integracijo migrantov. Medresorska delovna skupina preko nosilcev posameznih stebrov spremlja izvajanje strategije in koordinira dejavnosti ter redno poroča vladi.

3.4 Ključni strokovni viri za ocenjevanje varnostnih tveganj in ogroženosti

V nadaljevanju so predstavljeni izsledki pregleda ključnih mednarodnih dokumentov, standardov, usmeritev, navodil in strokovnih virov, ki opisujejo metodologije na področju ocenjevanja varnostnih tveganj.

3.4.1 Standard ISO 31000:2018 »Risk management – Guidelines«

Standard ISO 31000:2018 opisuje smernice za obvladovanje tveganj v organizacijah, ne glede na vrsto tveganja, sektor ali posamezno industrijo. Smernice so zastavljene splošno in se lahko uporabljajo skozi celoten življenjski cikel organizacije, ki se ukvarja s katero koli dejavnostjo. Namenjen je uporabi čez celotno življenjsko dobo organizacije in se lahko aplicira na katero koli dejavnost, vključno z odločanjem na vseh ravneh.

Predstavlja najsplošnejše usmeritve na področju obvladovanja tveganj. V osnovi opisuje tri glavne komponente obvladovanja tveganj:

1. načela,
2. okvir obvladovanja tveganj in
3. proces obvladovanja tveganj.

V nadaljevanju na kratko opisujemo načela in okvir, nekoliko podrobneje pa se posvečamo procesu, ki predstavlja konkretne smernice za sistematično in učinkovito obvladovanje tveganj.

Načela

Načela so temelj za obvladovanje tveganja in jih je treba upoštevati pri vzpostavljanju organizacijskega okvira in procesov upravljanja tveganj. Osnovna načela obvladovanja tveganj skladno s standardom ISO 31000:2018 so:

- upravljanje tveganj mora biti sestavni del vseh dejavnosti organizacije;
- sistematičen in celovit pristop k obvladovanju tveganj prispeva k doslednim in primerljivim rezultatom;
- okvir in proces upravljanja tveganj morata biti prilagojena in sorazmerna z zunanjim in notranjim kontekstom organizacije ter povezana z njenimi cilji;
- ustrezna in pravočasna vključitev deležnikov omogoča ukrepanje na podlagi njihovega znanja, pogledov in zaznav;
- tveganja se lahko pojavijo, spremenijo ali izginejo, ko se spremenita zunanji in notranji kontekst organizacije;

- informacije, povezane s tveganji, morajo biti podane pravočasno, morajo biti jasne in dostopne vsem relevantnim deležnikom;
- človeška ravnanja in kultura pomembno vplivata na vse vidike obvladovanja tveganj na vseh ravneh;
- obvladovanje tveganj se nenehno izboljšuje z učenjem in izkušnjami.

Okvir obvladovanja tveganj

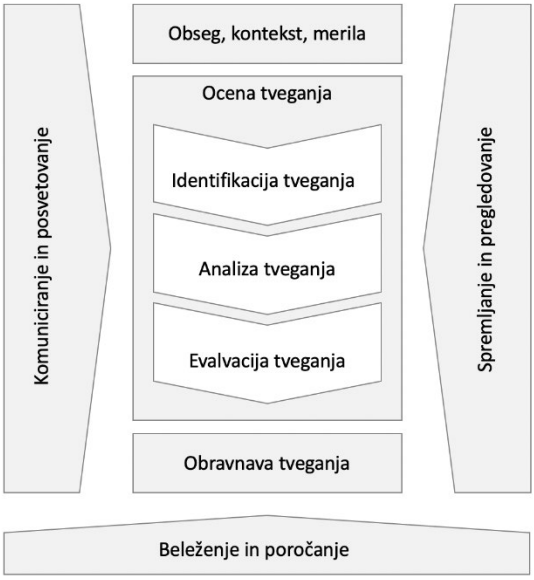
Razvoj okvira obvladovanja tveganj zajema integracijo, načrtovanje, izvajanje oz. implementacijo, vrednotenje in izboljšanje obvladovanja tveganj. Organizacija bi morala svoje obstoječe prakse in postopke obvladovanja tveganja ovrednotiti, nato oceniti vse vrzeli in odpraviti te vrzeli znotraj okvira.

Za uskladitev upravljanja tveganj z zastavljenimi cilji, strategijo in kulturo, prepoznavo in obravnavo vseh obveznosti, določitev količine in vrste tveganj, komuniciranje vrednosti obvladovanja tveganj, spodbujanje sistematičnega spremljanja tveganj in zagotavljanje, da okvir upravljanja tveganj ostane ustrezen kontekstu organizacije, bi vodstvo moralo zagotoviti, da je obvladovanje tveganj vključeno v vse organizacijske dejavnosti. To je treba storiti s prilagajanjem in izvajanjem vseh komponent okvira, sprejetjem namenske izjave ali politike, ki določa pristop, načrt ali potek ukrepanja obvladovanja tveganja, pri čemer se zagotovi, da so potrebna sredstva dodeljena za upravljanje tveganja, ter z dodelitvijo pooblastil in odgovornosti na ustrezne ravni znotraj organizacije.

Proces obvladovanja tveganj

Standard predpisuje proces obvladovanja tveganj, kot je prikazan na sliki 2. Proces deli na šest povezanih faz, ki jih podrobneje opisujemo v nadaljevanju.

Komuniciranje in posvetovanje. Namen komuniciranja in posvetovanja je pomagati ustreznim deležnikom pri razumevanju tveganja, podlage, na kateri se sprejemajo odločitve, in razlogov, zakaj so določena dejanja potrebna. Komunikacija spodbuja ozaveščenost in razumevanje tveganja, medtem ko posvetovanje vključuje pridobivanje povratnih informacij in informacij za podporo odločanju. Komuniciranje in posvetovanje morata biti prisotna pri vseh fazah procesa.



Slika 2: Proces obvladovanja tveganj (ISO 31000, 2022)

Obseg, kontekst, merila. Namen določitve obsega, konteksta in meril za ocenjevanje je prilagajanje procesa obvladovanja tveganj, ki omogoča učinkovito oceno in ustrezno obravnavo tveganja. Obseg, kontekst in merila vključujejo opredelitev obsega procesa ter razumevanje zunanjega in notranjega konteksta.

Ocena tveganja. Ocena tveganja je v grobem sestavljena iz identifikacije, analize in evalvacije tveganja.

- *Identifikacija tveganj.* Namen identifikacije tveganj je poiskati, prepoznati in opisati tveganja, ki bi lahko ovirala ali preprečila organizaciji doseganje njenih ciljev. Pri identifikaciji tveganj so pomembne relevantne, ustrezne in posodobljene (čim novejše) informacije.
- *Analiza tveganja.* Namen analize tveganja je razumeti naravo tveganja in njegove značilnosti, vključno s stopnjo tveganja. Analiza tveganja vključuje podrobno preučitev negotovosti, virov tveganja, posledic, verjetnosti, dogodkov, scenarijev, kontrol in njihove učinkovitosti.
- *Evalvacija tveganja.* Namen evalvacije tveganja je podpreti odločitve. Evalvacija tveganja vključuje primerjavo rezultatov analize tveganja z

uveljavljenimi merili tveganja, da se ugotovi, kje je potrebno dodatno ukrepanje. Odločitev o nadaljnjih ukrepih lahko vključuje katero koli od možnosti, npr. da se ne naredi nič več, se razmisli o možnostih obravnave tveganja, da se opravi nadaljnja analiza za boljše razumevanje tveganja, da se ohranijo obstoječe kontrole ali pa ponovno preuči cilje.

Obravnava tveganja. Namen obravnave tveganja je izbira in izvajanje možnosti za naslavljanje tveganja. Obravnava tveganja vključuje iterativni postopek, ki vključuje več faz:

- oblikovanje in izbira možnosti obravnave tveganja;
- načrtovanje in izvajanje obravnave tveganja;
- oceno učinkovitosti te obravnave;
- odločanje, ali je preostalo tveganje sprejemljivo;
- če ni sprejemljivo, se izvede nadaljnja obravnava.

Pri odločanju glede načina naslavljanja tveganj so na voljo različne možnosti:

- izogibanje tveganju (odločitev, da se dejavnost, ki ustvarja tveganje, ne bo nadaljevala);
- sprejem tveganja (z namenom izkoristiti priložnost se lahko tveganje sprejeme ali celo poveča);
- odstranitev vira tveganja;
- vplivanje na verjetnost;
- vplivanje na posledice;
- deljenje tveganj (skozi zavarovanja, pogodbe, prenos odgovornosti);
- ohranjanje tveganja skozi informirano odločitev.

Spremljanje in pregledovanje. Namen spremljanja in pregledovanja je zagotoviti in izboljšati kakovost in učinkovitost načrtovanja, izvajanja in rezultatov procesa. Ta faza vključuje načrtovanje, zbiranje in analizo informacij, beleženje rezultatov in zagotavljanje povratnih informacij. Stalno spremljanje in redni pregledi procesa obvladovanja tveganj in njegovih rezultatov morajo biti del procesa obvladovanja tveganj, z jasno opredeljenimi odgovornostmi. Spremljanje in pregledovanje morata potekati v vseh ostalih fazah procesa.

Beleženje in poročanje. Namen beleženja in poročanja je sporočanje dejavnosti in rezultatov obvladovanja tveganj v celotni organizaciji, zagotavljanje informacij za odločanje, izboljšanje obvladovanje tveganj ter pomoč pri interakciji z deležniki, vključno z odgovornimi za dejavnosti obvladovanja tveganj.

3.4.2 Standard IEC 31010:2019 »Risk management – Risk assessment techniques«

Mednarodni standard IEC 31010:2019 je logična nadgradnja standarda ISO 31000:2018. V procesu ocene tveganja skladno s standardom ISO 31000:2018 ocena vključuje prepoznavanje tveganj, njihovo analizo in uporabo z analizo pridobljenih znanj za oceno tveganja z oblikovanjem zaključkov o njihovem primerjalnem pomenu glede na cilje organizacije.

Standard IEC 31010:2019 pa opisuje tehnike ocenjevanja tveganja. Te se uporabljajo:

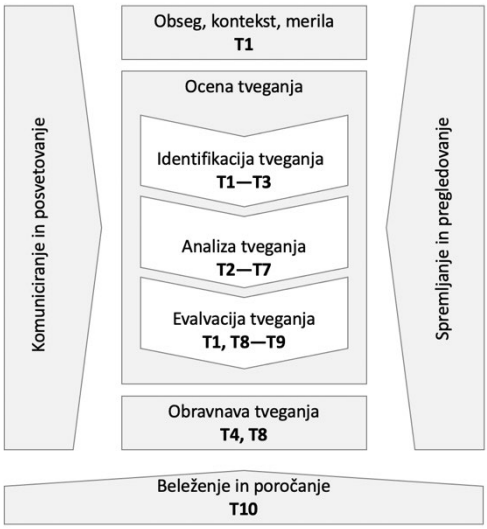
1. ko je potrebno nadaljnje razumevanje, kakšna tveganja obstajajo ali osredotočenost na določeno tveganje;
2. v procesu obvladovanja tveganja, ki vodi do ukrepov za obravnavo tveganja;
3. o odločitvi, glede katere je treba primerjati ali optimizirati več različnih možnosti o naslavljanju tveganj.

S tem se IEC 31010:2019 glede procesa ocene tveganja naslanja na ISO 31000:2018. Opredeljuje torej različne tehnike, ki jih predlaga za posamezne faze procesa ocene tveganja, kot je opredeljen v ISO 31000:2018. Standard opredeljuje ter umešča tehnike s pomočjo različnih postavk, kot so: namen uporabe, časovni horizont (ročnost), raven odločanja, količina zahtevanih podatkov, potrebna znanja za izvedbo, metoda, zahtevnost. Predlagane tehnike so nato kategorizirane v različne kategorije (T1–T10). Vrste tehnik po posameznih kategorijah so predstavljene v tabeli 3.

Omenjene tehnike se uporabljajo v različnih fazah v procesu ocene tveganja. Posamezne skupine tehnik (T1–T10) so prikazane na sliki 3.

Tabela 3: Tehnike upravljanja podatkov (IEC 31010, 2019)

KATEGORIJA	VRSTA
Tehnike za pridobivanje mnenj od deležnikov in strokovnjakov (T1)	– možgansko viharjenje (ang. *brainstorming*) – tehnika Delphi – tehnika nominalnih skupin – strukturirani in polstrukturirani intervjuji – ankete
Tehnike za identifikacijo tveganj (T2)	– kontrolni seznami, klasifikacije, taksonomije – analiza možnih napak in njihovih posledic (FMEA) – študija nevarnosti in operativnosti (HAZOP) – analiza scenarijev – strukturirana »kaj če« tehnika (SWIFT)
Tehnike za ugotavljanje virov, vzrokov in gonilnikov tveganja (T3)	– diagram vzrokov in rezultatov po Ishikawi (diagram ribje kosti) – cilindrični pristop
Tehnike za analizo kontrol (T4)	– tehnika metuljčka – analiza tveganja in ugotavljanja kritičnih kontrolnih točk (HACCP) – analiza plasti zaščite (LOPA)
Tehnike za razumevanje posledic in verjetnosti (T5)	– Bayesova analiza – Bayesove mreže – analiza vpliva na poslovanje (BIA) – vzročno-posledična analiza (CCA) – drevo dogodkov (ETA) – drevo odpovedi (FTA) – analiza človeške zanesljivosti (HRA) – Markova analiza – Monte Carlo simulacija – ocene učinkov v zvezi z varstvom podatkov (DPIA)
Tehnike za analizo odvisnosti in interakcij (T6)	– grafi vzročnih povezav – analiza navzkrižnih vplivov
Tehnike, ki omogočajo meritve tveganja (T7)	– toksikološka ocena tveganja – model »value at risk« in »conditional value at risk«
Tehnike za ocenjevanje pomembnosti tveganja (T8)	– model »kolikor nizko je še praktično mogoče« (ALARP) in »kolikor daleč je še praktično mogoče« (SFAIRP) – Paretov diagram – indici tveganj, – frekvenčno-številčni grafi (F-N) – v zanesljivost usmerjeno vzdrževanje (RCM)
Tehnike za izbiranje med možnostmi (T9)	– analiza stroškov in koristi (CBA) – analiza s pomočjo odločitvenih dreves – teorija iger – večkriterijska analiza (MCA)
Tehnike za beleženje in poročanje (T10).	– registri tveganj – matrike tveganj (matrike posledic in verjetnosti) – S-krivulje

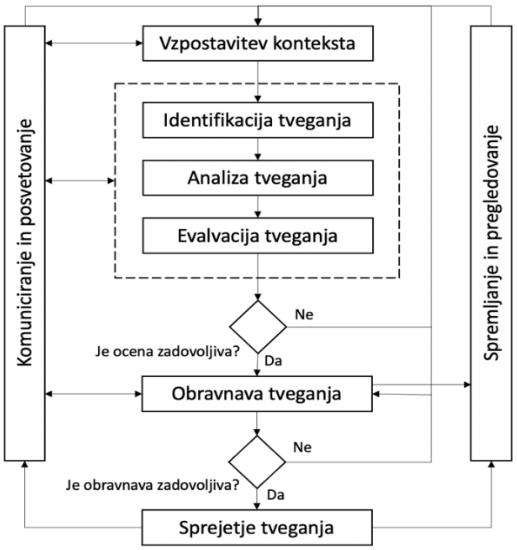


Slika 3: Tehnike upravljanja podatkov v okviru posameznih faz ocene tveganj (IEC 31010, 2019)

3.4.3 Standard ISO/IEC 27005:2018 »Information technology – Security techniques – Information security risk management«

Standard ISO/IEC 27005:2018 okvir procesa ocene tveganja gradi na standardu ISO 31000:2018 s tem, ko za oceno tveganja v osnovi predpisuje enak proces, kot je prikazan na sliki 2. Pomembno pa ga dopolnjuje v dodanih vejitvah in novem koraku – sprejetje tveganja. V tem poglavju tako naslavljamo zgolj spremembe procesa, ki smo ga opisali pri predstavitvi standarda ISO 31000:2018. Proces, skladen s standardom ISO/IEC 27005:2018, prikazuje slika 4.

Kot je razvidno s slike 4, sta procesu standarda ISO 31000:2018 dodani dve vejitvi, in sicer: po izvedeni oceni tveganja (*»Ali je ocena zadovoljiva?«*) in po obravnavi tveganja (*»Ali je obravnava zadovoljiva«*). Če je odgovor na kateri koli vejitvi negativen, se proces vrne na prvo fazo (»Vzpostavitev konteksta«), če pa je odgovor pritrdilen, se proces nadaljuje. Iz obravnave tveganja k sprejetju tveganja in po sprejetju tveganja na »Komuniciranje in posvetovanje« ter »Spremljanje in pregledovanje«. Največja sprememba na diagramu je tako dodana faza »Sprejetje tveganja«. Ker smo ostale faze opisali že v poglavju standarda ISO 31000:2018, se na tem mestu osredotočamo samo na dodano fazo.



Slika 4: Proces ocene tveganja (ISO/IEC 27005, 2020)

Sprejetje tveganja. Organizacije morajo sprejeti merila, pod katerimi bodo tveganja sprejela. Načrti obravnave tveganj morajo opisati, kako je treba obravnavati ocenjena tveganja, da se izpolnijo merila za sprejemljivost tveganja. Za vodstvo je pomembno, da pregledajo in odobrijo predlagane načrte obravnave tveganj in posledično preostala tveganja ter zabeležijo vse pogoje, povezane s tako odobritvijo.

Omenjeni standard predvideva kvalitativno ali kvantitativno analizo tveganja ali pa kombinacijo obeh pristopov. Izbira pristopa mora temeljiti na okoliščinah in potrebah posamezne ocene tveganja.

Kvalitativna analiza tveganja. Kvalitativna analiza tveganja uporablja lestvico kvalifikacijskih atributov za opis obsega možnih posledic in verjetnosti, da bo do teh posledic prišlo. Lestvica je lahko poljubno stopenjska, pri čemer je podana opisno. Primeroma je tako obseg možnih posledic lahko »majhen«, »srednji«, »velik« in verjetnost škodnega dogodka »nizka«, »srednja«, visoka. Prednost kvalitativne analize je njena enostavnost razumevanja vsem relevantnim kadrom, pomanjkljivost pa je odvisnost od subjektivne izbire lestvice. Kvalitativna analiza mora kljub svoji naravi temeljiti na dejstvih in dejanskih podatkih, kjer koli je to mogoče.

Kvantitativna analiza tveganja. V nasprotju s kvalitativno se pri kvantitativni analizi namesto opisnih vrednosti na lestvicah uporabljajo številčne vrednosti – tako za verjetnost nastanka škodnega dogodka kot tudi njegovega vpliva (resnost posledic). Prednost kvantitativne analize je, da uporablja pretekle podatke o incidentih, saj jih je tako mogoče povezati s cilji in usmeritvami organizacije. Pomanjkljivosti pa se kažejo predvsem v tem, da je takšna analiza zanesljiva le toliko, kolikor so zanesljivi podatki, na katerih temelji. S tem lahko ustvarja le iluzijo o točnosti in vrednosti takšne analize.

3.4.4 Smernice NIST: »Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments«

NIST Posebna publikacija 800-30 Rev 1 (Joint Task Force Transformation Initiative, 2012) zagotavlja smernice za izvajanje ocen tveganja informacijskih sistemov in organizacij. Zlasti opisuje smernice za izvajanje vsakega od korakov v postopku ocene tveganja ter kako se ocene tveganja in drugi organizacijski procesi obvladovanja tveganj dopolnjujejo. Posebna publikacija 800-30 predpisuje tudi napotke organizacijam za ugotavljanje specifičnih dejavnikov tveganja, ki jih je treba spremljati, tako da lahko organizacije ugotovijo, ali so se tveganja povečala na nesprejemljive ravni in s tem, ali je treba sprejeti določene ukrepe.

Postopek ocene tveganja po teh smernicah je sestavljen iz štirih korakov:

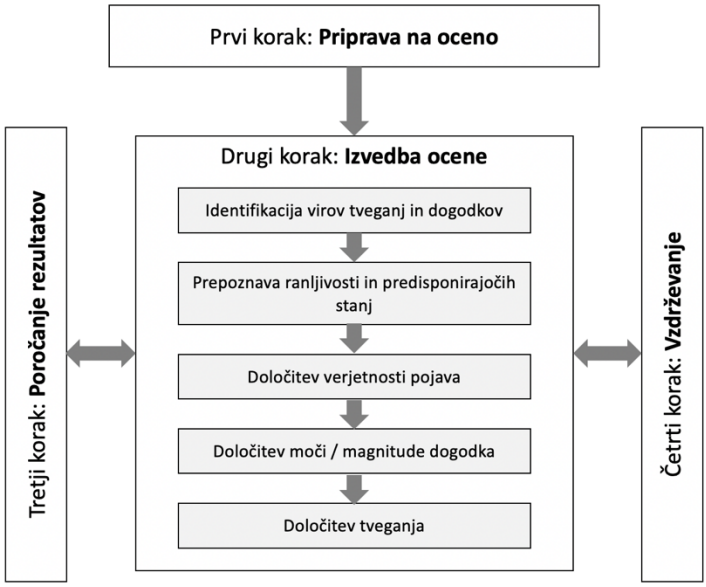
1. priprava na oceno tveganja,
2. izvedba ocene tveganja;
3. sporočanje rezultatov ocene in
4. vzdrževanje.

Vsakemu koraku so dodeljene naloge. Osnovna struktura procesa je prikazana na sliki 5.

Priprava na oceno tveganja. Prvi korak v postopku ocene tveganja je priprava na oceno. Cilj tega koraka je vzpostaviti ustrezni kontekst. Ta kontekst je vzpostavljen in podan na podlagi rezultatov okvirjanja tveganja v procesu upravljanja tveganj. V sklopu okvirjanja tveganj, organizacija npr. identificira: informacije v zvezi s politikami in zahtevami za izvajanje ocen tveganja, posebne metodologije

ocenjevanja, ki jih je treba uporabiti, postopke za izbiro dejavnikov tveganja, ki jih je treba upoštevati, obseg ocene, strogost analiz, stopnjo formalnosti in zahteve, ki jih je treba upoštevati. Organizacije uporabljajo strategijo obvladovanja tveganja, če je to izvedljivo, da pridobijo informacije za pripravo na oceno tveganja. Med naloge v prvem koraku NIST 800-30 Rev 1 umešča:

- določitev namena ocene tveganja;
- določitev obsega ocene tveganja;
- določitev predpostavk in omejitev, povezanih z oceno tveganja;
- določitev virov informacij, ki jih je treba uporabiti v oceni tveganja;
- določitev uporabe modela tveganja in analitičnih pristopov (tj. pristope ocenjevanja in analize), ki jih je treba uporabiti med oceno.



Slika 5: Proces ocene tveganja (Joint Task Force Transformation Initiative, 2012)

Izvedba ocene tveganja. Drugi korak v postopku ocene tveganja je izvedba ocene. Cilj tega koraka je izdelati seznam tveganj, ki jih je mogoče razvrstiti glede na stopnjo tveganja in uporabiti za odločanje o odzivanju na tveganja. Organizacije morajo analizirati grožnje in ranljivosti, vplive in verjetnost ter negotovost, povezano s

postopkom ocene tveganja. Ta korak vključuje tudi zbiranje bistvenih informacij kot del vsake naloge in se izvaja v skladu s kontekstom ocenjevanja, določenim v prvem koraku. Ocene tveganja morajo ustrezno nasloviti vse grožnje v skladu s smernicami in usmeritvami, določenimi med korakom priprave. Izvedba ocene tveganja vključuje naslednje specifične naloge:

- identifikacija virov (za organizacijo pomembnih) groženj;
- identifikacija škodnih dogodkov, ki bi jih lahko identificirani viri povzročili;
- identifikacija ranljivosti organizacije;
- določitev verjetnosti, da bi identificirani viri groženj sprožili določene škodne dogodke, in verjetnost, da bodo škodni dogodki uspešni;
- določitev škodljivih učinkov na operativo in sredstva organizacije, posameznike, druge organizacije in državo;
- določitev tveganja kot kombinacijo verjetnosti, ranljivosti in resnosti posledic.

Poročanje rezultatov. Tretji korak v postopku ocene tveganja je sporočanje rezultatov ocene in izmenjava informacij, povezanih s tveganjem. Cilj tega koraka je zagotoviti, da imajo odločevalci ustrezne informacije o tveganjih, ki so potrebne za informiranje in usmerjanje odločitev o tveganjih. Komuniciranje in izmenjava informacij sestoji iz dveh nalog:

- sporočanje rezultatov ocene tveganja;
- izmenjava informacij, pridobljenih v postopku ocene, da bi bile v oporo drugim dejavnostim obvladovanja tveganj.

Vzdrževanje. Četrti korak v postopku ocene tveganja je vzdrževanje. Cilj tega koraka je ohraniti aktualno, specifično znanje o tveganjih organizaciji. Rezultati ocene tveganja so podlaga za odločitve obvladovanja tveganj in usmerjajo odzive. Za podporo tekočemu pregledu odločitev o obvladovanju tveganj morajo organizacije vzdrževati ocene tveganja, za vključitev vseh sprememb, odkritih s spremljanjem tveganja. Spremljanje tveganj organizacijam omogoča: ugotavljanje učinkovitosti odzivov na tveganja, opredelitev sprememb organizacijskih

informacijskih sistemov in okolij, v katerih ti sistemi delujejo, in preverjanje skladnosti. Ta korak predvideva dve nalogi:

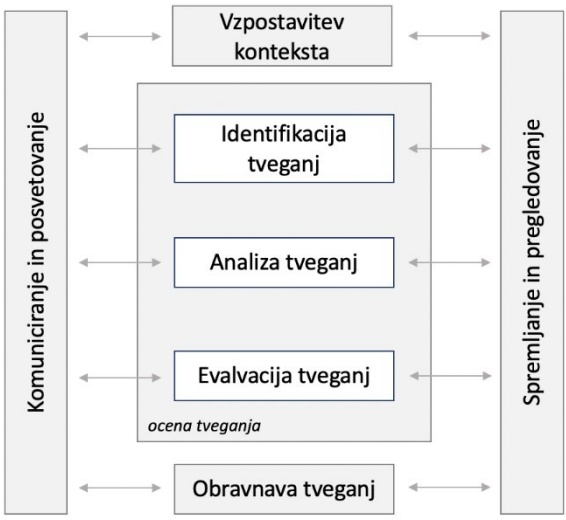
- stalno spremljanje dejavnikov tveganja, ugotovljenih v ocenah tveganja, in razumevanje kasnejših sprememb teh dejavnikov;
- posodobitev komponent ocene tveganja, ki odražajo dejavnosti spremljanja, ki jih izvajajo organizacije.

3.4.5 Smernice EU: EU Commission Staff Working Paper – Risk Assessment and Mapping Guidelines for Disaster Management SEC(2010) 1626 final

Namen Delovnega dokumenta služb Komisije o Smernicah za ocenjevanje in prikaz tveganj na področju obvladovanja nesreč, SEC(2010) 1626 končna (European Commission, 2010) je, da bi državam pomagal pri razvoju nacionalnih pristopov in postopkov za obvladovanje tveganj nesreč. S tem se želita izboljšati skladnost in doslednost med ocenami tveganja, ki se izvajajo v državah članicah na nacionalni ravni. Poenotenost metod za ocenjevanje nacionalnih tveganj bo omogočila skupno razumevanje tveganj, s katerimi se soočajo države članice in EU ter olajšala sodelovanje pri prizadevanjih za preprečevanje in blaženje skupnih tveganj.

Vsebine dokumenta so usklajene s standardom ISO 31010 in so osredotočene na procese ter metode nacionalnih ocen tveganja v fazah preprečevanja, pripravljenosti in načrtovanja. Pri tem smernice temeljijo na pristopu, ki upošteva več nevarnosti in več tveganj (ang. *multi-hazard* in *multi-risk approach*). Splošen opis procesa in okvira ocenjevanja tveganj je razviden s slike 6, v nadaljevanju pa podrobneje opisujemo faze, dimenzije in merila analiziranja ter ocenjevanja tveganj.

Na začetku samega procesa izdelave nacionalne analize tveganj je treba določiti odgovornega za delitev, organizacijo in koordiniranje med sodelujočimi skupinami. Uspešno načrtovanje zahteva usklajevanje med različnimi vladnimi oddelki ali agencijami, ki so odgovorne za obvladovanje posledic različnih vrst izrednih razmer. Nacionalna ocena tveganja tako vključuje dogovorjeno delitev prednostnih nalog, kar olajšuje to usklajevanje.



Slika 6: Proces ocene tveganja (European Commission, 2010)

Proces izdelave nacionalne analize tveganj vključuje javne organe, nevladne organizacije, podjetja, širšo javnost in raziskovalne skupine. Cilj nacionalne ocene tveganja je, da ti akterji dosežejo skupno razumevanje tveganj, s katerimi se soočajo. To mora vključevati tako tveganja, ki so ocenjena kot pomembna, kot tudi stopnjo nevarnosti in odzivi v primeru uresničitve.

Vse vpletene skupine:

- se morajo strinjati glede ocenjevalne lestvice na začetku izdelave analize tveganj,
- zapisovati uporabljene metode in njihovo stopnjo prepričanosti,
- navesti razloge za vključitev ali izključitev določenih tveganj,
- zapisovati ocene, dodeljene posameznim tveganjem, in njihove razloge,
- urediti protokol za pridobitev zunanjega mnenja.

Ko je narejen sam osnutek analize tveganj, se je treba posvetovati še z ostalimi zainteresiranimi akterji, kot so lokalni in regionalni organi in specializirane organizacije, kar se najbolje doseže tako, da se osnutek javno objavi. Javne informacije o samem procesu in izbranih tveganjih za analizo in izdelavo ocene so

potrebne za boljše razumevanje tveganj, hkrati pa to omogoči vsem interesnim skupinam in širši javnosti, da se vključijo v načrtovanje, pripravljenost in odziv. To zagotovi tudi večjo objektivnost in nepristranskost analize ter poveča zaupanje, ki ga ima javnost do teh akterjev.

Podatke za izdelavo nacionalne ocene tveganj je treba pridobiti iz več virov, kar predstavlja velik izziv. Problem lahko predstavljajo predvsem sledljivost in zanesljivost podatkov, pravilna dokumentacija in interoperabilnost. Zato je pomembno, da so viri jasno citirani, tudi kar zadeva uporabo strokovnega znanja in izkušenj. Nacionalne ocene tveganja bi morale upoštevati zahteve zakonodaje EU glede primerljivosti in interoperabilnosti podatkov, kar bo pripomoglo k širši uporabnosti podatkov. Pomembno je, da se podatki posodabljajo, saj to omogoča nadzor novih potencialnih tveganj in ranljivosti. Spremljanje tveganj, povratne informacije in izkušnje iz prejšnjih nesreč, usposabljanje in redna ocena preventivnih ukrepov bodo olajšali vsako prihodnjo oceno tveganja in ponovno vrednotenje ukrepov. Ker je uveljavljenih načinov za merjenje verjetnosti in posledic nesreč ter tveganj še vedno relativno malo, to pomeni, da je v analize in ocene pogosto treba vključiti nekaj predvidevanj in sklepanj. Zato je pomembno, da so ta sklepanja in predvidevanja razločno in razumljivo zapisana v ocenah.

Čeprav obstaja več pristopov, kako pripraviti nacionalno analizo tveganj, morajo vsebovati vsaj naslednje tri faze:

1. Identifikacija tveganja
2. Analiza tveganja
3. Vrednotenje tveganja

Pred začetkom procesa pa je treba izvesti tri uvodne korake:

- izbira območja (na nacionalni ravni),
- izbira časovnega okvira (kratkoročno ali dolgoročno),
- definiranje enotnega načina ocenjevanja tveganja in vplivov.

Ko so ti trije koraki dokončani, se lahko začne proces:

1. faza: Identifikacija tveganj

Ugotavljanje tveganj je proces iskanja, izbiranja, prepoznavanja in opisovanja tveganja. Kot omenjeno, mora identifikacija tveganja, kolikor je le možno temeljiti na kvantitativnih (zgodovinskih in statističnih) podatkih. Vendar glede na to, da gre za iskanje in prepoznavanje tveganj, je primerno uporabiti tudi kvalitativne metode, kot so mnenja strokovnjakov, obveščevalne informacije, kontrolni seznami in sistematični timski pristopi, tehnike induktivnega razmišljanja. Cilj te faze so seznam in scenariji različnih tveganj, ki so nato podrobno in natančneje analizirani v naslednji fazi. Vsako tveganje spremlja kratek opis.

Scenarij tveganja je realna predstavitev situacije, kjer se je uresničilo eno ali več tveganj in so nastale resne posledice. V primerih več tveganj je zelo verjetno, da je uresničitev enega tveganja sprožila drugo tveganje, kar je v scenariju tudi treba opisati. Scenariji omogočajo predvsem nazornejše in podrobnejše vrednotenje posameznega tveganja, ker vsebujejo verjeten opis postopkov in dejanj, ki se bodo v primeru uresničitve tveganja, zgodila. Temeljijo predvsem na preteklih izkušnjah, vendar vsebujejo tudi ukrepe in dogodke, ki se morda v preteklosti niso zgodili, vendar bi jih bilo smiselno implementirati.

Pri nacionalni oceni tveganj je število izbranih scenarijev omejeno in je zato pomembno, da se izberejo scenariji, ki se bodo najbolj verjetno zgodili, kajti le tako bo ocena uporabna in najbolje odražala realnost. Navadno se uporabljajo v prvi in drugi fazi procesa izdelave ocene tveganja, v drugi predvsem s ciljem vrednotenja posledic in verjetnosti.

Obstajata dve vrsti scenarijev, in sicer tista, ki vsebuje eno tveganje, in tista, ki vsebuje več tveganj. V primerih, kjer scenariji vsebujejo eno tveganje, govorimo predvsem o eni grožnji, ki se uresniči na določenem geografskem območju v določenem časovnem obdobju. Primer tega so poplave. Pri scenarijih, ki vsebujejo več tveganj, upoštevamo tveganja, ki se zgodijo hkrati ali si sledijo, ker so soodvisni, so bili povzročeni z isto nesrečo ali pa ogrožajo iste elemente brez kronološke povezave. Primer tega so domino učinki, torej plaz, ki je nastal zaradi poplave.

Nesreče lahko namreč pogosto sprožijo več tveganj, zato je to v scenarijih treba opredeliti.

Pristop, kjer se upošteva več tveganj hkrati, je na območju EU zelo pomemben, saj so taka ogrožena območja kar pogosta. Če se podrobno osredotočimo le na eno tveganje, to poveča ranljivost pri vseh ostalih tveganjih.

Ker so članice EU v različnih stopnjah razvoja in različnih velikosti, Komisija priporoča med 50 in 100 različnih scenarijev oz. v primeru, da država prvič izdeluje nacionalno oceno tveganja, med 10 in 20 scenarijev. Komisija je kot pomoč za lažjo izdelavo naredila tudi smernice:

- Izdelava scenarija: nacionalne ocene tveganja naj identificirajo vse pomembnejše nesreče, ki se bodo predvidoma zgodile vsaj enkrat v naslednjih 100 letih in tiste, katerih posledice prizadenejo več kot 50 ljudi, povzročijo več kot 100 milijonov evrov škode ali so na lestvici označene kot pomembne/zelo resne.
- Obseg kvantitativne analize: z razvojem izkušenj naj se progresivno uvajajo kvantitativne analize, še posebej na področju ocenjevanja vplivov.
- Število tveganj in obravnavani scenariji: z izkušnjami narašča število tveganj, vključenih v analizo, v začetnih fazah pa se je smiselno omejiti na manjše število. Pri tem je treba vključiti enostavne scenarije z enim tveganjem in scenarije z več tveganji.
- Časovni okvir: ocena tveganja naj bi vsebovala scenarije za nesreče, ki se lahko zgodijo v bližnji prihodnosti oz. v naslednjih petih letih, za nacionalno oceno pa priporočajo, da se za kakovostno oceno upošteva obdobje do 35 let, kajti tako lahko zajamemo še nastajajoča tveganja in nesreče ter globalno perspektivo in prepoznamo tudi mednarodna tveganja in soodvisnosti.

2. faza: Analiza tveganja

Fazi identifikacije sledi proces analize tveganja. V tem procesu se ugotavlja narava tveganja in ovrednoti stopnja ogroženosti ter stopnja tveganja. Za vsakega izmed identificiranih tveganj je treba narediti podroben opis, nato pa oceniti verjetnost

uresničitve in resnost možnih posledic. Verjetnost naj, kolikor je le možno, temelji na podobnih zgodovinskih dogodkih in statističnih podatkih, resnost možnih posledic pa naj bo izražena kvantitativno. Pri tem mora biti določen tudi geografski obseg analize, pri čemer lahko konkretna lokacija ostane nedoločena. Ocena posameznega tveganja mora biti objektivna in poudarjati kakršno koli negotovost ali dvomljive ugotovitve.

Na ravni EU je na voljo precej smernic za izvajanje ocen za posamezna tveganja, kot so poplave, suše in nesreče z nevarnimi snovmi. V splošnem pa naj bi oceno sestavljali naslednji analizi:

- Analiza narave tveganja:
  - geografska analiza (lokacija, obseg),
  - časovni okvir (pogostost, trajanje ipd.),
  - dimenzijska analiza (obseg, intenzivnost),
  - verjetnost uresničitve.
- Analiza ranljivosti:
  - identifikacija ogroženih elementov in ljudi (izpostavljenost),
  - identifikacija ranljivih dejavnikov (psihološki, ekonomski, okoljski, politični ali socialni),
  - vrednotenje verjetnih posledic,
  - analiza zmožnosti obrambe in zmanjšanja izpostavljenosti.

3. faza: Ovrednotenje tveganja

Vrednotenje tveganja je proces, kjer se primerjajo rezultati analize tveganj z vnaprej definiranimi merili, z namenom določitve magnitude tveganja. Merila določajo pomembnost tveganja in omogočajo sklep, ali je treba ukrepati takoj ali je tveganje sprejemljivo. Merila lahko vsebujejo stroške, zakonske zahteve, socialno-ekonomske in okoljske faktorje ipd. Mednarodni svet za upravljanje tveganj opisuje, da je cilj vrednotenja tveganj sprejem odločitve o zanesljivosti in sprejemljivosti, ki temelji na ravnotežju prednosti in slabosti ter omogoča možnost merjenja in testiranja vplivov na kakovost življenja, gospodarstvo in družbo.

Izvedba analize in ocene tveganja, kot je predstavljena zgoraj, je usklajena s smernicami standarda ISO 31010. Po tem standardu je tveganje opredeljeno kot kombinacija posledic dogodka in verjetnosti njegove uresničitve. Posledice so opredeljene kot negativni učinki, ki lahko prizadenejo prebivalce, ekonomijo in politične oz. socialne razmere. Enačba za izračun tveganja je:

$$tveganje = posledice\ dogodka \times verjetnost\ uresničitve$$

Situacijo, kjer je lahko verjetnost pojava dogodka količinsko določena oz. je velika verjetnost ponovitve v naslednjih nekaj letih, se ima za podobno tveganje kot dogodek, ki ima hujše posledice, vendar se verjetno ne bo ponovil v naslednjih nekaj desetletjih.

Ker so posledice dogodkov pogosto odvisne od različnih okoliščin in jih je težko neposredno ocenjevati, se lahko za natančnejšo oceno tveganja uporabi kompleksnejši pristop. V takem primeru se v izračunu tveganja poleg verjetnosti (p), vključita ocena ranljivosti (V), to so okoliščine skupnosti, sistema ali sredstva, ki povzročajo njihovo dovzetnost za negativne učinke v primeru nesreče, in izpostavljenost (E), ki je celota ljudi, lastnine in sistemov, ki obstajajo na ogroženih območjih in so posledično izpostavljeni možnim izgubam. Na takšen način se lažje nakažejo in načrtujejo tudi preventivni in pripravljalni ukrepi. Za izračun tveganja se v teh primerih uporabi naslednja enačba:

$$tveganje = f(p \times E \times V)$$

Odvisno od kompleksnosti in posledic posameznega tveganja se lahko za izračun tveganja uporabijo tudi druge spremenljivke, ki omogočajo večjo mero natančnosti, vendar je to priporočljivo le, če se s tem poveča tudi stopnja prepričanosti oz. točnosti.

Glede na smernice Komisije naj bi se pri vrednotenju tveganja upoštevale tri vrste posledic/vplivov, in sicer:

- Človeški vplivi, kjer se upoštevajo predvideno število smrti, število hujše poškodovanih ali bolnih ljudi in število ljudi, ki morajo biti stalno izseljeni. Človeški vplivi se torej merijo s predvidevanjem števila prizadetih ljudi.

- Ekonomski in okoljski vplivi, kjer se upošteva vsota sredstev, porabljenih za zdravstvo, kratkotrajne in dolgotrajne nujne ukrepe, prenove zgradb, javni prevoz in infrastrukturo, izplačilo zavarovalnic, posredne in neposredne vplive na ekonomijo in ostale relevantne stroške. Ekološki in okoljski vplivi se merijo skozi oceno stroškov (v evrih).
- Politični in socialni vplivi, ki se merijo na polkvantitativni lestvici in vsebujejo kategorije, kot so ogorčenje javnosti, kršitve demokracije, psihološki vplivi, vplivi na javno varnost in mir, poškodbe kulturnih spomenikov in ostali podobni pojavi, ki se ne morejo meriti s številkami, kot je npr. ekološka škoda. Priporočeno je, da se pri ocenjevanju tovrstnih vplivov uporabijo lestvice od 1 do 5, kjer 1 pomeni omejeni/nepomembni, 2 – majhni/precejšnji, 3 – zmerni/resni, 4 – pomembni/zelo resni in 5 – katastrofalni.

Pri sami identifikaciji in analizi tveganj morajo biti upoštevane vse tri kategorije vplivov. Vplivi se morajo tudi, kolikor je le možno, opirati na empirične podatke, izkušnje iz preteklih podobnih nesreč in tveganj ter uveljavljene modele, s katerimi se izračunajo vplivi. Vse tri kategorije so lahko izračunane posamično ali odvisno ena od druge. Predvsem ekonomski vplivi so v veliki meri odvisni od ostalih vplivov. Kot primer soodvisnosti je navedeno število mrtvih ali poškodovanih kot posledica porušene stavbe zaradi potresa. Pri tem je na voljo precej različnih tehnik, standardov, metod in modelov, ki se lahko uporabijo za izračun vplivov in so največkrat prilagojeni za specifične vrste tveganj oz. nesreč (odpornost zgradb na potrese, neurja, poplave ipd.).

Pomembno je, da se za vsako izmed treh skupin vplivov pri merjenju posameznih tveganj uporablja isto merilo. Torej pri človeških vplivih naj se vedno ocenjuje, koliko ljudi bo v primeru nesreče prizadetih, pri okoljskih in ekonomskih naj se škoda vedno izraža v evrih, pri političnih oz. socialnih pa naj bo to lestvica od 1 do 5. Treba je torej sestaviti različne matrike za vsako skupino vplivov, kajti med seboj so zelo težko primerljive in ne bi bilo smiselno uporabljati iste.

Po oceni vplivov in verjetnosti se tveganje vizualizira v matriki tveganj. Matrika tveganja je vizualno orodje, ki omogoča boljšo predstavo in nazornost ocene posameznega tveganja in omogoča lažjo primerjavo med različnimi tveganji. Matrike

so običajno sestavljene v dvodimenzionalni obliki, kjer se na osi x prikaže ocena verjetnosti tveganja, na osi y pa ocena vpliva tveganja. Obe osi sta razdeljeni na pet točk oz. stopenj, tako polje v grafu tvori skupaj 25 polj, ki prikazujejo končno oceno/resnost tveganja. Rdeča barva prikazuje zelo visoko, oranžna visoko, rumena, srednje in zelena nizko tveganje. Med nizka tveganja se umeščajo tveganja, ocenjena z vplivom 1, ne glede na oceno verjetnosti; in oceno vpliva 2 ob verjetnosti z oceno 1. Nasprotno pa se z oceno zelo visoko tveganje oceni tveganje z oceno vpliva 4 ali 5 in oceno verjetnosti 3, 4 ali 5. Primer takšne matrike je prikazan na sliki 7.

Vpliv						
	5	Srednje	Visoko	Zelo visoko	Zelo visoko	Zelo visoko
	4	Srednje	Visoko	Zelo visoko	Zelo visoko	Zelo visoko
	3	Srednje	Visoko	Visoko	Visoko	Visoko
	2	Nizko	Srednje	Srednje	Srednje	Srednje
	1	Nizko	Nizko	Nizko	Nizko	Nizko
		1	2	3	4	5
				Verjetnost		

Slika 7: Matrika tveganja (European Commission, 2010)

V oceni tveganja morajo biti povzete tudi kakršne koli negotovosti, ki so se pojavile med izdelavo ocene. To je ključnega pomena za zanesljivost in učinkovitost rezultatov. Tukaj se vključijo variacije ali netočni rezultati in sklepanja.

Pri ocenah, ki vsebujejo več tveganj, takšen pristop k oceni predstavlja izziv, kajti težko je v oceni zajeti vse povezane dogodke in vplive nesreče. Izziv predstavlja tudi sodelovanje med več akterji, ki so zadolženi za specifično področje, kajti redkokdaj imajo vsi sodelujoči popoln pregled nad celotno situacijo in posledično lahko s svojim ravnanjem povzročijo domino učinek in še večjo škodo. Zelo pomembno je tudi koordiniranje in sodelovanje med temi organizacijami in agencijami. Komisija je tudi za take primere razvila naslednje smernice:

- identifikacija več možnih tveganj, najprej se opredeli tisto, ki lahko sproži druge in izvede ocena verjetnosti;
- sledi ocena izpostavljenosti in ranljivosti za posamezna tveganja in dogodke, ki se lahko sprožijo kot posledica;
- nazadnje se izvede vrednotenje tveganja za vsako nevarnost in neželen dogodek ter nato za scenarij.

V teh primerih se pogosto uporabljajo programske opreme za izračun ocen in vizualizacijo teh dogodkov.

Ker imajo lahko večje nesreče tudi čezmejne posledice, se priporoča, da so informacije glede analiziranja in upravljanja tveganj ene države, dostopne tudi ostalim državam, predvsem tistim, s katerimi si deli meje. Za lažji doseg tega, predvsem pa za spopadanje z različno terminologijo in večjezičnostjo, Komisija priporoča Leksikon terminologije, ki omogoča poenotenje in prevajanje ocene tveganja.

Pri pripravi nacionalne ocene tveganja se priporoča tudi izvedba kartiranja tveganj. Zemljevidi so namreč pomembna orodja, s katerimi se lahko prikažejo podatki o nesrečah, ranljivosti in tveganja na določenem območju. Pripomorejo predvsem pri zmanjšanju tveganj in omogočajo, da imajo vsi udeleženi akterji enake informacije o nesreči. Priprava zemljevidov je sicer kompleksen proces, ki se navadno začne izvajati v fazi analiziranja tveganj in se nadaljuje v fazi vrednotenja tveganj.

Kartiranje nesreč, tveganj in ranljivosti je praksa, ki jo uporabljajo tako evropske kot ostale države po svetu in se najpogosteje uporabijo za naravne nesreče in različna tehnološka ter industrijska tveganja. Raziskave in razni projekti na evropski ravni izpostavljajo, da je kartiranje izjemno kompleksno in poudarjajo nekatere pomanjkljivosti, ki obstajajo v metodologijah. Z razvojem tehnologije geografskega informacijskega sistema (GIS) se je proces sicer izboljšal, vendar odsotnost poenotenja socialnih, ekonomskih in okoljskih spremenljivk ostaja velik izziv. Pri kartiranju z GIS je namreč težko združevati raznolike lestvice, na katerih so predstavljene različne družbene in ekonomske razsežnosti ranljivosti. Težavo predstavlja tudi mapiranje tveganj, katerih povzročitelj je človek. Tako še vedno ni nekega univerzalnega uveljavljenega modela kartiranja in vsaka država uporablja svoj pristop.

Komisija za kartiranje priporoča naslednje korake:

- Zemljevidi naj prikazujejo pričakovano prostorsko porazdelitev večjih groženj. Različne grožnje in različne intenzitete naj bodo predstavljene na različnih zemljevidih.

- Zemljevidom nesreč naj se dodajo pomožni zemljevidi, ki prikazujejo prostorsko porazdelitev vseh relevantnih elementov, ki so potrebni zaščite (prebivalstvo, infrastruktura, naravna zaščitena območja ipd.).
- Tretja vrsta zemljevidov naj prikazuje prostorsko porazdelitev ranljivosti in dojemljivosti za škodo vseh povezanih dejavnikov/elementov.
- Vsi ti zemljevidi lahko služijo kot osnova za pripravo zemljevida tveganja v smislu prikaza kombinacije verjetnosti in posledic za določen dogodek kot tudi za skupne zemljevide nevarnosti.

Poplave so v Evropi najpogostejša nesreča in pogosto povzročijo tudi največ stroškov. Zaradi tega je to tudi področje, kjer so metodologije mapiranja najnaprednejše oz. najbolj razvite. Zemljevidi nesreč naj bi pokrili vsa geografska območja, ki so lahko poplavljena, zemljevidi tveganj pa naj bi nakazali možne posledice, ki so lahko rezultat poplave. V Evropi obstaja tudi neformalni krog izmenjave EXCIMAP, kjer so se povezali člani 24 evropskih držav in pripravili priročnik za mapiranje poplav z naslovom *Atlas of Flood Maps in Handbook on Good Practice for Flood Mapping in Europe* (EXCIMAP, 2007a, 2007b).

3.4.6 Druge strokovne smernice: COSO in MOSAR

Smernice COSO: »Enterprise Risk Management—Integrating with Strategy and Performance«

Committee of Sponsoring Organizations of the Treadway Commission (COSO) je leta 2017 izdal posodobljene smernice, ki naslavljajo obvladovanje tveganj v organizacijah, ki so nadomestile smernice iz leta 2004. Dokument se osredotoča na okvir za obvladovanje tveganj (ang. *a focused framework*) in poudarja pomen upoštevanja tveganj v procesu določanja strategije. Tako pojasnjuje pomen upravljanja tveganj v podjetju pri strateškem načrtovanju in vključevanju v celotno organizacijo, saj tveganje lahko vpliva na uspešnost vseh oddelkov in funkcij v organizaciji.

Okvir za obvladovanje tveganj predstavljajo načela, ki so organizirana v pet medsebojno povezanih komponent:

1. upravljanje in kultura,
2. strategija in postavljanje ciljev,
3. izvedba,
4. pregled in popravki,
5. informiranje, komunikacija in poročanje.

Načela, ki sestavljajo posamezne komponente, opisujejo prakse, ki se lahko uporabljajo na različne načine za različne organizacije, ne glede na velikost, vrsto ali sektor. Upoštevanje teh načel lahko vodstvu zagotovi, da organizacija razume in si prizadeva za obvladovanje tveganj, povezanih z njeno strategijo in cilji. V nadaljevanju opisujemo glavne komponente in jim pripisujemo načela, kot jih predvideva.

Upravljanje in kultura. Upravljanje določa ton organizacije, krepi pomen upravljanja tveganj v podjetju in določa odgovornosti za nadzor. Kultura pa se nanaša na etične vrednote, želeno vedenje in razumevanje tveganj. Podjetje naj (predvidena načela):

- izvaja nadzor nad tveganji;
- vzpostavi operativne strukture;
- opredeli želeno kulturo;
- izkazuje predanost temeljnim vrednotam;
- pritegne, izobrazi in zadrži kompetentne posameznike.

Strategija in postavljanje ciljev. Upravljanje tveganj v podjetju, strategija in postavljanje ciljev sodelujejo v procesu strateškega načrtovanja. Dovzetnost za tveganje mora biti opredeljena in usklajena s strategijo; poslovni cilji morajo udejanjati strategijo v praksi, hkrati pa služijo kot osnova za prepoznavanje, ocenjevanje in odzivanje na tveganja. Podjetje naj (predvidena načela):

- analizira kontekst poslovanja;
- opredeli ranljivost za tveganja;
- evalvira alternativne strategije;
- oblikuje poslovne cilje.

Izvedba. Tveganja, ki lahko vplivajo na doseganje strategije in poslovnih ciljev, je treba identificirati in oceniti. Tveganja se razvrstijo glede na resnost in ranljivost. Organizacija nato izbere odzive na tveganja in si prevzame portfeljski pogled na obseg tveganja, ki ga prevzema. O rezultatih tega procesa se poroča ključnim deležnikom. Podjetje naj (predvidena načela):

- opredeli tveganja;
- oceni resnost tveganj;
- določi prednostna tveganja (razvrsti glede na resnost);
- implementira odzive na tveganja;
- razvija portfelj.

Pregled in popravki. S pregledom uspešnosti lahko organizacija dobi vpogled, kako dobro delujejo komponente upravljanja tveganj podjetja skozi čas. Prav tako lahko načrtuje bistvene spremembe ter ugotovi, kakšni popravki so potrebni. Podjetje naj (predvidena načela):

- ocenjuje bistvene spremembe;
- ocenjuje tveganja in uspešnost;
- si prizadeva za izboljšanje upravljanja tveganj.

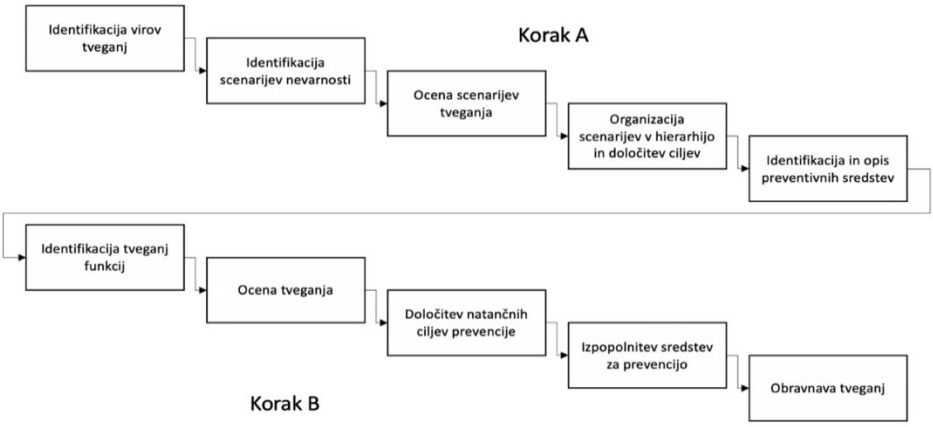
Informiranje, komunikacija in poročanje. Upravljanje tveganj zahteva stalen proces pridobivanja in izmenjave potrebnih informacij, tako iz notranjih kot zunanjih virov, ki tečejo navzgor, navzdol in preko celotne organizacije. Podjetje naj (predvidena načela):

- uporablja in izkorišča informacije in tehnologijo;
- komunicira informacije o tveganjih;
- poroča o tveganjih, kulturi in uspešnosti.

Metoda MOSAR »Method Organized for a Systematic Analysis of Risk«

Metoda, organizirana za sistematično analizo tveganj, t. i. MOSAR, je bila oblikovana (in je namenjena) identifikaciji tehničnih tveganj in sredstev za zaščito pred njimi. V osnovi je sestavljena iz dveh korakov: »A« in »B«, ki sta nadalje razdeljena na skupno

deset (pod)korakov. Korak »A« omogoča izvedbo analize večjih tveganj, medtem ko korak »B« omogoča podrobno analizo glede na funkcije, ki jih omogoča sistem, za katerega se opravlja ocena tveganja. Sosledje in predvidene korake prikazuje shema metode (slika 8). Ker je izvedba predvidena stopničasto, je vsaka izpolnjena predhodna faza pogoj za prehod na naslednjo fazo. Na splošno je za korak »A« potrebnih manj informacij, ki so lahko tudi manj podrobne, kot za korak »B«, ki zahteva podrobnejše informacije in več njih (Cherkaoui in Lopez, 2009).



Slika 8: Proces analize tveganja (MOSAR)

Univerzitetna založba
Univerze v Mariboru

4 Ocenjevanje varnostnih razmer v Sloveniji

Poglavje zajema ugotovitve analize pristopov, ki se uporabljajo za ocenjevanje varnostne ogroženosti in varnostnih tveganj v Sloveniji, s poudarkom na metodah, modelih, indikatorjih in merilih. V analizo smo vključili izvedbe zahteve in metodologije ocenjevanja, ki se v povezavi z varnostnimi razmerami oz. varnostnimi grožnjami uporabljajo na:

- nacionalni oz. širši teritorialni in sektorski ravni;
- evropski ravni ter prenašajo (z dejansko uporabo ali posredovanjem podatkov) na nacionalno.

4.1 Sistem ocene tveganj za nesreče

Med najbolj pomembne analize in ocene na področju varnostne ogroženosti v Sloveniji sodijo ocene tveganj za nesreče. Primarno podlago tovrstnim ocenam predstavlja Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o Mehanizmu Evropske unije na področju civilne zaščite (2013), ki je v uporabi od 1. januarja 2014. Ta dokument med drugim v točki a 6. člena določa pripravo ocen tveganj za nesreče.

Vlada RS je za izvajanje nalog, povezanih z ocenami tveganj za nesreče, avgusta leta 2014 sprejela »Uredbo o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite« (2014). Z uredbo je določila vrste in vsebine ocen tveganja za nesreče, proces izdelave ocen tveganja za posamezne nesreče in Državne ocene tveganj za nesreče.

V uredbi se določa oz. opredeljuje (Uprava Republike Slovenije za zaščito in reševanje, 2021):

- vrste ocen tveganj za nesreče,
- nosilci in njihova odgovornost,
- postopke izdelave ocen tveganj za nesreče,
- metode, ki so na voljo za izdelavo ocen tveganj za nesreče,
- vsebine ocen tveganj za nesreče,
- način sprejemanja ter dopolnjevanja in spreminjanja ocen tveganj za nesreče,
- način vključevanja vsebin v zvezi s podnebnimi spremembami.

Zakonsko podlago za izdelavo ocen ogroženosti predstavlja tudi »Zakon o varstvu pred naravnimi in drugimi nesrečami« (2006) in »Navodilo o pripravi ocen ogroženosti« (1995), ki ga sprejme minister za obrambo.

V Sloveniji je bilo na podlagi uredbe do zdaj izdelanih 15 ocen tveganja za posamezne nesreče. Izdelali so jih posamezni nosilci (ministrstva) med letoma 2015 in 2018.[6]

Skupno oceno tveganj za nesreče lahko najdemo v Državni oceni tveganj za nesreče (Uprava Republike Slovenije za zaščito in reševanje, 2018), v kateri so strnjeni izsledki ocen tveganj za posamezne nesreče in primerjane posledice ter pogostost oz. verjetnost njihovega pojavljanja ob upoštevanju enotnih meril tveganja. Vsebina teh ocen je načeloma enotna za vse nesreče in izhaja iz smernic za ocenjevanje

[6] Leta 2015 je bilo izdelanih 12 ocen tveganja za posamezne nesreče, s katerimi so bila ugotovljena tveganja za 13 nesreč. Ocene so izdelala pristojna ministrstva v sodelovanju s preostalimi ministrstvi in drugimi sodelujočimi organi. Nekatere ocene tveganja za posamezne nesreče so bile leta 2016 dopolnjene z vsebinami, povezanimi s podnebnimi spremembami. Leta 2018 so bile izdelane še tri nove ocene tveganja za posamezne nesreče (nesreče na morju, kibernetska tveganja, tveganja za bolezni in škodljivce gozdnega drevja), ena obstoječa pa je bila dopolnjena (Uprava Republike Slovenije za zaščito in reševanje, 2018).

tveganj za nesreče, ki jih je leta 2010 izdala Evropska komisija. Najpomembnejša vsebina teh ocen so:

- scenariji tveganj za nesreče,
- analiza scenarijev tveganja (ocena posledic nesreč prek določenih vplivov),
- vrednotenje rezultatov analiz scenarijev tveganja za vse nesreče z enotnimi merili tveganja in
- prikaz rezultatov v matrikah tveganj za nesreče.

Državni koordinacijski organ za področje ocenjevanja tveganj za nesreče je Uprava RS za zaščito in reševanje, ocene posameznih nesreč pa so v pristojnosti ministrstev. Ocene tveganj za posamezne nesreče so naslednje (Uprava Republike Slovenije za zaščito in reševanje, 2021):

1. Potres (nosilec: ministrstvo, pristojno za graditev)
2. Poplave (nosilec: ministrstvo, pristojno za okolje)
3. Nevarnosti biološkega, kemijskega, okoljskega in neznanega izvora na zdravje ljudi (nosilec: ministrstvo, pristojno za zdravje)
4. Posebno nevarne bolezni živali (nosilec: ministrstvo, pristojno za kmetijstvo)
5. Jedrska ali radiološka nesreča (nosilec: ministrstvo, pristojno za okolje)
6. Velik požar v naravnem okolju (nosilec: ministrstvo, pristojno za gozdarstvo)
7. Žled (nosilec: ministrstvo, pristojno za varstvo pred naravnimi in drugimi nesrečami)
8. Nesreče z nevarnimi snovmi (nosilec: ministrstvo, pristojno za okolje)
9. Nesreče na morju (nosilec: ministrstvo, pristojno za promet)
10. Kibernetska tveganja (nosilec: ministrstvo, pristojno za informacijsko družbo in elektronske komunikacije)
11. Bolezni in škodljivci gozdnega drevja (nosilec: ministrstvo, pristojno za gozdarstvo)
12. Letalska nesreča (nosilec: ministrstvo, pristojno za infrastrukturo)
13. Železniška nesreča (nosilec: ministrstvo, pristojno za infrastrukturo)
14. Terorizem (nosilec: ministrstvo, pristojno za notranje zadeve)
15. Suša (nosilec: ministrstvo, pristojno za okolje in prostor)

Vse ocene tveganja so javne in so objavljene na spletnih straneh ministrstev, ki so jih izdelala. Le ocena tveganja za terorizem, ki je označena s stopnjo tajnosti interno, ni javno objavljena. Na vpogled je na voljo na MNZ. Javno dostopna je tudi Državna ocena tveganj za nesreče, tako na sedežu Državnega koordinacijskega organa za ocene tveganj za nesreče in ocene zmožnosti obvladovanja tveganj za nesreče kot na spletni strani RS (Uprava Republike Slovenije za zaščito in reševanje, 2021).

Ker ocene tveganja za posamezne nesreče izdelujejo različna ministrstva, je bil skladno z uredbo ustanovljen tudi Državni koordinacijski organ za ocene tveganj za nesreče, ki se je leta 2017 preimenoval v Državni koordinacijski organ za ocene tveganj za nesreče in ocene zmožnosti obvladovanja tveganj za nesreče (DKO).

Temeljne naloge DKO so (Uprava Republike Slovenije za zaščito in reševanje, 2018):

- usklajevanje, pomoč in podpora ministrstvom pri izdelavi ocen tveganja za posamezne nesreče,
- seznanjanje Vlade RS in Medresorske delovne skupine za ocene tveganj za nesreče,
- poročanje Evropski komisiji skladno z obveznostmi iz Sklepa o mehanizmu Unije na področju civilne zaščite in izdelava Državne ocene tveganj za nesreče.

4.2 Državna ocena tveganj za nesreče

Državna ocena tveganj za nesreče je torej skupna (sintezna) ocena tveganj za nesreče, ki za državo predstavljajo že ugotovljena tveganja. Prva takšna ocena je bila sprejeta leta 2015 in posodobljena v letih 2016 in 2018. Državna ocena tveganj za nesreče naj bi se dopolnjevala na vsaka tri leta (»Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite«, 2014b). Oceno v koordinaciji z nosilci, pristojnimi za izdelavo ocen tveganja za posamezne nesreče, izdeluje Uprava RS za zaščito in reševanje kot DKO, s sklepom pa jo potrdi Vlada RS.

V uvodu Državne ocene tveganj za nesreče (Uprava Republike Slovenije za zaščito in reševanje, 2018) je opredeljeno, da so ocene tveganj za nesreče zaradi narave in širine vsebine lahko podlaga za številne dejavnosti na več področjih, predvsem pri:

- načrtovanju za obvladovanje tveganj za namene preventive in pripravljenosti;
- izvajanju ustreznih ukrepov za preventivo pred tveganji in pripravljenosti;
- izdelavi ocen zmožnosti obvladovanja tveganj za nesreče;
- razvoju finančnih strategij pri preventivnih ukrepih za preprečevanje ali zmanjšanje možnosti za nastanek nesreč ter za ukrepanje, pomoč in odpravo posledic ob nesrečah;
- načrtovanju finančne podlage za obvladovanje tveganj za nesreče, kar vključuje: določitev prednostnih naložb za zmanjšanje možnosti za nastanek nesreč ali njihovih posledic, načrtovanje javnih naložb, načrtovanje socialne zaščite;
- izdelavi ocen ogroženosti in načrtov zaščite in reševanja ob nesreči;
- ugotavljanju vrzeli v silah in sredstvih za zaščito, reševanje in pomoč ter načrtovanju popolnitve in dopolnjevanja sil in sredstev za zaščito, reševanje in pomoč;
- prostorskem načrtovanju.

Državna ocena tveganj za nesreče vsebuje enajst točk:

1. uvod;
2. merila za ovrednotenje vplivov tveganja in verjetnosti za nesreče;
3. povzetke in zaključke ocen tveganja za posamezne nesreče in primerjavo rezultatov analiz tveganja za nesrečo iz ocen tveganja za posamezne nesreče z merili tveganja, vključno z matrikami tveganja za posamezne nesreče;
4. skupno oceno tveganj za nesreče na podlagi rezultatov prejšnje točke, skupne matrike tveganj za nesreče, obravnavane v Državni oceni tveganj za nesreče;
5. pregled izbranih scenarijev posameznih tveganj in scenarijev več mogočih tveganj ter analiz teh tveganj;

6. pregled izbranih scenarijev, ki opredeljujejo potek več mogočih medsebojno neodvisnih nesreč na istem območju ter analiz teh tveganj;
7. zaključek;
8. razlago pojmov, kratic in krajšav;
9. vire;
10. priloge;
11. evidenčni list sprememb, dopolnitev in posodobitev.

V oceno so lahko vključene tudi vsebine iz ocene tveganja zaradi podnebnih sprememb, ki jih zagotovi in koordinira ministrstvo, pristojno za področje podnebnih sprememb. Prav tako se vanjo lahko vključijo tudi vsebine iz obstoječih državnih ocen ogroženosti za posamezno nevarnost naravne ali druge nesreče in druge vsebine.

V nadaljevanju podrobneje predstavljamo še proces analiziranja tveganj, kot poteka pri izdelavi Državne ocene tveganj za nesreče in postopek izračuna ocen.

Slovenska državna ocena tveganj se ravna po smernicah Evropske komisije (2010). Proces ocenjevanja tveganj tako vsebuje naslednje glavne faze: (1) Ugotavljanje tveganja (odkrivanje, prepoznavanje in opisovanje tveganj z oblikovanimi scenariji); (2) Analiza tveganja (ocena verjetnosti in ocena vplivov, opredelitev negotovosti); (3) Ovrednotenje tveganja (primerjava rezultatov z merili tveganja za ugotavljanje (ne)sprejemljivosti stopnje tveganja).

Za ugotavljanje resnosti oz. teže posameznih tveganj je DKO leta 2015 sprejel merila za ovrednotenje vplivov tveganja in verjetnosti za nesreče. Merila so enotna za vsa tveganja, kar omogoča primerjavo rezultatov analiz več scenarijev tveganja v okviru enega tveganja in tudi primerjavo vplivov oz. posledic in verjetnosti za nesrečo posameznega tveganja z drugimi tveganji.

Merila so oblikovana v pet stopenj in se nanašajo na ovrednotenje vplivov tveganja na:

1. ljudi,
2. gospodarske in okoljske vplive tveganja ter vplive tveganja na kulturno dediščino in
3. politične ter družbene vplive tveganja.

Petstopenjska lestvica meril glede na vpliv oz. verjetnost vsebuje naslednje stopnje (Vlada RS, 2018): 1 – zelo majhna, 2 – majhna, 3 – srednja, 4 – velika, 5 – zelo velika. V nadaljevanju predstavljamo posamezna merila za ovrednotenje vplivov tveganja in verjetnosti za nesrečo, kot so zapisana v Državni oceni tveganj za nesreče.

Merila za ovrednotenje vpliva tveganj na ljudi se izražajo s številom mrtvih, ranjenih, bolnih ali trajno preseljenih ljudi, ki ga povzroči neko tveganje. Stopnje vpliva se določijo na podlagi meril, prikazanih spodaj (tabela 4).

Tabela 4: Merila za ovrednotenje vplivov tveganja na ljudi (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Merila za ovrednotenje vplivov tveganja na ljudi	1	2	3	4	5
število mrtvih	do 5	5–10	10–50	50–200	nad 200
število mrtvih (10 let)*	do 5	5–10	10–50	50–100	nad 100
število ranjenih ali bolnih**	do 10	10–50	50–200	200–1000	nad 1000
število ranjenih ali bolnih (10 let)*	do 10	10–50	50–200	200–500	nad 500
število trajno preseljenih	do 20	20–50	50–200	200–500	nad 500

1–5: Stopnje vpliva.

*Za nesreče z morebitnimi dolgotrajnimi učinki (npr. do 10 let), kot so npr. nesreče z nevarnimi snovmi, jedrske ali radiološke nesreče, se dolgoročne vrednosti za mrtve in ranjene ali bolne (10 let), če je treba, določijo posebej oziroma upoštevajo, kot je navedeno zgoraj.

** Med ranjene ali bolne spadajo tudi obsevani, kontaminirani ali zastrupljeni, ki se v analizah tveganj lahko ob posameznih tveganjih obravnavajo posebej.

Merila za ovrednotenje gospodarskih in okoljskih vplivov tveganja in vplivov tveganja na kulturno dediščino se izražajo z višino stroškov in škode, ki jo povzroči neko tveganje. Stopnje vpliva se določijo na podlagi meril, prikazanih spodaj (tabela 5).

Tabela 5: Merila za ovrednotenje gospodarskih in okoljskih vplivov ter vplivov tveganja na kulturno dediščino (Uprava Republike Slovenije za zaščito in reševanje, 2018)

1	2	3	4	5
do 100 milijonov evrov	od 100 milijonov evrov do 0,6 % BDP	0,6 % do 1,2 % BDP	1,2 % do 2,4 % BDP	nad 2,4 % BDP
	100–260 milijonov evrov	260–520 milijonov evrov	520–1040 milijonov evrov	več kot 1.040 milijonov evrov

1–5: Stopnje vpliva.

V preglednici so zaokrožene vrednosti v evrih glede na BDP iz leta 2017 (43,3 milijarde evrov).

Nadalje pa so **merila za ovrednotenje političnih in družbenih vplivov tveganja** polkvalitativna, saj gre v največji meri za ocenjevanje velikostnega reda obravnavanih vplivov, za razliko od prejšnjih dveh skupin vplivov, pri katerih so na voljo pretežno konkretne številke. Končna stopnja političnih in družbenih vplivov tveganja se določi tako, da se seštejejo končne vrednosti oz. stopnje vseh skupin političnih in družbenih vplivov tveganja in se delijo s številom skupin vplivov, torej praviloma s šestimi skupinami. Vplivi tveganja, ki niso bili ocenjeni, se pri tem ne upoštevajo. Pri vrednotenju se ocenjujejo naslednje skupine vplivov in njihove podskupine:

1. *Vpliv tveganja na delovanje državnih organov*. V tem segmentu se ocenjujeta dva vidika:
   a) (Ne)zmožnost opravljanja nalog iz pristojnosti državnih organov (vlada, ministrstva, organi v sestavi, upravne enote) na prizadetem območju. Stopnja vpliva se določi na podlagi kombinirane ocene, ki vključuje opis stopnje okrnjenosti in trajanje motnje v dnevih (tabela 6).

Tabela 6: Merila za ovrednotenje vplivov tveganja na delovanje državnih organov – opravljanje nalog (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Trajanje	Omejena	Zelo okrnjena	Onemogočena
do 2 dni	1	1	2
do 7 dni	1	1	2
do 15 dni	2	2	3
do 30 dni	2	3	4
več kot 30 dni	3	4	5

1–5: Stopnje vpliva.

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če vplivi nesreče ne posegajo v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

   b) Število ljudi, za katere je od državnih organov fizično ali funkcionalno ovirano ali moteno izvajanje storitev. Stopnja vpliva se določi na podlagi kvantitativne ocene, ki vključuje število prizadetih ljudi in čas okrnjenega delovanja v dnevih (tabela 7).

Tabela 7: Merila za ovrednotenje vplivov tveganja na delovanje državnih organov – izvajanje storitev (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Število ljudi/ trajanje	Do 500	Od 500 do 5.000	Od 5.000 do 50.000	Več kot 50.000
do 2 dni	1	1	1	2
do 7 dni	1	2	2	3
do 15 dni	2	3	3	4
do 30 dni	3	4	4	5
več kot 30 dni	4	5	5	5

1–5: Stopnje vpliva.

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

2. *Vpliv tveganja na delovanje pomembnih infrastrukturnih sistemov.* V tem segmentu se prav tako ocenita dva vidika:
   a) Število ljudi, ki se sooča s pomanjkanjem ali oteženim dostopom do pitne vode, hrane in energentov (elektrika, ogrevanje, gorivo). Stopnja vpliva se določi na podlagi kvantitativne ocene, ki vključuje število prizadetih ljudi in čas okrnjenega dostopa v dnevih (tabela 8).

Tabela 8: Merila za ovrednotenje vplivov tveganja na delovanje pomembnih infrastrukturnih sistemov – dostop do dobrin (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Število ljudi/ trajanje	Do 500	Od 500 do 5.000	Od 5.000 do 50.000	Več kot 50.000
do 2 dni	1	1	1	2
do 7 dni	1	2	2	3
do 15 dni	2	3	3	4
do 30 dni	3	4	4	5
več kot 30 dni	4	5	5	5

1–5: Stopnje vpliva.

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če ima več vsebin enako stopnjo vpliva, se upošteva vpliv, zaradi katerega je prizadetih največ ljudi. Če je najmanj v dveh primerih prizadeto enako število ljudi, se upošteva tisti, ki traja dlje.

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

   b) Število ljudi, ki se sooča z okrnjeno ali onemogočeno uporabo interneta in telekomunikacijskih sistemov, prihodom na delovna mesta in v vzgojno-izobraževalne ustanove, uporabo javnih storitev (dostop do medijev, zdravstvene storitve, bančne storitve itn.), uporabo javnega prometa, oskrbo oz. nakupom življenjskih

potrebščin. Stopnja vpliva se določi na podlagi kvantitativne ocene, ki vključuje število prizadetih ljudi in čas okrnjenega dostopa v dnevih (tabela 9).

Tabela 9: Merila za ovrednotenje vplivov tveganja na delovanje pomembnih infrastrukturnih sistemov – uporaba interneta in telekomunikacijskih storitev (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Število ljudi/ trajanje	Do 500	Od 500 do 5.000	Od 5.000 do 50.000	Več kot 50.000
do 2 dni	1	1	1	2
do 7 dni	1	2	2	3
do 15 dni	2	3	3	4
do 30 dni	3	4	4	5
več kot 30 dni	4	5	5	5

1–5: Stopnje vpliva.

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če ima več vsebin enako stopnjo vpliva, se upošteva vpliv, zaradi katerega je prizadetih največ ljudi. Če je najmanj v dveh primerih prizadeto enako število ljudi, se upošteva tisti, ki traja dlje.

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

3. *Psihosocialne vplive tveganja.* V tem segmentu se ocenijo trije vidiki:
   a) Število ljudi, pri katerih nesreča povzroči nenavadno ali neželeno obnašanje (ang. *behavioural reactions*), kot je izogibanje obiskovanju šol, vrtcev, zavestno odsotnost z dela, zavestno izogibanje javnemu prevozu, težnje po preselitvi, neracionalne finančne operacije (npr. množični dvigi gotovine), kopičenje in prisvajanje zalog življenjskih potrebščin ipd. Stopnja vpliva se določi na podlagi kvantitativne ocene, ki vključuje število prizadetih ljudi in čas trajanja nenavadnega vedenja v dnevih (tabela 10).

   b) Socialni vplivi, ki se nanašajo na domet posledic oz. obseg podanih prošenj za dodelitev pomoči, ki jih vložijo prebivalci. Stopnja vpliva se določi na podlagi opisne ocene, koliko skupin prebivalcev občuti posledice in poda prošnjo za socialno pomoč (tabela 11).

Tabela 10: Merila za ovrednotenje psihosocialnih vplivov tveganja – nenavadno ali neželeno vedenje (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Število ljudi/ trajanje	Do 500	Od 500 do 5.000	Od 5.000 do 50.000	Več kot 50.000
do 2 dni	1	1	1	2
do 7 dni	1	2	2	3
do 15 dni	2	3	3	4
do 30 dni	3	4	4	5
več kot 30 dni	4	5	5	5

1–5: Stopnje vpliva.

Upošteva se vpliv, ki povzroči največje posledice in traja najdlje. Če ima več vsebin enako stopnjo vpliva, se upošteva tista, pri kateri je prizadetih največ ljudi, in nato tista, ki traja najdlje. Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevano vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Tabela 11: Merila za ovrednotenje psihosocialnih vplivov tveganja – socialni vplivi (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Vrste socialnih vplivov	Stopnja vpliva
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	se ne ocenjuje (NO)
Majhen/nepomemben vpliv.	1
Revnejši sloji prebivalstva se znajdejo v hudi socialni stiski, poveča se število prošenj za izredno denarno socialno pomoč.	2
Posledice nesreče občuti tudi srednji sloj prebivalstva, to se kaže v povečanem številu vlog za izredno denarno socialno pomoč.	3
Posledice nesreče občuti večina prebivalstva, kar se kaže v velikem povečanju števila vlog za socialno pomoč.	4
Posledice občutijo vsi prebivalci, kar se kaže predvsem z novimi vlogami za socialno pomoč ter ponovnimi vlogami za dodelitev pomoči.	5

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

c) Psihološki vplivi, ki se nanašajo na pojav strahu in zaupanje prebivalcev. Stopnja vpliva se določi na podlagi opisne ocene razširjenosti strahu med prebivalci, nezaupanja v delovanje pristojnih organov in težnje po preseljevanju (tabela 12).

4. *Vpliv tveganja na notranjepolitično stabilnost.* Stopnja vpliva se določi na podlagi opisne ocene obsežnosti oz. števila kršitev javnega reda in miru, razširjenosti strahu za varnost in nezaupanja v delovanje državnih institucij med prebivalstvom ter stanja notranjepolitične stabilnosti (tabela 13).

Tabela 12: Merila za ovrednotenje psihosocialnih vplivov tveganja – psihološki vplivi (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Vrste psiholoških vplivov	Stopnja vpliva
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	se ne ocenjuje (NO)
Majhen/nepomemben vpliv.	1
Pojavljajo se posamezni primeri strahu med prebivalci zaradi nepoznavanja vzrokov in značilnosti nesreče ter njenih posledic.	2
Povečan je pojav strahu med prebivalci, predvsem pred novo nesrečo in njenimi posledicami.	3
Med prebivalci vlada strah za obstanek, zaupanje v pristojne organe, povezane z odzivom ter odpravljanjem posledic nesreče, upade, povečuje se želja po preselitvi.	4
Zaradi negativnih dogodkov ali posledic nesreče je večina ljudi izgubila zaupanje v to, da bi se življenje na prizadetem območju lahko vrnilo v normalne okvire, pojavlja se množično preseljevanje.	5

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

Tabela 13: Merila za ovrednotenje vpliva tveganja na notranjepolitično stabilnost (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Vrste vplivov	Stopnja vpliva
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	se ne ocenjuje (NO)
Majhen/nepomemben vpliv.	1
Pojavljajo se posamezni primeri javnega izražanja nestrinjanja z ukrepanjem pristojnih institucij ali posamezne motnje delovanja političnih institucij (vlada, parlament itn.) ter posamezni pojavi sovražnih kampanj.	2
Znani so posamezni primeri kršitev javnega reda in miru ter kaznivih dejanj zaradi nesreče in izražanje občutka strahu za svojo varnost in premoženje; posamezniki ali skupine skušajo omajati notranjepolitične razmere, zmanjšano je zaupanje prebivalstva v delovanje političnih institucij.	3
Povečano je število kršitev javnega reda in miru ter organiziranih kaznivih dejanj, povečan je tudi strah med prebivalstvom; politične stranke in druge interesne skupine skušajo spodkopati notranjepolitično stabilnost ter pridobiti politične koristi z »vsiljevanjem« svojih programov za izboljšanje razmer, zmanjšano je zaupanje v delovanje državnih institucij.	4
Kršitve javnega reda in miru, vključno z nasilnimi demonstracijami, so množične, veliko več je kaznivih dejanj, notranja varnost države je ogrožena. Notranjepolitična stabilnost države je spodkopana, temeljne ustavno zagotovljene pravice in vrednote so ogrožene in razvrednotene.	5

Če se oceni, da vplivi nesreče ne morejo posegati v ocenjevano vsebino, se stopnja vpliva ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np). Vrednost te skupine vplivov je lahko le celo število.

Tabela 14: Merila za ovrednotenje vpliva tveganja na finančno stabilnost – plačilna sposobnost zaradi nedelovanja plačilnega prometa (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Vrednost izpada Trajanje izpada	Izpad poravnave plačil v vrednosti, manjši kot 10 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti, med 10 % in 20 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti med 20 % in 50 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti med 50 % in 80 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj	Izpad poravnave plačil v vrednosti, večji kot 80 % načrtovane vrednosti plačilnega prometa v obdobju trajanja motenj
Ni vpliva, ker vplivi nesreče ne morejo posegati v ocenjevano vsebino.	se ne ocenjuje (NO)	se ne ocenjuje (NO)	se ne ocenjuje (NO)	se ne ocenjuje (NO)	se ne ocenjuje (NO)
Motnje v plačilnem prometu, ki trajajo do 2 uri.	1	1	2	3	3
Motnje v plačilnem prometu, ki trajajo do 4 ure.	1	2	2	3	4
Motnje v plačilnem prometu, ki trajajo do 8 ur.	2	3	3	4	4
Motnje v plačilnem prometu, ki trajajo ves poslovni dan, ali motnje, ki do konca poslovnega dne niso odpravljene.*	3	4	4	5	5
Motnje v plačilnem prometu, ki trajajo več kot en poslovni dan.	4	5	5	5	5

1–5: Stopnje vpliva.

* Motnje ob koncu poslovnega dne, tudi če je obdobje motenj kratko, lahko povzročijo enodnevni zamik poravnave plačil.

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Ne upoštevajo se tudi vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

5. *Vpliv tveganja na finančno stabilnost.* V tem segmentu se ocenijo trije vidiki:
   a) Vpliv na plačilno sposobnost pravnih in fizičnih oseb zaradi nedelovanja plačilnega prometa. Stopnja vpliva se določi na podlagi kvantitativne ocene, ki vključuje delež (%) izpada plačilnega prometa in časa trajanja motnje v urah (tabela 14).

   b) Vpliv na plačilno sposobnost pravnih in fizičnih oseb zaradi pomanjkanja gotovine. Stopnja vpliva se določi na podlagi kvantitativne ocene, ki vključuje število prizadetih oseb in trajanje motnje v dnevih (tabela 15).

Tabela 15: Merila za ovrednotenje vpliva tveganja na finančno stabilnost – plačilna nesposobnost zaradi pomanjkanja gotovine (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Število prizadetih oseb/trajanje	Do 5.000	Do 50.000	Več kot 50.000
do 2 dni	1	2	3
od 2 do 7 dni	2	3	4
več kot 7 dni	3	4	5

Če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se vpliv nesreče na ocenjevalno vsebino ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).
Legenda:
1 – Ni nobenega vpliva oziroma je majhen.
2 – Gotovina je pravnim in fizičnim osebam težje dostopna v njihovem kraju.
3 – Gotovina je pravnim in fizičnim osebam dostopna v sosednjih krajih.
4 – Gotovina je pravnim in fizičnim osebam dostopna v večjih mestih oziroma posameznih krajih.
5 – Gotovina ni dostopna.

Tabela 16: Merila za ovrednotenje vpliva tveganja na finančno stabilnost – sprememba BDP (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Sprememba rasti BDP	Stopnja vpliva
ni vpliva, ker vplivi nesreče ne posegajo v vsebino/brez posledic	se ne ocenjuje (NO)
od 0 do –0,5 odstotne točke	1
do –1 odstotne točke	2
do –1,5 odstotne točke	3
do –2 odstotni točki	4
več kot –2 odstotni točki	5

Če se oceni, da nesreča ne bo imela negativnega vpliva na gibanje BDP oziroma če vplivi nesreče ne morejo posegati v ocenjevano vsebino, se stopnja vpliva ne ocenjuje (NO). Ne upoštevajo se vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np).

c) Spremembe rasti BDP zaradi posledic nesreče v letu nesreče ali naslednjem letu. Stopnja vpliva se določi na podlagi kvantitativne ocene vpliva, ki ga ima tveganje na gibanje BDP v odstotnih točkah (tabela 16).

6. Vpliv tveganja na zunanjepolitično oz. mednarodno stabilnost, ki se nanaša na to, kako tveganje vpliva na mednarodni položaj države, prejem mednarodne pomoči in odzivanje drugih držav. Stopnja vpliva se določi na podlagi opisne ocene spremembe položaja države v mednarodnem okolju, višine prejete mednarodne pomoči, mednarodne odmevnosti dogodka in stopnje zaskrbljenosti drugih držav (tabela 17).

Tabela 17: Merila za ovrednotenje vpliva tveganja na zunanjepolitično stabilnost (Uprava Republike Slovenije za zaščito in reševanje, 2018)

Vrsta zunanjepolitičnega oziroma mednarodnega vpliva	Stopnja vpliva
Vplivi nesreče ne morejo posegati v ocenjevano vsebino.	se ne ocenjuje (NO)
Majhen/nepomemben vpliv.	1
Ni nobenega večjega neposrednega vpliva na mednarodni položaj države, ki bi bil zaznan. Posamezne tuje države spremljajo dogajanje v RS.	2
Posamezne (sosednje) države in nekatere regionalne ter mednarodne organizacije se po diplomatski poti odzivajo na dogodek z izražanjem podpore ali zaskrbljenosti zaradi razmer.	3
Del mednarodne skupnosti (države, mednarodne organizacije) se odziva na dogodek z izražanjem močne podpore ali zaskrbljenosti zaradi razmer. RS je deležna mednarodne pomoči, predvsem v opremi in človeških virih. Kljub mednarodni pomoči je še vedno stabilna država. Tuja diplomatsko-konzularna predstavništva v RS svojim državljanom odsvetujejo potovanja na nekatera območja v RS.	4
Večji del mednarodne skupnosti se intenzivno odziva na dogodke v državi, saj dogodki močno vplivajo na varnost drugih držav. RS je deležna večje mednarodne pomoči (oprema, denar, človeški viri). Za normalno delovanje celotnega sistema RS nujno potrebuje pomoč. Tuja diplomatsko-konzularna predstavništva svojim državljanom odsvetujejo potovanja v RS in zaradi razmer zmanjšujejo ali povečujejo število osebja v predstavništvih. Mednarodni dogodki, katerih glavna tema je položaj oziroma razmere v RS.	5

Če se oceni, da vplivi nesreče ne morejo posegati v ocenjevano vsebino, se stopnja vpliva ne ocenjuje (NO). Prav tako se ne upoštevajo vplivi, ki so povezani z ocenjevano vsebino, a zaradi različnih vzrokov niso bili ocenjeni (Np). Vrednost te skupine vplivov je lahko le celo število.

Poleg ocene predstavljenih vplivov se ovrednoti še verjetnost nastanka nesreče, ki se prav tako poda na lestvici od 1 do 5. Ocena, da se bo tveganje uresničilo, se določi na podlagi kvantitativne in opisne napovedi, ki vključuje verjetnost pojava dogodka na letni ravni v deležu (%) in pojasnilo stopnje nevarnosti (tabela 18).

Tabela 18: Ocena verjetnosti nastanka nesreče (Uprava Republike Slovenije za zaščito in reševanje, 2018)

1	2	3	4	5
enkrat na več kot 250 let (letna verjetnost do 0,4 %)	Enkrat na 100 do 250 let (letna verjetnost od 0,4 do 1 %)	enkrat na 25 do 100 let (letna verjetnost od 1 do 4%)	enkrat na 5 do 25 let (letna verjetnost od 4 do 20 %)	enkrat ali večkrat na 5 let (letna verjetnost nad 20 %)
ni skoraj nobene nevarnosti (grožnje)	mogoča, vendar malo verjetna nevarnost (grožnja)	mogoča nevarnost (grožnja)	splošna nevarnost (grožnja)	posebna in takojšnja (trajna) nevarnost (grožnja)

Opisna razlaga se uporablja predvsem za nesreče, ki nimajo nekega naravnega cikla pojavljanja, oziroma za namerna dejanja, ki jih je glede na posebnosti pojavljanja nemogoče napovedati (npr. terorizem). Za druge nesreče se upoštevajo v zgornjem delu preglednice navedena časovna obdobja.

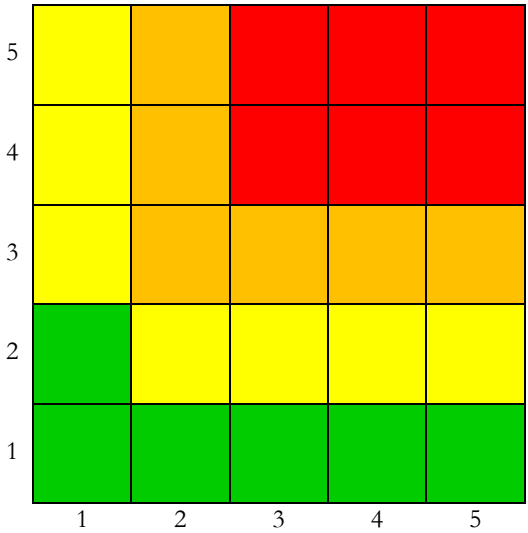
Matrike tveganja za nesreče se uporabljajo za grafični prikaz vplivov tveganja in verjetnosti tveganja (predstavljene na tabeli 19) za nesreče oz. posamezne scenarije tveganja, če se obravnava le eno tveganje. Matrike tveganja so eden glavnih ciljev pri izdelavi ocen tveganja za posamezne nesreče oz. pri Državni oceni tveganj za nesreče.

Matrike tveganja za nesreče (tabela 19) imajo pet polj na ordinatni osi za prikaz velikosti vplivov tveganja in pet polj na abscisni osi za prikaz stopnje verjetnosti tveganja. Polja so obarvana od zelene do rdeče, pri čemer se stopnje vplivov in verjetnosti stopnjujejo od zelene preko rumene in oranžne do rdeče barve. Obarvanost polj od zelene do rdeče se hitreje spreminja na ordinatni osi kot na abscisni, kar pomeni, da je v matrikah tveganja za nesreče večji poudarek na vplivih tveganja kot na verjetnosti tveganja za nesrečo. Matrika ima skupaj 25 polj, v katera odvisno od vsebine matrike lahko uvrstimo posamezna tveganja (ali posamezne vplive tveganja) glede na odnos med velikostjo v analizah tveganja ugotovljenih vplivov in merili za ovrednotenje tveganja za nesrečo. Enako velja tudi za verjetnost tveganja. Kombinacija verjetnosti in vplivov je v matrikah tveganja za nesreče predstavljena v štirih stopnjah:

- majhno tveganje z zeleno obarvanimi polji,
- srednje tveganje z rumeno obarvanimi polji,
- veliko tveganje z oranžno obarvanimi polji,
- zelo veliko tveganje z rdeče obarvanimi polji.

Obenem pri končni oceni nosilec ovrednoti še zanesljivost scenarijev na podlagi poznavanja pojava. Ocena zanesljivosti temelji predvsem na pogostosti pojava obravnavane nesreče, resničnosti scenarija, pa tudi od kakovosti podatkov, ki so bili uporabljeni v analizi tveganja.

Tabela 19: Matrika tveganja za nesreče
(Uprava Republike Slovenije za zaščito in reševanje, 2018)



STOPNJE VPLIVOV IN VERJETNOSTI	
5	zelo velika
4	velika
3	srednja
2	majhna
1	zelo majhna

STOPNJE TVEGANJA	
	zelo velika
	velika
	srednja
	majhna

ZANESLJIVOST REZULTATOV ANALIZ TVEGANJA	BARVA ZAPISA V MATRIKI TVEGANJA
razmeroma zanesljiva	črna
srednje zanesljiva	temno siva
razmeroma nezanesljiva	svetlo siva

4.3 Primer državne ocene tveganj: kibernetska tveganja

V okviru državne ocene tveganj in na podlagi »Uredbe o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite« (2014) je Direktorat za informacijsko družbo (2018) v okviru Ministrstva za javno upravo RS izdelal nacionalno oceno kibernetskih tveganj. Njen namen je, da se celovito ugotovijo in opišejo pojavne oblike kibernetskih tveganj v Sloveniji, njihove značilnosti in posledice ter obseg posledic, ki ga lahko pričakujemo v primeru uresničitve izbranih scenarijev.

Ocena kibernetskih tveganj je metodološko in procesno usklajena s procesom izvedbe državne ocene tveganja za nesreče. Pri izdelavi ocene so bili uporabljeni strokovni in poljubni viri ter več raziskovalnih metod, kot so: deskriptivna metoda, zgodovinska metoda in metoda analize ter sinteze. Pri tem so se proučili različna področja kibernetskih groženj, njihovi akterji, vektorji napadov in pretekli zgodovinski dogodki.

V dokumentu je sprva podana klasifikacija, ki zajema 15 različnih najpogostejših in najnevarnejših kibernetskih groženj, kot jih opredeljuje ENISA (Agencija EU za varnost omrežij in informacij), hkrati pa je podan še kratek opis vsake grožnje. Grožnje, vključene v oceno, so: škodljiva koda (ang. *malware*); spletni napadi (ang. *web based attacks*); napadi na spletne aplikacije (ang. *web application attacks*); zvabljanje (ang. *phishing*); nezaželena elektronska pošta (ang. *spam*); onemogočanje storitve (ang. *denial of service*); izsiljevalsko programje (ang. *ransomware*); botneti; grožnje od znotraj (ang. *insider threat*); fizična manipulacija/poškodba/kraja/izguba (ang. *physical manipulation/damage/theft/loss*); kršitev varnosti osebnih podatkov (ang. *data breaches*); kraja identitete (ang. *identity theft*); odtekanje informacij (ang. *information leakage*); kompleti za izkoriščanje (ang. *exploit kits*); kibernetsko vohunjenje (ang. *cyber-espionage*).

Za omenjeno klasifikacijo groženj je poudarjena še nevarnost hibridnih groženj, ki se nanaša na kompleksno kombinacijo kompleksnih tradicionalnih, nereguliranih vojaških ali nevojaških dejavnosti, ki spremljajo kibernetske grožnje (ekonomske, politične, propagandne, kriminalne dejavnosti).

Opisu groženj nato sledi klasifikacija in opis sedmih skupin akterjev, ki povzročajo omenjene grožnje. Glavni storilci, ki ustvarjajo grožnje, so: kibernetski kriminalci; osebe znotraj; države; hektivisti; kibernetski bojevniki; kibernetski teroristi; hekerski malčki (ang. *script kiddies*).

Za opisom navedenih elementov sledi povezovanje posameznih akterjev s posameznimi grožnjami. Zatem so opredeljeni še vektorji napadov. To so sredstva, s katerimi lahko akter kibernetske grožnje zlorabi slabost ali ranljivost na napadenih sredstvih (vključno z ljudmi), da doseže določen cilj. Poznavanje vektorjev napada je pomembno za razumevanje delovanja različnih kibernetskih groženj, tehnik, taktik in postopkov ter za učinkovito obrambo pred njimi. Skupaj je opredeljenih 13 vektorjev s pripadajočimi podskupinami (npr. napad na človeški element vključuje socialni inženiring, zvabljanje, prevare, zbiranje javno dostopnih podatkov; vektorji napada na spletu in v brskalnikih pa so prenosi ali rudarjenje v mimohodu, zlonamerne skripte ali strani, kompleti za izkoriščanje, oglaševanje škodljive kode itd.).

Opisane vsebine so pomembne za razumevanje narave groženj in prepoznavanje možnosti za njihovo preprečevanje oz. učinkovito spopadanje. Splošni del ocene vključuje še opis ureditve sistema upravljanja kibernetske varnosti v Sloveniji in predstavitev statističnih podatkov glede zaznanih napadov v Sloveniji.

Ključni del ocene tveganja pa so scenariji tveganj. Scenariji tveganj opisujejo okoliščine in posledice nekega dogodka in so narejeni z namenom, da se ugotovijo in ocenijo te posledice v primeru uresničitve grožnje. Predstavljajo pa tudi pomembno podlago za samo analizo tveganja. V oceni so opredeljeni trije taki scenariji (S1 – Napad na spletišča državne uprave; S2 – Napad z izsiljevalskim programjem; S3 – Napad na kritično infrastrukturo v energetskem sektorju). Vsi temeljijo na resničnih kibernetskih napadih, od katerih se je eden zgodil v Sloveniji, drugi je imel svetovne razsežnosti, vključno v Sloveniji, tretji pa se je uresničil v Ukrajini. V oceni so predstavljeni zgolj osnovni scenariji, brez vključitve delovanja več kibernetskih groženj.

Najprej je vsak izmed treh scenarijev podrobno opisan. Vsak opis vsebuje opredelitev naslednjih elementov:

- Kdaj se je dogodek zgodil?
- Kje je prizadeto območje?
- Kaj se je zgodilo?
- Kako je prišlo do tega?

- Kdo je bil napaden/koga je dogodek prizadel?
- Kdo je za dogodek/napad odgovoren?
- Kakšne so bile posledice?

Ker so bili scenariji narejeni po dogodkih, ki so se že zgodili, vsebujejo tudi informacije, kako so se takrat odgovorni soočili z negativnimi posledicami. Vsak scenarij je pravzaprav podlaga za nadaljnjo analizo tveganja.

Po izdelavi scenarijev sledi ocena verjetnosti in zanesljivosti scenarijev tveganja. Za vsak scenarij posebej se opisno oceni, kako verjeten je in kdo bi lahko bil krivec zanj ter njihova zanesljivost, ki je glede na to, da temeljijo na preteklih resničnih dogodkih, dokaj velika.

Na začetku analize se predstavi tveganje, pretekli podobni primeri in verjeten akter. Če gre za podrobnejšo analizo, se lahko predstavi tudi sam postopek oz. koraki, kako je prišlo do uresničitve tveganja. V primeru, da lahko do uresničitve pride na različne načine, naj se predstavijo vsi ali pa vsaj najverjetnejši.

V nadaljevanju se nato pregleda, kakšne bi lahko bile dejanske posledice uresničitve posameznega kibernetskega napada. Poimensko se izpostavijo ogrožene organizacije, sistemi, infrastrukture, spletne strani ipd., katerih okužba oz. targetiranost bi imela vplive na ljudi, gospodarstvo ali okolje, kulturno dediščino ter politiko in družbo. V analizi je treba opredeliti še, v kolikšnem obsegu se bo merila škoda (npr. ali se bo upoštevala zgolj škoda poslovnih subjektov, kritične infrastrukture, posameznikov).

Pri posameznih tveganjih se nato številsko izpostavi, koliko procesov, ki bi drugače potekali, bi bilo z uresničitvijo tveganja onemogočenih, kar se izračuna na podlagi lanskoletnih poročil. Na podlagi tega je potem izračunana škoda, ki je izražena v evrih. V primeru napada na kritično infrastrukturo se lahko posledice izrazijo tudi z deležem BDP države. Denimo, če pride do napada na kritično infrastrukturo v energetskem sektorju, se lahko zgodi, da se onemogoči delovanje podjetij po Sloveniji. Posledice za državo bi bile lahko katastrofalne.

Vplivi tveganja, ki so vključeni v oceno so: vplivi na ljudi (izraženi v številu mrtvih, ranjenih ali bolnih in trajno evakuiranih ljudi); gospodarski in okoljski vplivi ter vplivi na kulturno dediščino (izraženi v številu in višini škode v evrih in skozi vpliv na gibanje BDP); politični in družbeni vplivi (izraženi v obliki polkvalitativnih merilih). Po oceni vseh relevantnih posameznih vplivov in skupnih vplivov se nato izračuna končni vpliv tveganja. Stopnja skupnega vpliva se izračuna tako, da seštevek stopenj vseh treh skupin vplivov deli s tri. V primeru, da ima kateri koli vpliv za stopnjo decimalno številko, se mu dodeli celo število po naslednjem merilu (tabela 20):

Tabela 20: Merilo za zaokroževanje ocene vpliva tveganj v primeru decimalnih števil (Direktorat za informacijsko družbo, 2018)

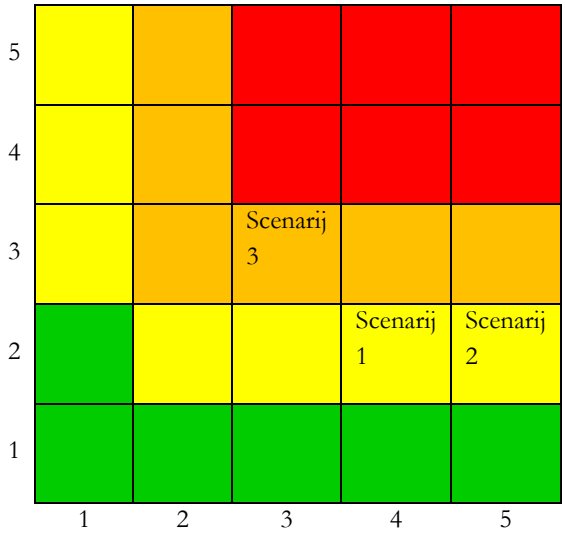
Izračunana vrednost vseh treh vrst vplivov	Stopnja vpliva tveganja v matrikah tveganja z združenim prikazom vplivov tveganja
Do 1,49	1
1,50–2,49	2
2,50–3,49	3
3,50–4,49	4
4,50–5,00	5

Ko so skozi predstavljene korake pridobljeni vsi podatki za oceno tveganja, se združeno v preglednici prikažejo vsi pomembni izračuni in ocene, kot je prikazano v primeru spodaj (tabela 21).

Tabela 21: Preglednica izračunov za oceno tveganja (Direktorat za informacijsko družbo, 2018)

Scenariji tveganja	Stopnja vplivov na ljudi	Stopnja gospodarskih in okoljskih vplivov in vplivov na kulturno dediščino	Stopnja političnih in družbenih vplivov	Izračunana vrednost skupnih (povprečnih) vplivov	Stopnja skupnih (povprečnih) vplivov tveganja	Verjetnost	Zanesljivost rezultatov analize tveganja
Scenarij tveganja 1	/	1	2	1,50	2	4	Razmeroma zanesljiva
Scenarij tveganja 2	2	1	2	1,67	2	5	Srednje zanesljiva
Scenarij tveganja 3	4	3	3	3,33	3	3	Razmeroma zanesljiva
Reprezentativni scenarij in analiza tveganja (S2)	2	1	2	1,67	2	5	Srednje zanesljiva

Tabela 22: Matrika scenarijev (Direktorat za informacijsko družbo, 2018)



STOPNJE VPLIVOV IN VERJETNOSTI	
5	zelo velika
4	velika
3	srednja
2	majhna
1	zelo majhna

STOPNJE TVEGANJA	
	zelo velika
	velika
	srednja
	majhna

ZANESLJIVOST REZULTATOV ANALIZ TVEGANJA	BARVA ZAPISA V MATRIKI TVEGANJA
razmeroma zanesljiva	črna
srednje zanesljiva	temno siva
razmeroma nezanesljiva	svetlo siva

Vsi ti podatki se nato predstavijo še v združeni ali razdruženi matriki. V primeru, da se vplivi tveganja prikazujejo posamezno, bodo prikazane tri matrike, kjer je za vsakega izmed vplivov opredeljena njihova stopnja. Matrike so ne glede na izbran način prikaza za vse vplive enake. Končna merila za ovrednotenje tveganja in verjetnosti za izvedbo grožnje so enotna na ravni URSZR za vsa tveganja in so razdeljena na pet stopenj: 1. zelo majhno tveganje in 5. zelo veliko tveganje. Posamezen scenarij se na podlagi ocene umesti v matriko s pripadajočo legendo, z barvo pisave pa se označi še njegova stopnja zanesljivosti, kot je prikazano na tabeli 22. Kot vizualni pripomoček se pri analizi lahko dodajo tudi grafi in tabele, da si

bralec lažje razlaga informacije oz. predstavlja, kakšna škoda bi pravzaprav nastala ali pa zgolj kot pripomoček za predstavitev časovnega razvoja tveganja.

4.4 Ocena tveganj na področju kritične infrastrukture

»Zakon o kritični infrastrukturi (ZKI)« (2017) od upravljavcev kritične infrastrukture zahteva izdelavo ocene tveganj. Podlaga za izdelavo ocene so »Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije« (2019), ki ga je sprejelo Ministrstvo za infrastrukturo in strokovne usmeritve, ki jih pripravijo nosilci sektorjev kritične infrastrukture.[7]

Ocena tveganj za delovanje kritične infrastrukture je v zakonu opredeljena kot rezultat celovitega postopka identifikacije, analize in ovrednotenja različnih virov tveganj za delovanje kritične infrastrukture, ki se izvede za zagotovitev podlage za zaščito kritične infrastrukture.

Skladno z zakonom morajo upravljavci na podlagi izvedene ocene tveganj in na podlagi pričakovanih posledic povečane ogroženosti prav tako definirati stalne in začasne ukrepe za zaščito kritične infrastrukture. Stalni ukrepi se pri tem izvajajo v vseh razmerah, lahko pa se stopnjujejo ob povečani ogroženosti, izrednih dogodkih ali krizah. Dodatni ukrepi pa se izvedejo, če v takšnih razmerah oz. situacijah stopnjevalni ukrepi ne zadostujejo.

Navodilo za ocenjevanje tveganj določa temeljne podlage za izdelavo, postopek izdelave ter obveznosti in posodabljanje ocen tveganja za delovanje kritične infrastrukture. Oceno tveganja izdelujejo posamezni upravljavci kritične infrastrukture, sprejme pa jo predstojnik ali organ upravljanja upravljavca. Ocena tveganja temelji na identifikaciji, analizi in ovrednotenju različnih virov tveganj za delovanje kritične infrastrukture. Skladno z navodili mora ocena tveganja vsebovati:

1. Strokovne usmeritve pristojnega nosilca sektorja kritične infrastrukture, kar obsega opise: značilnosti posameznega sektorja; pomena posledic uničenja ali prekinitve delovanja; metodologije in smernic za ocenjevanje

[7] Sektorji kritične infrastrukture so sektor energetike, sektor prometa, sektor prehrane, sektor preskrbe s pitno vodo, sektor zdravstva, sektor financ, sektor varovanja okolja ter sektor informacijsko-komunikacijskih omrežij in sistemov.

tveganj; ključnih tveganj in vpliva mednarodnega okolja na delovanje kritične infrastrukture.

2. Opis stanja kritične infrastrukture v razmerah rednega delovanja, kjer se opredelijo: poslanstvo in temeljne naloge upravljavca; tehnološke in materialno-tehnične zmogljivosti nalog; kadrovske zmogljivosti; finančne vire in; druge zmogljivosti za izvajanje poslanstva in temeljnih nalog kritične infrastrukture.
3. Seznam identificiranih virov tveganj za delovanje kritične infrastrukture: seznam naredi upravljavec.
4. Opisno analizo in ovrednotenje virov tveganj za delovanje kritične infrastrukture, kjer upravljavec opredeli: verjetnost uresničitve vira tveganja; resnost potencialne škode; potencialne vplive uresničitve na poslovne procese in druge dejavnike. Na podlagi tega upravljavec ovrednoti in določi vire, ki lahko povzročijo izredni dogodek ali krizo pri delovanju kritične infrastrukture.

Pri izdelavi ocene lahko upravljavci uporabijo veljavne standarde in metode ter upoštevajo obstoječe ocene ogroženosti in tveganj za opravljanje dejavnosti kritične infrastrukture. Upravljavec je dolžan posodobiti oceno ob nastanku novih okoliščin, ki lahko na delovanje kritične infrastrukture pomembno vplivajo, oz. najmanj enkrat letno. V primeru, da pride do sprememb ocene tveganja, mora upravljavec pridobiti soglasje pristojnega nosilca sektorja.

4.5 Nacionalna in sektorska ocena tveganj za pranje denarja in financiranje terorizma

Ocena tveganja za pranje denarja in financiranje terorizma (PD/FT) se izdeluje na nacionalni in sektorski ravni.

4.5.1 Ocena tveganj na nacionalni ravni

Ukrepe, pristojne organe in postopke v zvezi z odkrivanjem in preprečevanjem pranja denarja in financiranja terorizma v Sloveniji ureja »Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1)« (2016), ki v slovenski pravni red prenaša evropsko zakonodajo o preprečevanju uporabe finančnega sistema za pranje denarja ali financiranja terorizma.

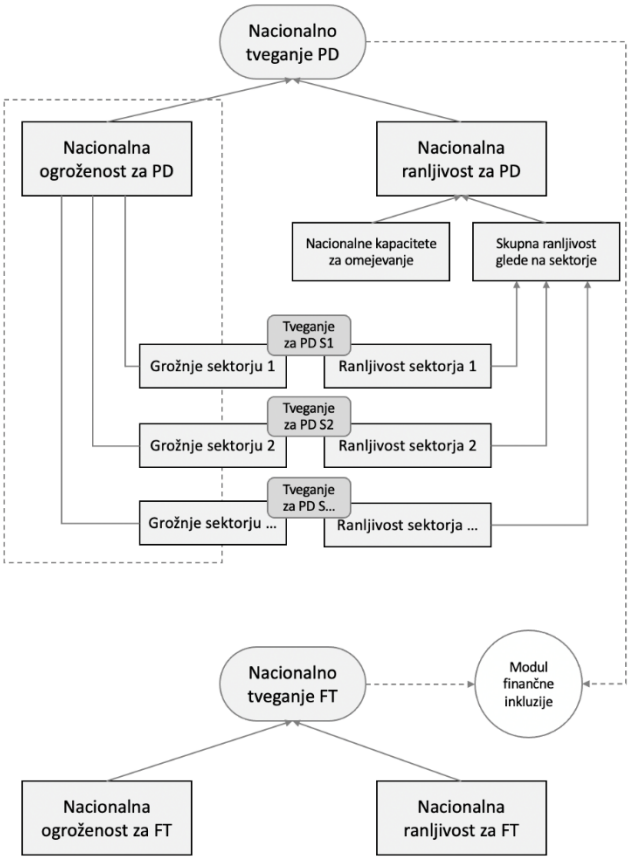
V zakonu je določeno, da za ugotovitev, oceno, razumevanje in ublažitev tveganj PD/FT RS izvaja nacionalno oceno tveganja za pranje denarja in financiranje terorizma, ki se posodobi najmanj vsake štiri leta. Vlada za izvedbo nacionalne ocene tveganja ustanovi stalno medresorsko delovno skupino,[8] ki jo usmerja in usklajuje Urad RS za preprečevanje pranja denarja v okviru Ministrstva za finance (UPPD). Med drugim so ugotovitve nacionalne ocene tveganja namenjene ugotavljanju sektorjev ali dejavnosti neznatnega ali povečanega tveganja PD/FT ter opredeljevanju prednostne razporeditve vseh virov in sredstev, namenjenih za preprečevanje PD/FT.

Nacionalna ocena tveganja je v zakonu opredeljena kot proces identifikacije in analize glavnih tveganj PD/FT v določeni državi, razvijanja ustreznih ukrepov preprečevanja PD/FT na podlagi ugotovljenih tveganj ter čim bolj učinkovitega usmerjanja razpoložljivih virov za nadzor, ublažitev oz. odpravo ugotovljenih tveganj. Tveganje PD/FT pa je v zakonu opredeljeno kot tveganje, da bo stranka izrabila finančni sistem za pranje denarja ali financiranje terorizma oz. bo stranka poslovno razmerje, transakcijo, produkt, storitev ali distribucijsko pot ob upoštevanju dejavnika geografskega tveganja (država ali geografsko območje) posredno ali neposredno uporabila za pranje denarja ali financiranje terorizma.

UPPD za namen priprave nacionalne ocene tveganja na letni ravni med drugim zbira statistične podatke o številu sporočenih sumljivih transakcijah, ki so mu bile poslane v skladu z zakonom, številu in deležu sumljivih transakcij, na podlagi katerih so bili uvedeni ukrepi iz pristojnosti policije, tožilstva ali sodišča, številu prejetih, zavrnjenih in odgovorjenih zaprosil tujih finančnih obveščevalnih enot, razčlenjenih po državah, številu podanih zaprosil tujim finančnim obveščevalnim enotam, razčlenjenim po državah.

Slovenija nacionalno oceno tveganja za PD/FT izdeluje z uporabo metodologije Svetovne banke. Proces in model za izdelavo prikazuje slika 9.

[8] Skupino vodi UPPD, v njej pa poleg urada sodelujejo še predstavnik Ministrstva za pravosodje, MNZ, Ministrstva za finance, Policije, Vrhovnega državnega tožilstva RS, Vrhovnega sodišča RS, Finančne uprave RS, Komisije za preprečevanje korupcije, Slovenske varnostno-obveščevalne agencije, Banke Slovenije, Agencije za trg vrednostnih papirjev, Agencije za zavarovalni nadzor, Tržnega inšpektorata RS, Agencije RS za javnopravne evidence in storitve, Statističnega urada RS, Agencije za javni nadzor nad revidiranjem in po potrebi tudi predstavniki drugih organov (Urad RS za preprečevanje pranja denarja, 2021).



Slika 9: Orodje Svetovne banke za pripravo nacionalne ocene tveganja na področju PD/FT (povzeto po World Bank Group, 2015)

Izdelava ocene traja nekje med osem in 12 mesecev ter zajema tri faze:

- V prvi fazi, tj. fazi priprav, Svetovna banka svetuje, kako naj se sestavi delovna skupina za izdelavo nacionalne ocene tveganja ter kateri so nujni primarni podatki.
- V drugi fazi, tj. izdelavi ocene, se delo začne s tridelno delavnico, na kateri so člani delovne skupine seznanjeni z načinom dela, potekajo pa tudi delavnice z viharjenjem možganov glede PD/FT v državi ter izveden je trening uporabe orodja za oceno tveganja. Druga faza po navadi traja med pet in 10 mesecev in v tem času Svetovna banka nudi

potrebno pomoč. Znotraj druge faze se naredi vpogled v ranljivost in ogroženost posameznega sektorja in ti vpogledi potem omogočajo tudi argumentacijo za izdelavo krovne – nacionalne ocene. Predvsem rezultati sektorskih analiz ranljivosti so uporabljeni pri skupni oceni ranljivosti za PD/FT.

– Tretja faza predstavlja finalizacijo procesa, kjer se prav tako izvede tridnevna delavnica, na kateri se pridobljeni rezultati kot tudi akcijski načrt za zmanjševanje tveganj, povezanih s PD/FT, prediskutirajo ter predstavijo ključnim deležnikom in odločevalcem.

Smernice Svetovne banke so precej konkretne v navodilih in nasvetih, katere podatke, informacije in indikatorje naj delovne skupine pridobijo ter analizirajo. Omogoča tudi analizo scenarijev in tako združuje uporabo kvalitativnih in kvantitativnih pristopov. Prvo orodje svetovne banke je vključevalo tudi tabele v programskem orodju Excel, v katere so lahko delovne skupine vnašale pridobljene podatke in ki so potem omogočale lažje (pre)kalkulacije v končne ocene. Svetovna banka je prvotno orodje nagradila z vključitvijo Bayesovih mrež (ang. *Bayesian Network*), ki se poglavitno uporablja pri računanju verjetnosti. Tudi po tej dopolnitvi je Excel ostal primarno orodje, v katero se vnašajo podatki in tudi ocene ocenjevalcev. Te ocene so v razponu med 0,00 in 1,00, in sicer v petih razredih, kar je pri svojem delu povzela tudi Slovenija. Orodje je dovolj fleksibilno, da se lahko brez večjih posebnosti prilagodi za delo v posamezni državi (FATF, 2021; World Bank Group, 2015, 2016). Slednje je vidno v slovenski nacionalni oceni ogroženosti za PD/FT, ki jo izdeluje medresorska delovna skupina. Ocena je skupek dela sedmih skupin, po katerih so razdeljeni predstavniki naštetih subjektov, sodelujočih v medresorski delovni skupini. Prva skupina poda oceno ogroženosti za PD/FT, druga skupina pa oceno ranljivosti države za PD/FT. Ostalih pet skupin se osredotoča na ranljivost posameznega sektorja, in sicer bančnega sistema, ranljivost sektorja vrednostnih papirjev, ranljivost zavarovalniškega sektorja, ranljivost drugih finančnih institucij, ranljivost samostojnih dejavnosti in poklicev. Rezultate teh ocenjevanj pri svoji krovni oceni upošteva skupina, ki podaja oceno ranljivosti države. Slednja skupaj z nacionalno oceno tveganja predstavlja splošno nacionalno oceno (Urad RS za preprečevanje pranja denarja, 2021).

Vsaka skupina na podlagi pridobljenih podatkov, ki se pritičejo posameznega sektorja[9] ter v primeru prve skupine splošnih podatkov glede kriminalitete v povezavi s PD/FT, poda segmentno oceno in potem še skupno oceno za sektor. Za ocenjevanja tveganja se uporablja lestvica, izpisana v tabeli 23.

Tabela 23: Lestvica za oceno tveganja na področju PD/FT (Urad RS za preprečevanje pranja denarja, 2015)

VREDNOST	STOPNJA TVEGANJA (SLO.)	STOPNJA TVEGANJA (ANG.)
0,00–0,20	NIZKO tveganje	low – L
0,21–0,40	NIZKO/SREDNJE tveganje	low/medium – L/M
0,41–0,60	SREDNJE tveganje	medium – M
0,61–0,80	SREDNJE/VISOKO tveganje	medium/high – MH
0,80–1,00	VISOKO tveganje	high – H

Tudi skupina, ki ocenjuje ranljivost države, uporablja enako lestvico, le v obrnjenem pomenu. Višja ocena pomeni večjo odpornost oz. zaradi vpeljanih elementov in mehanizmov proti PD/FT manjše tveganje za PD/FT.

[9] Podatke prispevajo vsi v medresorsko skupino vključeni akterji in po potrebi tudi drugi. Podatki se potem posredujejo oziroma si jih za svoj sektor/področje ocenjevanja priskrbi posamezna skupina. 1. skupina (ocena ogroženosti za PD/FT) zbira podatke o kaznivih dejanjih, iz katerih izhaja protipravna, premoženjska korist, ki se lahko opere (npr. prejete ovadbe, vložene obtožnice, izdane sodbe, podatki o premoženjski koristi). 2. skupina (nacionalna ranljivost) preverja zakonodajna določila, pregleda podatke o sumljivih transakcijah, mednarodnem in domačem medinstitucionalnem sodelovanju, presoja stopnjo integritete akterjev, katerih delo se dotika preiskovanje pregon in sodelovanje v primerih pranja denarja, stopnjo transparentnosti delovanja ključnih deležnikov ipd. 3. skupina (ranljivost bančnega sektorja) preverja ustreznost zakonodaje na področju omejevanja PD/FT znotraj bančnega sektorja učinkovitost nadzora, sankcije in kršitve, tehnične skladnosti, obseg resursov, ki so namenjeni omejevanju PD/FT. 4. skupina (ranljivost sektorja vrednostnih papirjev) upošteva podatke, kot so velikost sektorja, obseg transakcij, delež nerezidentov v strukturi strank in delež njihovih transakcij, število sporočenih transakcij UPPD, podatki iz nadzorov nad zavezanci ipd. 5. skupina (ranljivost zavarovalniškega sektorja): podatki, ki se pritičejo zavarovalnic, pozavarovalnic ter njihovi zastopniki ali posredniki ter pokojninske družbe, kot npr. število oseb vključenih v pokojninsko in drugo vrstno zavarovanje in regulatorni okvir, ustreznost zakonodajnih določil, še posebej tistih, ki se tičejo PD/FT ipd. 6. skupina (ranljivost ostalih finančnih institucij, npr. menjalnice, plačilne institucije, zastavljalnice, družbe za izdajo elektronskega denarja, dajalce kreditov ter kreditne posrednike, ki niso banke, hranilnice ali leasing hiše) zbira podatke o številu teh subjektov, številu transakcij ki presegajo mejo 15.000 EUR, ter povprečne vrednosti transakcij v obravnavanih subjektih ter število sporočenih transakcij UPPD. 7. skupina (nefinančne dejavnosti in poklici, npr. odvetnikov, notarjev, računovodij in revizorjev, trgovcev s plemenitimi kovinami in dragimi kamni, nepremičninski posredniki, Nepridobitne organizacije, igralnice in igralnih salonov) je tako zbirala podatke o njihovem številu, prometu, nadzoru, številu sporočenih transakcij UPPD.

Nacionalna ocena tveganja za PD/FT je bila v Sloveniji narejena trikrat (Urad RS za preprečevanje pranja denarja, 2015, 2016, 2021):

- Prvič, predvsem na naboru podatkov do leta 2013 in zakonodajnih določil, ki so bila oblikovana, in v veljavi leta 2014. Takrat je bila nacionalna ocena ogroženosti in ocena ranljivosti za PD srednje nizka, za FT pa nizka. V primerjavi s protokolom svetovne banke je Slovenija izvedla oceno brez tretjega koraka, torej brez zaključnega tridnevnega sestanka.
- Medresorska delovna skupina je leta 2016 izdala drugo poročilo, ki je zajelo še podatke za leti 2014 in 2015. V tem poročilu je ocena ogroženosti za PD ostala srednje nizka in za FT nizka.
- V tretjem poročilu, kjer je bil uporabljen nabor podatkov do leta 2019, je bila za PD ponovno podana ocena srednje nizka in za FT nizka.

Vse države morajo pri izdelavi ocene upoštevati tudi t. i. zunanjo ogroženost. Pri ocenjevanju se upoštevajo geostrateški položaj Slovenije in podatki o številu izmenjav podatkov z drugimi državami in število tujih pravnih/fizičnih oseb, ki so bile predmet analiz UPPD. V vseh treh poročilih je bila zunanja ogroženost ocenjena s srednjo stopnjo. Glede na rezultate ocene se izdela tudi akcijski načrt za zmanjševanje in odpravljanje identificiranih pomanjkljivosti.

4.5.2 Ocena tveganj na sektorski ravni

Zavezanci[10] »ZPPDFT-1« (2016) morajo izdelati oceno tveganja posamezne skupine ali vrste stranke, poslovnega razmerja, transakcije, produkta, storitve ali distribucijske poti in pri tem upoštevati dejavnike geografskega tveganja glede na možne zlorabe za PD/FT. V izdelavi ocene tveganja se opredeli raven izpostavljenosti določene stranke, poslovnega razmerja, transakcije, storitve ipd.

[10] Zavezanci so različne finančne institucije in organizacije, ki sodelujejo v finančnem sistemu, kot so: banke, hranilnice, plačilne institucije, pošta, borznoposredniške družbe, investicijski skladi, družbe za upravljanje investicijskih skladov, upravljavci vzajemnih pokojninskih skladov, pokojninskih družb in drugih skladov, vezanih na zavarovanja, zavarovalnice, izdajatelji elektronskega denarja, menjalnice, revizijske družbe in revizorji, prireditelji in koncesionarji iger na srečo, zastavljalnice in druge pravne in fizične osebe, ki opravljajo posle v zvezi z dejavnostjo dajanja kreditov oz. posojil, lizinga, izdajanja in upravljanja plačilnih sredstev, storitev menjav, izdajanja garancij in jamstev, upravljanja naložb, oddajanja sefov, posredovanja pri sklepanju kreditnih in posojilnih poslov, zavarovalnega zastopstva in posredništva, računovodskih storitev, storitev davčnega svetovanja, posredovanja v trgovini z umetniškimi deli, izvajanja dražb, poslovanja z nepremičninami itd. (»ZPPDFT-1«, 2016).

Ocena tveganja in postopek določanja ocene tveganja se prilagodita specifičnosti zavezanca in njegovega poslovanja. Oceno tveganja zavezanci pripravijo v skladu s podanimi smernicami, ki jih izda pristojni nadzorni organ. Ugotovitve ocene tveganja iz drugega odstavka pa zavezanci dokumentirajo in posodabljajo najmanj vsaki dve leti.

Zavezanci morajo med drugim prav tako izvajati ukrepe za poznavanje stranke, pripraviti seznam indikatorjev za prepoznavanje strank in transakcij, v zvezi s katerimi obstajajo razlogi za sum PD/FT, in sporočati UPPD informacije o sumljivih transakcijah.

Ukrepi, vezani na poznavanje stranke, se nanašajo na pregled strank. Če zavezanci ocenijo, da stranka, poslovno razmerje, transakcija, produkt, storitev, distribucijska pot, država ali geografsko območje predstavljajo neznatno tveganje za PD/FT, lahko izvajajo ukrepe poenostavljenega pregleda stranke, če pa ocenijo, da predstavljajo povečano tveganje za PD/FT, pa morajo izvajati ukrepe poglobljenega pregleda stranke.

Pri pregledu stranke morajo zavezanci ugotoviti identiteto stranke in dejanskega lastnika stranke; pridobiti podatke o namenu in predvideni naravi poslovnega razmerja ali transakcije ter redno skrbno spremljati poslovne dejavnosti, ki jih stranka izvaja pri zavezancu.

Pregled stranke se opravi: pri sklepanju poslovnega razmerja s stranko; pri vsaki transakciji v vrednosti 15.000 evrov ali več, ne glede na to, ali poteka posamično ali z več transakcijami, ki so med seboj očitno povezane; pri prireditelјih in koncesionarjih, ki prirejajo igre na srečo, ob izplačilih dobitkov, vplačilu stav ali obojem, kadar gre za transakcije v vrednosti 2.000 evrov ali več; pri dvomu o verodostojnosti in ustreznosti predhodno pridobljenih podatkov o stranki ali dejanskem lastniku stranke; vedno, kadar v zvezi s transakcijo, stranko, sredstvi ali premoženjem obstajajo razlogi za sum PD/FT, ne glede na vrednost transakcije.

Kot omenjeno morajo zavezanci po zakonu sestaviti tudi seznam indikatorjev za prepoznavanje strank in transakcij, v zvezi s katerimi obstajajo razlogi za sum PD/FT. Pri sestavi seznama indikatorjev upoštevajo zapletenost in obseg izvajanja transakcij, neobičajno sestavo, vrednost ali povezanost transakcij, ki nimajo jasno

razvidnega ekonomskega ali pravno utemeljenega namena oz. niso v skladu ali so v nesorazmerju z običajnim oz. pričakovanim poslovanjem stranke, in druge okoliščine, ki so povezane s statusom ali drugimi lastnostmi stranke.

Sodišča, državna tožilstva in drugi državni organi pa za namen priprave nacionalne ocene tveganja zbirajo in letno posredujejo statistične podatke o: številu oseb, zoper katere poteka kriminalistična preiskava ali je vložena kazenska ovadba za kaznivo dejanje pranja denarja ali kaznivo dejanje financiranja terorizma; številu oseb, zoper katere je uvedena preiskava ali pa so bili obtoženi ali obsojeni za kaznivo dejanje pranja denarja ali kaznivo dejanje financiranja terorizma; vrsti predhodnega kaznivega dejanja za kaznivo dejanje pranja denarja ali kaznivo dejanje financiranja terorizma, če je podatek na voljo; in vrednosti zavarovanega, zaseženega ali odvzetega nezakonitega premoženja v evrih.

Skladno z omenjenim zakonom je bil sprejet »Pravilnik o dejavnikih neznatnega in povečanega tveganja za pranje denarja ali financiranje terorizma« (2018), v katerem so opredeljeni dejavniki tveganja (v zvezi s stranko, poslovnim razmerjem, transakcijo, produktom, storitvijo, distribucijsko potjo ali državo), ki nakazujejo na tveganja neznatnega ali povečanega pomena. Omenjeni dejavniki so povzeti v tabeli 24.

Tabela 24: Dejavniki tveganja na področju PD/FT (povzeto po »Pravilniku o dejavnikih neznatnega in povečanega tveganja za pranje denarja ali financiranje terorizma«, 2018)

DEJAVNIKI NEZNATNEGA TVEGANJA	DEJAVNIKI POVEČANEGA TVEGANJA
V zvezi s stranko	
– Stranka je družba, katere vrednostni papirji so uvrščeni v trgovanje na organiziranem trgu v skladu z zakonodajo EU ali primerljivimi mednarodnimi standardi. – Stranka je del javnega sektorja. – Stranka je pravna ali fizična oseba iz države, povezane z neznatnim geografskim tveganjem.	– Poslovni odnos s stranko poteka v nenavadnih okoliščinah. – Stranka je pravna ali fizična oseba iz države, povezane s povečanim geografskim tveganjem. – Stranka je pravna oseba ali pravni subjekt tujega prava, ki je namenjen upravljanju zasebnega premoženja. – Stranka je delniška družba, ki omogoča tretjim osebam, da opravljajo vlogo zastopnika v imenu delničarja. – Stranka intenzivno posluje v gotovini. – Lastniška struktura oz. spremembe v lastniški strukturi stranke so neobičajne.

DEJAVNIKI NEZNATNEGA TVEGANJA	DEJAVNIKI POVEČANEGA TVEGANJA
	– V zvezi s stranko se je že pojavil sum ali druga vrsta obravnave v zvezi s PD/FT. – Stranka je državljan tretje države, ki zaprosi za pravico do prebivanja ali za državljanstvo v državi članici v zameno za izvedbo finančnih zadev.
V zvezi s poslovnim razmerjem, transakcijo, produktom, storitvijo ali distribucijsko potjo	
– Police življenjskega zavarovanja z nižjimi premijami. – Nižje, običajne, neprenosljive ali kolektivne oblike poslov pokojninskega zavarovanja. – Finančni produkti ali storitve, ki so ustrezno opredeljeni in omejeni ter namenjeni določenim vrstam strank zaradi zagotavljanja njihove finančne vključenosti. – Produkti, pri katerih se tveganja za PD/FT v zadostni meri obvladujejo z ukrepi. – Produkti, ki so opredeljeni kot klasične igre na srečo.	– Upravljanje premoženja stranke v okviru zasebnega bančništva. – Produkti ali transakcije, ki bi lahko spodbujali anonimnost. – Poslovna razmerja ali transakcije brez navzočnosti stranke in brez določenih zaščitnih ukrepov vezanih na storitve zaupanja. – Vplačila od neznanih ali nepovezanih tretjih oseb. – Novi produkti ali nove poslovne prakse. – Transakcije, povezane z nafto, orožjem, plemenitimi kovinami, tobačnimi izdelki, kulturnimi predmeti in drugimi predmeti arheološkega, zgodovinskega, kulturnega in verskega pomena ali posebne znanstvene vrednosti ter s slonovino in zaščitenimi vrstami.
V zvezi z geografsko lokacijo (registracija, ustanovitev, prebivališče)	
– Države članice EU. – Tretje države, ki imajo vzpostavljene učinkovite sisteme preprečevanja in odkrivanja PD/FT ali za katere je na podlagi zanesljivih virov ugotovljeno, da imajo nizko stopnjo korupcije ali drugih kaznivih dejanj.	– Države, ki so uvrščene na seznam visoko tveganih tretjih držav ali za katere je na podlagi zanesljivih virov ugotovljeno, da imajo precejšnjo stopnjo korupcije ali drugih kaznivih dejanj. – Države, za katere veljajo sankcije oz. ukrepi, izdani s strani mednarodnih organizacij. – Države, ki zagotavljajo financiranje ali podporo terorističnim organizacijam ali v katerih delujejo teroristične organizacije s seznama potrjenih terorističnih organizacij.

Kot omenjeno, konkretne smernice za izdelavo ocen tveganja po posameznih sektorjih pripravijo pristojni organi. V nadaljevanju podajamo primer takšnih usmeritev.

Skladno z »ZPPDFT-1« (2016) je Banka Slovenije (2019) izdala smernice, s katerimi zavezancem (to so banke, hranilnice, podružnice tujih bank, plačilne institucije, izdajatelji e-denarja in menjalnice) podaja enotne usmeritve za učinkovito obvladovanje tveganj s področja PD/FT.

Med drugim je v smernicah opisana metodologija za izvedbo dveh vrst ocen tveganj, in sicer:

- Oceno tveganja zavezanca – OTZ: to je presoja, v kateri zavezanec analizira in oceni: (a) inherentno tveganje, (b) kontrolno okolje in (c) preostalo tveganje ter tako identificira področja zavezanca, ki so izpostavljena tveganjem PD/FT, kar je podlaga za sprejetje ustreznih ukrepov za obvladovanje tveganj.
- Oceno tveganja stranke – OTS: to je presoja meril tveganj in ocena, ali posamezna stranka pomeni manjše ali večje tveganje, da bo zlorabila sistem zavezanca za namen PD/FT.

V smernicah so opisani tudi osnovni termini, povezani z ocenjevanjem tveganj:

- Tveganje je opredeljeno kot verjetnost, da se bo zgodilo pranje denarja ali financiranje terorizma oz. da bo stranka izrabila finančni sistem ali poslovno razmerje, transakcijo, produkt, storitev ali distribucijsko pot, ob upoštevanju dejavnika geografskega tveganja, za PD/FT.
- Merila tveganja so spremenljivke, ki bodisi vsaka zase ali v kombinaciji z drugimi lahko povečajo ali zmanjšajo tveganje PD/FT.
- Metodologija je opredeljena kot skupek pravil, postopkov in algoritmov, ki določajo način upoštevanja posameznih meril tveganja v OTZ ali OTS.
- Inherentno tveganje (ang. *inherent risk*) je tveganje, ugotovljeno pred vzpostavitvijo kontrolnega okolja;
- Kontrolno okolje je sistem notranjih politik, postopkov in kontrol, ki jih je vzpostavil zavezanec z namenom blažitve tveganj PD/FT.
- Preostalo tveganje (ang. *residual risk*) je tveganje, ki mu je zavezanec izpostavljen, po tem, ko sta bila ocenjena inherentno tveganje in učinkovitost kontrolnega okolja.

Zavezanci morajo opraviti OTS, da lahko na podlagi ugotovitev določijo vrsto pregleda stranke (običajen, poglobljen ali poenostavljen), hkrati pa morajo pripraviti tudi OTZ, ki je podlaga za sprejem ustreznih ukrepov za zmanjševanje ugotovljenih tveganj. OTS odraža posebnost stranke in njenega poslovanja, OTZ pa odraža

posebnost zavezanca in njegovega poslovanja. OTZ morajo zavezanci posodabljati najmanj enkrat na leto, OTS pa najmanj enkrat na dve leti.

OTZ je zavezancu v pomoč pri razumevanju tega, katera poslovna področja so izpostavljena večjemu tveganju za morebitne zlorabe z vidika PD/FT in na katerih je treba okrepiti kontrolno okolje, da bodo tveganja PD/FT uspešno obvladovana. Področja in dejavniki ocenjevanja v okviru OTZ se predstavljeni na tabeli 25.

Tabela 25: Področja in dejavniki ocenjevanja v okviru OTZ (Banka Slovenije, 2019)

<table>
<tr><th colspan="3">OCENA TVEGANJA ZAVEZANCA</th></tr>
<tr><td>Inherentno tveganje</td><td>Kontrolno okolje</td><td>Preostalo tveganje</td></tr>
<tr><td rowspan="2">Stranke</td><td>Upravljanje tveganj PPDFT</td><td rowspan="11">Na podlagi ocene inherentnega tveganja in kontrolnega okolja, se oceni preostalo tveganje kot:

– nizko tvegano
– običajno tvegano
– povečano tvegano
– visoko tvegano</td></tr>
<tr><td>Politike in postopki</td></tr>
<tr><td rowspan="2">Geografska območja</td><td>Pregled stranke</td></tr>
<tr><td>Poročanje</td></tr>
<tr><td rowspan="2">Produkti in storitve</td><td>Vodenje evidenc in hramba podatkov</td></tr>
<tr><td>Služba PPDFT</td></tr>
<tr><td rowspan="2">Transakcije</td><td>Zaznava in poročanje suma PD/FT</td></tr>
<tr><td>Monitoring in kontrole</td></tr>
<tr><td rowspan="2">Distribucijske poti</td><td>Izobraževanja</td></tr>
<tr><td>Neodvisna revizija</td></tr>
<tr><td>Druga tveganja</td><td>Nadzorniški ukrepi</td></tr>
</table>

Za vsako skupino dejavnikov, vezanih na inherentna tveganja, so v smernicah podani tudi podrobnejši opisi za metodologijo, merila ter indikatorje ocenjevanja. Po opravljeni analizi meril tveganja se oceni končna vrednost oz. stopnja inherentnega tveganja, pri čemer s stopnjo 1 »nizko tveganje« oceni inherentno tveganje, kadar merila ne predstavljajo večjega tveganja; stopnja 2 predstavlja »običajno tveganje«; stopnja 3 »povečano tveganje«; medtem ko s stopnjo 4 »visoko tveganje« označi inherentno tveganje, v katerem večina meril pomeni visoko tveganje.

Po oceni inherentnega tveganja sledi ocena kontrolnega okolja. Tudi v tem primeru so metodologija, indikatorji in merila posameznih področij ocenjevanja v smernicah podrobneje obrazloženi. Kontrolno okolje se na koncu oceni s štiristopenjsko lestvico, pri čemer se z oceno 1 »dobro« oceni kontrolno okolje, v katerem se izvaja učinkovita in redna kontrola, ocena 2 predstavlja »sprejemljivo« kontrolo, ocena 3 »pomanjkljivo kontrolo«, z oceno 4 »slabo« pa se oceni kontrolno okolje, ki ni učinkovito ali ne obstaja.

Na podlagi analize in ocene inherentnega tveganja in kontrolnega okolja se nato oceni še preostalo tveganje. Ocena preostalega tveganja je izražena v eni izmed štirih stopenj: nizko, običajno, povečano ali visoko. Način izračuna tovrstnega tveganja je predstavljen na tabeli 26.

Tabela 26: Ocena preostalega tveganja (Banka Slovenije, 2019)

OCENA TVEGANJA ZAVEZANCA					
Ocena preostalega tveganja		**Kontrolno okolje**			
		Dobro	**Sprejemljivo**	**Pomanjkljivo**	**Slabo**
Inherentno tveganje	Visoko				
	Povečano				
	Običajno				
	Nizko				

Glede na smernice lahko sicer zavezanci vzpostavijo lastno metodologijo ocenjevanja preostalega tveganja, vendar morajo pri tem upoštevati naslednje pogoje:

- ocena preostalega tveganja naj nima več kot pet stopenj tveganja;
- preostalo tveganje ne more biti ocenjeno kot nizko tveganje, kadar je inherentno tveganje ocenjeno kot visoko tvegano;
- preostalo tveganje ne more biti ocenjeno kot nizko tveganje, kadar je kontrolno okolje ocenjeno kot slabo.

Po izvedeni oceni sledi: (a) dokumentiranje metodologije in pojasnilo rezultatov ocen, (b) potrditev vodstva, (c) predstavitev rezultatov odgovornim osebam, (d) priprava ukrepov za obvladovanje tveganj. To vključuje pripravo akcijskega načrta za odpravo ugotovljenih pomanjkljivosti, posodobitev varnostne strategije in politik zavezanca.

Kot omenjeno pa z OTS zavezanec ugotovi, kakšne vrste pregleda stranke je treba opraviti in kakšen bo način spremljanja njenih dejavnosti. Pri tem velja načelo sorazmernosti, v skladu s katerim so (ob upoštevanju OTS) bolj tvegane stranke predmet pogostejših in obsežnejših kontrol, manj tvegane pa so predmet manj pogostih in manj obsežnih kontrol.

Da bi lahko izvedli OTS z vidika PD/FT, je treba najprej:

- identificirati merila tveganja in
- določiti pomembnost oz. vpliv posameznega merila tveganja na OTS.

Smernice priporočajo, da se tveganost stranke oceni na štiristopenjski lestvici: 1 – nizko, 2 – običajno, 3 – povečano, 4 – visoko tveganje.

Med merila tveganja sodijo:

- Značilnosti stranke (dejavnost, status, ugled, obnašanje).
- Geografsko območje (lokacija prebivališča, državljanstva fizične osebe in ustanovitve, registracije pravne osebe).
- Značilnosti produkta, storitve, transakcij (preglednost, kompleksnost, vrednost ali velikost).
- Distribucijske poti (osebna navzočnost stranke, ponudba produktov/storitev preko tretjih oseb, narava odnosa med zavezancem in stranko).
- Druga tveganja.

V smernicah so podrobneje v tabelarni obliki predstavljeni posamezni indikatorji za omenjena merila in priporočene ocene stopenj tveganja posameznih indikatorjev. Zavezanec sicer sam podrobneje določi lastno metodologijo OTS, vendar mora upoštevati naslednje pogoje:

- Merila ocenjevanja morajo imeti najmanj takšno stopnjo, kot je opredeljena v smernicah.
- Stopnjevanje mora biti določeno tako, da imajo bolj tvegana merila večji vpliv na OTS.
- Merila, določena z visoko oceno tveganja v smernicah, morajo stranko avtomatsko umestiti v kategorijo visoke tveganosti.
- Končna OTS mora imeti najmanj tri stopnje tveganosti (nizko, običajno, visoko) in ne več kot pet kategorij.

- Prihodki zavezanca, povezani s stranko, ne smerjo vplivati na metodologijo OTS.
- Metodologija ne sme voditi do situacije, v kateri nobene stranke ni mogoče umestiti v kategorijo visoke tveganosti.

Na podlagi OTS se nato stranka umesti v eno izmed kategorij tveganosti in ustrezno prilagodi izvajanje ukrepov za preprečevanje PD/FT (zlasti ustrezen obseg pregleda in skrbno spremlja poslovne dejavnosti stranke), kot je razvidno s tabele 27. V primeru štiristopenjske lestvice se med običajnim in visokim tveganjem doda še kategorija povečano tveganje, pri tem pa poteka ali običajen ali poglobljen pregled stranke.

Tabela 27: Kategorije tveganja in način ukrepanja (Banka Slovenije, 2019)

Kategorija tveganosti stranke	Vrsta pregleda stranke	Spremljanje poslovanja stranke	Preverjanje in posodabljanje podatkov in dokumentacije
Nizko tveganje	Poenostavljen pregled	Letno	3–5 let
Običajno tveganje	Običajni pregled	Polletno	2–3 leti
Visoko tveganje	Poglobljen pregled	Mesečno	1–2 leti

4.8 Nacionalna ocena teroristične ogroženosti

Teroristično ogroženost Slovenije ocenjuje Medresorska delovna skupina za protiterorizem, ki jo je ustanovila Vlada RS aprila 2017. S tem so se formalizirali delovanje in dejavnosti, ki so pred tem potekali pod okriljem Delovne skupine za boj proti terorizmu, podskupine Medresorske delovne skupine za boj proti nadnacionalnim grožnjam v okviru sekretariata Sveta za nacionalno varnost. Oceno ogroženosti RS z vidika terorizma je začela pripravljati omenjena Delovna skupina za boj proti terorizmu, in sicer leta 2004 po terorističnih napadih v Madridu (Urad Vlade RS za komuniciranje, 2022).

Medresorska delovna skupina za protiterorizem uporablja petstopenjski model od leta 2016, ko je ta zamenjal prejšnjega, tristopenjskega, ki je bil v veljavi od leta 2004.[11]

[11] Kot zanimivost navajamo Britovškovo ugotovitev, da so ZDA leta 2011 petstopenjsko barvno lestvico ocene teroristične ogroženosti opustile in prešle na nov sistem, ki vsebuje večjo vsebinsko konkretizacijo groženj (Britovšek, 2019).

Stopnja teroristične ogroženosti se določa na podlagi območja in nevarnosti pojava ter ocene vpliva terorističnih dejavnosti na ostalih območjih na varnost RS. Območje pojava pomeni območje, v katerem se je zgodilo teroristično dejanje ali pa obstaja nevarnost za izvršitev tovrstnega dejanja. Nevarnost pojava se oceni na podlagi matrike za oceno nevarnosti pojava z vidika delovanja terorističnih skupin ali posameznikov, kjer se upoštevajo indikatorji, povezani z *namero izvedbe*, *zmogljivostmi* ter *dejavnostmi* in *pripravami za izvedbo terorističnih dejavnosti*. Medresorska delovna skupina ob tem opozarja, da zaradi narave terorizma lahko neodvisno od trenutne stopnje teroristične ogroženosti in brez predhodnega opozorila pride do izvedbe nasilnega terorističnega dejanja. Trenutna ocena teroristične ogroženosti (ocena sprejeta 11. februarja 2022) je nizka (druga stopnja od petih).

Na tabeli 28 predstavljamo petstopenjski model teroristične ogroženosti, ki se uporablja v Sloveniji.

Tabela 28: Petstopenjski model teroristične ogroženosti v Sloveniji (Urad Vlade RS za komuniciranje, 2022)

Stopnja ogroženosti		Opis verjetnosti
	Zelo nizka	Verjetnost napada je neznatna. Ni indikatorjev grožnje ali obetov, da bi se grožnje uresničile v kratkoročnem obdobju.
	Nizka	Nizka verjetnost napada, vendar možnosti napada ni mogoče zavreči. Zelo omejeni indikatorji groženj, vendar ni verjetno, da bi se grožnje uresničile v kratkoročnem obdobju.
	Srednja	Verjetnost napada je srednja. Omejeni indikatorji groženj, ki bi se uresničile v kratkoročnem obdobju. Napad je zelo verjeten oz. pričakovan.
	Visoka	Jasni indikatorji, da se bodo grožnje verjetno uresničile v kratkoročnem obdobju. Točno določen cilj ali časovni okvir nista znana.
	Zelo visoka	Visoka neposredna ogroženost zaradi terorističnega napada. Jasni indikatorji neizbežnih groženj: znani so čas, namen in cilji.

4.9 Ocena tveganj na področju protiobveščevalne in varnostne dejavnosti

Področje analiziranja ogroženosti in tveganj na obveščevalno-varnostnem (OV) področju je v slovenski strokovni literaturi razmeroma skromno obdelana tematika. Specifične vidike ocenjevanja ogroženosti in tveganj v strokovnem prispevku opisuje Britovšek (2019), ki obenem podaja predlog modela za izdelavo tovrstnih ocen na OV področju, ki je namenjen praktikom. V prispevku je poudarjeno, da v OV stroki na splošno primanjkuje enotnih metodologij in terminologije in da OV službe

pogosto delujejo v kompleksnem, negotovem in nepredvidljivem okolju, kar zahteva določeno mero previdnosti v oblikovanju metodologij. Praktiki v tej stroki morajo delovati predvsem po načelu preprostosti in prilagodljivosti.

Ključni elementi, ki so del analiziranja in ocenjevanja na OV področju, so tarče, grožnje in tveganja. Tarče so dobrine ali vrednote oz. cilji posameznih groženj, v postopku ocenjevanja gre torej za tiste vidike, ki jih varujemo ali želimo obvarovati (ljudi, objekte, podatke, opremo, območja, državo, interese, cilje ipd.). Grožnje so opredeljene kot viri ogrožanja in dejavnosti, ki bi lahko ogrozile tarčo. Na OV področju je poudarek predvsem na tveganjih, ki jih povzročajo zlonamerne oz. namerne grožnje. Tveganja pa so opredeljena kot izpostavljenost tarče posameznim grožnjam, verjetnost uspešne uresničitve groženj ter škoda, ki lahko ob tem nastane. Pri tem je izpostavljenost, odvisna od oddaljenosti tarče od grožnje, verjetnost od ranljivosti in zmogljivosti tarče, da se zoperstavi grožnji, medtem ko je potencialna škoda, ki nastane ob uresničitvi grožnje odvisna predvsem od pomembnosti tarče. Tveganja so torej odvisna od ogroženosti, ranljivosti in pomembnosti tarč.

Britovšek (2019) nadalje razlaga, da se na obveščevalnem in protiobveščevalnem področju najpogosteje izvajajo analize in ocene ogroženosti, ki jih lahko razumemo kot oceno verjetnosti, da bo v določnem obdobju prišlo do uresničitve določene grožnje zoper določeno tarčo. Sestavni elementi ocene ogroženosti so torej: tarče, grožnje, verjetnost uresničitve in časovno obdobje (kratko-, srednje- in dolgoročno). Posebnost pri tovrstnih ocenah na OV področju, za razliko od drugih področij, so besedni opisi verjetnosti, saj je, kot omenjeno, okolje, v katerem delujejo OV službe, negotovo, kompleksno in težko predvidljivo, zato je popolne in resnične podatke težje pridobiti in zbrati.

Čeprav se po svetu uporabljajo različne opredelitve in načini opisovanja stopenj verjetnosti, Britovšek (2019) predlaga tristopenjsko lestvico ogroženosti (tabela 29) ter dodatne razlage in indikatorje v pomoč pri podajanju ocene.

Pri tem se opozarja, da je pri podajanju ocene ogroženosti potrebna previdnost in prilagodljivost glede na razmere in okoliščine. V večjih okoljih je denimo težko podati oceno ogroženosti za celotno območje, ker so razmere v različnih regijah lahko zelo različne, ocene pa lahko podajo lažen občutek nevarnosti na območjih, ker ta nevarnost ne obstaja (in obratno). Obstajajo tudi alternativni pristopi k

ocenjevanju ogroženosti, kot to npr. uporabljajo ZDA (npr. redno objavljanje splošnih trendov na področju terorizma; če obstajajo konkretni podatki o grožnji, se obvešča o povišani ogroženosti, če pa obstajajo konkretni podatki o lokaciji in času pričakovanega napada, pa se obvešča o pričakovani ogroženosti).

Tabela 29: Tristopenjska lestvica ogroženosti na obveščevalnem in protiobveščevalnem področju (Britovšek, 2019)

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

Ocene tveganj sicer niso tako pogost koncept v OV dejavnosti kot ocene ogroženosti, kljub temu pa se delno srečujejo z njimi predvsem na varnostnem področju (npr. pri ocenjevanju tveganj za posamezne objekte). Zaradi narave okoliščin, v katerih delujejo OV službe, je priporočila mednarodnih standardov, ki predlagajo kompleksne metodologije, težje upoštevati. Pretirana kvantifikacija in matematizacija ocen ogroženosti in ocen tveganj je v tej dejavnosti lahko nevarna, saj so pogosto prisotni elementi zavajanja in prikrivanja, popolni in resnični podatki pa so težje dosegljivi. Nasprotno pa lahko tudi nedoločenost postopkov ob časovnih pritiskih ali impulzivnem odločanju vodi do podcenjevanja ali precenjevanja. Britovšek (2019) zato predlaga poenostavljeno metodologijo, ki vključuje enostavnejše ovrednotenje vseh elementov tveganj (tabela 30).

Tabela 30: Poenostavljena ocena tveganj na obveščevalnem in protiobveščevalnem področju (Britovšek, 2019)

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			

4.10 Ocena varnostnih razmer na občinski ravni

Na podlagi 6. člena »Zakona o občinskem redarstvu (ZORed)«, (2017) morajo občine izdelati Občinski program varnosti (OPV), ki je temeljni strateški dokument, v katerem so opredeljena izhodišča za zagotavljanje varnega in kakovostnega življenja prebivalcev občine. Sprejme ga občinski svet na predlog župana in na podlagi programa določi vrsto in obseg nalog občinskega redarstva. Občinski organi pa najmanj enkrat letno ocenijo izvajanje OPV.

OPV mora biti usklajen s predpisi, programskimi dokumenti MNZ in policije na področju javne varnosti ter potrebami varnosti v občini. Dve ali več občin lahko sprejme tudi skupen program. MNZ pri sami izdelavi in pripravi programa nudi tudi strokovno pomoč v obliki predavanj, odgovorov na ustna in pisna vprašanja ter v obliki pregledov OPV. Za izdelavo OPV je MNZ (2015) izdalo tudi Smernice za izdelavo občinskega programa varnosti. Izhodišča za vzpostavitev in zagotavljanje obsega in kakovosti javne varnosti ter javnega reda v občini so pravnosistemski in organizacijski ukrepi. V smernicah je opredeljeno, da morajo občine za zagotavljanje večje varnosti občanov:

- izdelati oceno varnostnih razmer,
- izdelati OPV in
- vzpostaviti občinsko redarstvo.

Ocena varnostnih razmer, ki je priloga OPV, predstavlja izhodiščni dokument za opredelitev obsega varnostnih potreb občine, za izdelavo OPV ter za določitev vsebine dela oz. konkretnih nalog občinskega redarstva. V oceni morajo zato biti opredeljeni vrsta, oblika in obseg dejavnikov ogrožanja v občini oz. dejavnikov, ki vplivajo na javno varnost in javni red. Ocena varnostnih razmer v občini obvezno vsebuje naslednje štiri elemente:

1. posnetek stanja (zbiranje podatkov za analizo; operativni ogled območja občine; pregled organiziranosti občine in delovanja služb; pregled gradiva, vezanega na občinsko redarstvo; razgovori s pristojnimi);
2. analiza in ocena varnostnih razmer (ugotovitev stopenj ogroženosti: od naravnih nesreč, cestnega prometa, cest in okolja, občinskih javnih poti, javnega premoženja, naravne in kulturne dediščine, javnega reda in miru, od kriminalnih pojavov, na javnih shodih in prireditvah, okolja; ocena vpliva varnostnih razmer v sosednjih občinah; oblikovanje ključnih ugotovitev strateške in operativne narave; identifikacija kritične infrastrukture v občini, ki zahteva stalno pozornost občinskih redarjev);
3. identificiranje in obvladovanje varnostnih tveganj (varnostna tveganja na področju: varnosti v cestnem prometu, varnosti občinskih javnih poti, zagotavljanja javnega reda in miru, preprečevanja kriminalnih dejanj, zagotavljanja varnosti javnega premoženja ter naravne in kulturne dediščine, javnih shodov in prireditev, varstva okolja, zaščite živali; opredelitev načinov obvladovanja varnostnih tveganj s strani redarske službe);
4. opredelitev varnostnih potreb občine (opredelitev izhaja iz zakonskih določil, ocene varnostnih razmer in varnostnih tveganj).

Cilji OPV so strateški in operativni. Strateški cilji se nanašajo na dvig kakovosti življenja in dela občanov ter dvig stopnje varnosti javnega prostora v občini. Gre za dolgoročni cilj dvigovanja stopnje javne varnosti oz. varnosti prebivalcev v občini. Njegova vsebina izhaja iz nacionalne varnostne politike, zakonskih določil, nacionalnih programov varnosti in iz splošnih varnostnih potreb občine. Nosilci so občinski organi, vodje občinskih redarskih služb, policijska postaja in ministrstva, pristojna za posamezna področja varnosti.

Operativni cilji se nanašajo na delovanje skupnosti, ki s predpisi in ukrepi državnih in drugih organov zagotavlja, da se preprečijo ravnanja in nevarnosti, ki ogrožajo varnost ter javni red in mir, kadar te grozijo skupnosti ali posamezniku. Nosilci so občinsko redarstvo, policijska postaja, lastniki, upravljavci, skrbniki, upravitelji in najemniki javnih površin in zgradb, organizatorji shodov in prireditev na javnih in drugih površinah in subjekti zasebnega varovanja, ki pogodbeno varujejo javna zbiranja in premoženje ter osebje pri uporabnikih varnostnih storitev.

4.11 Drugo

Ob pregledu usmeritev in pristopov k ocenjevanju ogroženosti/tveganj, ki se v Sloveniji uporabljajo na področjih, pomembnih za javno varnost, velja omeniti, da je pregled zaobjel izključno najpomembnejše nacionalne in sektorske ocene. Zaradi obsežnosti področij, na katerih se izvajajo tovrstne ocene, so iz podrobnejše analize izvzeti nekateri specifični vidiki. Neposredno ali posredno so za javno varnost pomembne tudi druge ocene ogroženosti ali tveganj, ki se morajo izvajati na določenih delovnih področjih in v organizacijah. Za lažjo predstavo raznolikosti in obsežnosti takšnih ocen povzemamo nekaj primerov.

- Analize, ocene in postopke z vrednotenjem tveganj morajo opravljati zavezanci »Zakona o informacijski varnosti (ZInfV)« (2018) (to so izvajalci bistvenih storitev, ponudniki digitalnih storitev in organi državne uprave, ki upravljajo informacijske sisteme in dele omrežja oz. izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti) ter na tej podlagi pripravljati in izvajati ukrepe za obvladovanje tveganj pri zagotavljanju varnosti informacijskih sistemov in omrežij. Podrobnejše pogoje in postopke v povezavi z analizo in oceno informacijskovarnostnih tveganj ureja »Uredba o informacijski varnosti v državni upravi« (2018), kjer so podani sklici na dodatne usmeritve glede metodologije.
- Skladno z »Uredbo o obveznem organiziranju službe varovanja na javnih prireditvah« (2010) morajo organizatorji – zavezanci po 12.a členu »Zakona o javnih zbiranjih« (2011) zagotavljati službo varovanja, kar vključuje tudi izdelavo ocene stopnje tveganja, da bi na javni prireditvi prišlo do hujše kršitve reda ali do ogrožanja javnega reda, nasilja, splošnega nereda in s tem ogrožanja varnosti ljudi, premoženja ali

javnega prometa. Omenjena ocena je podlaga za izdelavo načrta varovanja. Oceno izdela izvajalec (varnostna služba) organizatorja v sodelovanju z zavezancem, policijo, občinskim redarstvom in lokalno skupnostjo.

- Policija mora skladno s »Pravilnikom o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi« (2013) izdelati oceno ogroženosti jedrskih objektov in jedrskih ter radioaktivnih snovi v RS in oceno ogroženosti v primeru prevoza jedrske snovi na ozemlju RS.
- Po »Zakonu o preprečevanju nasilja v družini« (2008) morajo Centri za socialno delo izdelati oceno ogroženosti žrtve nasilja, na podlagi ocene pa določiti ukrepe, potrebne za zaščito žrtve. Obravnava žrtev navadno poteka v multidisciplinarnih timih, v katerih sodeluje tudi policija, kar omogoča boljšo izmenjavo podatkov in izdelavo ocene. V namen lažje priprave ocene ogroženosti so strokovnim delavcem, ki sodelujejo v teh timih, na voljo tudi različne smernice (npr. Strokovne smernice za obravnavo nasilja v družini pri izvajanju zdravstvene dejavnosti (Brecelj Anderluh idr., 2015); Priročnik za zdravstveno osebje (Šimenc, 2015); Strokovna izhodišča za delo z odraslimi žrtvami in povzročitelji nasilja v družini za strokovne delavce centrov za socialno delo (Hrovat Svetičič idr., 2008, 2010); spletna platforma, ki je nastala v okviru projekta IMPRODOVA (2021)).

Ocenjevanje varnostne ogroženosti in varnostnih tveganj na nacionalni ravni je v nekaterih primerih tesno povezana tudi z ocenami, ki se izvajajo v širših teritorialnih okvirih. EU s ciljem zagotavljanja notranje varnosti v okviru različnih agencij izvaja področne ocene ogroženosti/tveganj na celotnem območju članic in širše, kar vključuje aktivno udeležbo posameznih članic – ali skozi izvajanje lastnih ocen (ob vnaprej določeni metodologiji) in prispevanje k izdelavi skupne (evropske) ocene ali pa skozi aktivno sodelovanje pri izdelavi ocene skozi podajanje strokovnih mnenj in posredovanje podatkov. Sledi še krajši pregled nekaterih evropskih pristopov k izdelavi ocene ogroženosti in tveganj na področju transnacionalne kriminalitete in migracij.

Ocena ogroženosti na področju organizirane kriminalitete s transnacionalnimi razsežnostmi – Europol

Europol v podporo članicam in partnerjem (med katerimi je od leta 2004 tudi Slovenija) spremlja trende kriminalitete in pri tem ustvarja redne analize stanja v EU, in sicer na področjih: (a) resne in organizirane kriminalitete; (b) terorizma in (c) internetne organizirane kriminalitete.

V povezavi z resno in organizirano kriminaliteto Europol izdeluje t. i. poročila SOCTA (ang. *Serious and Organised Crime Threat Assessment* – SOCTA), ki so integralen del EU Policy Cycle – EMPACT (ang. *European Multidisciplinary Platform Against Criminal Threats*), s katerim določa prioritete in s tem načine dela vseh deležnikov, ki delujejo na področju notranje varnostne politike (Europol, 2022). Europol je predhodno izdeloval poročila OCTA (ang. *Organised Crime Threat Assessment*), ki pa so bila deležna številnih kritik na račun netransparentnosti metodologije (Van Duyne, 2010; Zoutendijk, 2010). Podrobna metodologija izdelave poročil SOCTA ni javno dostopna, razvil pa jo je Europol ob pomoči Evropske komisije, predstavnikov članic EU, zunanjih partnerjev in drugih ključnih deležnikov (Council of the European Union, 2015, 2020; Europol, 2021a).

Prvo poročilo SOCTA je bilo izdano leta 2013, čez leta pa se je metodologija adaptirala glede na identificirane zahteve. Krovni namen poročil SOCTA je izdelati oceno groženj in tveganj, ki izhajajo iz delovanja organizirane oz. resne kriminalitete. Med drugim to vključuje identifikacijo ranljivosti in priložnosti za kriminaliteto, identifikacijo organiziranih kriminalnih skupin, kriminalnih žarišč ipd.

Oceno tveganja za posamezne grožnje predstavlja kombiniranje verjetnosti in obsega posledic, ki bi jih delovanje takih skupin oz. resna kriminaliteta lahko imela na družbo kot celoto. Prav tako metodologija SOCTA kot ključno prepoznava okolje, v katerem se kriminaliteta izvaja oz. v katerem delujejo kriminalne skupine. Analize v povezavi z okoljem tako vključujejo vpogled v faktorje, ki spodbujajo ali zavirajo razvoj kriminalitete na nekem območju, torej od geografskih, infrastrukturnih do družbenih dejavnikov.

Model izdelave poročil SOCTA zajema štiri korake:

1. fokusiranje na kriminalitetne skupine, okolje in vrste kriminalitete;
2. uporaba orodij za izdelavo oz. identifikacijo ključnih indikatorjev v povezavi z elementi iz prvega koraka;
3. analiza in prioritizacija (kjer se identificirajo vse možne grožnje in med njimi identificira tiste z največjo verjetnostjo pojavitve);
4. posredovanje rezultatov, ki vključujejo priporočila za delovanje.

Podatki za analize predstavljajo analitične delovne datoteke (ang. *Europol's Analytical Work Files*) v kombinaciji z zgodnjimi opozorili (ang. *Europol's Early Warning Notification*), operativnimi podatki, obveščevalnimi produkti, posameznimi ocenami tveganj, podatki iz javnih virov, carinskimi podatki ter drugimi produkti članic EU in Europolovih zunanjih partnerjev. Za identifikacijo vrzeli v znanju pa so poslani vprašalniki skoraj vsem ključnim deležnikom, ki delujejo na področju varnosti v EU in širše.

Indikatorji, na katerih temelji ocena, se delijo na deskriptivne indikatorje in indikatorje groženj. Prvi so namenjeni opisovanju in analiziranju trenutnih groženj (npr. nacionalnost, velikost skupine, modus operandi ipd.), drugi pa so namenjeni ocenjevanju groženj (npr. finančna sredstva, uporaba zakonitih poslovnih subjektov, notranje nasilje, korupcija).

Indikatorji so razčlenjeni v pet skupin:

- Skupina indikatorjev za kriminalitetne skupine (npr. nacionalnost, velikost skupine, stopnja razvitosti, povezave z drugimi kriminalnimi skupinami) vključuje kombinacijo ocenjevalnih in deskriptivnih (skupaj 21). Ocenjevalni (skupaj 13) imajo dodeljene relativne uteži (nizka, srednja, visoka pomembnost) in se ocenjujejo na petstopenjski lestvici obsega (neznan, ničen, nizek, srednji, visok).
- Skupina indikatorjev za okolja, v katerih se pojavlja organizirana kriminaliteta (npr. način delovanja, geografska razpršenost, število prisotnih skupin, dostopnost virov) (skupaj 16), vključuje pretežno ocenjevalne indikatorje (skupaj 12) in se ocenjujejo na enak način kot indikatorji v skupini za kriminalne skupine.

- Skupina indikatorjev vpliva (ekonomski, socialni, zdravstveni, varnostni, politični in okoljski vpliv) vključuje izključno ocenjevalne indikatorje (skupaj 6), s katerimi se ocenjuje vpliv organizirane kriminalitete. Učinek se oceni na podlagi vrednotenja razširjenosti, pogostosti in resnosti na štiri stopenjski lestvici (neznan, nizek, srednji, visok vpliv).
- Skupina indikatorjev kriminalitetne infrastrukture (npr. korupcija, pranje denarja, transportna infrastruktura) vključuje kombinacijo deskriptivnih in ocenjevalnih (skupaj 8), seznam deskriptivnih se potrebi dopolnjuje.
- Skupina okoljskih indikatorjev (npr. ekonomska geopolitična, sociološka situacija, zakonodaja, strategije) vključuje izključno deskriptivne indikatorje (skupaj 8), ki se po potrebi dopolnjujejo.

Pred publikacijo poročil naredi Europol še oceno kakovosti produkta SOCTA po t. i. štirih revizijskih merilih: doslednost, popolnost, jasnost in skladnost. Rezultati SOCTA s tem omogočijo razvoj priporočil in ustreznih politik na področju omejevanja in delovanja proti organizirani in resni kriminaliteti (Europol, 2021b).

Europol poleg omenjenega vsako leto izda poročilo o razmerah in trendih terorizma v EU (ang. *Terrorism Situation and Trend Report* – TE-SAT), ki ponuja pregled pojava terorizma v EU v določenem letu. Poročilo TE-SAT vsebuje podatke o terorističnih napadih in aretacijah, povezanih s terorizmom v EU. Temelji predvsem na informacijah, ki jih Europolu uradno prispevajo države članice EU in Eurojust, ki prav tako zbira podatke članic. Poleg tega so k sodelovanju vabljeni tudi Europolovi partnerji, da zagotovijo informacije o razmerah, povezanih s terorizmom v svojih državah. TE-SAT je poročilo o stanju, ki opisuje in analizira zunanje manifestacije terorizma, tj. teroristične napade in dejavnosti. Ne analizira temeljnih vzrokov terorizma, niti ne poskuša oceniti vpliv ali učinkovitost politik boja proti terorizmu in sprejetih ukrepov kazenskega pregona, čeprav lahko služi za ponazoritev nekaterih od teh. Namenjen je predvsem zato, da omogoči pregled terorizma in razmer v EU z vidika organov kazenskega pregona (Europol, 2021b).

Med strateške analize Europola pa sodi tudi ocena ogroženosti pred internetno organizirano kriminaliteto (ang. *Internet Organized Crime Threat Assessment* – IOCTA). Ocena je osredotočena na analizo groženj in razvojnih trendov na področju kibernetske kriminalitete, da bi identificirala grožnje, ki vplivajo na vlade, podjetja in

državljane v EU (Europol, 2023). IOCTA podaja tudi priporočila organom pregona, oblikovalcem politik in regulatorjem, ki jim omogočajo učinkovit in usklajen odziv na kibernetsko kriminaliteto. Podatke za pripravo poročila prispevajo vse države članice EU, nekatere tretje države, člani svetovalnih skupin Europola in notranji strokovnjaki, pri zbiranju podatkov pa je uveljavljena metoda anketiranja. Prednostne naloge glede kibernetske kriminalitete so del cikla politike EU – EMPACT (Europol, 2023).

Ocena tveganj na področju migracij – Frontex

Kot članica Schengenskega območja in EU je Slovenija dolžna skrbeti za ustrezno zaščito zunanjih meja, kar med drugim vključuje tudi izvajanje analize tveganja na področju varovanja meja. Za potrebe učinkovite izmenjave informacij in sodelovanja držav je agencija Frontex (2013) izdelala skupen integriran model analize tveganja (t. i. CIRAM), ki spodbuja skupno razumevanje analize tveganja in prispeva k večji usklajenosti pri upravljanju zunanjih meja.

Metodologijo, ki je predstavljena v nadaljevanju, so razvile države članice EU in agencija Frontex, namenjena pa je uporabi na nacionalni ravni in ravni celotne EU. Model predstavlja skupen analitičen okvir s poenoteno terminologijo in pristopom k analizi tveganja v državah članicah. S tem se želita zagotoviti skladno upravljanje in enoten nadzor zunanjih meja ter omogočiti lažje povezovanje med vsemi organi, ki sodelujejo pri varovanju meja in se ukvarjajo z vprašanji priseljevanja (policije, carinska uprava in uradi za priseljevanje).

Skladno s terminološkimi opredelitvami CIRAM:

- analiza tveganja pomeni sistematično proučevanje sestavin tveganja in predstavlja podlago za sprejemanje odločitev;
- tveganje pomeni obseg in verjetnost grožnje, ki se pojavlja na zunanjih meja, ob upoštevanju ukrepov na mejah in znotraj EU, in vpliva na notranjo varnost EU, varnost zunanjih meja, optimalen pretok potnikov na mejnih prehodih ali ima humanitarne posledice.

Tveganje je sestavljeno iz treh sestavin, ki so med seboj neločljivo povezane, zato je njihovo ocenjevanje medsebojno odvisno. Sestavine tveganj so:

1. Grožnja, ki se oceni glede na njen obseg in verjetnost.

Pri oceni verjetnosti grožnje naj se upoštevajo: načini izvedbe grožnje, storilci, čas, prostor, težavnost izvedbe, olajševalne/oteževalne okoliščine, trendi in predvidevanja glede gibanja (porast, upad, stabilnost).

Pri tem se predlaga, da se vnaprej pripravita izčrpen seznam in opis vseh možnih groženj, analiza pa naj bo usmerjena v prihodnost. Priporočeno je, da se po enotnih merilih grožnje primerjajo med seboj, obveščevalci pa so obveščani o prioritetnih grožnjah (npr. pet do deset grožnjah).

Za ocenjevanje verjetnosti uresničenja grožnje se priporoča uporaba sedemstopenjske lestvice, kot je prikazana na tabeli 31.

Tabela 31: Ocena verjetnosti grožnje na področju migracij (Frontex, 2013)

IZRAZOSLOVJE ZA OCENO VERJETNOSTI GROŽNJE		
Stopnja verjetnosti	**Merjenje (odstotno ocenjevanje) verjetnosti (ni vedno mogoče)**	**Fraze verjetnosti**
Zanesljivo	100-odstotna verjetnost	Ni dvoma, da se bo zgodilo.
Skoraj zanesljivo	93-odstotna verjetnost (s toleranco 6 %)	Skoraj popolnoma je verjetno, da se bo zgodilo.
Zelo verjetno	75-odstotna verjetnost (s toleranco 12 %)	Zelo je verjetno, da se bo zgodilo.
Verjetno	50-odstotna verjetnost (s toleranco 10 %)	Ravno toliko možnosti, da se bo zgodilo, kot da se ne bo zgodilo.
Malo verjetno	30-odstotna verjetnost (s toleranco 10 %)	Malo možnosti, da se bo zgodilo. Obstaja določena stopnja dvoma, da se bo zgodilo.
Zelo malo verjetno	7-odstotna verjetnost (s toleranco 5 %)	Zelo malo je možnosti, da se bo zgodilo. Skoraj nemogoče je, da se bo zgodilo. Možnosti dogodka so minimalne.
Ničelna verjetnost	0-odstotna verjetnost	Ni možnosti, da bi se zgodilo.

2. Ranljivost, ki je odvisna od zmožnosti učinkovitega odziva na grožnjo.

Pri oceni verjetnosti naj se upoštevajo: zemljepisne značilnosti območja, operativne dejavnosti in zmogljivosti zaščite na območju, učinkovitost obstoječih ukrepov, dejavniki privlačnosti. Ranljivost je torej odvisna od zmožnosti vzpostavljenih sistemov, da zaznajo ali preprečijo grožnjo.

Podatke za ocenjevanje ranljivosti naj predstavljajo evidence in ocene o opremljenosti s terena. Z ocenjevanjem ranljivosti se želijo izpostaviti območja, ki so najbolj izpostavljena določenim grožnjam.

Za ocenjevanje ranljivosti se priporoča uporaba štiristopenjske lestvice, kot je prikazano na tabeli 32.

Tabela 32: Ocena ranljivosti na področju migracij (Frontex, 2013)

Stopnja	**Prepustnost meje**	**Operativne zmogljivosti in pravni odzivi**	**Dejavniki spodbujanja: velike skupnosti v državah članicah, mnenje, da je mogoče z goljufijo zlahka priti do mednarodne zaščite in ugodnosti socialnega varstva**
Zelo visoka ranljivost	Pri tej grožnji se izkoriščajo teren ali naravne razmere na zunanji meji	Za obravnavo te grožnje niso na voljo pristojnosti ali pravni odzivi	Prisotni so vsi ti dejavniki
Visoka ranljivost	Teren ali naravne razmere na zunanji meji spodbujajo nastanek te grožnje	Za obravnavo te grožnje je na voljo malo pristojnosti ali pravnih odzivov	Prisotnih je več dejavnikov
Srednja ranljivost	Teren ali naravne razmere ne vplivajo na nastanek te grožnje	Za obravnavo te grožnje je na voljo zmerno število pristojnosti ali pravnih odzivov	Prisoten je eden od treh dejavnikov
Nizka ranljivost	Teren ali naravne razmere preprečujejo nastanek te grožnje	Za obravnavo te grožnje je na voljo dovolj pristojnosti ali pravnih odzivov	Prisoten ni nobeden od teh dejavnikov

3. Vpliv, ki se nanaša na učinek uresničene grožnje.

Pri oceni vpliva naj se upoštevajo učinki na notranjo varnost, varnost zunanjih meja, upravljanje prestopov meje in humanitarni vplivi. Če vpliva groženj ni mogoče izmeriti na podlagi konkretnih podatkov, naj se uporabijo strokovna mnenja in analize scenarijev. Pri ocenjevanju vplivov se priporoča uporaba štiristopenjske lestvice, kot je prikazano na tabeli 33.

Tabela 33: Ocena vpliva tveganja na področju migracij (Frontex, 2013)

PRIMER KVALITATIVNIH OCEN STOPNJE VPLIVA, POVEZANEGA Z NEZAKONITIM PRISELJEVANJEM				
Vpliv	**Kritičen**	**Zelo pomemben**	**Pomemben**	**Nizek**
Izguba človeških življenj	Človeška življenja so ogrožena v večini primerov (npr. > 75 %)	Človeška življenja so ogrožena v veliko primerih (npr. 20 % < x < 75 %)	Človeška življenja so ogrožena v zmernem številu primerov (< 20 %)	Ni vpliva na človeška življenja

Pri izračunu končne ocene tveganja na podlagi omenjenih sestavin se priporoča izogibanje natančnim, kvantitativnim izračunom v deležih, saj lahko to pri odločevalcih ustvarja napačen vtis o natančnosti ocene. Takšne ocene naj se uporabljajo zgolj v primerih, ko je na voljo veliko podatkov, ocene pa je možno tudi potrditi.

Kadar se ocene posameznih elementov opirajo na kvalitativne opise, je primernejše razvrščanje tveganj v stopnje pomembnosti, kot je prikazano na tabeli 34.

Tabela 34: Ocena tveganja na področju migracij (Frontex, 2013)

PRIMER TREH STOPENJ TVEGANJA	
Stopnja tveganja	**Opis**
Majhna	Sprejemljivo tveganje. Posledica je obvladljiva, ranljivost je sprejemljiva. Grožnjo moramo spremljati, da zaznamo spremembe stopnje tveganja.
Srednja	Še vedno razmeroma sprejemljivo tveganje, vendar posledice ne moremo z lahkoto obvladovati z obstoječimi zmogljivostmi sistema. Majhna sprememba obsega grožnje lahko ogrozi učinkovitost ukrepov za obvladovanje situacije. Razvoj grožnje je treba redno spremljati in obenem sproti ocenjevati, ali je treba izvesti dodatne ukrepe.
Velika	Tveganje ni sprejemljivo. Posledic ne moremo ustrezno obvladovati z obstoječimi zmogljivostmi in brez dodatnih ukrepov za zmanjševanje tveganja.

V analizi tveganja je treba določiti tudi referenčno obdobje (dan, teden, mesec ali leto) glede na odločevalno raven – nižja, kot je odločevalna raven v hierarhiji, za krajše obdobje se proučujejo tveganja; za operativno raven se analizirajo tveganja, ki podpirajo kratkoročne odločitve; za strateško raven pa tveganja, ki omogočajo lažje dolgoročne odločitve. V procesu analiziranja tveganj tako sodelujeta dve skupini deležnikov – analitiki, pristojni za ocenjevanje tveganj, o rezultatih obveščajo odločevalce (na strateški ali operativni ravni).

Podatke (metrične in nemetrične) za lažje ocenjevanje posameznih sestavin tveganj lahko analitiki pridobijo iz različnih javnih in zaupnih virov, kot so:

- mednarodne specializirane zbirke podatkov;
- nacionalne zbirke podatkov in evidence;
- zbirke podatkov posameznih državnih organizacij;
- mednarodna in nacionalna analitična poročila o trendih, razmerah;
- odprti viri.

Posebno vrednost pri ocenjevanju posameznih sestavin tveganj predstavljajo obveščevalni podatki, ki se običajno nanašajo na informacije o dogajanju na določenih območjih, zlasti nezakonitih dejavnostih.

Za namene izdelave obveščevalnih izdelkov, kot so ocene groženj, ranljivosti in vpliva, je mogoče uporabiti različne tehnike. Med najpogosteje uporabljene sodijo:

- Zbiranje zamisli oz. viharjenje možganov med skupino poučenih udeležencev, ki je posebej uporabna, ko ni na voljo nikakršnih podatkov.
- Privabljanje strokovnjakov z različnih področij za potrebe širjenja baze znanja.
- Analiza vzorcev in trendov na podlagi statističnih podatkov o preteklih dogodkih.
- Ankete med specifičnimi ciljnimi populacijami za potrebe analiziranja ranljivosti in groženj.

Pri tem je priporočeno oceniti zanesljivost in veljavnost informacij, vsaka informacija vključena v analizo pa naj se temu primerno tudi ovrednoti (kombinacija črke in številke). Primer načina ocenjevanja tovrstnih vidikov kakovosti informacij je prikazan na tabeli 35.

Tabela 35: Ocena zanesljivosti in veljavnosti na področju migracij (Frontex, 2013)

OCENA ZANESLJIVOSTI VIRA	
Ocena	**Opis**
A	Nikakršnega dvoma ni o pristnosti, zanesljivosti in verodostojnosti vira, če informacije priskrbi vir, ki se je v preteklosti vedno izkazal za zanesljivega
B	Vir, katerega informacije so se večinoma izkazale za zanesljive
C	Vir, katerega informacije so se večinoma izkazale za nezanesljive
X	Zanesljivosti vira ni mogoče oceniti
OCENA VELJAVNOSTI INFORMACIJ IN PODATKOV	
Ocena	**Opis**
1	Informacije, o katerih točnosti ni dvoma in so pogosto potrjene iz drugih virov
2	Informacije, ki so viru osebno poznane, niso pa osebno poznane uradniku, ki jih je prenesel naprej
3	Informacije, ki viru osebno niso poznane, vendar jih potrjujejo druge informacije, ki so bile že zabeležene
4	Informacije, ki viru osebno niso poznane in jih ni mogoče potrditi

Na osnovi predlagane metodologije agencija Frontex izdeluje:

- Letne analize tveganja: Letno poročilo o razmerah na področju nezakonitega priseljevanja v predhodnem letu, obeti in priporočila za prihodnost, podpora načrtovanju operativnih dejavnosti agencije Frontex za naslednje leto.
- Polletne analize tveganja: polletna dopolnitev letne analize tveganja, ki po potrebi vključuje pregled in prilagoditev priporočil.
- Četrtletne analize tveganja: Četrtletno poročilo s povratnimi informacijami in analizo gibanj na področju nezakonitega priseljevanja na podlagi izmenjave informacij v okviru Frontexove mreže za analizo tveganja.
- Ciljne analize tveganja: Analitično poročilo, osredotočeno na točno določen pojav ali geografsko območje; npr. nezakonito priseljevanje Iračanov v EU ali vpliv finančne krize na nezakonito priseljevanje v EU.
- Taktično osredotočena ocena: Analitično poročilo v podporo načrtovanju posebne skupne operacije.

- Tedensko analitično poročilo: Tedenska analiza informacij, zbranih med določeno skupno operacijo, za operativno skupino in organe države gostiteljice.

Agencija Frontex vse države članice spodbuja k vzpostavitvi lastne enote za analizo tveganja, ki naj bo pristojna za zbiranje informacij, povezanih z varnostjo meje in nasploh z notranjo varnostjo EU. Tovrstne enote naj pripravljajo in razširjajo analitična poročila in ocene agenciji Frontex ter zadevnim državam članicam.

Za zaključek velja poudariti še, da ocenjevanje (varnostne) ogroženosti in/ali tveganj ni omejeno izključno na širše družbene interese, temveč je tovrsten proces pogosto sestavni del internih strateško-upravljavskih dejavnosti v organizacijah. V podporo zagotavljanju organizacijske uspešnosti, pripravljenosti oz. odpornosti in uresničevanju načrtovanih dejavnosti, organizacije v okviru upravljanja ogroženosti/tveganj izvajajo interne analize in ocene (navadno na podlagi lastno določene metodologije). V teh primerih ne gre za ocenjevanje varnostnih razmer v družbenem interesu, temveč je namen prepoznati grožnje, ki bi ogrozile delovanje organizacije, pri čemer so v oceno lahko zajete različne oblike zunanjih in notranjih groženj. Kljub temu pa so v nacionalnovarnostnih organizacijah takšne ocene pomembne za zmogljivosti na področju zagotavljanja javne varnosti, v analizo pa so zajete tudi varnostne grožnje. Za potrebe uspešnega izvajanja nalog v programih in uresničevanja ciljev ter indikatorjev uspešnosti, ki so določeni v letnem in srednjeročnem načrtu dela policije ter usklajeni s temeljnimi in letnimi usmeritvami ministrstva, slovenska policija denimo letno pripravlja t. i. register tveganj. V tem registru se prepoznavajo in vrednotijo tveganja, ki bi lahko ogrozila izvedbo ciljev in nalog. Prepoznana tveganja se nanašajo tako na različne organizacijske zadeve in varnostne ter druge razmere. Tako kot v slovenski policiji tudi v Slovenski vojski poteka proces internega upravljanja ogroženosti in tveganj. Zbiranje in obdelava podatkov ter izdelava ocen groženj in tveganj so podlaga za načrtovanje in izvajanje ukrepov zaščite sil, ki je sestavni del bojnega in nebojnega delovanja Slovenske vojske in se nanaša na dejavnosti za zmanjševanje ranljivosti vojaških elementov (ljudi, opreme, objektov itd.) pred vsemi potencialnimi grožnjami.

Univerzitetna založba
Univerze v Mariboru

5 Ocenjevanje varnostnih razmer v tujini

5.1 Prakse izvajanja državnih ocen tveganj v drugih državah

V poglavju je predstavljen pregled pristopov, ki se uporabljajo za ocenjevanje varnostnih razmer oz. izvajanje ocene nacionalnovarnostne ogroženosti v tujih državah. Pregled je osredotočen na države, ki so po sistemski ureditvi ali gospodarskem položaju primerljive s Slovenijo oz. predstavljajo potencialno referenčno prakso. V analizo smo zajeli Nemčijo, Švico, Združeno kraljestvo, Irsko, Avstralijo, Dansko, Švedsko in Hrvaško (v nadaljevanju opisane v tem vrstnem redu).

Ocenjevanje in vzdrževanje nacionalne varnosti ter upravljanje nacionalnovarnostne ogroženosti v Nemčiji[12] ureja zakonodaja s področja civilne zaščite in pomoči ob nesrečah. Za zaščito državljanov pred nevarnostmi, ki izhajajo iz možnosti vojaških spopadov in vojn, je pristojna Zvezna vlada, za vse ostale primere nevarnosti oz. groženj pa so pristojne in odgovorne Zvezne dežele. V procesu ocenjevanja nacionalne ogroženosti sodelujejo Usmerjevalni odbor (predstavniki ministrstev, ki

[12] Opis za Nemčijo je pripravljen na podlagi pregleda naslednjih virov: Deutscher Bundestag (2013) in OECD (2018).

jih koordinira Zvezno ministrstvo za notranje zadeve), zadolžen za odločitve o splošnem metodološkem okviru analize tveganj na zvezni ravni; Delovni odbor (predstavniki zveznih agencij, ki jih koordinira Zvezni urad za civilno zaščito in pomoč ob nesrečah); Podskupine za posamezna tveganja (strokovnjaki dotičnih področij) in Zvezni urad za civilno zaščito in pomoč ob nesrečah (ang. Federal Office of Civil Protection and Disaster Assistance; nem. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) je osrednji organ za organizacijo in koordinacijo dela delovnih skupin za specifična področja in delovnega odbora). Na zvezni ravni postopek ocene tveganja za civilno zaščito jasno razlikuje med analizo tveganja in oceno tveganja.

V Nemčiji so v preteklosti izvedli analize tveganj za poplave, izredne epidemične situacije, zimske nevihte, huda neurja, izpuste radioaktivnih snovi iz nuklearnih elektrarn in tveganja zaradi sproščanja kemijskih snovi. Za to, da ocenjujejo oceno tveganja kot uspešno, so določena številna merila, kot npr.: potrebno je uravnoteženje znanstvenih pristopov s pragmatizmom; dosledno dokumentiranje; upoštevanje zgornjega praga, ki lahko vpliva na razvoj in stopnjevanje tveganj z ene upravne ravni na drugo; upoštevanje čezmejnih tveganj in ponovitev analize po določenem času.

Proces je izveden v petih korakih:

1. opis/določitev referenčnega območja;
2. izbor nevarnosti in opis scenarijev;
3. ocena verjetnosti;
4. ocena vpliva/resnosti;
5. vizualizacija tveganja.

Zaradi specifičnosti državne ureditve Zvezne republike Nemčije se v prvem koraku, tj. opisu oz. določitvi referenčnega območja, določi geografsko območje za analizo. Tako se določi, ali se bo analiza tveganj opravljala za a) območje celotne zvezne republike, b) zvezne dežele, c) administrativna območja ali d) ruralna območja ali okrožja. V tem koraku se opišejo splošne geografske značilnosti območja (npr. podnebje, kmetijska zemljišča), populacija (npr. število prebivalcev in gospodinjstev, gostota prebivalstva), okolje (npr. morebitna zaščitena okolja), gospodarstvo (npr.

uspešnost gospodarstva, dohodki z naslova davščin) in oskrba (npr. električna infrastruktura in oskrba s plinom, pitno vodo in telekomunikacijska infrastruktura).

V naslednjih korakih delovni odbor opredeli vrsto nevarnosti, za katero se ocenjuje tveganje, in nato razvije scenarij tveganja. Parametri omenjenega scenarija se morajo nanašati na:

- vrsto nevarnosti,
- njeno prostorsko oz. geografsko razsežnost,
- potencialno intenziteto in
- trajanje pričakovanega incidenta.

V tem procesu se izhaja iz obstoječih znanstveno dokazanih in dokumentiranih predpostavk in napovedi. Negativni učinki oz. škoda se določi v dveh korakih, in sicer z določitvijo »parametrov škode« in določitvijo »mejnih vrednosti«. Za vsako oceno tveganja se določijo drugačni parametri škode in mejne vrednosti, velja pa, da morajo parametri zaobjeti najpomembnejše subjekte, ki jih je treba zaščititi (npr. ljudje, okolje, gospodarstvo, nematerialne dobrine). Vpliv dogodkov na vsakega od parametrov se nato ocenjuje na petstopenjski lestvici, od A do E. Podobno kot učinke škodnih dogodkov, se verjetnost uresničitve ocenjuje na petstopenjski lestvici, le da v tem primeru od 1 – zelo malo verjetno do 5 – zelo verjetno. Pri tem področno-specifična delovna skupina verjetnost ocenjuje na logaritemski (nelinearni) lestvici. Tako se šteje, da se bo dogodek »zelo verjetno« zgodil, če je možnost, da se zgodi enkrat v desetih letih in »zelo malo verjeten«, če je možnost, da se zgodi enkrat na deset tisoč let. Rezultate se na koncu vizualizira s pomočjo matrike tveganja, ki prikazuje scenarije tveganja kot točko, ki jo določata glavna dejavnika: a) verjetnost uresničitve in b) vpliv/učinek škodnega dogodka. Takšna vizualizacija je kot podpora rezultatom nato odločevalcem (ki je lahko Zvezna vlada ali pa so to Zvezne dežele) v pomoč pri načrtovanju ukrepov za preprečevanje in obvladovanje škodnih dogodkov.

Nacionalni postopek ocenjevanja tveganja v Švici[13] se uporablja za prednostno obravnavanje nevarnosti, za pomoč pri pripravi načrtov in zmogljivosti za izredne razmere ter za namene usposabljanja. Odgovornost za razvoj nacionalne ocene

[13] Opis za Švico je pripravljen na podlagi pregleda naslednjih virov: Federal Office for Civil Protection – FOCP (2020a, 2020b) in OECD (2018).

tveganj nosi Zvezni urad za civilno zaščito, ki je vzpostavil tudi dodaten mehanizem za neodvisno evalvacijo nacionalne ocene tveganj. V Švici za ocenjevanje nacionalne ogroženosti uporabljajo kombinacijo dveh pristopov: *bottom-up* (od spodaj navzgor) in *top-down* (od zgoraj navzdol). Gre torej za izmenjevanje pristojnosti za posamezna področja tveganj med kantoni in zveznimi oblastmi. Kantoni so odgovorni za izvedbo ocene tveganj in pripravo osnutkov načrtov pripravljenosti za svoja geografska območja. Zvezne oblasti (Zvezni urad za civilno zaščito po pooblastilu Zveznega sveta Švice) so odgovorne za pet potencialnih groženj: povišana radioaktivnost; ponovni vstop satelitov; nesreče, povezane z nevihtami in točo; pandemije in obolenja živali.

Pri določanju, katera ostala tveganja bodo ocenjena na zvezni ravni, se upošteva, ali je potrebna koordinacija dveh ali več agencij preko ravni sodelovanja, ki se pričakuje med sosedskimi kantoni. Podlago za izvajanje ocene tveganj in pristojnosti določa zakonodaja o zaščiti prebivalstva in civilni zaščiti. Pri pripravi ocene sodelujejo delovne skupine za posamezna področja tveganj. Znotraj teh delovnih skupin delujejo predstavniki Zveznega urada za civilno zaščito, predstavniki zveznih agencij za posamezna področja, predstavniki kantonov, prvih posredovalcev, gospodarstva, subjektov kritične infrastrukture in akademske skupnosti. Razmerja med subjekti, ki tvorijo delovne skupine, so: dve tretjini predstavnikov iz javnega sektorja, ena četrtina iz zasebnega sektorja in deset odstotkov iz akademske skupnosti.

Proces nacionalne analize tveganja zaradi nesreč in izrednih razmer deli grožnje v tri glavne skupine: nevarnosti, ki izhajajo iz: a) narave, b) tehnologije in c) družbe. V skupino nevarnosti, ki izhajajo iz narave, prištevajo npr. potrese, poplave, snežne nevihte, padec meteorita, vročinski val. V skupino nevarnosti zaradi tehnologije prištevajo npr. izpad električne energije, prometne ali železniške nesreče z nevarnimi snovmi, letalske nesreče in odpoved dobave plina. V zadnjo skupino nevarnosti, ki izhaja iz družbe, pa prištevajo npr. teroristične napade, pandemije, biološke napade, nasilne izgrede in migracijske valove. V oceni tveganja iz leta 2012) so identificirali 12 tipov nevarnosti, v oceni iz leta 2015 so dodali še 21 tipov, v oceni leta 2020 pa so dodali še 11 tipov. Izvedba in dopolnitve ocene tveganj se tako izvajajo periodično, a po potrebi. Analiza omenjenih tipov nevarnosti temelji na primerjavi možnih scenarijev. Ti scenariji ponazarjajo tri stopnje vpliva/resnosti nevarnosti: 1) velike, 2) zelo velike in 3) ekstremne. Te stopnje odražajo naslednje tri stopnje možnosti uresničitve: 1) pričakovan scenarij, 2) razumno slab scenarij in 3) najslabši

možni scenarij. Proces analize tveganja opredeljuje tveganje kot zmnožek povzročene škode in verjetnosti uresničitve škodnega dogodka. Obstaja dvanajst meril za presojo vpliva/resnosti (ali škode), ki odražajo najpomembnejša področja varovanja (v nadaljevanju so zapisana podpodročja):

- prebivalstvo (življenje in zdravje, pomoč in izredne razmere),
- okolje (ekosistem),
- družba (zagotavljanje ključnih dobrin in storitev, zakon in red, podoba in zaupanje v institucije, teritorialna integriteta, kulturne dobrine).

Ocena verjetnosti (ang. *likelihood*) poteka na osnovi osemstopenjske logaritmične lestvice, pri čemer vsaka stopnja predstavlja trikratno povečanje glede na prejšnjo stopnjo. Kljub temu je lestvica kvalitativne narave, saj so stopnje izražene opisno in številčno. Npr. prva (najnižja) stopnja je zapisana kot: »Zelo malo verjetno kjerkoli na svetu; še bolj v Švici, vendar ni povsem nepredstavljivo« (kvalitativno) in možnost uresničitve v desetih letih znaša < 0,03 % (številčno); tretja stopnja je zapisana kot: »V Švici se to doslej še ni zgodilo, po svetu pa je malo znanih primerov« (kvalitativno) in možnost uresničitve v desetih letih znaša od 0,1 % do 0,3 % (številčno); peta stopnja je zapisana kot: »V Švici se doslej ni zgodilo, je pa znano iz drugih primerljivih držav« (kvalitativno) in možnost uresničitve v desetih letih znaša od 1 % do 3 % (številčno); osma (najvišja stopnja) pa je zapisana kot: »V Švici se v povprečju zgodi nekajkrat v življenju« (kvalitativno), možnost uresničitve v desetih letih pa znaša > 30 % (številčno).

Lestvica za oceno prepričljivosti (ang. *plausibility*) pa je petstopenjska. Enako kot pri oceni verjetnosti gre za kvalitativno lestvico, ki ji je dodeljen P-indeks. Npr. prva (najnižja) stopnja prepričljivosti P1 ima dodeljena indeksa 1,0 in 1,5; v tem primeru gre za oceno »komaj prepričljivo« z opisom »Možnosti, da bi se dogodek zgodil v Švici, si je v primerjavi z drugimi scenariji težko predstavljati, vendar je ni mogoče v celoti izključiti. Ni znakov o naklepu potencialnega storilca. Izvedljivost scenarija je na splošno zapletena.« Na drugi strani ima peta (najvišja) stopnja prepričljivosti P5 dodeljen indeks 5,0; v tem primeru gre za oceno »visoko prepričljivo« z opisom »Možnost, da bi se dogodek zgodil v Švici, si je v primerjavi z drugimi scenariji mogoče prepričljivo zamisliti. Obstajajo nesporni znaki naklepa potencialnega storilca. Izvedljivost scenarija je na splošno preprosta.« Za namene poročanja se

rezultati vizualizirajo s pomočjo diagramov. Nevarnosti so izrisane na dveh matrikah. V obeh primerih je na horizontalni osi prikazana ocenjena potencialna škoda (v švicarskih frankih), na vertikalni osi pa je v enem primeru ocenjena verjetnost uresničitve grožnje, v drugem primeru pa frekvenca oz. pogostost.

Vlada Združenega kraljestva[14] izvaja nacionalno ocenjevanje tveganj na podlagi zakonodaje o izrednih civilnih razmerah. Do nedavnega so v Združenem kraljestvu izvajali dve medsektorski ocenjevanji tveganj – National Risk Assessment (NRA) (nacionalna ocena tveganj) in National Security Risk Assessment (NSRA) (nacionalna ocena varnostnih tveganj). Od leta 2019 sta obe združeni v eno oceno tveganja – National Security Risk Assessment (NSRA), ki obravnava domača, mednarodna, zlonamerna in nezlonamerna tveganja. Postopek koordinira Kabinet Združenega kraljestva in se obnavlja v petletnem časovnem obdobju. Nacionalna ocena tveganj črpa strokovna znanja iz široke palete vladnih oddelkov, agencij, akademskih krogov in zunanjih strokovnjakov. Ima vsevključujoči vladni pristop (vključuje vsa področja vlade), ki uporablja na dokazih utemeljena dejstva za določitev obsega tveganj, na katera mora biti Združeno kraljestvo pripravljeno. Nacionalna ocena tveganj je zasnovana tako, da deluje kot proces od zgoraj navzdol in usmerja identifikacijo tveganj za celotno Združeno kraljestvo ter usmerja regionalne subjekte pri identifikaciji njihovih lastnih tveganj.

NSRA vključuje posamezne dogodke oz. razmere, ki lahko povzročijo resno škodo in za katere obstaja razumna verjetnost, da se bodo zgodile v dveh letih od datuma ocene tveganja. Tveganja so smiselno vsebinsko združena,[15] z namenom, da se lahko primerjajo glede na verjetnost in vpliv. Tveganja so definirana glede na najslabše možne scenarije (ang. *reasonable worst case scenarios*), ki predstavljajo verjetnost za uresničitev tveganja. Postopek priprave osnutka NSRA vodi Sekretariat za izredne civilne razmere, ki je umeščen znotraj kabineta Vlade. Za vsako tveganje je zadolženo posamezno ministrstvo, ki izvede začetne ocene vpliva in verjetnosti tveganja, pri čemer se opirajo na razpoložljivo strokovno znanje. Sekretariat prevzame vlogo podpore ministrstvom pri tem delu in združi ocene tveganj, ki jih nato pregledajo ostali deležniki iz vrst vladnih uradnikov in zunanjih strokovnjakov.

[14] Opis za Združeno kraljestvo je pripravljen na podlagi pregleda naslednjih virov: Hilton in Baylon (2020; Home Office Government (2015); OECD (2018) in Russell Vastveit, (2011).
[15] Denimo »pojavljanje nalezljive bolezni« (ang. *emerging infectious desease*) se obravnava kot eno tveganje.

NSRA, katere rezultati so zaupni, je podlaga za nacionalni register tveganj (ang. National Risk Register). Ta dokument pa je dostopen javnosti in omogoča pregled razmer, za katere vlada meni, da bi lahko močno vplivale na celotno državo ali njene dele ter na dobrobit in varnost njenih prebivalcev. Objavljen je najmanj vsako drugo leto. V pripravo registra tveganj so denimo vključeni sekretariat, kabinet Vlade, oddelki in organizacije, ki prispevajo vsebino glede na specifična tveganja, strokovnjaki vladne službe za komuniciranje, strokovnjaki s področja vedenjske znanosti in raziskovalni univerzitetni centri.

Proces ocenjevanja tveganj v okviru NSRA vsebuje naslednje glavne faze:

1. Identifikacija tveganj: V tej fazi sekretariat izvaja posvetovanja s širokim naborom strokovnjakov v različnih vladnih službah s ciljem, da ocena tveganj temelji na celovitem razumevanju možnih nesreč, groženj in nevarnosti v skladu z merili, določenimi v zakonodaji.
2. Razvoj najslabših možnih scenarijev: Na podlagi identificiranih tveganj se opredelijo najslabši možni scenariji. Glavni namen te faze je izključiti teoretično možne scenarije, ki pa imajo tako malo verjetnosti, da bi načrtovanje verjetno vodilo v nesorazmerno porabo virov. Scenariji niso mišljeni kot napovedi, kako se bo neka vrsta dogodka odvijala, temveč kot najslabši način, na katerega bi se lahko. Glavno odgovornost za scenarije običajno nosi ministrstvo, ki je pristojno za področje nevarnosti. Znotraj ministrstva se angažirajo številni strokovnjaki za oblikovanje glavnih parametrov scenarija. Lahko se posvetujejo tudi s podrejenimi agencijami in drugimi ministrstvi ter strokovnimi in znanstvenimi zunanjimi svetovalci. Ključno je, da so scenariji čim bolj splošni in tako pokrijejo vrsto možnih dogodkov ter geografskih območij. Na ta način so uporabni kjer koli v državi in na kateri koli ravni – nacionalni, regionalni in lokalni.
3. Ocena verjetnosti in vpliva: Končni scenariji se razdelijo posameznim ministrstvom v analizo in oceno verjetnosti nastanka scenarija ter njegovih možnih posledic. Analiza scenarijev poteka v dveh korakih. Najprej strokovne skupine, ki so bile usklajene znotraj ministrstev, ocenijo scenarije z uporabo razpoložljivih objektivnih zgodovinskih, statističnih in znanstvenih podatkov. O ugotovitvah nato razpravljajo na sestankih, na katerih sodelujejo vse relevantne vlade službe (glede na

vsebino, ki jo pokriva scenarij). V drugem koraku sledi medresorska ocena, v kateri sodelujejo različne skupine strokovnjakov in znanstvenih zunanjih svetovalcev (pripadniki partnerskih agencij, akademskih institucij in gospodarstva).

Verjetnost scenarijev določijo s pomočjo petstopenjske lestvice, za obdobje enega leta. Pri nezlonamernih tveganjih (npr. naravne nesreče) uporabijo zbirke podatkov, modeliranje in strokovno vsebinsko analizo. Za zlonamerne grožnje določijo ločeni oceni za ranljivost in ogrožanje, ki se nato združita v oceno vpliva. Primeroma, pripravljenost in motiviranost posameznikov ali skupin za izvedbo napadov je treba oceniti in uravnovesiti glede na to, kar je znano o njihovih zmožnostih in zmogljivostih za napad ter glede na ranljivost njihovih potencialnih žrtev ali tarč.

Analiza vpliva tveganj poteka preko sedmih različnih postavk:

- vplivi na dobrobit ljudi, vključno s smrtnimi žrtvami, ki jih je mogoče neposredno pripisati dogodku; ostale žrtve zaradi dogodka (vključno z boleznimi, poškodbami in psihološkimi vplivi); potrebe po evakuaciji in zavetiščih;
- vplivi na vedenje, vključno s spremembami v vedenju posameznikov in zaskrbljenost javnosti;
- vplivi na osnovne storitve, vključno z motnjami pri transportu, zdravstvu, izobraževanju, dobavi hrane, vode, energije; nujne službe in telekomunikacije;
- gospodarska škoda, vključno z izgubo na področju turizma in zmanjšanja obsega delovnega časa;
- vplivi na okolje;
- vplivi na varnost, vključno z vplivom na sistem kazenskega pregona in pravosodja;
- mednarodne posledice, vključno s škodo za mednarodne odnose.

Večina tveganj v NSRA se ocenjuje na letni ravni; po potrebi in presoji ministrstev ali sekretariata se dodajo novi scenariji. Ocene verjetnosti in vpliva za različne scenarije se združijo in na podlagi tega se vsak scenarij umesti v nacionalno matriko tveganj.

Krovni dokument za ocenjevanje tveganj na Irskem[16] je nacionalna ocena tveganj (National Risk Assessment – NRA), ki se osredotoča na prepoznavanje in razpravo o pomembnih tveganjih, ki se v državi lahko pojavijo kratkoročno, srednjeročno in dolgoročno. Proces izvedbe nacionalne ocene tveganj se še posebej osredotoča na strateška ali strukturna tveganja. Ta tveganja se lahko pojavijo v različnih časovnih okvirih in imajo zelo različne učinke v smislu aktualnosti, dosega in stroškov. Postopek ocenjevanja tveganj je zasnovan tako, da zagotovi širok razpon obravnave tveganj za državo, preprečuje tako imenovano skupinsko razmišljanje (ang. *group think*),[17] je vključujoč in zagotavlja prepoznavo in upoštevanje celotnega obsega strateških tveganj, s katerimi se država sooča. Osnutek seznama strateških tveganj vsako leto pripravi usmerjevalna skupina, ki ji predseduje kabinet predsednika vlade, sestavljajo pa jo predstavniki vseh vladnih služb in relevantnih agencij. Osnutek nacionalne ocene tveganj je nato objavljen za javno razpravo, v kateri se spodbuja vključevanje javnosti, organizirajo tudi posebne seminarje za razpravo in izmenjavo mnenj. Končno nacionalno oceno tveganj nato objavi vlada.

Faze procesa ocenjevanja tveganj so naslednje:

1. Določitev ključnih tveganj: Vse vladne službe in relevantne agencije pripravijo seznam tveganj, ki so po njihovem mnenju nacionalnega pomena. Za nadaljnjo analizo je bilo v procesu nastajanja nacionalne ocene tveganj za leto 2020 identificiranih 182 tveganj. Delovna skupina, ki so jo sestavljali različni področni in zunanji strokovnjaki, je po pregledu sestavila konsolidiran seznam tveganj, ki je vseboval 38 tveganj. Ta seznam so nato natančneje analizirali in izločili tveganja z nizko verjetnostjo in velikim vplivom (ang. *low probability risks with a high impact*), kar je skrčilo seznam na 22 tveganj.
2. Konsolidacija: V tej fazi je bilo 22 tveganj razvrščenih v štiri kategorije – naravna, transportna, tehnološka in civilna tveganja. Sledi naslednja faza izločanja tveganj, ki jo opravijo člani posebne podskupine vladne delovne skupine za tveganja. Na tej točki izločijo še tveganja, ki so obvladljiva na resorski, agencijski ali regionalni ravni. Končni seznam tako vsebuje 16 ključnih tveganj.

[16] Opis za Irsko je pripravljen na podlagi pregleda naslednjih virov: Government of Ireland (2021a, 2021b).
[17] Skupinsko mišljenje v tem kontekstu razumemo kot nekritično sprejemanje skupinskih vrednot in vedenja.

3. Ocenjevanje: Za vsako kategorijo tveganj (naravna, transportna, tehnološka in civilna) so ustanovljene posebne ekspertne fokusne skupine, ki jih sestavljajo strokovnjaki iz ustreznih vladnih služb. Za vsako ključno tveganje ekspertna fokusna skupina opravi naslednje naloge:
   - opredelitev najslabšega možnega scenarija;
   - ocena verjetnosti uresničitve scenarija (petstopenjska lestvica od ekstremno neverjetno (ang. *extremely unlikely*) do zelo verjetno (ang. *very likely*));
   - določitev vpliva na ljudi, okolje, gospodarstvo in družbo (petstopenjska lestvica od zelo nizek vpliv (ang. *very low impact*) do zelo visok vpliv (ang. *very high impact*)).
4. Analiza: Vsako od tveganj se na podlagi poglobljene analize razvrsti v matriko tveganj – posebej za vsako kategorijo – in nato v skupno matriko za vse kategorije tveganj.
5. Odobritev in objava: V zadnjem delu sledi potrditev nacionalne ocene tveganj, predložitev dokumenta vladi in Evropski komisiji ter javna objava.

Avstralija[18] je v svetovnem merilu ena od začetnic razvoja pristopa k obvladovanju tveganj, saj so leta 1995 skupaj z Novo Zelandijo razvili standard upravljanja tveganj (AS/NZS 4360: 1995 Risk Management), katerega kasnejša različica (iz leta 2004) je predstavljala osnovo za ISO standard 31000. Leta 2010 je avstralska vlada sprejela nacionalne smernice za ocenjevanje izrednih tveganj (National Emergency Risk Assessment Guidelines – NERAG), ki v aktualni različici (usklajen s standardom ISO 31000 in revidiran na podlagi evalvacij izvajanja v praksi), posodobljeni leta 2020, predstavlja usklajeno podlago za ocene tveganja na vseh ravneh (lokalni, državni, nacionalni) in za organizacije v javnem, zasebnem in nevladnem sektorju. V praksi se NERAG uporablja tako za začetno kot tudi za podrobno oceno tveganj. Začetna ocena tveganj se uporablja za hitro prepoznavanje in analizo tveganj ter običajno temelji na kvalitativnih metodah in povzetkih informacij v širšem obsegu. Namen začetne ocene je, da v grobem pomaga pri določanju prednostnih nevarnosti in tveganj ter pri identifikaciji tveganj, ki terjajo podrobno ocenjevanje. Slednje se

[18] Opis za Avstralijo je pripravljen na podlagi pregleda naslednjih virov: Australian Institute for Disaster Resilience (2020); OECD (2018).

uporablja za tveganja visoke prioritete in tveganja, ki imajo najboljši potencial za uspešno obravnavo. Podrobna ocena se pogosto izvaja za specifične nevarnosti in je namenjena celovitemu razumevanju tveganj in pripravo ustreznih priporočil za njihovo obravnavo.

NERAG predvideva obravnavo tveganj po naslednjih merilih:

1. stopnja resnosti posledic (od nepomembno (ang. *insignificant*) do katastrofalno (ang. *catastrophic*));
2. stopnja verjetnosti (od ekstremno redko (ang. *extremely rare*) do skoraj zagotovo (ang. *almost certain*));
3. stopnja tveganja (od zelo nizka (ang. *very low*) do ekstremna (ang. *extreme*));
4. stopnja zanesljivosti[19] (od najnižje (ang. *lowest*) do najvišje (ang. *highest*)).

Glede na ocene posameznih postavk se nato tveganje razvrsti v kvalitativno matriko.

Nacionalna ocena tveganja, ki jo izvaja Danska,[20] je nacionalni profil tveganj (ang. National Risk Profile – NRP). Profil izdela agencija za krizno upravljanje (The Danish Emergency Management Agency – DEMA), ki je del danskega ministrstva za obrambo. Fokus danske ocene je na najbolj verjetnih in nevarnih naravno ali od človeka povzročenih groženj. DEMA je izdelala metodologijo za oceno NRP preko petih korakov. V prvem koraku so pripravili okvirni seznam možnih incidentov (ang. *incident types* – ITs). Gre za krovni termin, ki pokriva vrste dogodkov oz. proces razvoja dogodka, pri čemer pa opozarjajo, da ne gre za klasične scenarije, saj se ti tipi dogodkov lahko manifestirajo v različnih oblikah. Ključno pri identifikaciji ITs je, da gre za dogodek, ki presega urgentne reakcije in kapacitete lokalnih enot. Vsakodnevni incidenti, ki jih urgentne službe lahko upravljajo, niso zajeti v analizo.

Zadnja ocena tveganj iz leta 2022 opisuje naslednje grožnje: suše in vročinski vali, orkani in močne nevihte, obalne poplave, ekstremne padavine, zelo nalezljive bolezni, bolezni živali, obolenja od kontaminirane vode in hrane, jedrske nesreče,

[19] Stopnja prepričanja se nanaša na zanesljivost, ustreznost in veljavnost dokazov, ki so bili uporabljeni za določitev ocene; uporabo primernega strokovnega znanja in na raven soglasja med deležniki.
[20] Opis za Dansko je pripravljen na podlagi pregleda naslednjih virov: Danish Emergency Management Agency (DEMA) (2022); OECD (2018).

nesreče s kemičnimi sredstvi, pomorske nesreče, prometne nesreče, kibernetski incidenti, teroristična dejanja, incidenti v vesolju.

Pri presoji omenjenih groženj oz. ITs je velik poudarek podan na škodi in posledicah, ki jih imajo ITs, torej ali lahko povzročijo takojšne izgube življenj oz. imajo vpliv na zdravje ljudi, okolje, gospodarstvo družbe (vključno s funkcionalnostjo finančnih in drugih sistemov), zasebno/javno lastnino in vitalne družbene funkcije. V tej fazi se naslovijo tudi dogodki s kaskadnimi vplivi (pristop, ki upošteva več tveganj). V drugem koraku je DEMA izdelala metodologijo, s pomočjo katere so izluščili 10 najpomembnejših ITs in jih vključili v prvo končno oceno. V zadnji NRP pa so vključili 14 ITs. V tretjem koraku so izdelali osnutek ocene za izbrane ITs. V oceno so vključili uvodni opis karakteristik, vključno z možnimi vzroki, opis možnih posledic, opis dejanskega primera, ocenjevanje zahtevnosti kriznega upravljanja/odzivanja ter analizo morebitnih trendov, ki bi lahko imel vpliv na ITs. Četrti korak je zajemal posvetovanje DEMA z ostalimi deležniki danske vlade na uradni/ekspertni ravni, peti korak pa je vključeval posredovanje osnutka ocene v podpis ministru za obrambo.

Znotraj tretjega koraka, torej analize posameznih ITs je vidno, da se predvsem v opisih ITs precej naslanjajo na izkušnje iz zgodovine, saj ocena vključuje opise incidentov, ki so se že zgodili. Gradijo torej na izkušnjah glede samih značilnostih incidenta in na izkušnjah, kako so se njihove urgentne službe odzvale na incident. Ocena ob koncu analize za vsak incident navede najslabši (t. i. ang. *what if*) scenarij, ki pa ne vključuje načrta odzivanja urgentnih služb, ampak samo oriše izredno problematičen, morebiten razvoj dogodka. ITs analizirajo v 0–5-letnem časovnem okvirju. Za vsak incident NRP tudi našteje ključne akterje odzivanja. Incidenti, ki so vključeni v NRP, so izbrani glede na možnost pojavitve na Danskem. Ker imata Grenlandija in Farski otoki svojevrstne geografske in demografske značilnosti, so izključeni iz analize. Pri ocenjevanju zahtevnosti odzivanja uporabljajo osem ključnih meril, ki zajemajo:

1. Znanje o incidentu – kjer je ključno vprašanje, kako dobro so akterji urgentnega odzivanja seznanjeni s takšnimi incidenti.
2. Zmožnost prevencije – kjer je ključno vprašanje, kako obsežno je preprečevanje ključnih dejavnikov, ki povzročijo razvoj takega incidenta.

3. Pogostost incidenta – kjer je ključno vprašanje, kako pogosto prihaja do pojavljanja tega incidenta.
4. Zgodnje opozarjanje – kjer je ključno vprašanje, kako močno, odsotnost priložnosti za zgodnje opozarjanje prebivalstva pred pojavom incidenta, vpliva na zmožnost kriznega upravljanja incidenta.
5. Ublažitev posledic incidenta – kjer je ključno vprašanje, kako zahtevno je preprečiti razvoj resnih posledic incidenta, po tistem, ko se je že pojavil.
6. Geografski obseg – kjer je ključno vprašanje, kako veliko je območje v državi, kjer se incident sočasno razvije in kako to vpliva na krizno upravljanje incidenta.
7. Trajanje incidenta – kjer je ključno vprašanje, kako dolgo lahko tak incident traja in ali lahko to predstavlja težavo.
8. Obnova/okrevanje po incidentu – kjer je ključno vprašanje, kako zahtevno z vidika časa in sredstev, je okrevanje/obnova po incidentu. Torej koliko časa lahko traja, da se družba vrne v normalno stanje.

NRP ocena naslavlja tudi t. i. trende, ki so procesi, ki bi se lahko razvili v situacijo, ki bo zahtevala odziv kriznega upravljanja. Gre torej za odgovor na vprašanje ali lahko ima v naslednjih 5–15 letih določen trend posledice na identificiran ITs ali pa bo vplival na pojavitev novega ITs oz. vplival na družbeno zmožnost kriznega upravljanja – tudi v smislu, da bi povzročil preusmerjanje kapacitet družbenega upravljanja.

Poglavitna nacionalna ocena tveganja, ki jo izvaja Švedska,[21] je nacionalna analiza tveganj in zmogljivosti (National Risk and Capability Analysis – NRC), ki jo pripravi Agencija za izredne civilne razmere (MSB). Namen tovrstne ocene je spodbujati bolj informirano analizo glavnih tveganj, s katerimi se bo Švedska kot družba verjetno soočila. Fokus analize so grožnje, ki bi lahko imele resne posledice za ključne družbene dobrine oz. vrednote, tj. življenje in zdravje ljudi, delovanje družbe, gospodarstvo in okolje, demokracija, vladavina prava, človekove pravice in svoboščine ter nacionalna suverenost. Grožnje v NRC so porazdeljene v štiri glave kategorije: naravne nesreče, večje nesreče, motnje v tehnični infrastrukturi in

[21] Opis za Švedsko je pripravljen na podlagi pregleda naslednjih virov: OECD (2018); The Swedish Civil Contingencies Agency (MSB) (2016).

oskrbovalnem sistemu ter antagonistične nevarnosti (to so oboroženi spopadi, terorizem in druge antagonistične grožnje). Proces izvajanja NRC vključuje pristop od spodaj navzgor k oceni tveganja in ranljivosti z usklajenim pristopom k oceni tveganja od zgoraj navzdol. V poročilu iz leta 2016 so opisali naslednje grožnje: potres in vulkanski izbruh, plaz, poplava, nevihta, vročinski val, gozdni in požar v naravi, nalezljive bolezni, odpornost na antibiotike, napadi žuželk škodljivcev (rastlinskih škodljivcev), sončna nevihta, nesreče v transportu, obsežni požari, emisije nevarnih snovi (kemična, biološka, radiološka in jedrska obramba), okvara jezu, motnje v oskrbi z energijo, motnje v elektronski komunikaciji, motnje v plačilnem sistemu, motnje v oskrbi s hrano, motnje v oskrbi s pitno vodo, motnje v transportnem sistemu, motnje v oskrbi z zdravili, kibernetski napadi, terorizem, streljanje v šolah, izbruhi nasilja.

Protokol analize groženj poteka po naslednjih korakih:

1. opredelitev področij varovanja – nacionalnih vrednot vrednih zaščite;
2. identifikacija groženj – identifikacija neželenih dogodkov (tj. dogodki, ki izpolnjujejo merila, da se lahko dogodek označi kot kriza na družbeni ali državni ravni);
3. izbor dogodkov (tveganj) za analizo;
4. razvoj scenarija izbranih neželenih dogodkov;
5. analiza scenarijev – ocena vpliva (škode), verjetnosti, variacije in negotovosti;
6. sinteza in ocena groženj.

Časovni okvir, za katerega se izdeluje ocena tveganj, je 5 let. Pri razvoju scenarija se upošteva ter vključi tudi opis zmožnosti družbe za odzivanje na pojav posamezne grožnje. Pri tem MSB poudarja, da so scenariji le en zapis možne manifestacije ogrožanja. Za oceno vpliva (škode) se uporablja lestvica, ki ima določene mejnike glede na karakterizacijo resnosti nekega dogodka.

Za povečanje verodostojnosti oz. veljavnosti ocene izvajalci za vsako identificirano grožnjo naredijo tudi oceno negotovosti. Negotovost nakazuje stopnjo zaupanja v podatke oz. odsotnosti ustreznih podatkov in/ali izkušenj. Pri tem se uporabi tristopenjska lestvica, in sicer v razponu nizka, srednja in visoka. Nizka stopnja označuje izdelavo ocene na trdnih izkušnjah, statistikah in drugih podatkih. Ocena

je sicer lahko nenatančna, toda to je malo verjetno. Srednja stopnja je odsev omejenega obstoja statistik in podatkov, pri čemer eksperti verjamejo, da je ocena logična, toda lahko obstaja določena stopnja napake. Visoka stopnja negotovosti označuje malo statističnih in drugih podatkov, ki se lahko uporabijo za izdelavo ocene, stopnja napake pa je zato pomembna. Analiza variacije pri vsakem scenariju pa predstavlja opis in oceno vpliva, v primeru, če bi se določen element znotraj scenarija spremenil.

Vse pridobljene vrednosti – elemente ocene se mapira tudi v matriki tveganja, ki uporablja dimenzijo verjetnosti in dimenzijo vpliva (škode). Pri izdelavi takšnih ocen MSB posebej poudarja, da ne izvaja rangiranja oz. razvrščanja groženj glede na oceno tveganja, ampak (če že) bi se morale grožnje razvrstiti glede na identificirane ranljivosti in pomanjkljivosti v kapacitetah odzivanja, ki so jih nakazale analize scenarijev. Končni izdelek izvedene analize je posredovan civilnim deležnikom, ki izvedejo recenzijo kakovosti. Podobno je v recenzijo poslan tudi osnutek poročila. Celoten proces sledi dorečeni in transparentni metodologiji, zato nobeno poročilo še ni bilo zaupne narave. MSB izvaja tudi anketiranje vključenih strokovnjakov in tako dobi ustrezno povratno informacijo glede delavnic ipd.

Poročilo NRC in nasploh švedski pristop k oceni tveganj daje velik poudarek kapacitetam za odzivanje na (identificirana) ogrožanja, saj je posebna pozornost namenjena štirim elementom:

- Pomen dela s posameznimi tveganji na podlagi perspektive vseh tveganj.
- Zmožnost vzdrževanja kritične infrastrukture.
- Zmožnost varnega upravljanja informacij.
- Sposobnost usklajenega delovanja v primeru incidenta.

Tudi analiza scenarijev nasploh poudarja kapacitete, saj analiza vključuje trenutne zmožnosti in segmente, ki jih je v okviru izboljšanja treba nasloviti.

Nacionalna ocena, ki jo izvaja Hrvaška[22] je nacionalna ocena tveganja za katastrofe (Nacionalna procjena rizika od katastrofa – NPRK). Usklajevanje procesa ocene

[22] Opis za Hrvaško je pripravljen na podlagi pregleda naslednjih virov: Aurer-Jezerčić (2017); Državna uprava za zaštitu in spašavanje (2009); Glavna radna skupina Hrvatske platforme za smanjenje rizika od katastrofa (2019);

tveganj koordinira notranje ministrstvo in izvede glavna delovna skupina hrvaške platforme za zmanjševanje tveganj, povezanih s katastrofami. Omenjena platforma predstavlja stičišče politične, operativne in tudi znanstvene sfere na področju zmanjševanja tveganja v povezavi z nesrečami, medtem ko je omenjena delovna skupina znotraj te platforme zadolžena za izdelavo ocene tveganj. V prvem procesu je bilo primarno identificiranih 28 groženj, ki so jih porazdelili v 11 kategorij, v poročilo pa so vključili opise 11 enovrstnih groženj in ene kombinirane. V NPRK iz leta 2015 je bilo vključenih naslednjih 11 groženj: Bolezni rastlin; Bolezni živali; Ekstremne temperature; Epidemije in pandemije; Industrijske nesreče; Poplave zaradi prelivanja celinskih vodnih teles; Potres; Požari v naravi; Sneg in led; Suša; Zasoljevanje tal ter ena (kompleksnejša grožnja) nevarnost potresov in poplav (v Zagrebu). V NPRK iz leta 2019 pa še Jedrske nesreče; Radiološke nesreče; Plazovi; Onesnaževanje morja.

Za identifikacijo ključnih groženj se je primarno uporabil dokument Ocena ogroženosti z naravnimi in tehnično-tehnološkimi katastrofami in velikimi nesrečami, ki ga je izdelala hrvaška uprava za zaščito in reševanje in ga lahko obravnavamo kot prvi pristop k hrvaški nacionalni oceni tveganj.

Za vseh 28 groženj je bil izdelan scenarij, ki predstavlja opis poteka dogodkov in opis posledic na treh ključnih področjih, tj. življenje in zdravje oseb, gospodarstvo ter stabilnost družbe in politike. Scenarije so izdelale delovne skupine, sestavljene iz vseh ključnih akterjev, tj. predstavnikov organizacij, pod katero delovno področje spada določena grožnja. Glavna delovna skupina, ki je prav tako sestavljena iz predstavnikov ključnih akterjev, je potem izbrala scenarij, ki bi imel največje nacionalne posledice. Pri vsaki izmed identificiranih groženj je določen glavni koordinator, ki je določen tudi kot ključni akter odzivanja in upravljanja v primeru realizacije grožnje. Scenarij vključuje opis vzrokov – razvoj dejavnikov in situacij, ki pripeljejo do dogodka, ter stopnjo ogroženosti na eni strani in stopnjo odpornosti prebivalstva in infrastrukture na drugi. Prav tako vključuje možne posledice. Scenariji za enovrstne grožnje vključujejo opis najverjetnejšega neželenega dogodka in opis dogodka z najhujšimi možnimi posledicami. Ocena tveganj poteka po naslednjem postopku:

Ministarstvo unutarnjih poslova Republike Hrvatske (2021); »Pravilnik o metodologiji za izradu procjena ugroženosti i planova zaštite i spašavanja« (2008); Ravnateljstvo civilne zaštite (2021); Vlada Republike Hrvatske (n. d.).

- Za ocenjevanje verjetnosti/frekvence je uporabljena petstopenjska kategorizacija, kjer je najvišja, peta stopnja, tista kategorija, ko gre za najverjetnejše/najbolj pogoste dogodke, saj se lahko pojavijo najmanj 1x (lahko pa tudi pogosteje) letno. Pri najnižji (tj. prvi) kategoriji pa gre za dogodke, ki se lahko pojavijo enkrat v 100 letih ali manj. Ostale kategorije so druga stopnja (frekvenca 1 dogodek v 20 do 100 letih), tretja stopnja (1 dogodek v 2 do 20 letih) in četrta stopnja (1 dogodek v 1 do 2 letih).
- Pri ocenjevanju škode v povezavi z življenjem in zdravjem ljudi se prav tako uporablja petstopenjska kategorizacija, kjer je najvišja peta stopnja – stopnja katastrofalnih razsežnosti oz. posledic in kjer je število oseb, ki so občutile posledice nekega dogodka, večje od 1.500 oseb. Pri četrti stopnji – pomembnih razsežnosti, posledice občuti med 501 in 1.500 oseb, pri tretji stopnji – zmernih posledic je število oseb med 201 in 500, pri drugi stopnji – majhnih posledic je število med 50 in 200, in najnižja stopnja – neznatne posledice je število oseb pod 50. Pri oceni škode za gospodarstvo in za stabilnost družbe in politike se uporablja delitev glede na finančno škodo in kjer se prav tako uporabi petstopenjska lestvica.
- Ocene vrednosti se vnesejo v matriko, kjer je ena komponenta verjetnost in druga komponenta obseg posledic. Vnos ocen v matriko se naredi ločeno za scenarij z največjimi možnimi posledicami in ločeno za scenarij z najverjetnejšimi posledicami ter za vsako izmed treh ključnih področij ogrožanja: življenje in zdravje oseb, gospodarstvo ter stabilnost družbe in politike. Skupna ocena tveganja predstavlja seštevek vrednosti obeh scenarijev, torej najbolj verjetna oblika dogodka in najhujša oblika dogodka. NPRK vključuje tudi kartografski prikaz stopenj tveganja za vsako enovrstno grožnjo, in sicer na ravni hrvaških županij oz. samoupravne skupnosti).

Za vsako grožnjo je izdelana tudi ocena (ne)zanesljivosti – to predstavlja štiristopenjsko oceno virov, vključenih strokovnjakov in metodologije, ki se je uporabila za izdelavo ocene tveganja. Prav tako se naredi ocena vplivov podnebnih sprememb ter čezmejnega vpliva tveganja. Obe oceni sta precej opisni, saj uporabljata zgolj pritrdilno/nikalni pristop in kvalitativni opis verjetnosti teh vplivov. Poleg ocen tveganj NPRK vsebuje tudi oceno zmogljivosti za odzivanje na nesreče ter strategijo zmanjševanja tveganja nesreč.

Univerzitetna založba
Univerze v Mariboru

6 Pregled ugotovitev

6.1 Predlogi za sistematično upravljanje in ocenjevanje varnostnih razmer

Z namenom predstavitve dobrih praks in pomanjkljivosti v trenutnih pristopih k ocenjevanju varnostnih tveganj ter ogroženosti sledi pregled podobnosti in razlik v pristopih, ki jih priporočajo mednarodni standardi in uporabljajo različne države, vključno s Slovenijo.

Med standardi družine ISO in IEC (ISO 31000, ISO/IEC 27005), smernicami NIST SP 800-30, COSO in metodo MOSAR, ki so zajete v pregled strokovnih usmeritev, ni opaziti bistvenih razlik v splošnih usmeritvah glede postopka ocene in obvladovanja tveganj, odstopanja pa so razvidna pri opredeljevanju posamičnih korakov. Pri tem velja omeniti, da je Evropska komisija standarda ISO 31000 in IEC 31010 določila kot osnovo za terminologijo in priporočila, podana v smernicah za ocenjevanje in prikaz tveganj na področju obvladovanja nesreč (European Commission, 2010), kar pomeni, da je takšen pristop uveljavljen v državah članicah EU pri ocenjevanju tveganj, povezanih z naravnimi in drugimi nesrečami.

Priprava na izvedbo ocene tveganj. Kot prvi korak v procesu ocene tveganj vsi omenjeni standardizirani pristopi predvidevajo določitev ciljev, obsega ocene tveganja, konteksta in meril, medtem ko metoda MOSAR, ki sodi med starejše v tej skupini, predpriprave na identifikacijo virov tveganj neposredno ne predvideva. V

tem koraku, kot predfazi dejanskega procesa ocenjevanja tveganj, se tako postavijo temelji, na katerih bo ocena grajena in merila, po katerih bo podana končna sodba. Gre za ključni korak, brez katerega ocene tveganja ne bi bilo mogoče izvesti objektivno in učinkovito.

Ocena tveganja. V fazi dejanske ocene določenega tveganja se posamezni pristopi nekoliko razlikujejo, pri čemer so razlike relativno majhne – predvsem v različnih ravneh abstrakcije. Standarda ISO 31000 in ISO/IEC 27005 v tej fazi predvidevata tri glavne procese: (1) identifikacijo tveganja, (2) analizo tveganja, in (3) evalvacijo tveganja. Gre za nekoliko višjo raven abstrakcije, kot jo predvidevajo metoda MOSAR, smernice NIST in COSO. Smernice COSO to fazo imenujejo »Izvedba«, znotraj nje pa predvidevajo tri glavne procese: (1) opredelitev tveganja, (2) ocena resnosti tveganja, (3) prioritizacija tveganja. Smernice NIST procese opredeljuje na še nižji ravni abstrakcije, in sicer: (1) identifikacija tveganj in dogodkov, (2), prepoznava ranljivosti in predisponirajočih stanj, (3) določitev verjetnosti pojava, (4) določitev magnitude dogodka in (5) določitev tveganja. Metoda MOSAR na drugi strani deli proces ocene tveganja na dva dela (A in B), pri čemer prvi omogoča izvedbo analize večjih tveganj (torej širše), drugi pa omogoča podrobno analizo glede na funkcije, ki jih omogoča sistem, za katerega se ocena tveganja opravlja. Ne glede na višjo raven abstrakcije v modelu, ki ga predvidevata standarda družine ISO/IEC, so koraki in procesi, ki jih predvideva povsem skladni s koraki in procesi, ki jih predvidevajo ostali standardi in smernice.

Obravnava tveganja. Obravnavo tveganja kot korak v procesu ocene tveganja predvidevajo smernice COSO, metoda MOSAR in standarda družine ISO/IEC. Smernice COSO obravnavo tveganja postavljajo v fazo dejanske izvedbe ocene tveganja: četrtki korak ocene tako predstavlja »Implementacija odzivov na tveganja«, peti pa »razvoj portfelja«. Standarda družine ISO/IEC predvidevata obravnavo tveganja, pri čemer standard ISO 31000 v tem koraku predvideva tudi odločanje o učinkovitosti obravnave, sprejemljivosti tveganja in zanko nazaj na obravnavo, če tveganje ni sprejemljivo. Na drugi strani standard ISO/IEC 27005 to razdeljuje v dva ločena koraka. Metoda MOSAR preprosto predvideva obravnavo tveganja kot zadnjo izmed faz drugega koraka izvedbe ocene tveganja (Korak B).

Sprejetje tveganja. Odločitev o tem, ali je tveganje, ki ostaja po izvedeni obravnavi tveganja sprejemljivo ali ne, posebej predvideva le standard ISO/IEC 27005. Kot omenjeno, ga ISO 31000 vključuje v fazo obravnave tveganja (in s tem še vedno vključuje v proces ocenjevanja in obravnave tveganja), medtem ko tega koraka ne predvidevajo smernice NIST, COSO in metoda MOSAR.

Poročanje rezultatov in vzdrževanje. Poročanje rezultatov predvidevajo vsi standardi in smernice, razen metode MOSAR. Prav tako vsi standardi in smernice predvidevajo vzdrževanje stanja skozi spremljanje in pregledovanje. Tako so s trenutnim stanjem seznanjeni vsi deležniki, vključno z odgovornimi za dejavnosti obvladovanje tveganj.

Tudi pregled pristopov, ki se uporabljajo za ocenjevanje varnostnih razmer oz. nacionalnovarnostne ogroženosti v različnih državah, nakazuje na nekatere podobnosti in hkrati razlike v sistemski ureditvi in metodologijah, ki se uporabljajo v praksi.

Upravljanje in ocenjevanje nacionalnovarnostne ogroženosti je v vseh analiziranih državah urejeno v področni zakonodaji, navadno takšni, ki ureja področje civilne zaščite. Poleg zakonodajnih aktov so navadno v državah sprejete tudi nacionalne smernice ali pravilniki za ocenjevanje tveganj, ki podrobneje opisujejo metodologije. Zaznati je tudi, da se ponekod identificirana tveganja vključujejo v nacionalni register tveganj, rezultati ocene pa so navadno objavljeni v uradnih poročilih, ki so lahko javne ali zaupne narave. Izsledki ocenjevanja so nato vključeni v nacionalne (akcijske) načrte kriznega odzivanja oz. kriznega upravljanja in strategije zagotavljanja nacionalne varnosti.

Ocenjevanje nacionalnovarnostne ogroženosti večinoma poteka po večstranskem oz. vse vključujočem (tudi vse družbenem) pristopu, kar pomeni, da so vloge in odgovornosti oz. pristojnosti razporejene med različne organe oz. subjekte. Za izvajanje ocenjevanja so navadno pristojni raznovrstni subjekti, ki so povezani v različne skupine, kot so denimo platforme, usmerjevalni odbori oz. skupine (predstavniki ministrstev), delovni odbori oz. delovne skupine (predstavniki različnih agencij), pa tudi strokovne podskupine (ki poleg predstavnikov državnih organov vključujejo tudi predstavnike lokalnih oblasti, prvih posredovalcev, gospodarstva, kritične infrastrukture in akademske skupnosti). V tovrstnih

skupinskih postopkih pogosto osrednjo koordinacijsko vlogo prevzemajo uradi s področja civilne zaščite, organizirani v okviru obrambnih ali notranjih ministrstev ali pa vladne agencije, lahko pa tudi nacionalni inštituti.

Iz opisov posameznih pristopov je mogoče razbrati tudi, da je večinoma uveljavljen t. i. *top-down* pristop, kar pomeni, da se ocenjevanje in obravnavanje tveganj usmerja od zgoraj navzdol, na ravni celotne družbe/države, ter nato skozi načrte usmerja regionalne in lokalne subjekte pri njihovi obravnavi in identifikaciji tveganj. Neredko pa države pri izvajanju ocene nacionalnovarnostne ogroženosti uporabljajo tudi kombinacijo pristopov *bottom-up* in *top-down*, kar vključuje izmenjavo pristojnosti za posamezna področja tveganj med regionalnimi in zveznimi/nacionalnimi oblastmi. V takem primeru denimo posamezni subjekti (npr. posamezna ministrstva ali skupine) pripravijo delna poročila o tveganjih s svojega področja.

V nekaterih državah je zaradi možnosti nezanesljivih ocen tveganj vzpostavljen tudi dodaten mehanizem za neodvisno presojo zanesljivosti in kakovosti končne ocene nacionalnovarnostne ogroženosti, najpogosteje pa se odgovorno ravnanje in transparentnost v tovrstnih postopkih spodbujata skozi javne razprave ocen in javne recenzije kakovosti (npr. v parlamentih, v javnosti), zaznati pa je tudi prakse anketiranja vključenih strokovnjakov za pridobitev vpogleda v kakovost izvedbe skupinskih delavnic, skozi katere je potekal proces usklajevanja in analiziranja tveganj.

Izvajanje ocene nacionalnovarnostne ogroženosti, skladno s priporočili EU v vseh analiziranih državah poteka periodično, pri čemer se v nekaterih državah proces izvaja na letni ravni bienalno ali pa vsaj na vsake tri leta. V nacionalno oceno ogroženosti analizirane države zajemajo tveganja, ki so ali naravnega ali zlonamernega človeškega izvora, ne glede na to, ali gre za nacionalno ali mednarodno naravo. Pri tem je glavni poudarek na tistih grožnjah in tveganjih, ki presegajo zmožnosti lokalnih oblasti oz. vsakodnevne možne varnostne dogodke, katerih vpliv je manjšega pomena in je lokalno omejen. Fokus je torej na situacijah, ki izpolnjujejo merila, da se lahko dogodek označi kot kriza na družbeni ali državni ravni. V presoji, katere grožnje bodo vključene, pa ima pomembno vlogo tudi upoštevanje potencialnega vpliva groženj – v analizo so denimo vključene tiste grožnje, ki bi lahko imele bistven vpliv na ključne in temeljne družbene vrednote ter dobrine (npr. na življenje, zdravje in varnost ljudi, okolje, gospodarstvo, demokracijo, človekove

pravice, vladavino prava, državno suverenost). Za vsako grožnjo, vključeno v oceno, se navadno izdelajo tudi različni možni scenariji (od najlažjega do najhujšega), ki vključujejo tudi opis vzrokov, vplivov in družbene kapacitete. Pri vsaki izmed identificiranih groženj je poleg ocene tveganja, opisa scenarija, določen tudi glavni koordinator kot ključni akter odzivanja in upravljanja v primeru realizacije grožnje.

Število groženj, vključenih v postopek ocenjevanja, se med državami močno razlikuje, kar je logična posledica raznolikosti in specifik držav. Ne glede na to, se v večini analiziranih državah grožnje kategorizirajo v skupine, npr. grožnje, ki izhajajo iz narave, tehnologije in družbe, ali zlonamerni napadi, organizirana in resna kriminaliteta, okoljske nevarnosti, tveganja za zdravje ljudi in živali, večje nesreče, socialna tveganja ali civilne, naravne, transportne, tehnološke grožnje. Pri tem nekatere države vojaških ogrožanj ali kriminalitete ne zajemajo v tovrstne ocene, druge pa, pri čemer so najpogosteje v to oceno zajeti teroristični napadi, izbruhi nasilja, množično streljanje, organizirana kriminaliteta in korupcija. Pri tem lahko kot zanimivost izpostavimo prakso, ki tveganja oz. grožnje deli na enovrstne (samostojne) in kompleksne (kombinacija več tveganj). V večini primerov se za vsako tveganje analizirajo tudi potencialni scenariji (od najlažjega do najslabšega), vzroki za nastanek, ponekod pa je zaslediti tudi ocene zahtevnosti odzivanja, odpornosti, analiziranje trendov, ki bi lahko vplivali na analizirane scenarije ali pojav novih tveganj, pa tudi možnosti čezmejnega vpliva tveganj.

Postopki ocenjevanja tveganj so v vseh primerih sestavljeni iz več zaporednih korakov (od štiri do šest). Če korake, kot so ugotovljeni v analizi posameznih držav, združimo in povzamemo postopek poteka po naslednjem protokolu:

1. Določitev pristojnosti institucij, subjektov, skupin;
2. Določitev referenčnega in geografskega območja analize;
3. Identifikacija in izbor nevarnosti/groženj;
4. Konsolidacija izbora groženj;
5. Konsolidacija metodologije;
6. Opis oz. razvoj različnih scenarijev za posamezne grožnje (tudi vzrokov);
7. Ocena vpliva in posledic uresničene grožnje;
8. Ocena verjetnosti uresničitve grožnje;
9. Ocena verodostojnosti/zanesljivosti;

10. Ocena zahtevnosti odziva;
11. Ocena vplivnih trendov;
12. Izračun tveganja;
13. Vizualizacija in umestitev v matriko;
14. Priprava poročila in posvetovanje z interesnimi skupinami (lahko tudi javna razprava);
15. Odobritev in objava.

V nekaterih državah se poleg ključnih dimenzij tveganj (vzroki, vplivi, posledice, verjetnost) ocenjuje tudi stopnja samozavesti oz. verodostojnosti, zanesljivosti ali gotovosti.

Pri ocenjevanju posameznih dimenzij tveganj so države pretežno poenotene. Ocenjevanje posledic (nevarnosti oz. resnosti groženj/scenarijev) navadno poteka skozi oceno dveh vidikov: vpliv na ključne vrednote in ocena škode v materialnem oz. finančnem obsegu. Tovrstne ocene so v večini primerov tako kvalitativne (opisne), kot kvantitativne narave. Pri ocenjevanju vpliva na družbene vrednote gre za analiziranje vpliva, ki bi ga lahko imeli scenariji na: (dobrobit, zdravje, vedenje, varnost) ljudi/prebivalce, okolje, družbo/družbeno in politično stabilnost, gospodarstvo, fizično (zasebno in javno) lastnino, nematerialne dobrine, infrastrukturo, osnovne storitve/vitalne družbene funkcije, mednarodne posledice. Kategorije teh vrednot so številčno različne, navadno pa gre za ocenjevanje vpliva na tri ali štiri skupine vrednot, je pa zaslediti tudi več skupin (pet do sedem). V ocenjevanju teh vplivov in škode se navadno uporabljajo pet stopenjske lestvice (ki vplive razdelijo od nepomembnih/minimalnih/neznatnih vse do katastrofalnih/zelo pomembnih posledic oz. zelo nizkega do zelo visokega vpliva). Pri presoji škode pa se lestvice navadno stopnjujejo glede na višino finančne škode, izražene v denarju in obsegu/številčnosti smrtnih žrtev ter poškodovanih oseb.

Ocenjevanje verjetnosti uresničitve oz. pojavnosti neke grožnje/scenarija, tako kot ocenjevanje posledic, poteka kvalitativno in kvantitativno. Navadno so za končne ocene verjetnosti uporabljene petstopenjske lestvice, ki verjetnost opisujejo od zelo neverjetno/zelo redko/ekstremno neverjetno/zelo nizka do zelo verjetno/ zelo visoka. Za končen izračun oz. oceno tveganj se navadno uporabljajo logaritmične lestvice, ki opisujejo štiri ali pet stopenj tveganj (od zelo nizko do zelo visoko oz. ekstremno), vizualizacija pomembnosti tveganj pa je dosežena z umestitvijo grožnje

v dvodimenzionalno matriko tveganj (osi predstavljajo stopnje posledic in verjetnosti). Sicer ocenjevanje tveganj v obliki končnega sklepa ni praksa, značilna za vse države; nekatere države denimo ne izvajajo rangiranja groženj glede na končno oceno tveganja.

Tako kot v ostalih državah med najbolj transparentne in celovito urejene ocene na področju varnostne ogroženosti na nacionalni ravni v Sloveniji sodi ocena tveganj za nesreče, kar je gotovo posledica enotnih usmeritev in ureditve na ravni EU. V Sloveniji je sistem zelo natančno zakonsko urejen in opredeljen, tako z uredbo, ki v slovenski nacionalni pravni red prenaša evropsko zakonodajo, kot tudi v področni zakonodaji s področja varstva pred naravnimi in drugimi nesrečami.

Upravljanje in ocenjevanje tveganj za nesreče poteka v sodelovanju različnih deležnikov (kar je značilno tudi za vse ostale analizirane države), saj so v ocene posameznih tveganj zajeta različna ministrstva. Za koordinacijo delovanja, kot Državni koordinacijski organ skrbi Uprava RS za zaščito in reševanje v okviru Ministrstva za obrambo. Glede na teritorialno ureditev je za Slovenijo značilen t. i. pristop *top-down*, kjer se ocenjevanje in obravnavanje tveganj usmerja od zgoraj navzdol. Takšen pristop je značilen predvsem za države s pretežno centraliziranim sistemom upravljanja.

Ocene tveganj za posamezna področja nesreč so javno objavljena (z izjemo ocene tveganj za področje terorizma), skupna ocena, kot sinteza posameznih ocen, pa je javno objavljena v dokumentu Državna ocena tveganj. Izsledki ocen predstavljajo podlago za pripravo različnih nacionalnih strategij, ugotavljanju vrzeli v zmogljivostih in načrtovanje preventivnih ter drugih upravljavskih ukrepov. Skupno se ocenjevanje ogroženosti izvaja za 15 različnih nesreč in drugih tveganj. Pri tem se uporablja enotna metodologija, ki omogoča primerljivost ocen in rezultatov. Iz dosedanjih ugotovitev izhaja, da največje tveganje v RS pomenijo poplave, sledijo pa potres, epidemija ali pandemija nalezljive bolezni pri ljudeh, letalska nesreča, terorizem, žled in jedrska nesreča.

Metodologija ocenjevanja tveganj za nesreče vključuje izdelavo različnih scenarijev za posamezna tveganja, večravninsko oceno vplivov, oceno verjetnosti, oceno tveganja in oceno zanesljivosti rezultatov. Za vplive in verjetnost se uporabljajo petstopenjske ordinalne lestvice (kombinacija kvalitativnih in kvantitativnih meril),

ocena tveganja se poda na štiristopenjski ordinalni lestvici, ocena zanesljivosti pa na tristopenjski ordinalni lestvici.

Med prednosti nacionalnega sistema ocenjevanja tveganj za nesreče v Sloveniji sodijo:

- natančna zakonska in podzakonska ureditev;
- poenotenost metodologije za ocenjevanje različnih tveganj;
- širok nabor tveganj, vključenih v državno oceno;
- visoka osredotočenost na tveganja, na katera lahko močno vplivajo tudi podnebne spremembe (suša; poplava; požar; nevarne bolezni živali; nevarnosti, povezane z zdravjem ljudi; žled);
- vse vključujoč pristop k oceni tveganj in natančno določene oz. razmejene odgovornosti različnih deležnikov;
- transparentnost rezultatov, ki omogoča informiranost vseh interesnih subjektov.

Poleg državne ocene tveganj nesreč so z analiziranjem nekaterih vidikov varnostne ogroženosti v Sloveniji povezane še določene druge ocene tveganj. Med tovrstne lahko umestimo denimo nacionalno oceno teroristične ogroženosti in nacionalno oceno tveganj za PD/FT. Med pomembne sodijo ocene ogroženosti na področju organizirane kriminalitete in migracij ter ocene tveganj za kritično infrastrukturo.

Na podlagi pregleda lahko strnemo, da se analize in ocene varnostne ogroženosti ter tveganj v Sloveniji delijo glede na raven in področje izvajanja. Posplošeno, jih lahko skupinimo na naslednje ravni:

- Evropska raven: analize in ocene, ki jih izvajajo organi in organizacije EU, države članice in njihovi organi pa v teh analizah sodelujejo s prispevanjem podatkov in mnenj ali pa lastnimi ocenami stanja v državi (npr. na področju organizirane kriminalitete, internetne kriminalitete, terorizma, migracij).
- Državna raven: nacionalne ocene, ki se izvajajo za območje celotne države in vključujejo medsektorsko sodelovanje in ocenjevanje (npr. nacionalna ocena tveganj za nesreče; nacionalna ocena za preprečevanje pranja denarja in financiranja terorizma; nacionalna ocena teroristične

ogroženosti). Nacionalne ocene so lahko vključene tudi v ocene na ravni EU.

- Področna raven: ocene, ki se izvajajo v določenem sektorju in jih tako izvajajo specifični zavezanci. Njihove ocene so lahko nato vključene v nacionalne ocene (npr. na področju kritične infrastrukture, bančnega in finančnega sektorja).
- Lokalna raven: ocene, ki jih izvajajo občine za pripravo občinskih programov varnosti.

Primerjava tovrstnih metodologij, ki se uporabljajo v ocenah, neposredno povezanih z ocenjevanjem varnostnih razmer oz. varnostnih tveganj (tabela 36), pokaže, da med najbolj transparentne in natančno določene sodijo evropske in nacionalne ocene. Sektorske oz. področne in občinske pa so prepuščene izvajalcem, ki morajo upoštevati splošne zakonske usmeritve in priporočila posamičnih pristojnih organov. Posledično metodologije niso poenotene, preglednosti in primerljivosti rezultatov pa ni mogoče zagotoviti. S časovnega vidika so posodobitve zelo različne. Letno se denimo posodabljajo ocene na področju migracij, teroristične ogroženosti, kritične infrastrukture in na lokalni ravni, kjer se predvideva večja spremenljivost in dinamika groženj. Daljša, štiriletna obdobja pa so predvidena za grožnje, povezane s PD/FT, organizirano kriminaliteto in naravnimi nesrečami, čeprav je na teh področjih tvegano predpostavljati večjo stabilnost oz. nespremenljivost tveganj. Metodologije so med področji izjemno nepoenotene. Čeprav je treba upoštevati raznolikost indikatorjev, ki so vezani in vplivajo na različna tveganja, bi se lahko procesno in terminološko zagotovila večja primerljivost. Že osnovni pregled pokaže, da se končni rezultati nanašajo na oceno stopnje tveganja, oceno ogroženosti ali oceno verjetnosti. Najpogosteje analize vključujejo ocene verjetnosti, ranljivosti (zmogljivosti) in vplivov (posledic) oz. nevarnost in pri tem ranljivosti ter vplive podrobneje razčlenjujejo, druge pa upoštevajo tudi geografske in okoljske dejavnike. Kot posebnost je smiselno omeniti izdelavo scenarijev (npr. realističnih ali najnevarnejših), določanje časovne in odločevalske ravni, ocenjevanje kakovosti informacij in dopolnjevanje končnih rezultatov s presojanjem njihove zanesljivosti, popolnosti, doslednosti. Glede na podrobno analizo metodologij, bi lahko kot najbolj dovršeno ocenili metodologijo za ocenjevanje tveganj na področju naravnih nesreč in PD/FT, najmanj transparentne pa so metodologije na lokalni ravni in na področju kritične infrastrukture (če zaradi zaupne narave področja izvzamemo oceno teroristične ogroženosti).

Tabela 36: Primerjava metodologij, ki se uporabljajo v ocenah varnostnih razmer

PODROČJE	RAVEN	METODOLOGIJA	ZAVEZANCI IN PRISTOJNE ORG.	ČASOVNICA	PROCES ANALIZE	IZRAČUN TVEGANJA	DODATNE INFORMACIJE
Ocena tveganj za nesreče	Nacionalna Sektorska (15 skupin groženj, osem ministrstev)	Metodologija EU Metodologija področij poenotena	Medresorsko sodelovanje – ministrstva; delo usklajuje Državni koordinacijski organ (URSZR)	Na štiri leta	– Identifikacija tveganj in scenarijev – Ocena vplivov: 15 različnih vplivov v treh skupinah (petstopenjska kombinirana lestvica) – Ocena verjetnosti (petstopenjska kombinirana lestvica)	– Ocena stopnje tveganja – Kombinacija ocene vpliva in verjetnosti – Petstopenjska ordinalna lestvica – Opisna ocena: majhno do zelo visoko tveganje – Prikaz v matriki	Ocena zanesljivosti rezultatov (tristopenjska ordinalna lestvica). Metodologija je javna.
Ocena tveganj za PD/FT	Nacionalna Sektorska (pet sektorjev)	Metodologija Svetovne banke Metodologije sektorjev (niso poenotene)	Medresorska delovna skupina, ki jo vodi UPPD Sektorske smernice za zavezance pripravijo pristojni organi	Nacionalna ocena – na štiri leta Ocena zavezancev – na dve leti	Nacionalna ocena: – Ocena ogroženosti – Ocena ranljivosti (na osnovi ocene ranljivosti sektorjev) Sektorska ocena: – Ocena zavezanca: ocena inherentnega tveganja (šest skupin na štiristopenjski ordinalni lestvici nizko–visoko), kontrolnega okolja (ocena izvedenih ukrepov na skupno 11 področjih z uporabo štiristopenjske ordinalne lestvice; dobro–slabo) – Ocena stranke: pet skupin meril tveganj	Nacionalna ocena – Ocena stopnje tveganja – Razpon ocene od 0 do 1 – Opisna ocena na petstopenjski ordinalni lestvici (nizko–visoko) Sektorska ocena: – Ocena stopnje tveganja zavezanca predstavlja kombinacijo ocene inherentnega tveganja in ocene kontrolnega okolja. Ocena se poda na štiristopenjski ordinalni lestvici (nizko–visoko) s prikazom v matriki – Ocena stranke: tri- ali štiristopenjska ordinalna lestvica (nizko–visoko)	Metodologije so javne.

PODROČJE	RAVEN	METODOLOGIJA	ZAVEZANCI IN PRISTOJNE ORG.	ČASOVNICA	PROCES ANALIZE	IZRAČUN TVEGANJA	DODATNE INFORMACIJE
Ocena za teroristično ogroženost	Nacionalna	Lastna metodologija	V pristojnosti Medresorske delovne skupine za protiterorizem na ravni Vlade RS	Večkrat-letno dopolnjevanje	Merila ocene: – Območje pojava/lokacija – Nevarnost pojava – Vpliv	– Ocena ogroženosti – Petstopenjska ordinalna lestvica (zelo nizka–zelo visoka)	Metodologija ni javna
Ocena tveganj na področju kritične infrastrukture	Sektorska	Lastna metodologija glede na zakonske usmeritve	V pristojnosti zavezancev (upravljavci kritične infrastrukture; skupaj osem sektorjev)	Letno	– Seznam virov ogrožanja – Ocena verjetnosti – Ocena resnosti posledic – Ocena vplivov na poslovne procese – Identifikacija virov ogrožanj, ki lahko vodijo v krizne ali izredne situacije	Podrobna metodologija ni znana.	Metodologija ni natančno predpisana – prepuščena v izdelavo upravljavcem. Priporoča se sledenje veljavnim standardom in metodam.
Ocena tveganj na področju organizirane kriminalitete	Evropska	Metodologija Europol (SOCTA)	Europol; k pridobivanju podatkov prispevajo države članice in zunanji partnerji	Na štiri leta	Ocena 59 indikatorjev (po potrebi se dopolnijo), ki se delijo v pet skupin in na opisne ter ocenjevalne: – Kriminalitetne skupine – Kriminalitetna okolja – Vpliv – Kriminalitetna infrastruktura – Okoljski faktorji Ocenjevalni indikatorji imajo dodeljene relativne uteži (tristopenjska lestvica) in se ocenjujejo glede na obseg (petstopenjska lestvica), vpliv pa se ocenjuje na štiristopenjski lestvici.	Ocena verjetnosti pojava organizirane kriminalitete, ki vključuje prepoznavo rizičnih okolij in faktorjev, ki spodbujajo organizirano kriminaliteto. Podrobna metodologija ni znana.	Metodologija je delno javna. Po pripravi ocen sledi še presoja kakovosti produkta SOCTA po merilih: doslednost, popolnost, jasnost, skladnost

PODROČJE	RAVEN	METODOLOGIJA	ZAVEZANCI IN PRISTOJNE ORG.	ČASOVNICA	PROCES ANALIZE	IZRAČUN TVEGANJA	DODATNE INFORMACIJE
Ocena tveganj na področju migracij	Evropska Nacionalna	Metodologija Frontex	Države članice oz. njihove policije, carinske uprave in uradi za priseljevanje	Letne analize, polletne dopolnitve in četrtletna poročila	– Izdelava seznama groženj – Ocena verjetnosti (sedemstopenjska kombinirana lestvica) – Ocena ranljivosti (štiristopenjska ordinalna lestvica), ki vključuje presojo zmogljivosti na treh ravneh – Ocena vpliva (petstopenjska kombinirana lestvica), ki vključuje oceno učinkov na štirih ravneh	Stopnja tveganja se oceni na tristopenjski ordinalni lestvici (majhna, srednja velika)	Metodologija je delno javna. Pri oceni stopnje tveganja se določi še referenčno obdobje in odločevalska raven. Ocena vključuje tudi ocena zanesljivosti in veljavnosti informacij
Ocena ogroženosti in varnostnih tveganj na občinski ravni	Lokalna: občinska, medobčinska	Lastna glede na zakonske usmeritve in priporočila MNZ	Občine oz. občinski svet na predlog župana, ocena se izdela v sodelovanju z območno policijsko postajo	Pri sprejemu OPV, letno pregledovanje in dopolnjevanje	– Posnetek stanja – Analiza in ocena varnostnih razmer – ugotovitev stopenj ogroženosti na devetih področjih – Identificiranje in obvladovanje varnostnih tveganj – Opredelitev varnostnih potreb občine	Ocena je deskriptivna, opisna.	Opredelitev strateških, operativnih ciljev in nosilcev. Upoštevanje varnostnih razmer iz sosednjih občin.

Predstavljene ugotovitve je možno strniti v nabor predlogov za izboljšave oz. nadgradnjo aktualnih pristopov k ocenjevanju varnostnih razmer in strateških usmeritev v Sloveniji. Poleg prednosti in dobrih praks, ki so se izkazale v obstoječih pristopih k ocenjevanju varnostnih razmer v tujini in Sloveniji, je na podlagi primerjalne analize mogoče identificirati tudi nekatere pomanjkljivosti. Ob medsebojni primerjavi pristopov k ocenjevanju varnostne ogroženosti/tveganj v Sloveniji in z izbranimi drugimi državami lahko izpostavimo naslednje priložnosti za izboljšave.

Krepitev prizadevanj v smeri večje poenotenosti metodologij na področju ocenjevanja varnostnih razmer in terminologije. Metodologije so med različnimi področji ocenjevanja varnostnih razmer, ki smo jih vključili v pregled in analizo, izjemno nepoenotene. Čeprav je treba upoštevati raznolikost indikatorjev, ki so vezani in vplivajo na različne grožnje/tveganja, bi se lahko procesno in terminološko zagotovila večja primerljivost med pristopi.

Nadgradnja metodologij z vključevanjem dodatnih elementov/vidikov. Na podlagi pregleda tujih praks in pristopov je opaziti, da bi trenutno metodologijo na področju ocenjevanja tveganj za nesreče lahko nadgradili in v ocenah upoštevali tudi zahtevnost kriznega upravljanja oz. kapacitete odzivanja ter možnost čezmejnega delovanja grožnje.

Preglednost groženj skozi mapiranje oz. gručenje. Po vzoru drugih držav bi bilo smiselno zagotoviti večjo preglednost groženj, vključenih v ocenjevanje tveganj. Z razčlenitvijo groženj oz. mapiranjem groženj po kategorijah (glede na področje, izvor in dobrino ogrožanja) bi se zagotovil bolj sistematičen pristop k identifikaciji groženj kot tudi primerjavi podobnih tveganj.

Vključevanje kompleksnih groženj. Pristop, ki upošteva več groženj/tveganj, se večinoma v praksi ne izvaja. Kombiniranje različnih groženj/tveganj namreč omogoča identifikacijo realnih scenarijev v sodobnem času kompleksnih varnostnih razmer. V opisih nekaterih tveganj na področju nesreč je to sicer prisotno, vendar se večinoma takšna kombinacija zgolj omenja kot možnost, upošteva pa se v zgolj v redkih scenarijih, najpogosteje v povezavi s tveganji, vezanimi na podnebne spremembe (primer žleda).

Aktivnejše posodabljanje ocen. Čeprav je bila v preteklosti državna ocena tveganj za nesreče večkrat posodobljena, je v zadnjih letih to zamrlo. Državna ocena tveganj je bila sprejeta leta 2015 in posodobljena leta 2018, kasneje do leta 2022 pa ne, kar kaže na nižjo ažurnost in aktualnost ocen kot v nekaterih drugih državah. Pri tem velja omeniti še, da »Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite« (2014) določa, da je posodabljanje treba zagotoviti najmanj vsake tri leta. Tudi na splošno se ocene ogroženosti/tveganj na različnih področjih javne varnosti posodabljajo različno intenzivno. Določene ocene se posodabljajo letno ali še pogosteje, nekatere pa zgolj na štiri leta.

Razvoj natančnih smernic, k ocenjevanju in upoštevanju kakovosti ocen. Čeprav je v nekaterih pristopih značilno presojanje zanesljivosti ocen (denimo pri nacionalni oceni tveganj za nesreče ali na področju migracij) prisotno, konkretnejša metoda ocenjevanja zanesljivosti in kakovosti ocen ni določena. Prav tako ni opredeljeno, kako ravnati ob različnih ocenah kakovosti/zanesljivosti oz. kako te ocene upoštevati v odločitvenih procesih.

Upoštevanje groženj, povezanih s kriminaliteto v državni oceni tveganj. Slovenija v državno oceno tveganj ne vključuje vojaških ogrožanj ali kriminalitete (izjema sta terorizem in kibernetska kriminaliteta), kar je značilno za nekatere druge države. Ker so zlonamerne oz. namerno povzročene človeške grožnje in zunanji/čezmejni viri ogrožanj, poleg nesreč, prav tako izjemnega pomena za notranjo varnost bi bilo smiselno nacionalne ocene tveganj dopolniti ali smiselno navezati z ocenami tveganj, povezanimi s kriminaliteto in varnostnim dogajanjem v zunanjem okolju.

Upoštevanje aktualnih razmer v državni oceni tveganj. Pri izdelavi scenarijev na področju tveganj za nesreče bi bilo smiselno poleg podnebnih sprememb upoštevati še druge aktualne razmere in trende, ki bi lahko imele implikacije za varnostno situacijo (npr. širjenje nevarnih ali visoko nalezljivih bolezni; množični dogodki; pomanjkanje surovin; namerno ogrožanje okolja, hibridne grožnje ipd.).

Natančnejša opredelitev pristopov in metodologij ocenjevanja varnostnih razmer na lokalni ravni. Podrobnejši pregled OPV po posameznih občinah kaže, da so OPV vsebinsko in strukturno med občinami zelo podobni. Občine se pri oceni varnostnih razmer zanašajo predvsem na statistične podatke policije in občinskih organov ter operativne preglede in informativne razgovore. Stopnje varnostne ogroženosti niso

jasno definirane, temveč so zgolj opisne narave. Metodologije, ki bi pripomogle k izboru, analizi ali oceni, iz programov niso razvidne. Posodabljanje OPV je med občinami sicer izjemno različno, pregled pa kaže, da veliko programov v zadnjem desetletju ni bilo nadgrajenih.

Pregled strateških usmeritev kaže, da ima Slovenija zelo sistematično urejeno strateško podlago za naslavljanje področij, pomembnih za nacionalno varnost. Opaziti je, da je večina strategij aktualnih in so bile posodobljene v zadnjih štirih letih. Med manj ažurne sodijo strategije ali strateške usmeritve na področju kibernetske varnosti in prometa, predvsem pa na področjih preprečevanja nasilja v družini, korupcije in obrambe. Prav tako je ob pregledu slovenskih strategij opaziti nekatere izzive, povezane s transparentnostjo. Procesi in metodologije določanja ciljev, ukrepov in prioritetnih področij v strateških ali spremljajočih dokumentih niso podrobno predstavljeni, kar onemogoča razumevanje argumentov izbranih vsebin. Na podlagi tovrstnih izsledkov lahko sklepamo, da bi bilo treba zagotoviti tudi aktualnejše posodabljanje strategij in okrepiti transparentnost metodologij oblikovanja strateških usmeritev.

Univerzitetna založba
Univerze v Mariboru

7 Teoretični model za ocenjevanje varnostnih razmer

7.1 Predlog modela za ocenjevanje varnostnih razmer v Sloveniji

Na podlagi strukturiranega pregleda mednarodnih standardov, evropskih usmeritev in nacionalnih pristopov ter izvedbenih zahtev ob sočasnem upoštevanju izsledkov primerjalne analize ter izoblikovanih predlogov za izboljšave v nadaljevanju predstavljamo celovit, enovit in praktično uporaben »*Model za ocenjevanje ogroženosti/tveganja na področju javne varnosti*«. Model je primarno namenjen organizacijam, ki delujejo na področju javne varnosti, in sicer njihovim izvajalcem (analitikom) ter odločevalcem v podporo pri izvajanju postopka analize in ocene varnostne ogroženosti oz. varnostnih tveganj. Model predstavlja vodilo in orodje za izvajalce (analitike) ter je zasnovan v obliki navodila, ki omogoča izvedbo ocene skozi analitično in sistematično zasnovan proces, skozi katerega se odločevalcem zagotovi ustrezna informacijska podpora za odločanje. Model je splošno in enotno uporaben za vse oblike varnostnih groženj (namerne ali nenamerne, predvidljive ali nepredvidljive). Prav tako je uporaben v zasledovanju organizacijskih ali širših družbenih ciljev.

Model v svoji zasnovi predstavlja nadgradnjo obstoječih pristopov in standardov oz. smernic na področju ocenjevanja ogroženosti/tveganj, saj:

- je oblikovan za potrebe izdelave ocen na področju javne varnosti oz. organizacije, ki delujejo na tem področju;
- vključuje podroben opis korakov posameznih faz z jasnimi izvedbenimi navodili;
- faze procesa povezuje s konkretnimi tehnikami zbiranja, analiziranja in predstavljanje podatkov;
- prikazuje rezultate in odgovorne subjekte po posameznih fazah;
- razlikuje med oceno ogroženosti in oceno tveganja ter na tej osnovi predstavlja izvedbo obeh procesov;
- predstavlja možnosti prilagoditve procesa in postopkov glede na potrebe izvajalcev ocen;
- omogoča uporabo poenostavljenega postopka v primeru izvedbenih ovir na strani izvajalca.

Tovrstne karakteristike modela naslavljajo pomanjkljivosti obstoječih rešitev, pristopov in smernic na področju ocenjevanja varnostnih razmer in ocen ogroženosti/tveganj. Model smo za potrebe evalvacije posredovali tudi v pregled in evalvacijo organizacijam, ki so vpete v procese analiziranja varnostnih tveganj na področju javne varnosti. Skupaj smo pridobili devet povratnih komentarjev iz petih organizacij. V povratnih informacijah so ocenjevalci izpostavili, da:

- model proces in postopek izdelave ocene ogroženosti/tveganj predstavlja celostno, sistematično, analitično in matematično;
- model vključuje oz. pokriva vse ključne in standardne faze izdelave ocene ogroženosti/tveganj;
- model vključuje pomembne pripomočke za izdelavo in razumevanje postopkov izdelave ocen ogroženosti/tveganj;
- je model uporaben za srednjeročne in dolgoročne napovedi in celostne ocene;
- je model uporaben za strateško in odločevalsko raven pri pripravi načrtov;

- model predstavlja dobro vodilo, za analitike, ki so vešči poznavalci varnostnih razmer, groženj in tveganj;
- je model primarno uporaben na področju varnostnih, obrambnih zadev in ocenjevanja groženj, povezanih s kriminaliteto.

Ocenjevalci so v evalvaciji poudarili tudi, da zaradi časovnih pritiskov, omejenih sredstev ali pomanjkanja kadra, izvajanje kompleksnih in zapletenih postopkov pogosto praktično ni izvedljivo. Skladno s pridobljenimi povratnimi informacijami smo model revidirali in tako pripravili model s standardnim postopkom, ki vključuje vse korake in faze (Poglavje 7.2), in model s skrajšanim postopkom, ki vključuje izključno najpomembnejše faze in je uporaben za hitro izdelavo ocen (Poglavje 7.3).

Ocenjevalci so v povratnih informacijah omenili tudi, da bi bilo treba model testirati v realnih okoliščinah in za njegovo lažjo uporabo zagotoviti ustrezno tehnološko podporo. Zato predlagamo: testiranje uporabe modela v skupini analitikov, kar bi omogočilo ugotovitev časovnih in kadrovskih zahtev za njegovo uporabo; izobraževanja analitikov na področju predlaganih tehnik zbiranja, analiziranja in predstavljanja podatkov; ter razvoj programske opreme na osnovi modela, ki bi omogočila hitrejšo izvedbo postopka ocene. Za slednje bi bilo treba izvesti poglobljeno raziskavo na različnih delovnih področjih zagotavljanja javne varnosti o specifičnih indikatorjih, ki jih je treba pri ocenah posameznih elementov vključiti v izračun ogroženosti/tveganja, in njihovi pomembnosti. To bi seveda zahtevalo aktivno sodelovanje institucij, za katere bi se razvijala programska oprema.

7.2 Model za ocenjevanje ogroženosti/tveganja – standardni postopek

Model je primarno namenjen organizacijam, ki delujejo na področju javne varnosti, in sicer njihovim izvajalcem (analitikom) ter odločevalcem v podporo pri izvajanju postopka analize in ocene varnostne ogroženosti oz. varnostnih tveganj.

Ocena ogroženosti/tveganja je sestavni del širšega procesa upravljanja tveganj. Cilj upravljanja tveganj je zagotoviti pripravljenost (organizacije, države ali nekega subjekta) na potencialne nevarnosti in pravilno odzivanje oz. nemoteno delovanje tudi ob morebitni uresničitvi groženj. Z oceno ogroženosti/tveganja se ugotavlja, katere grožnje/tveganja ogrožajo analiziran sistem/področje, katera so bolj ali manj pogosta in nevarna, kar omogoča sprejem odločitev, kako se nanje

pripraviti/odzivati. S tem se ustvari podlaga za odločanje, katere ukrepe (če sploh) je treba sprejeti, da se poveča pripravljenost ali zmanjša tveganja.

Model predstavlja praktično orodje za izvajalce (analitike) in je zasnovan v obliki navodila, ki omogoča izvedbo ocene skozi analitično in sistematično zasnovan proces, skozi katerega se odločevalcem zagotovi ustrezna informacijska podpora za odločanje.

Model je splošno in enotno uporaben za vse oblike varnostnih groženj (namerne ali nenamerne, predvidljive ali nepredvidljive). Prav tako je uporaben v zasledovanju organizacijskih ali širših družbenih ciljev.[23]

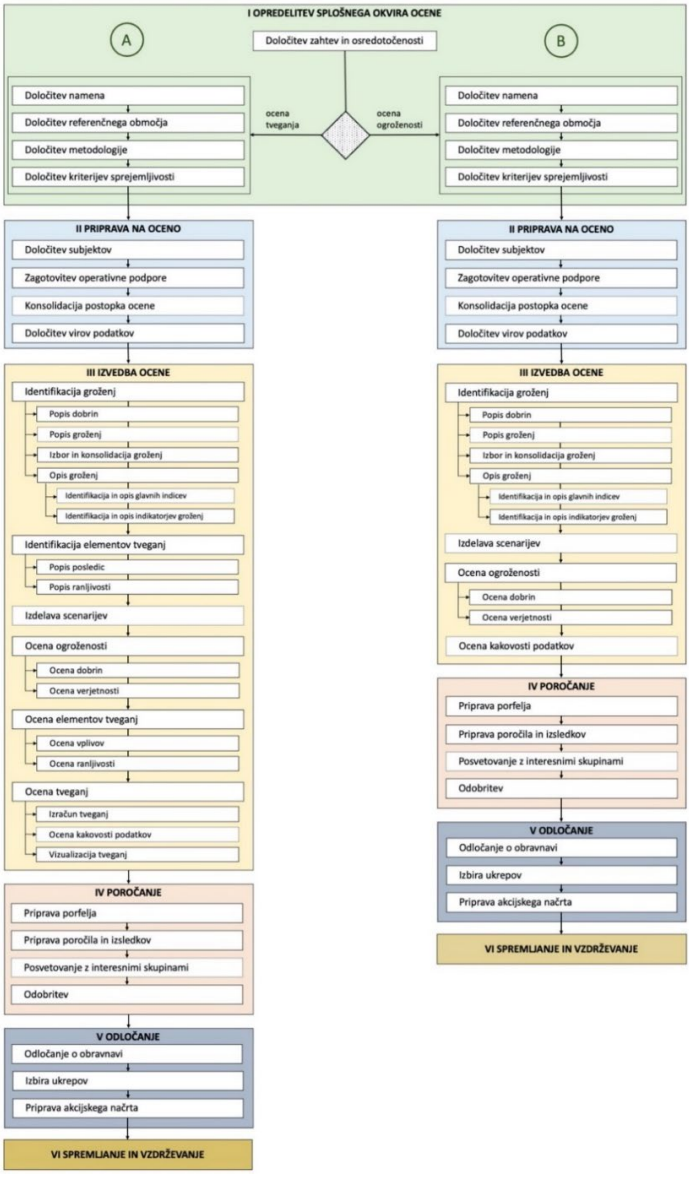
Zasnovan je tako, da se že v prvi fazi deli na dva dela, izvedbo *ocene tveganja* (diagram A) ali *ocene ogroženosti* (diagram B). Če izvajalec želi izvesti le oceno ogroženosti, sledi fazam in korakom v diagramu B, če pa želi izvesti celotno oceno tveganja, pa sledi diagramu A.

V besedilnem opisu modela v obliki navodila je vsaka faza (skupaj s koraki in podkoraki) podrobneje opisana. Podani so tudi predlogi glede rezultatov posamezne faze in odgovornih subjektov. Za vsako fazo so tudi predlagane tehnike ravnanja s podatki, ki jih je možno smiselno uporabiti pri izvedbi posamezne faze. Čeprav so pri izvedbi ocene predlagani nekateri postopki in tehnike izračunavanja in vizualizacije tveganj, gre le za primere in smernice za izvedbo celotnega procesa in posameznih postopkov. Izvajalec lahko pri izračunavanju uporabi različne metode in tehnike, najpogosteje z računalniško podprtimi možnostmi izračunavanja.

Model spremljajo trije dodatni pripomočki. Prvi (pripomoček I) predstavlja in podrobneje opisuje tehnike zbiranja, analiziranja in predstavljanja podatkov. Tehnike obsegajo vse od možganskega viharjenja do naprednih metod strojnega učenja. Namenjene so kakovostni in učinkoviti izvedbi ogroženosti/tveganja. Drugi (pripomoček II) predstavlja okvir ocene kakovosti, ki zajema oceno kakovosti

[23] Za organizacijski cilj gre v primeru, ko se izvajajo ocene za grožnje/tveganja, ki zadevajo le eno organizacijo (npr. ocena groženj/tveganj, ki vplivajo na doseganje ciljev organizacije ali njene poslovne procese). V tem primeru so ocene v individualnem interesu namenjene ohranjanju varnosti, stabilnosti in nemotenosti delovanja specifičnega subjekta. Za širši družbeni cilj pa gre v primeru, ko so grožnje ali tveganja večje družbene razsežnosti in presegajo interese posameznega subjekta. V tem primeru so ocene v javnem interesu oz. pomembne za ohranjanje dobrobiti družbe ali določene skupnosti (npr. naravne nesreče, kriminaliteta).

podatkov, njihovih virov in predstavitve. Tretji (pripomoček III) pa predstavlja primer izdelave registra groženj in registra tveganj, ki sta rezultata popisa elementov in ocene ogroženosti oz. tveganj. Model je grafično prikazan na sliki 10 spodaj.



Slika 10: Model za ocenjevanje ogroženosti/tveganja – standardni postopek

I Opredelitev splošnega okvira ocene

V tej fazi se zagotovi razumevanje zunanjega in notranjega konteksta procesa ocene. *Namen je zastaviti temelje in izhodišča za vse nadaljnje faze in korake procesa.* Določiti in zabeležiti je treba zahteve, kar predstavlja temelj, izhodišča pa se določijo skozi opredelitev namena, referenčnega območja in postopka ocene (z metodologijo in merili odločanja).

Oblikovanje splošnega okvira vključuje pretežno načrtovalne dejavnosti. Praviloma se ta faza izvede le ob prvi oceni, ob morebitnih ponovnih izvedbah ostaja nespremenjena, razen v primeru, če se za spremembe izkaže potreba.

Rezultat faze:

- Portfelj kontekstne dokumentacije (zahteve in izhodišča procesa);
- Potrjena in formalizirana metodologija postopka ocene.

Odgovorni subjekti:

- Odločevalci v sodelovanju z analitiki (izvajalci ocen) in področnimi strokovnjaki.

Predlagane tehnike:

- Tehnike za pridobivanje mnenj od deležnikov in strokovnjakov (T1).

I.A Določitev zahtev

Okvir ocene mora biti skladen z organizacijskim kontekstom, organizacijsko kulturo, potrebami organizacije, njenimi strateškimi in normativnimi podlagami ter predvsem politiko upravljanja groženj/tveganj v organizaciji (vsaka organizacija, ki izvaja oceno ogroženosti/tveganja, bi morala imeti predhodno sprejeto namensko politiko, ki ureja pristop, proces in odgovornosti upravljanja). Posebej pomembno je tudi, da so izhodišča ocene, ki se določijo v naslednjih korakih, usklajena z zakonodajnimi zahtevami, ki jih je treba upoštevati.

V ta namen se uredi portfelj dokumentacije in pri tem izvede pregled ter opis vseh ključnih internih dokumentov in zunanjih zahtev (strategije, politike, načela, vrednote, zakonodaja), ki usmerjajo izvedbo ocene.

V tem koraku se tudi, skladno z ugotovljenimi zahtevami, določi obseg ocene. Torej, ali bo proces ocene osredotočen na *oceno ogroženosti* ali *oceno tveganja*.

Namen ocene ogroženosti je presoditi verjetnost, da se bo (na določnem območju in/ali časovnem obdobju) uresničila določena grožnja. Usmerjena je izključno v analizo preteče nevarnosti (njenega namena, zmogljivosti, razsežnosti, potenciala, cilja). Namen je ugotoviti naravo in stopnjo nevarnosti, ki ogroža določeno tarčo, subjekt ali področje. Ocena tveganja pa poleg ocene ogroženosti vključuje še analizo in oceno lastnih okoliščin v povezavi s pretečo nevarnostjo (lastnih ranljivosti, dovzetnosti za posledice, zmogljivosti zaščite in priporočenih ukrepov). Namen je ugotoviti, kakšne vplive bi grožnja povzročila in kako se je treba odzvati na tveganje. Ocena ogroženosti se navadno izraža v oceni verjetnosti oz. stopnji ogroženosti, ocena tveganja pa v stopnji tveganja.

Ocena ogroženosti je torej lahko samostojna ocena ali pa sestavni del ocene tveganja. Ocena ogroženosti se navadno izvaja, kadar ni mogoče vplivati na pojav grožnje; kadar gre za kompleksne, nepredvidljive nevarnosti, pri katerih je težko pridobiti zanesljive in resnične podatke; kadar ni mogoče presoditi vplivov ali ranljivosti. Najpogosteje se ocena ogroženosti izvaja za težko določljive, nepredvidljive zlonamerne grožnje (npr. organizirana kriminaliteta, terorizem, nasilje v družini). Ocena tveganja pa se izvede, kadar je mogoče vplivati na pojav ali posledice grožnje, skozi preventivne ukrepe, lastno zaščito oz. zmanjševanje ranljivosti; kadar gre za poznane grožnje, pri katerih je mogoče oceniti lastno ranljivost in dovzetnost; kadar so (tudi zaradi preteklih izkušenj) na voljo dovolj zanesljivi in resnični podatki. Ocena tveganja ima tako širši okvir in namen, posledično pa vključuje kompleksnejši postopek analiziranja in ocenjevanja.

Glede na določen osnovni namen se v nadaljevanju uporabe tega modela sledi *diagramu A* (model za oceno tveganja) ali *diagramu B* (model za oceno ogroženosti).

I.B Določitev namena

V opisu namena se določi, kakšne grožnje bodo predmet ocene.

Najprej se izbere *osnovna raven abstrakcije groženj*, kar vključuje opredelitev, katere vrste groženj bodo vključene v oceno. To so lahko: (a) dejanske grožnje (tj. jasne in določljive grožnje, ki jih poznamo, s katerimi že imamo pretekle izkušnje in predvidevamo njihov ponovni pojav); (b) potencialne grožnje (tj. grožnje, ki jih lahko do neke mere vidimo na obzorju in predstavljajo potencial na podlagi aktualnih ali napovedanih trendov); in/ali (c) hipotetične grožnje (tj. povsem nove, morebitne in neodkrite grožnje, ki predstavljajo možnost oddaljenega neznanega scenarija, s katerim svetovna javnost še nima izkušenj).

Zatem sledi še *vsebinska opredelitev groženj*, kjer se določi tip groženj, ki bodo vključene v oceno (npr. naravne in druge nesreče, človeško povzročene zlonamerne ali nenamerne grožnje, zavirajoče okoliščine (pri doseganju ciljev)). S tem se določijo širše kategorije oz. gruče groženj, na katere bo osredotočen proces ocene v nadaljevanju, in hkrati zagotovi večja preglednost v nadaljnjih fazah in korakih.

I.C Določitev referenčnega območja

V določitvi referenčnega območja se določita *območna dimenzija* in *časovna dimenzija* za analizo in oceno.

Pri območni dimenziji se opredeli geografski obseg analize oz. ali se bo ocena opravljala za območje celotne države (nacionalna ocena), širšega teritorialnega območja (regionalna ocena), lokalne skupnosti (lokalna ocena) ali se bo nanašala na posamezno organizacijo oz. njene dobrine (organizacijska ocena). V tem delu se opišejo tudi splošne značilnosti izbranega območja (demografija in prebivalstvo, okolje, gospodarstvo, infrastruktura in oskrba). Alternativno lahko območje ostane *nedoločeno*.

Zatem se določi še ročnost ocene oz. časovno obdobje, na katero bo osredinjena analiza. Ocena se lahko nanaša na kratkoročno obdobje (do enega leta), srednjeročno (do tri leta), dolgoročno (do pet let). V primerih globalnih perspektiv (npr. tudi pri ocenjevanju hipotetičnih groženj) se lahko ocena nanaša na dogodke, oddaljene do

35 let, praviloma pa se nanaša na grožnje, ki imajo potencial v naslednjih petih letih. Ročnost ocene je tesno povezana z uporabnostjo končnih rezultatov ocen. Nižja, kot je odločevalska raven v hierarhiji, krajša je ročnost ocene. Če so denimo rezultati namenjeni podpori aktualnemu operativnemu delovanju, se analizira ogroženost/tveganje za krajše obdobje; če pa so ocene namenjene podpori strateškemu odločanju in upravljanju, je zajeto daljše časovno obdobje.

I.D Določitev metodologije

Na osnovi identificiranih zahtev in osredotočenosti (I.A) ter opredelitve namena (I.B) se določi še metodologija oz. način izvedbe postopka ocene. To vključuje odločitev o tem, kateri elementi ogroženosti oz. tveganja bodo vključeni v oceno, kako se bodo ocenjevali, kako bo potekal izračun končne ocene in umeščanje ocene v stopnje ogroženosti/tveganja. Oceno je namreč možno pridobiti skozi različne kombinacije posameznih elementov ogroženosti/tveganja (III.A.4; III.B). Skladno z odločitvijo o vključevanju različnih elementov se ustrezno prilagodijo koraki, ki so del tega modela.

Poleg odločitve o elementih ocene je treba opredeliti tudi, ali se bo uporabil standardni ali skrajšani postopek ocene. Standardni postopek vključuje vse korake in podkorake tega modela, ki so potrebni za natančno in zanesljivejšo oceno tveganj. Skrajšani postopek pa vključuje zgolj nujne in neizogibne korake in podkorake tega modela. Standardni postopek se predlaga v primeru, ko izvajalec razpolaga z ustreznimi viri (podatki, sredstva, čas), skrajšani pa, kadar izvajalec z omenjenimi viri ne razpolaga (npr. časovni pritisk, manko podatkov ali drugih sredstev).

V odločanju o pristopu k ocenjevanju je pomembno, da se zagotovita interoperabilnost in primerljivost rezultatov, zato naj se čez čas zagotavlja primerljivost metodologije tudi na področju različnih groženj. Zato je pomembno, da je metodologija standardizirana, odobrena in formalno potrjena od odločevalca/odločevalcev ter opredeljena oz. predstavljena v obliki navodila.

I.E Določitev kriterijev sprejemljivosti ogroženosti/tveganja

V pripravi na oceno je treba vnaprej določiti tudi kritične meje končne ocene. Skladno z opredeljeno metodologijo in načinom izvedbe postopka (I.D), se opredelijo merila, po katerih se bo v fazi odločanja presojalo, ali je ocenjena

ogroženost/tveganje sprejemljivo ali ne. Merila lahko poleg stopenj ogroženosti/tveganja (npr. zelo nizke in nizke stopnje so sprejemljive) vključujejo tudi druge vidike (npr. stroške, zakonske zahteve, življenjske, socialno-ekonomske in okoljske faktorje). (Ne)izpolnjevanje meril vodi torej v oceno (ne)sprejemljivosti in ugotovitev, ali je potrebno ukrepanje.

II Priprava na oceno

V tej fazi se vzpostavijo pogoji in zmogljivosti za izvedbo postopka ocene. *Namen je podrobneje opredeliti subjekte in njihove pristojnosti, zagotoviti ustrezno operativno podporo, izbrati vire podatkov in konsolidirati terminologijo ter postopek.* Ob vsaki ponovni izvedbi procesa ocene se preveri ustreznost teh določitev, ki se jih po potrebi prilagodi/spremeni. Priprava na oceno vključuje pretežno organizacijske in koordinacijske dejavnosti.

Rezultat faze:

- Vzpostavljen izvajalski sistem s potrjenimi vlogami in odgovornostmi;
- Zagotovitev materialne in nematerialne podpore;
- Dokumentirani viri podatkov.

Odgovorni subjekti:

- Odločevalci v sodelovanju z analitiki (izvajalci ocen).

Predlagane tehnike:

- Tehnike za pridobivanje mnenj od deležnikov in strokovnjakov (T1).

II.A Določitev subjektov

Za nemoten in učinkovit potek procesa je treba jasno opredeliti subjekte, ki bodo glede na zahtevnost procesa in pričakovane kompetence izvedli oceno (tj. izvajalci) ali sodelovali/pomagali pri izvedbi ocene. Kadar so ocene v individualnem interesu posamezne organizacije, so subjekti izvajalci interni analitiki v organizaciji, v primeru splošnega javnega interesa pa se pogosto združuje/povezuje deležnike iz različnih

organizacij. Navadno ocenjevanje ogroženosti/tveganj na nacionalni, regionalni ali lokalni ravni, kjer se zasledujejo širši družbeni cilji, zahteva sodelovanje širšega kroga deležnikov (tj. večdeležniški pristop).

Za izvajalce je treba določiti subjekte, ki imajo interes, motiv, predvsem pa znanja, izkušnje in ustrezna razumevanja elementov, vključenih v analizo. To so lahko predstavniki različnih državnih, javnih in zasebnih organizacij, civilne družbe, nevladnih organizacij, znanstvenoraziskovalnih institucij ali specifični zakonski zavezanci. Pri tem je treba vsem vključenim subjektom, natančno določiti vloge, pristojnosti in odgovornosti pri izvajanju ocene.

**Opomba:* V primeru večdeležniškega pristopa je treba določiti tudi koordinacijsko telo/subjekt, ki bo skrbel za delitev prednostnih nalog, organizacijo dela, koordinacijo in usklajevanje med sodelujočimi deležniki. Tovrsten organ prevzame del odgovornosti v vseh fazah, kjer so, kot odgovorni subjekti, navedeni *odločevalci.*

II.B Zagotovitev operativne podpore

Vsaka organizacija, v kateri se izvaja ocena ali pa je pristojna za izvedbo ocene, mora pristojnim subjektom (izvajalcem, analitikom) zagotoviti ustrezno podporo za njihovo delo. V ta namen je treba proučiti, kakšna sredstva (materialna in nematerialna) so potrebna, določiti realne časovne roke glede na pričakovanja in zahtevano kakovost ter zagotoviti druge vidike pomoči in podpore (možnost vključevanja strokovne pomoči).

Pri tem je ključnega pomena, da se izvajalcem (analitikom) zagotovita samostojnost in strokovno neodvisnost pri izvajanju postopka ocene.

II.C Konsolidacija postopka ocene

V primeru večdeležniškega pristopa k oceni ali sodelovanja več subjektov/analitikov znotraj institucije v procesu ocene je treba uskladiti postopek izvajanja ocene. Gre za korak, ki pripomore k večji skladnosti in primerljivosti rezultatov ocen, ki jih izvedejo različni deležniki.

Ko je opredeljen splošen okvir s temelji (I.A) in izhodišči (I.B–I.E) ocene ter ko so izvedeni predhodni koraki priprave na oceno (II.A; II.B), se pred pričetkom: (a) preveri enotno razumevanje izhodišč in vidikov dorečenih v pripravi; (b) dogovori o uporabi enotne terminologije; ter (c) izvede skupinski preizkus dorečene metodologije na referenčnem primeru. S tem se demonstrira praktična uporaba in preveri dejanska usklajenost med izvajalci ocene ter njihovo razumevanje terminologije in metodologije.

II.D Določitev virov podatkov

Izvajanje ocene ogroženosti/tveganja mora v čim večji meri temeljiti na dejstvih in dejanskih podatkih. Kjer koli je to mogoče, naj se uporabi kvantitativne (zgodovinske in statistične) podatke. Ker pa se pogosto obravnavajo tudi nepredvidljive, kompleksne in neznane grožnje, za katere niso na voljo kvantitativni podatki, so v ocene vključena tudi predvidevanja. V tem primeru naj bodo v podporo kvalitativni podatki (kot so mnenja, sklepanja, obveščevalni produkti).

Da bi bila končna ocena čim bolj zanesljiva, je treba podatke, ki naj bodo čim bolj aktualni, pridobiti iz več različnih virov. V tem koraku se določi, kateri viri podatkov bodo uporabljeni za izvedbo ocene. Podatki in njihovi viri so lahko:

- zgodovinski;
- statistični;
- organizacijski;
- interni;
- javno dostopni podatki;
- odprti podatki;
- znanstvenoraziskovalni;
- mnenja strokovnjakov;
- obveščevalni podatki;
- mednarodne ali nacionalne specializirane zbirke;
- zbirke podatkov posameznih državnih organizacij;
- mednarodna in nacionalna analitična poročila.

Določitev virov in vrste podatkov ne vpliva samo na kakovost ocene, ampak tudi izbiro metod zbiranja in analiziranja podatkov ter posledično na izbiro strokovnjakov za posamezne metode (npr. ang. *web scraping*, statistične analize, metode globokega učenja za napovedovanje).

Pri uporabi podatkov je pomembno še, da so njihovi viri jasno citirani/opredeljeni, da je zagotovljena njihova sledljivost in da so vsa sklepanja in predvidevanja jasno izpostavljena v ocenah.

III Izvedba ocene

V tej fazi se izvede postopek analize in ocene ogroženosti/tveganja v kontekstu, vzpostavljenem v prvih dveh fazah. *Namen je prepoznati in ovrednotiti grožnje/tveganja skozi sistematičen in dokazljiv postopek*. Analiza vključuje korake, vezane na identifikacijo dejavnikov ogroženosti, elementov tveganj in opredelitev scenarijev. Ocena pa temelji na oceni teh dejavnikov, elementov ali scenarijev, izračunu končne ocene in ugotovitvi stopnje ogroženosti/tveganja, presoji kakovosti in vizualizaciji rezultatov. Na podlagi popisa groženj in elementov tveganj ter ocene ogroženosti/tveganj se izdela register groženj oz. tveganj. Primer za izdelavo tovrstnih registrov je podan v prilogi III.

Ta faza vključuje pretežno operativno-analitične dejavnosti.

Rezultat faze:

- Seznam možnih groženj in izbor realnih groženj s spremljajočim opisom;
- Strukturiran popis dobrin, posledic in ranljivosti groženj;
- Izdelani scenariji;
- Ocene ogroženosti/tveganja;
- Register groženj/tveganj;
- Ocene zanesljivosti rezultatov;
- Vizualizacija rezultatov.

Odgovorni subjekti:

- Izvajalci (analitiki) v sodelovanju s področnimi strokovnjaki

Predlagane tehnike:

- Tehnike za pridobivanje mnenj od deležnikov in strokovnjakov (T1);
- Tehnike za identifikacijo tveganj (T2);
- Tehnike za ugotavljanje virov, vzrokov in gonilnikov tveganja (T3);
- Tehnike za analizo kontrol (T4);
- Tehnike za razumevanje posledic in verjetnosti (T5);
- Tehnike za analizo odvisnosti in interakcij (T6);
- Tehnike, ki omogočajo meritve tveganja (T7);
- Tehnike za ocenjevanje pomembnosti tveganja (T8);
- Tehnike za izbiranje med možnostmi (T9).

III.A Identifikacija groženj

Ta korak je praviloma osredotočen na zbiranje in predstavljanje podatkov, ki so vezani na zunanje dejavnike oz. dejavnike groženj.

Skladno z opredeljenim namenom (I.B) in referenčnim območjem (I.C) izvajalec ugotavlja ogrožene dobrine, možne vire groženj in prepoznava dogodke, ki bi jih lahko zoper dobrine uresničili tovrstni viri. Na podlagi tega se pripravita smiseln nabor in opis značilnosti groženj, ki bodo vključene v oceno.

III.A.1 Popis dobrin

Izvajalec popiše vse možne tarče, ki bi bile potencialno ogrožene. Tarče so dobrine ali vrednote oz. cilji posameznih groženj, torej tisti vidiki, ki jih varujemo ali želimo obvarovati. Gre za korak, ki se izvede pri ocenah, kjer se grožnje vežejo na točno določene dobrine oz. v primerih, ko je cilj ugotoviti, katere grožnje ogrožajo točno določene dobrine (npr. zoper določen objekt). V primeru, ko dobrin ni mogoče jasno popisati ali to ni smiselno, se ta korak preskoči.

Dobrine se lahko smiselno gručijo. Med elemente (gruče) lahko primeroma prištevamo cilje, procese in sredstva organizacije, objekte, temeljne družbene funkcije, premoženje, življenje, zdravje, delovanje države in njenih organov, gospodarstvo (npr. BDP), družbene vrednote (npr. varnost, demokracija, človekove pravice) in/ali okolje.

III.A.2 Popis groženj

Izvajalec identificira vse možne vire in s tem povezane grožnje, ki so smiselne in izpolnjujejo merila, zastavljena v splošnem okviru ocene. Namen je zagotoviti ustrezno situacijsko zavedanje in pridobiti celosten pregled nad potencialnimi ogrožajočimi situacijami oz. nevarnostmi. Končni produkt tega koraka je seznam vseh identificiranih relevantnih groženj, ki so lahko tudi gručene (če gre za vsebinsko povezane grožnje (I.B)). Popis groženj je lahko vezan na popis dobrin (III.A.1).

III.A.3 Izbor in konsolidacija groženj

Zaradi potencialno velikega števila vseh potencialnih groženj je treba oceno osredotočiti na realne grožnje in pripraviti, glede na razpoložljive vire, za ocenjevanje izvedljiv nabor groženj. Grožnje, ki bodo vključene v nadaljnji proces in predmet natančne analize, se določijo na podlagi intuitivnega odločanja in tehnik usklajevanja. Osredotočiti se je treba predvsem na tiste grožnje, ki bi lahko imele pomembne škodljive posledice.

Končni (obvladljiv) seznam izbora realnih groženj naj konsolidira in potrdi več deležnikov.

**Opomba:* Pri izboru in konsolidaciji groženj je treba upoštevati tudi potencialne verižne grožnje, ki imajo kaskadne učinke oz. pri katerih gre za »domino učinek«. Gre za t. i. kompleksne ali večstranske grožnje, v katerih se kombinira več nevarnosti in dogodkov. Praviloma je ena grožnja povod, ostale grožnje pa so posledica povodne.

III.A.4 Opis groženj

Opis groženj je namenjen razumevanju karakteristik in narave posamezne grožnje ter pripomore k lažjemu ocenjevanju v nadaljnjih korakih. Opis vključuje predstavitev grožnje skozi prepoznavanje osnovnih indicev in indikatorjev.

III.A.4.1 Identifikacija in opis glavnih indicev

Za vsako identificirano realno grožnjo (III.A.3) je treba najprej pripraviti splošen pregled (spremni opis) njenih značilnosti (vključno s preteklimi (tudi tujimi) izkušnjami, trenutnimi trendi in drugimi napovedmi) ter določiti in opisati njene

indice (tj. znamenja, znaki). Gre za okoliščine, vzorce in sosledje dogodkov, ki omogočajo prepoznavanje groženj in nakazujejo na njihovo potencialno uresničitev.

III.A.4.2 Identifikacija in opis indikatorjev groženj

Indikatorji groženj so okoliščine, na katere ni mogoče (ali je praktično nemogoče) vplivati, so pa pomembni za kasnejšo oceno ogroženosti. Indikatorje je treba izbrati oz. določiti glede na namen ocene (I.B) ter dostopnost podatkov, praviloma pa se nanašajo na namen, razsežnosti in zmogljivosti grožnje.

Indikatorji so lahko deskriptivni ali ocenjevalni. Deskriptivni so namenjeni razumevanju grožnje skozi opis, ocenjevalni pa vrednotenju grožnje. Izvajalec sam smiselno določi, kateri indikatorji so deskriptivni in kateri ocenjevalni. Pri vsaki identificirani realni grožnji (III.A.3) se za vsak izbran indikator pripravi opis, za ocenjevalne pa določi tudi način ocenjevanja (kvalitativen, kvantitativen, kombiniran).

V primeru večjega števila je treba indikatorje smiselno gručiti (primer v nadaljevanju).

Med primerne indikatorje za področje kriminalitete lahko prištevamo npr.:

- vir kriminalitete – subjekt oz. skupina (npr. velikost, namen, motiv, cilj/tarča, zmogljivosti/zmožnosti, razvitost/sofisticiranost, modus operandi);
- narava kriminalitete (npr. zahtevnost izvedbe, čas uresničitve, čas trajanja, lokacija uresničitve);
- dejavniki kriminalitete (npr. podporne in spodbujevalne okoliščine – ozemlje, prebivalstvo, gospodarstvo, socialne razmere, infrastruktura, tehnologije, zakonodaja, politični sistem, pravosodje in kazenski sistem, družbeno nadzorstvo, korupcija, mobilnost);
- preteklost kriminalitete (npr. zgodovinski statistični podatki; gibanje kriminalitete),
- potencial kriminalitete (npr. vpliv, ogroženi cilji/viri/procesi/sredstva).

Indikatorji se razlikujejo glede na tip grožnje in dostopnost podatkov, zato univerzalnega seznama ni mogoče podati. Tako se za ocenjevanje ogroženosti pred naravnimi nesrečami indikatorji bistveno razlikujejo od zgoraj navedenih. Med primerne indikatorje za področje naravnih nesreč lahko prištevamo npr. podnebne, okoljske in urbanistične okoliščine. Na izbor indikatorjev vpliva tudi sama osredotočenost ocene (ali se bo opravila zgolj ocena ogroženosti ali pa ocena tveganja (I.A)). V primeru, da se bo opravila samo ocena ogroženosti, se med pomembne indikatorje, ki se kasneje upoštevajo pri oceni, umešča vpliv oz. posledice uresničene grožnje. To pomeni, da se pri oceni ogroženosti ob verjetnosti upošteva tudi potencial ali resnost grožnje. Nasprotno pa se pri oceni tveganj ogroženost presoja na osnovi verjetnosti, vpliv pa se upošteva kasneje pri izračunu tveganja v kombinaciji z ostalimi elementi tveganj.

**Opomba:* Gruče in ocenjevalne indikatorje lahko izvajalec obteži po pomembnosti s pomočjo ene izmed uveljavljenih metod (npr. z ordinalnimi lestvicami (od 1 do 3/5) ali z analitičnim hierarhičnim procesom – AHP). Uteži pripomorejo k prioritizaciji indikatorjev in posledično natančnejši oceni ogroženosti.

III.B Identifikacija elementov tveganj

Ta korak je praviloma osredotočen na zbiranje in predstavljanje podatkov, vezane na notranje dejavnike (lastne okoliščine).

Skladno z vnaprej določenimi elementi, ki bodo vključeni v oceno tveganja (I.D) in identificiranimi realnimi grožnjami (III.A.3), izvajalec identificira oz. popiše posledice, ki bi jih povzročila posamezna grožnja; in/ali ranljivosti, ki ustvarjajo lastno dovzetnost za uresničitev grožnje in s tem povezane posledice.

III.B.1 Popis posledic

Izvajalec za vsako posamezno realno grožnjo popiše možne posledice (tj. vplivi in negativni učinki), ki bi jih uresničena grožnja lahko povzročila. Upoštevajo se potencialne posledice tako v notranjem kot tudi zunanjem okolju.

Posledice se lahko vežejo na ogrožene dobrine (III.A.1) in se vsebinsko gručijo, pri čemer primere gruč posledic predstavljajo npr. vplivi na delovanje organizacije (njene zmogljivosti, procese, infrastrukturo, procese, poslovanje ipd.), države ali

skupnosti, človeški vplivi oz. vplivi na življenje in zdravje, ekonomski in gospodarski vplivi, vplivi na okolje, politični in družbeni vplivi, psihološki in humanitarni vplivi.

III.B.2 Popis ranljivosti

Izvajalec za vsako posamezno realno grožnjo popiše tudi ranljivosti (tj. šibke točke, ki spodbujajo ali omogočajo uresničitev grožnje). Popis ranljivosti se lahko veže na dobrine (III.A.1) in posledice (III.B.1) ter se jih vsebinsko gruči po področjih (npr. ranljivosti na operativni, nadzorstveni, okoljski, upravljavski, sistemsko politični, normativni in zakonodajni ravni).

Popis ranljivosti naj konkretno obsega:

- popis okoliščin, ki ustvarjajo ranljivost območij/lokacij, skupnosti, področij, procesov, subjektov, sistemov, sektorjev, sredstev, premoženja, objektov;
- popis priporočenih ukrepov (preventivnih in reaktivnih); ter
- popis obstoječih ukrepov/kontrol/dejavnosti/zmogljivosti/dostopnosti opreme in sredstev.

**Opomba:* Gruče in ranljivosti znotraj gruč lahko izvajalec obteži po pomembnosti s pomočjo ene izmed uveljavljenih metod (npr. z ordinalnimi lestvicami (od 1 do 3/5) ali z analitičnim hierarhičnim procesom – AHP). Uteži pripomorejo k prioritizaciji posameznih ranljivosti in posledično natančnejši končni oceni.

III.C Izdelava scenarijev

Proces odkrivanja, določanja, opisovanja in okvirjanja ocene ogroženosti/tveganja lahko, če je za to na voljo dovolj časa, sredstev in podatkov, vključuje tudi izdelavo scenarijev. V tem primeru so scenariji vezani na posamezne grožnje, vključene v oceno.

Ta faza je namenjena predvsem globinskemu in realističnemu razumevanju narave ogroženosti/tveganja. To pripomore k natančnejšemu ocenjevanju. Z opredelitvijo scenarijev se namreč lahko izključijo teoretične ogroženosti/tveganja, ki imajo tako

nizko verjetnost, da ne zahtevajo obravnave. Scenariji se lahko izdelajo za nesreče in večje nevarnosti družbi, zlonamerne grožnje oz. kriminaliteto ali pa na področju vojaških/obrambnih zadev.

Scenariji niso napovedi, kako bi se lahko neka grožnja uresničila oz. kako bi lahko potekali dogodki zatem, temveč so namenjeni opredelitvi situacij, ki so povsem realistične, zato pretežno temeljijo na preteklih izkušnjah. Opis scenarija navadno vključuje povzetek splošnih značilnosti posameznih elementov ogroženosti/tveganja, npr.: vrsto nevarnosti, možne vzroke in odgovornosti, opis poteka, prostorsko/geografsko razsežnost, čas uresničitve in trajanje, potencialne posledice in ogrožene dobrine. Opis scenarija je treba vezati na identificirane indikatorje groženj in elemente tveganj.

Praviloma se za posamezno grožnjo izdelata en do dva scenarija (npr. najslabši možni scenarij; najbolj verjetni oz. realistični). Ker gre za zahteven in kompleksen proces, se ob prvi taki izdelavi scenarijev priporoča priprava manjšega števila (do 20), ki se nato ob ponovitvah ocen dopolnjujejo.

**Opomba:* Scenariji lahko zajemajo primere enostavnih (enovrstnih) ali kombiniranih groženj (večvrstne). V primerih, kjer scenariji vsebujejo eno grožnjo/tveganje, je fokus na eni nevarnosti, ki se uresniči na določenem geografskem območju v določenem časovnem obdobju. Pri scenarijih, ki vsebujejo več groženj/tveganj, pa se upoštevajo nevarnosti, ki se zgodijo hkrati ali si sledijo, ker so soodvisne, so bile povzročene z istim virom ali pa ogrožajo iste elemente brez kronološke povezave.

III.D Ocena ogroženosti

Ocena ogroženosti se nanaša na presojo verjetnosti, da se bo v določenem časovnem obdobju in v določenem prostoru uresničila določena grožnja. Če je to smiselno, se presoja verjetnosti veže na identificirane dobrine/tarče.

III.D.1 Ocena dobrin

Z oceno dobrin se ovrednoti, kako pomembne so možne izgube ob uresničenju grožnje (ali scenarija). Ocenjevanje dobrin je, kot omenjeno, alternativni korak, primeren predvsem v situacijah, ko tveganje oz. grožnja, ki povzroča tveganja,

ogroža jasno določljive in oprijemljive tarče/cilje, ki jih je možno ovrednotiti. Najpogosteje se dobrine ocenjujejo, ko grožnja ogroža eno dobrino ali v primeru organizacijskih analiz/ocen tveganj.

V oceno je treba zajeti vse identificirane dobrine (III.A.1). Dobrine se vrednotijo glede na njihovo pomembnost/kritičnost oz. vrednost za organizacijo, državo ali skupnost. Ocena se praviloma poda na tri- do petstopenjski ordinalni lestvici (slika 11), stopnje vrednosti pa lahko spremljajo kvalitativni opisi (npr. izguba dobrine je nesprejemljiva) ali kvantitativne vrednosti (npr. v oceni denarne vrednosti).

1	2	3	4	5
Zanemarljiva /zelo nizka	Manj pomembna /nizka	Srednja	Pomembna /visoka	Zelo pomembna /zelo visoka

Slika 11: Primer ocene vrednosti dobrine

V primeru več dobrin se končna ocena vrednosti dobrin poda s povprečenjem vseh ocen posameznih dobrin.

Ocena dobrin se v postopku ocene ogroženosti upošteva ali kot indikator ali pa kot podporna informacija v odločanju glede načina naslavljanja ogroženosti.

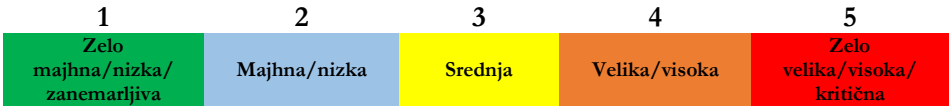
III.D.2 Ocena verjetnosti

Ogroženost se presoja za vsako identificirano realno grožnjo (III.A.3) ali scenarij (III.C). Ogroženost izvajalec tako oceni na podlagi identificiranih indikatorjev groženj (III.A.4) ali opredeljenih scenarijev.

Ocena ogroženosti prioritetno izraža verjetnost, da se bo grožnja (ali scenarij) uresničila ob upoštevanju njenega potenciala.

Končna ocena ogroženosti se praviloma izrazi s pomočjo ordinalne lestvice, ki določa stopnje ogroženosti. Lestvica ima lahko različno število stopenj, najpogosteje so v uporabi tri- in petstopenjske lestvice (slika 12). Ko izvajalec razpolaga z bolj zanesljivimi podatki, se predlaga lestvica z več stopnjami (navadno petstopenjska), v primeru manj zanesljivih podatkov pa lestvica z manj stopnjami (navadno

tristopenjska). Vsaka stopnja ima svojo vrednost, ki jo spremlja kvalitativen in/ali kvantitativen opis.



Slika 12: Primer ocene ogroženosti

Skladno z vsebino in naravo ocene ogroženosti izvajalec določi kvalitativni opis. Za najnižjo stopnjo (ocena 1) tako določi eno izmed možnosti: *ni možnosti, da bi se grožnja uresničila*; *ni skoraj nobene nevarnosti; verjetnost je neznatna*; *dogodek se zgodi zelo redko*. Na drugi skrajnosti lestvice (ocena 5) pa določi eno izmed naslednjih možnosti: *takojšnja nevarnost grožnje; visoka neposredna ogroženost; dogodek se dogaja zelo pogosto oz. redno; ni dvoma, da se bo grožnja uresničila*.

Kvalitativne opise lahko spremljajo tudi kvantitativne vrednosti, kot sta npr. *verjetnost pojava v letih* (npr. enkrat na več kot 100 let) in *verjetnost pojava na letni ravni* v relativnem deležu (letna verjetnost je manj kot 1 %). V primeru zanesljivih, statističnih podatkov ali preteklih izkušenj se predlaga kvantitativno vrednotenje verjetnosti uresničitve grožnje.

Tudi v primeru nepredvidljivih dogodkov, nezanesljivih podatkov in pomanjkanja preteklih izkušenj se ocena ogroženosti lahko pripravi s pomočjo kvantitativne ocene na podlagi presoje in kombiniranja (uteženih) indikatorjev. V primeru določitve uteži (III.A.4.2) se na tem mestu lahko izračuna končna ocena na podlagi ocen posameznih indikatorjev (i – indikator, w – utež indikatorja):

$$i_1 \times w_1 + i_2 \times w_2 \dots i_n \times w_n.$$

Če se izvajalec odloči za kvantitativno ocenjevanje indikatorjev (npr. z ordinalnimi lestvicami ali realnimi števili), je dobljene vrednosti treba normalizirati in jim določiti intervale, ki bodo umeščeni pod posamezne stopnje ogroženosti. Končni rezultat ocene mora biti nato umeščen v eno izmed stopenj (slika 12).

**Opomba:* V primeru pristopa, ki upošteva več groženj hkrati (verižne grožnje), se najprej ocenjuje grožnjo, ki je sprožilec oz. povod in nato posamezne grožnje, ki se lahko sprožijo kot posledica. V takšnem primeru se pripravi enotna ocena ogroženosti/tveganja, ki vključuje tako oceno tveganja sprožilnega dogodka, kot tudi njegovih kaskadnih dogodkov.[24]

III.E Ocena elementov tveganj

Tveganje izvajalec oceni na podlagi izbranih elementov tveganj (III.B) ali opredeljenih scenarijev tveganja (III.C). Elementi se tako presojajo za vsako identificirano realno grožnjo (III.A.3) ali scenarij.

Za pridobitev končne ocene tveganja je v izračunu treba kombinirati ocene različnih elementov, zato je te elemente (vplive, ranljivosti) treba sprva oceniti.

III.E.1 Ocena vplivov

Z oceno vplivov se presodi velikost oz. resnost posledic, ki bi nastale ob uresničeni grožnji (ali scenariju). S tem se pravzaprav ovrednoti nevarnost tveganja. V oceno se zajamejo vse identificirane posledice (III.B.1).

Proces ocene vpliva sestoji iz več korakov. V prvem koraku se ocenjujejo posledice za vsak posamezni vpliv znotraj gruč vplivov (tj. *Ocena posledic*). V drugem koraku se vpliv izračuna na ravni vsake gruče s povprečenjem ocen znotraj gruče. V tretjem koraku se izračuna končna ocena vpliva tveganja s povprečenjem ocen gruč (tj. *Ocena vpliva*). Ocenjuje se torej več vrst gruč vplivov in konkretnejši vplivi znotraj teh gruč.

Ocenjevanje posledic in vpliva poteka na tri- do petstopenjski ordinalni lestvici, ki lahko vključuje zgolj kvalitativne indikatorje, zgolj intervale kvantitativnih ocen ali kombinacijo obojega. V primeru kvalitativnega ocenjevanja izvajalec oceno poda opisno (npr. lestvično z opisi), v primeru kvantitativnega pa je ocena podana v realnih številih (npr. število prizadetih enot, stroški, čas trajanja). Število stopenj na lestvici mora biti enotno za vse posamične vplive in njihove gruče (slika 13).

[24] Zaradi kompleksnosti tovrstne ocene glej smernice Principles of Multi-risk Assessment (European Commission, 2009).

Izvajalec lahko vpliv uresničene grožnje oceni zgolj skozi ocenjevanje posledic ali pa skozi ocenjevanje posledic v kombinaciji z ogroženimi dobrinami (III.D.1). V primeru kombiniranja posledic z ogroženimi dobrinami se končna ocena posledic izračuna z množenjem *Ocene posledic* z oceno vrednosti dobrine.

1	2	3	4	5
Nepomemben /zelo majhen	Omejen /majhen	Zmeren /srednji	Pomemben /velik	Zelo pomemben /kritičen

Slika 13: Primer ocene posledic in ocene vpliva.

III.E.2 Ocena ranljivosti

Z oceno ranljivosti se presodi lastna dovzetnost za uresničitev grožnje (ali scenarija) in zmožnosti obstoječih ukrepov (poimenovano tudi kot ocena kontrolnega okolja), da prepoznajo, ali preprečijo uresničitev grožnje.

V oceno se zajamejo vse identificirane šibke točke in zmogljivosti (III.B.2). Ranljivost se lahko izrazi v stopnji izpostavljenosti ali stopnji zaščite. Za oceno se uporabijo tri- do petstopenjske ordinalne lestvice. Za pridobitev končne ocene je možno oceniti vsako ranljivost in gručo posebej ter ocene nato povprečiti, kot v primeru ocene dobrin (III.D.1) ali vplivov (III.E.1). V primeru uteževanja se ocene ranljivosti primerno ovrednotijo, izračun pa poda kot v primeru ocene verjetnosti (III.D.2).

Alternativno se lahko končna ocena določi tudi na podlagi določanja meril, ki morajo biti izpolnjeni za umestitev v določeno stopnjo. V tem primeru posamezne stopnje ranljivosti spremlja opis, kateri dejavniki (šibke točke ali odsotnost ukrepov) so na posamezni stopnji prisotni/odsotni in vplivajo na oceno. Primer petstopenjske lestvice je predstavljen na sliki 14.

1	2	3	4	5
Zelo nizka ranljivost/Zelo visoka zaščita	Nizka ranljivost/Visoka zaščita	Srednja ranljivost/zaščita	Visoka ranljivost/Nizka zaščita	Zelo visoka ranljivost/Zelo nizka zaščita

Slika 14: Primer ocene ranljivosti

Za lažjo pripravo na fazo odločanja in oblikovanje ukrepov za obvladovanje tveganj se na tem mestu priporoča še izvedba analize vrzeli (imenovana tudi kot analiza GAP). Gre za ugotavljanje razkoraka med obstoječimi in priporočenimi ukrepi

(III.B.2). To omogoča identifikacijo ukrepov oz. dejavnosti, ki so potrebne za doseganje priporočene stopnje zaščitenosti.

III.F Ocena tveganj

Ocena tveganja se izvede za vsako identificirano realno grožnjo (III.A.3) ali scenarij (III.C). Ocena se izvede na osnovi ocene verjetnosti (III.D.2) in izbranih elementov tveganj (III.E). Poleg izračuna višine tveganja in določitve stopnje tveganja ta faza vključuje tudi vizualizacijo ocenjenih tveganj in presojo kakovosti rezultatov.

III.F.1 Izračun tveganj

Izvajalec na podlagi identificiranih in ocenjenih elementov tveganja pripravi izračun tveganja. Možne so različne kombinacije naslednjih postavk:

- ocena ogroženosti (verjetnost uresničitve);
- vrednost dobrin(e);
- vpliv;
- ranljivost.

Izračun se tipično pripravi ali z množenjem ocen elementov in rangiranjem tveganj (tabela 37) ali pa s pomočjo t. i. prevajalnih tabel (tabele 38–40). Izračun predstavlja podlago za oceno, ki je navadno predstavljena na tri- do petstopenjski ordinalni lestvici. V nadaljevanju predstavljeni izračuni rangov in vrednosti v prevajalnih tabelah izvajalcu pomagajo oz. omogočajo določitev končne ocene, so pa tovrstni primeri prilagodljivi (prilagoditve so denimo možne v razponu ocen posameznih elementov tveganja, razponu stopenj tveganja).

V primeru *pristopa z množenjem ocen elementov in rangiranjem* izvajalec za vsako tveganje (ali scenarij) v tabelo vnese oceno posameznih elementov tveganj (npr. kombinacija verjetnosti, ranljivosti in vrednosti; ali vpliva in verjetnosti). Ocene se zmnožijo, rezultat pa vnese v stolpec »Izračun«. Na podlagi izračunanih vrednosti se določi rang za posamezno grožnjo. Višja ocena pomeni tudi višjo prioriteto. Na podlagi izračunanih vrednosti se določi še stopnja tveganja.

Tabela 37: Primer izračuna tveganj z množenjem ocen in rangiranjem (izračunana vrednost med 1 in 21 predstavlja *zelo nizko tveganje*, od 22 do 42 *nizko tveganje* od 43 do 83 *srednje tveganje*, 84 do 104 *visoko tveganje* in 105 do 125 *zelo visoko*).

	Verjetnost (1–5)	Ranljivost (1–5)	Vrednost (1–5)	Izračun (1–125)	Rang	Stopnja
Tveganje 1	1	3	4	12	4	Zelo nizko
Tveganje 2	2	2	2	8	5	Zelo nizko
Tveganje 3	3	4	5	60	2	Srednje
Tveganje 4	5	5	5	125	1	Zelo visoko
Tveganje 5	3	5	3	45	3	Srednje

V primeru *pristopa s pomočjo prevajalnih tabel* izvajalec izbere tabelo glede na število ocenjenih elementov tveganj. V primeru treh (tipično kombinacija verjetnosti, ranljivosti in vrednosti) izbere npr. pristop, ki je predstavljen na tabeli 38, medtem ko v primeru dveh (tipično vpliva in verjetnosti) izbere npr. pristop, ki je predstavljen na tabelah 39 in 40.

Tabela 38: Primer prevajalne tabele 1 (0–2: nizko tveganje; 3–5: srednje tveganje; 6–8: visoko tveganje).

	Verjetnost	1 – Nizka (N)			2 – Srednja (S)			3 – Visoka (V)		
	Ranljivost	1 (N)	2 (S)	3 (V)	1 (N)	2 (S)	3 (V)	1 (N)	2 (S)	3 (V)
Vrednost	**1**	0	1	2	1	2	3	2	3	4
	2	1	2	3	2	3	4	3	4	5
	3	2	3	4	3	4	5	4	5	6
	4	3	4	5	4	5	6	5	6	7
	5	4	5	6	5	6	7	6	7	8

Prevajalna tabela 1 (tabela 38) prikazuje primer, v katerem se kombinirajo ocene verjetnosti (1–3), ranljivosti (1–3) in vrednosti dobrin (1–5). Vrednosti tveganj se gibljejo v razponu med 0 in 8. Konkretni primer predlaga, da vrednosti 0–2 predstavljajo nizko tveganje, vrednosti 3–5 predstavljajo srednje tveganje in 6–8 predstavljajo visoko tveganje. Izvajalec lahko sam določi, katere vrednosti zanj

predstavljajo katero stopnjo tveganja, pri čemer morajo ocene v številih ostati nespremenjene.

Primer uporabe prevajalne tabele 1 (tabela 38):

- V primeru, ko je verjetnost ocenjena z oceno srednje (2), ranljivost z oceno visoko (3) in vrednost dobrine z oceno 4 (visoko), je končni izračun ocena 6, kar predstavlja oceno *visoko tveganje*.

Tabela 39: Primer prevajalne tabele 2 (0–2: nizko tveganje; 3–5: srednje tveganje; 6–8: visoko tveganje).

	Verjetnost	1	2	3	4	5
Vpliv	1	0	1	2	3	4
	2	1	2	3	4	5
	3	2	3	4	5	6
	4	3	4	5	6	7
	5	4	5	6	7	8

Enako velja v primeru prevajalnih tabel 2 (tabela 39) in 3 (tabela 40), pri čemer se kombinirata dve oceni (tipično ocena vpliva in ocena verjetnosti). Pri tem tabeli 38 in 39 predstavljata primer s tremi stopnjami ocene tveganja (nizko, srednje, visoko), tabela 40 pa štiri stopnje (nizko, srednje, visoko, zelo visoko).

Tabela 40: Primer prevajalne tabele 3 (zelena barva: nizko tveganje; rumena barva: srednje tveganje; oranžna barva: visoko tveganje; rdeča barva: zelo visoko tveganje).

	Verjetnost	1	2	3	4	5
Vpliv	1					
	2					
	3					
	4					
	5					

Primer uporabe prevajalne tabele 3 (tabela 40):

- V primeru, ko je vpliv ocenjen z oceno *srednje* (3), verjetnost pa z oceno *nizko* (2), je končna ocena tveganja *visoko* (oranžna).

III.F.2 Ocena kakovosti

V procesu analiziranja in ocenjevanja ogroženosti/tveganja se analitiki in praktiki pogosto soočajo s pomanjkanjem podatkov ali pa upravljajo informacije, ki so vprašljive kakovosti. Situacije oz. vidiki, ki so predmet vrednotenja v procesu analiziranja tveganj (kot npr. grožnje, ranljivosti in vplivi) so pogosto nepredvidljive in kompleksne narave, pogosto pa se zgodi tudi, da z določenimi scenariji nimamo preteklih izkušenj. Zato je pri ravnanju in uporabi informacij, na osnovi katerih se oblikujejo ocene, treba zagotoviti sledljivost s pravilno dokumentacijo in z beleženjem uporabljenih virov ter presoditi kakovost virov, podatkov in posledično končnih rezultatov.

Pri končni oceni izvajalec tako ovrednoti njihovo zanesljivost, predvsem na osnovi poznavanja pojava. Pri ocenjevanju zanesljivosti upošteva pogostost pojava obravnavane grožnje/tveganja, realnost scenarija, predvsem pa kakovost uporabljenih podatkov.

Izvajalec v ta namen pripravi poročilo o kakovosti podatkov, na katerih temelji ocena ogroženosti/tveganja. Poročilo vključuje vse podatke (lahko tudi gruče podatkov) in njihove ocene (ocene kakovosti podatkov so lahko binarne ali ordinalne (lestvične)). Vsak podatek (oz. gruče podatkov) oceni po različnih dimenzijah. Omenjeno poročilo je del ocene tveganja, a na oceno ne sme imeti vpliva. Predstavlja zgolj podporno informacijo odločevalcem.

Načini in dimenzije ocenjevanja kakovosti podatkov, virov in predstavitve podatkov so podrobneje predstavljeni v Prilogi II.

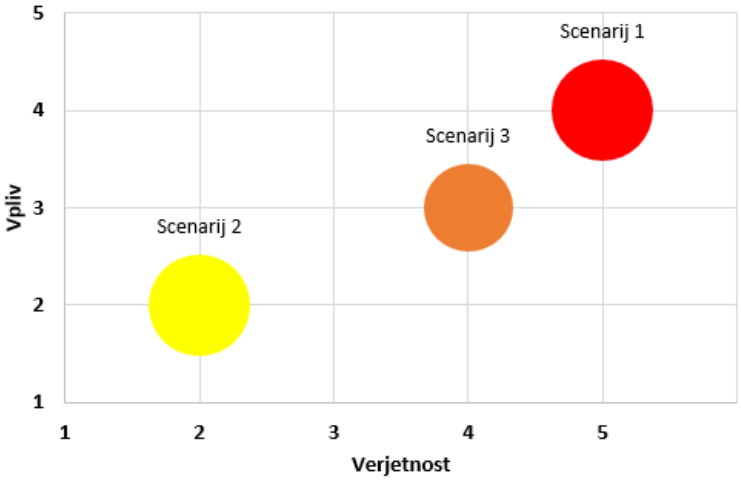
Če izvajalec oceni, da imajo informacije vprašljive kakovosti prevelik vpliv na končno oceno tveganja, lahko za boljše razumevanje zanesljivosti, izvede dve dodatni oceni: *oceno zgolj z informacijami vprašljive kakovosti* in *oceno zgolj z informacijami visoke kakovosti*. Rezultate vseh treh ocen tveganja nato medsebojno primerja. Ta obsežen, a neobvezen, korak pripomore k določanju stopnje napake, ki jo povzročajo informacije vprašljive kakovosti. V primeru, ko vse tri ocene tveganja vrnejo enako končno oceno, nakazuje na to, da informacije vprašljive kakovosti niso imele pomembnega vpliva, medtem ko velika odstopanja opozarjajo na previdnost pri interpretaciji ocene in sprejemanju odločitev o ukrepanju.

III.F.3 Vizualizacija tveganj

Končno oceno tveganj izvajalec predstavi v vizualizirani obliki. Vizualizacija zagotovi preglednost ocen, primerjavo med različnimi tveganji in predstavi rezultate na enostaven ter razumljiv način. Obstaja več načinov vizualizacije, npr. vizualizacija v tabelah, v diagramih, matrikah, zemljevidih.[25] Način vizualizacije izbere izvajalec sam. Tabela 41 prikazuje primer vizualizacije s pomočjo matrike, ki temelji na prevajalni tabeli in jo običajno sestavljata dve osi. V tem primeru izvajalec vsako ocenjeno grožnjo vstavi v ustrezno celico. Slika 15 pa prikazuje primer vizualizacije s pomočjo diagrama.

Tabela 41: Vizualizacija ocene tveganj v obliki matrike.

	Verjetnost	1	2	3	4	5
Vpliv	1					
	2					Grožnja 2
	3		Grožnja 1			
	4					
	5				Grožnja 3	



Slika 15: Vizualizacija tveganj v obliki diagrama

[25] Zemljevidi so uporabno orodje v primeru obsežnejših groženj/tveganj (npr. naravne nesreče, tehnološka in industrijska tveganja). Gre za kompleksnejšo vizualizacijo, ki vključuje zemljevide na več ravneh in zahteva vnaprejšnje planiranje. Več o izdelavi zemljevidov glej na primer smernice Risk & Recovery Mapping (European Commission, n. d.), Current practice in flood risk management in the European Union: September 2021 (European Commission in Royal HaskoningDHV, 2021) ali pa Handbook on good practice on flood mapping in Europe (EXCIMAP, 2007b) ter Atlas of flood maps (EXCIMAP, 2007a).

Vizualizacijo tveganj navadno spremljajo podporne informacije (npr. legende in ocene zanesljivosti).

IV Poročanje

V tej fazi se pripravi predstavitev rezultatov tretje faze. *Namen je zagotoviti ustrezno sledljivost postopku, obveščenost oz. informiranost vseh ključnih deležnikov in podlago za odločanje.* Pripraviti je treba strukturiran sistem ustvarjene dokumentacije in pregledno, razumljivo ter jasno poročilo o vseh rezultatih in ključnih izsledkih ocene, ki je usklajeno z interesnimi skupinami in potrjeno na odločevalski ravni. Ta faza vključuje pretežno poročevalske in koordinacijske dejavnosti.

Rezultat faze:

- Portfelj vseh rezultatov ocene ogroženosti/tveganja
- Potrjeno in odobreno končno poročilo

Odgovorni subjekti:

- Izvajalci (analitiki) v sodelovanju z interesnimi skupinami in odločevalci

Predlagane tehnike:

- Tehnike za beleženje in poročanje (T10)

IV.A Priprava portfelja

Izvajalec pripravi portfelj oz. skupno mapo vseh izdelkov, ki so nastali skozi celoten proces priprave in izvedbe ocene, vključno z vsemi rezultati.

Določijo se stopnja zaupnosti posameznih izdelkov in pravice dostopanja.

IV.B Priprava poročila in izsledkov

Za večjo preglednost rezultatov in ključnih ugotovitev izvajalec pripravi strnjeno poročilo, ki predstavlja izsledke vseh korakov. Namen poročila je na razumljiv in enostaven način predstaviti grožnje, rezultate analiz, ocene, ugotovljene potrebe in načrt ukrepanja.

Poročilo naj vključuje tudi jasen in jedrnat povzetek analize in ocene. V povzetku naj bo poudarek na kritičnih oz. visokih grožnjah/tveganjih, ki zahtevajo prioritetno obravnavo, vključno z najpomembnejšimi ranljivostmi in/ali izbranimi ukrepi ter morebitnimi drugimi informacijami, ki so ključni za odgovorne osebe.

IV.C Posvetovanje z interesnimi skupinami

Z namenom zagotovitve transparentnosti, veljavnosti in razumljivosti rezultatov ocene je poročilo treba uskladiti in preveriti z vsemi pomembnimi interesnimi in strokovnimi skupinami oz. subjekti. Komuniciranje in posvetovanje prispeva tudi k lažjemu razumevanju deležnikov, zakaj so potrebna določena dejanja ali ukrepi. Zagotovi tudi večjo objektivnost in nepristranskost analize ter poveča zaupanje v sklepe in izvedbo procesa.

Posvetovanje je lahko interno, priporočeno pa vključuje neodvisno evalvacijo, v obliki recenzije poročila in revizije procesa. Ob primerni stopnji zaupnosti in naravi poročila lahko evalvacija poteka tudi javno, z javno objavo osnutka in vključevanjem širše javnosti ter civilne družbe v razpravo. V ta namen so uporabne fokusne skupine, tehnika Delfi ali ankete. Zbrane povratne informacije je treba skrbno proučiti in upoštevati pri morebitnih popravkih in pripravi zaključne verzije poročila.

IV.D Odobritev

Zaključna verzija poročila mora biti formalno potrjena. Dokument se predloži vodstvenemu subjektu, ki se z njim seznani in ga sprejme. Pred tem se lahko za odločevalca izvede tudi predstavitev izsledkov.

Določijo se tudi stopnja zaupnosti poročila in pravice dostopanja. Po potrditvi sledi posredovanje poročila vsem interesnim subjektom s pravicami dostopa. Cilj je zagotoviti, ustrezno obveščenost in seznanjenost vseh, ki te informacije potrebujejo za odločanje in koordiniranje ukrepanja za obvladovanje tveganj/ogroženosti.

Ob primerni stopnji zaupnosti in naravi poročila je priporočena javna objava poročila ali izsledkov.

V Odločanje

V tej fazi sledi proces odločanja na podlagi potrjenih rezultatov in ugotovitev postopka ocene. *Namen je pripraviti načrt ukrepanja, ki bo zagotovil sprejemljivo raven ogroženosti/tveganj oz. pripravljenost na ogrožajoče nevarnosti in podlago za ukrepanje odgovornim subjektom.* Odločanje vključuje presojanje, katere grožnje/tveganja zahtevajo odziv, na kakšen način in pripravo akcijskega načrta. Ta faza vključuje pretežno načrtovalne odločitve.

Rezultat faze:

- Odločitve o naslavljanju groženj/tveganj;
- Načrti obravnave prednostnih groženj/tveganj;
- Akcijski načrt.

Odgovorni subjekti:

- Odločevalci v sodelovanju z odgovornimi subjekti za ukrepanje, izvajalci (analitiki) in področnimi strokovnjaki.

Predlagane tehnike:

- Tehnike za analizo kontrol (T4);
- Tehnike za ocenjevanje pomembnosti tveganja (T8).

V.A Odločanje o obravnavi

Na podlagi končnih ocen in stopenj se vse grožnje/tveganja razvrstijo v hierarhijo pomembnosti oz. kritičnosti. Razvrščanje naj bo izvedeno na osnovi stopnjevalnega merila, od najmanj do najbolj visoke ocene ali obratno. S tem se zagotovi preglednost nad rezultati in omogoča hitro prepoznavanje groženj/tveganj, ki so kritičnega pomena in predstavljajo prioriteto. Zatem se presodi (ne)sprejemljivost posamezne grožnje/tveganja. Namen presoje sprejemljivosti je podpreti odločanje o načinu odziva.

Ocene se primerjajo z vnaprej določenimi merili (I.D), da se ugotovi, kje je potrebno ukrepanje oz. ali je grožnjo/tveganje treba nasloviti ali pa je nasprotno, sprejemljivo.

Na podlagi ocene (ne)sprejemljivosti se nato sprejme odločitev o načinu ukrepanja, kar vključuje več možnosti, od nereagiranja do različnih načinov naslavljanja. Pri odločanju glede načina naslavljanja groženj/tveganj so na voljo naslednje možnosti:

- izogibanje (odločitev, da se dejavnost, ki ustvarja ogroženost/tveganje, ne bo nadaljevala oz. da se bo odstranila ogrožena dobrina/tarča – v primeru, ko je ogroženost/tveganje nesprejemljivo, dejavnost ali dobrina pa je nepomembna);
- sprejem/ohranjanje (odločitev, da se ukrepi za zmanjševanje ne bodo izvajali, temveč se bo spremljalo stanje ogroženosti/tveganja – v primeru, ko je grožnja/tveganje sprejemljivo ali pa se želi izkoristiti priložnost);
- obravnava (odločitev, da se bodo izvedli ukrepi, ki bodo vplivali na zmanjševanje ogroženosti/tveganja – v primeru, ko je tveganje nesprejemljivo), kar lahko vključuje odstranitev vira ogroženosti/tveganja; vplivanje na verjetnost; vplivanje na posledice; deljenje ogroženosti/tveganja (skozi zavarovanja, pogodbe, prenos odgovornosti).

Prednostno se morajo nasloviti grožnje/tveganja, ocenjene z visoko stopnjo, zatem tista, ki so srednje vrednosti, nizke stopnje pa se navadno v kratkoročnem ali srednjeročnem obdobju ne obravnavajo, temveč zgolj spremljajo.

V.B Izbira ukrepov

Za tveganja in grožnje, ki so prednostne narave oz. za katera je bila sprejeta odločitev glede obravnave, je treba opredeliti smiselne in učinkovite ukrepe. V ta namen je treba definirati merila (npr. zahtevnost, izvedljivost, sredstva oz. stroški, predviden učinek na tveganje), ki jih morajo ukrepi izpolnjevati. Pri tem je poleg vidika učinkovitosti treba upoštevati tudi pravne vidike, stališča deležnikov, socioekonomske in okoljske vidike. Zatem je treba oblikovati nabor možnih alternativ ukrepov (izhodišče za to so rezultati analize GAP (III.B.2; III.E.2)); primerjati alternative glede na merila in izbrati najboljšo alternativo.

Končni cilj izbora ukrepov je zagotoviti zmanjšanje tveganja na sprejemljivo raven ob upoštevanju stroškovne učinkovitosti in zakonodajnih zahtev (ob upoštevanju posledic).

Na podlagi izbranih ukrepov se za vsako posamezno grožnjo/tveganje, ki je prednostne narave, pripravi načrt obravnave. Načrti obravnave morajo opisati, kakšne so identificirane ranljivosti in kako je treba obravnavati grožnje/tveganja, da se izpolnijo merila za sprejemljivost. Za vodstvo je pomembno, da pregledajo in odobrijo predlagane načrte obravnave in posledično preostalo ogroženost/tveganje ter zabeležijo vse pogoje, povezane s tako odobritvijo.

**Opomba:* V primeru, da gre za dobro poznane in konstantne grožnje/tveganja, ki jih ni mogoče odpraviti in so stvar rednega presojanja, je smiselno vnaprej okvirno opredeliti nabor ukrepov, vezanih na oceno oz. stopnjo ogroženosti/tveganosti.

V.C Priprava akcijskega načrta

Na osnovi sprejetih odločitev glede naslavljanja groženj/tveganj in načrtov obravnave prednostnih groženj/tveganj odločevalec pripravi in potrdi načrt ukrepanja, z natančno opredeljeno časovnico in odgovornimi subjekti (za izvedbo načrta in posameznih ukrepov; za nadzor in spremljanje).

Rezultat se izkaže v obliki akcijskega načrta, pri pripravi katerega naj sodelujejo vsi vpleteni (odgovorni za izvajanje ukrepov) in zainteresirani deležniki.

VI Spremljanje in vzdrževanje

Ko je proces analize in izdelave ocene zaključen, sledijo postanalitične dejavnosti oz. faza spremljanja in vzdrževanja, ki je konstantna in del širšega procesa upravljanja ogroženosti/tveganj. *Namen je zagotoviti uspešnost in učinkovitost dejavnosti ter ukrepov, določenih v okviru analize in ocene, ohranjati aktualno znanje o grožnjah/tveganjih ter kontinuirano razvijati proces analiziranja ter ocenjevanja.* Ta faza vključuje pretežno poročevalske, nadzorstvene in načrtovalne dejavnosti.

Rezultat faze:

- Obdobna poročila o pregledih;
- Obdobna poročila o napredku.

Odgovorni subjekti

- Nadzorniki in pristojni za izvajanje ukrepov v sodelovanju z odločevalci.

V okvir upravljanja ogroženosti/tveganj sicer sodi skupek številnih dejavnosti in odgovornosti, z vidika procesa analize in ocene pa je pomembno, da se izvajajo redni pregledi in nadzorstvo. Spremljati je treba ustreznost izvajanja ukrepov, učinke izvedenih ukrepov ter ugotavljati njihov vpliv na obvladovanje oz. zmanjševanje groženj/tveganj. V ta namen morajo odgovorni izvajalci beležiti in poročati o izvajanju načrtovanih ukrepov.

Ogroženost in tveganja je treba stalno spremljati in jih ocenjevati na periodični ravni. S tem se ugotavljajo spremembe v stanju oz. gibanju (rast/upad/stagnacija) ranljivosti in ogroženosti ter ugotavlja pojav morebitnih novih groženj. V primeru, da ukrepi ne dosegajo želenih vplivov, so potrebne korekcijske odločitve.

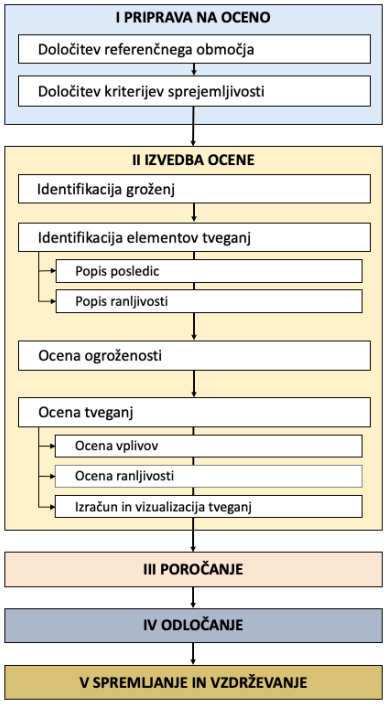
Obenem je treba ocenjevati uspešnost in učinkovitost uporabljene metodologije in jo po potrebi posodabljati, tudi v smeri zagotavljanja večje objektivnosti. Je pa treba upoštevati, da večje spremembe v metodologijah lahko onemogočijo primerljivost rezultatov čez čas in vplivajo na rezultate ocen, zato naj bodo spremembe nujne in premišljene.

Odgovornosti za spremljanje in pregledovanje morajo biti jasno in natančno določene, prav tako časovnica izvajanja.

Analize in ocene naj se izvajajo vsaj enkrat letno oz. ob vsaki spremembi, ki potencialno vpliva na stanje ogroženosti/tveganja. Spremembe se ugotavljajo vsaj na polletni ravni, pregledi učinkov oz. vplivov ukrepov pa na četrtletni. Izsledki pregledov se predstavijo v obdobnih poročilih, s katerimi se morajo seznaniti vodstveni subjekti in vsi ključni deležniki.

7.3 Model za ocenjevanje ogroženosti/tveganja na področju javne varnosti – skrajšani postopek

Zaradi kompleksnosti modela in nekaterih korakov ter potreb po optimizaciji izvedbe ocen predlagamo tudi *skrajšani model za ocenjevanje ogroženosti/tveganja na področju javne varnosti*. Če zaradi časovnih, stroškovnih, kadrovskih ali drugih primanjkljajev ocene po standardnem postopku ni možno izvesti, se sledi predlogu skrajšanega postopka. V skrajšanem postopku izvajalec nekatere faze, korake in podkorake zaradi njihove obsežnosti, stroškovne, kadrovske ali druge zahtevnosti oz. obremenitve izpusti in/ali prilagodi.



Slika 16: Model za ocenjevanje ogroženosti/tveganja na področju javne varnosti – skrajšani postopek

Enako kot standardni model skrajšani model predstavlja praktično orodje za izvajalce (analitike) in je zasnovan v obliki navodila, ki omogoča izvedbo ocene skozi analitično in sistematično zasnovan proces, skozi katerega se odločevalcem zagotovi ustrezna informacijska podpora za odločanje. Za razliko od standardnega modela je

osredotočen le na najbolj bistvene faze, korake in podkorake, ki so pomembni za pripravo kakovostne ocene ogroženosti/tveganja. Za podrobnejše prikaze rezultatov, odgovornosti in morebitna dodatna pojasnila ali prilagoditve, se upoštevajo razlage faz in korakov v Podpoglavju 7.2 (Standardni model). V primeru, če se izvaja zgolj oceno ogroženosti, se v skrajšanem postopku izpusti dva koraka: »Identifikacija elementov tveganj« in »Ocena tveganj«. Skrajšani postopek je skupaj z vsemi fazami, koraki in podkoraki predstavljen v tej prilogi (grafična predstavitev modela je razvidna na sliki 16).

I Priprava na oceno

V tej fazi se zagotovi razumevanje zunanjega in notranjega konteksta procesa ocene. *Namen je zastaviti temelje in izhodišča za vse nadaljnje faze in korake procesa.*

I.A Določitev referenčnega območja

V določitvi referenčnega območja se določita *območna dimenzija* in *časovna dimenzija* za analizo in oceno.

Pri območni dimenziji se opredeli geografski obseg analize oz. določi, ali se bo ocena opravljala za območje celotne države (nacionalna ocena), širšega teritorialnega območja (regionalna ocena), lokalne skupnosti (lokalna ocena) ali se bo nanašala na posamezno organizacijo oz. njene dobrine (organizacijska ocena). V tem delu se opišejo tudi splošne značilnosti izbranega območja (demografija in prebivalstvo, okolje, gospodarstvo, infrastruktura in oskrba). Alternativno lahko območje ostane *nedoločeno*.

Zatem se določi še ročnost ocene oz. časovno obdobje, na katero bo osredinjena analiza. Ocena se lahko nanaša na kratkoročno obdobje (do enega leta), srednjeročno (do tri leta), dolgoročno (do pet let). V primerih globalnih perspektiv (npr. tudi pri ocenjevanju hipotetičnih groženj) se lahko ocena nanaša na dogodke, oddaljene do 35 let, praviloma pa se nanaša na grožnje, ki imajo potencial v naslednjih petih letih. Ročnost ocene je tesno povezana z uporabnostjo končnih rezultatov ocen. Nižja, kot je odločevalska raven v hierarhiji, krajša je ročnost ocene. Če so denimo rezultati namenjeni podpori aktualnemu operativnemu delovanju, se analizira ogroženost/tveganje za krajše obdobje; če pa so ocene namenjene podpori strateškemu odločanju in upravljanju pa je zajeto daljše časovno obdobje.

I.B Določitev kriterijev sprejemljivosti ogroženosti/tveganja

V pripravi na oceno je treba vnaprej določiti tudi kritične meje končne ocene. Opredelijo se merila, po katerih se bo v fazi odločanja presojalo, ali je ocenjena ogroženost/tveganje sprejemljivo ali ne. Merila lahko poleg stopenj ogroženosti/tveganja (npr. zelo nizke in nizke stopnje so sprejemljive), vključujejo tudi druge vidike (npr. stroške, zakonske zahteve, življenjske, socialno-ekonomske in okoljske faktorje). (Ne)izpolnjevanje meril vodi torej v oceno (ne)sprejemljivosti in ugotovitev, ali je potrebno ukrepanje.

II Izvedba ocene

II.A Identifikacija groženj

Ta korak je praviloma osredotočen na zbiranje in predstavljanje podatkov, ki so vezani na zunanje dejavnike oz. dejavnike groženj.

Izvajalec identificira vse možne vire in s tem povezane realne grožnje, ki so smiselne in izpolnjujejo merila, zastavljena v splošnem okviru ocene. Namen je zagotoviti ustrezno situacijsko zavedanje in pridobiti celosten pregled nad potencialnimi ogrožajočimi situacijami oz. nevarnostmi v obliki »kataloga realnih groženj«. Končni produkt tega koraka je »katalog« vseh relevantnih realnih groženj, ki so lahko tudi gručene po vsebinsko povezanih kategorijah.

Če se grožnje vežejo na točno določene dobrine oz. v primerih, ko je cilj ugotoviti, katere grožnje ogrožajo točno določene dobrine (npr. zoper določen objekt), se pred identifikacijo groženj izvede še popis dobrin. Tarče so dobrine ali vrednote oz. cilji posameznih groženj, torej tisti vidiki, ki jih varujemo ali želimo obvarovati. V primeru, ko dobrin ni mogoče jasno popisati ali to ni smiselno, se ta korak preskoči. Dobrine se lahko smiselno gručijo. Med elemente (gruče) lahko primeroma prištevamo cilje, procese in sredstva organizacije, objekte, temeljne družbene funkcije, premoženje, življenje, zdravje, delovanje države in njenih organov, gospodarstvo (npr. BDP), družbene vrednote (npr. varnost, demokracija, človekove pravice) in/ali okolje.

II.B Identifikacija elementov tveganj

II.B.1 Popis posledic

Izvajalec za vsako posamezno realno grožnjo popiše možne posledice (tj. vplivi in negativni učinki), ki bi jih uresničena grožnja lahko povzročila. Upoštevajo se potencialne posledice tako v notranjem kot tudi zunanjem okolju.

Posledice se lahko vsebinsko gručijo, pri čemer primere gruč posledic predstavljajo npr. vplivi na delovanje organizacije (njene zmogljivosti, procese, infrastrukturo, procese, poslovanje ipd.), države ali skupnosti, človeški vplivi oz. vplivi na življenje in zdravje, ekonomski in gospodarski vplivi, vplivi na okolje, politični in družbeni vplivi, psihološki in humanitarni vplivi.

II.B.2 Popis ranljivosti

Izvajalec za vsako posamezno realno grožnjo popiše tudi ranljivosti (tj. šibke točke, ki spodbujajo ali omogočajo uresničitev grožnje). Popis ranljivosti se lahko vsebinsko gruči po področjih (npr. ranljivosti na operativni, nadzorstveni, okoljski, upravljavski, sistemsko politični, normativni in zakonodajni ravni).

Popis ranljivosti naj konkretno obsega:

- popis okoliščin, ki ustvarjajo ranljivost območij/lokacij, skupnosti, področij, procesov, subjektov, sistemov, sektorjev, sredstev, premoženja, objektov;
- popis priporočenih ukrepov (preventivnih in reaktivnih); ter
- popis obstoječih ukrepov/kontrol/dejavnosti/zmogljivosti/dostopnosti opreme in sredstev.

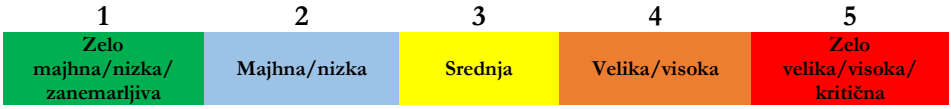
II.C Ocena ogroženosti

Ocena ogroženosti se nanaša na presojo verjetnosti, da se bo v določenem časovnem obdobju in v določenem prostoru uresničila določena grožnja.

Če je to smiselno, se presoja verjetnosti veže na določene dobrine/tarče, za katere se presoja ogroženost. Dobrine se vrednotijo glede na njihovo pomembnost/kritičnost oz. vrednost za organizacijo, državo ali skupnost. Ocena se praviloma poda na tri- do petstopenjski ordinalni lestvici (zelo nizka do zelo visoka pomembnost). Ocena dobrin se v postopku ocene ogroženosti upošteva ali kot indikator ali pa kot podporna informacija v odločanju glede načina naslavljanja ogroženosti. V primeru ocene tveganj se lahko ocena dobrin upošteva pri izračunu stopnje tveganja.

Ogroženost oz. verjetnost se presoja za vsako identificirano realno grožnjo. Ocena ogroženosti prioritetno izraža verjetnost, da se bo grožnja uresničila ob upoštevanju njenega potenciala.

Končna ocena ogroženosti se praviloma izrazi s pomočjo ordinalne lestvice, ki določa stopnje ogroženosti. Lestvica ima lahko različno število stopenj, najpogosteje so v uporabi tri- in petstopenjske lestvice (slika 17). Ko izvajalec razpolaga z bolj zanesljivimi podatki, se predlaga lestvica z več stopnjami (navadno petstopenjska), v primeru manj zanesljivih podatkov pa lestvica z manj stopnjami (navadno tristopenjska). Vsaka stopnja ima svojo vrednost, ki jo spremlja kvalitativen in/ali kvantitativen opis.



Slika 17: Primer ocene ogroženosti

Skladno z vsebino in naravo ocene ogroženosti izvajalec določi kvalitativni opis. Za najnižjo stopnjo (ocena 1) tako določi eno izmed možnosti: *ni možnosti, da bi se grožnja uresničila*; *ni skoraj nobene nevarnosti; verjetnost je neznatna*; *dogodek se zgodi zelo redko*. Na drugi skrajnosti lestvice (ocena 5) pa določi eno izmed naslednjih možnosti: *takojšnja nevarnost grožnje; visoka neposredna ogroženost; dogodek se dogaja zelo pogosto oz. redno; ni dvoma, da se bo grožnja uresničila*.

Kvalitativne opise lahko spremljajo tudi kvantitativne vrednosti, kot sta npr. *verjetnost pojava v letih* (npr. enkrat na več kot 100 let) in *verjetnost pojava na letni ravni* v relativnem deležu (letna verjetnost je manj kot 1 %). V primeru zanesljivih, statističnih podatkov ali preteklih izkušenj se predlaga kvantitativno vrednotenje verjetnosti uresničitve grožnje.

II.D Ocena tveganj

Za pridobitev ocene tveganja je v izračunu treba kombinirati ocene različnih elementov, zato je te elemente (vplive, ranljivosti) treba sprva oceniti.

II.D.1 Ocena vplivov

Z oceno vplivov se presodi velikost oz. resnost posledic, ki bi nastale ob uresničeni grožnji. S tem se pravzaprav ovrednoti nevarnost tveganja. V oceno se zajamejo vse identificirane posledice.

Proces ocene vpliva sestoji iz več korakov. V prvem koraku se ocenjujejo posledice za vsak posamezni vpliv znotraj gruč vplivov (tj. *Ocena posledic*). V drugem koraku se vpliv izračuna na ravni vsake gruče s povprečenjem ocen znotraj gruče. V tretjem koraku se izračuna končna ocena vpliva tveganja s povprečenjem ocen gruč (tj. *Ocena vpliva*). Ocenjuje se torej več vrst gruč vplivov in konkretnejši vplivi znotraj teh gruč.

Ocenjevanje posledic in vpliva poteka na tri- do petstopenjski ordinalni lestvici, ki lahko vključuje zgolj kvalitativne indikatorje, zgolj intervale kvantitativnih ocen ali kombinacijo obojega. V primeru kvalitativnega ocenjevanja izvajalec oceno poda opisno (npr. lestvično z opisi), v primeru kvantitativnega pa je ocena podana v realnih številih (npr. število prizadetih enot, stroški, čas trajanja). Število stopenj na lestvici mora biti enotno za vse posamične vplive in njihove gruče (slika 18).

1	2	3	4	5
Nepomemben /zelo majhen	Omejen /majhen	Zmeren /srednji	Pomemben /velik	Zelo pomemben /kritičen

Slika 18: Primer ocene posledic in ocene vpliva.

II.D.2 Ocena ranljivosti

Z oceno ranljivosti se presodi lastna dovzetnost za uresničitev grožnje in zmožnosti obstoječih ukrepov (poimenovano tudi kot ocena kontrolnega okolja), da prepoznajo ali preprečijo uresničitev grožnje.

Ranljivost se lahko izrazi v stopnji izpostavljenosti ali stopnji zaščite. Za oceno se uporabijo tri- do petstopenjske ordinalne lestvice. Za pridobitev končne ocene je možno oceniti vsako ranljivost in gručo posebej ter ocene nato povprečiti kot v primeru ocene vplivov.

Alternativno se lahko končna ocena določi tudi na podlagi določanja meril, ki morajo biti izpolnjena za umestitev v določeno stopnjo. V tem primeru posamezne stopnje ranljivosti spremlja opis, kateri dejavniki (šibke točke ali odsotnost ukrepov) so na posamezni stopnji prisotni/odsotni in vplivajo na oceno. Primer petstopenjske lestvice je predstavljen na sliki 19.

1	2	3	4	5
Zelo nizka ranljivost/Zelo visoka zaščita	Nizka ranljivost/Visoka zaščita	Srednja ranljivost/zaščita	Visoka ranljivost/Nizka zaščita	Zelo visoka ranljivost/Zelo nizka zaščita

Slika 19: Primer ocene ranljivosti

II.D.3 Izračun tveganj

Izvajalec pripravi izračun tveganja. Možne so različne kombinacije naslednjih postavk:

- ocena ogroženosti (verjetnost uresničitve);
- vrednost dobrine;
- vpliv;
- ranljivost.

Izračun se tipično pripravi ali z množenjem ocen elementov in rangiranjem tveganj (tabela 42) ali pa s pomočjo t. i. prevajalnih tabel (tabeli 43 in 44). Izračun predstavlja podlago za oceno, ki je navadno predstavljena na tri- do petstopenjski ordinalni lestvici. V nadaljevanju predstavljeni izračuni rangov in vrednosti v prevajalnih tabelah izvajalcu pomagajo oz. omogočajo določitev končne ocene, so pa tovrstni primeri prilagodljivi (prilagoditve so denimo možne v razponu ocen posameznih elementov tveganja, razponu stopenj tveganja).

V primeru *pristopa z množenjem ocen elementov in rangiranjem* izvajalec za vsako tveganje (ali scenarij) v tabelo vnese oceno posameznih elementov tveganj (npr. kombinacija verjetnosti, ranljivosti in vrednosti dobrine; ali vpliva in verjetnosti). Ocene se zmnožijo, rezultat pa vnese v stolpec »Izračun«. Na podlagi izračunanih vrednosti se določi rang za posamezno grožnjo. Višja ocena pomeni tudi višjo prioriteto. Na podlagi izračunanih vrednosti se določi še stopnja tveganja.

Tabela 42: Primer izračuna tveganj z množenjem ocen in rangiranjem (izračunana vrednost med 1 in 21 predstavlja *zelo nizko tveganje*, od 22 do 42 *nizko tveganje* od 43 do 83 *srednje tveganje*, 84 do 104 *visoko tveganje* in 105 do 125 *zelo visoko*).

	Verjetnost (1–5)	Ranljivost (1–5)	Vrednost (1–5)	Izračun (1–125)	Rang	Stopnja
Tveganje 1	1	3	4	12	4	Zelo nizko
Tveganje 2	2	2	2	8	5	Zelo nizko
Tveganje 3	3	4	5	60	2	Srednje
Tveganje 4	5	5	5	125	1	Zelo visoko
Tveganje 5	3	5	3	45	3	Srednje

V primeru *pristopa s pomočjo prevajalnih tabel* izvajalec izbere tabelo glede na število ocenjenih elementov tveganj. Izvajalec izbere npr. pristop, ki je predstavljen na tabeli 43.

Prevajalna tabela (tabela 43) prikazuje primer, v katerem se (tipično) kombinirajo ocene verjetnosti (1–5) in vpliva (1–5). Vrednosti tveganj se gibljejo v razponu med 0 in 8. Konkretni primer predlaga, da vrednosti 0–2 predstavljajo nizko tveganje, vrednosti 3–5 predstavljajo srednje tveganje in 6–8 predstavljajo visoko tveganje. Izvajalec lahko sam določi, katere vrednosti zanj predstavljajo katero stopnjo tveganja, pri čemer morajo ocene v številih ostati nespremenjene.

Primer uporabe prevajalne tabele (tabela 43):

- V primeru, ko je verjetnost ocenjena z oceno srednje (2), vpliv pa z oceno 4 (visoko), je končni izračun ocena 4, kar predstavlja oceno *srednje tveganje*.

Tabela 43: Primer prevajalne tabele (0–2: nizko tveganje; 3–5: srednje tveganje; 6–8: visoko tveganje).

	Verjetnost	1	2	3	4	5
Vpliv	1	0	1	2	3	4
	2	1	2	3	4	5
	3	2	3	4	5	6
	4	3	4	5	6	7
	5	4	5	6	7	8

Enako velja v drugem primeru prevajalne tabele (tabela 44), pri čemer se kombinirata dve oceni (tipično ocena vpliva in ocena verjetnosti). Pri tem tabela 44 predstavlja štiri stopnje (nizko, srednje, visoko, zelo visoko).

Tabela 44: Primer prevajalne tabele 2 (zelena barva: nizko tveganje; rumena barva: srednje tveganje; oranžna barva: visoko tveganje; rdeča barva: zelo visoko tveganje).

	Verjetnost	1	2	3	4	5
Vpliv	1					
	2					
	3					
	4					
	5					

Primer uporabe prevajalne tabele (tabela 44):

- V primeru, ko je vpliv ocenjen z oceno *srednje* (3), verjetnost pa z oceno *nizko* (2), je končna ocena tveganja *visoko* (oranžna).

Končno oceno tveganj izvajalec predstavi v vizualizirani obliki. Vizualizacija zagotovi preglednost ocen, primerjavo med različnimi tveganji in predstavi rezultate na enostaven ter razumljiv način. Obstaja več načinov vizualizacije, npr. vizualizacija v tabelah, v diagramih, matrikah, zemljevidih. Način vizualizacije izbere izvajalec sam. Tabela 45 prikazuje primer vizualizacije s pomočjo matrike, ki temelji na prevajalni tabeli in jo običajno sestavljata dve osi. V tem primeru izvajalec vsako ocenjeno grožnjo vstavi v ustrezno celico.

Tabela 45: Vizualizacija ocene tveganj v obliki matrike.

	Verjetnost	1	2	3	4	5
Vpliv	1					
	2					Grožnja 2
	3		Grožnja 1			
	4					
	5				Grožnja 3	

Vizualizacijo tveganj navadno spremljajo podporne informacije (npr. legende in informacije o zanesljivosti/kakovosti podatkov, virov).

III Poročanje

V tej fazi se pripravi predstavitev rezultatov tretje faze. *Namen je zagotoviti ustrezno sledljivost postopku, obveščenost oz. informiranost vseh ključnih deležnikov in podlago za odločanje.* Pripraviti je treba strukturiran sistem ustvarjene dokumentacije in pregledno, razumljivo ter jasno poročilo o vseh rezultatih in ključnih izsledkih ocene, ki je usklajeno z interesnimi skupinami in potrjeno na odločevalski ravni.

Univerzitetna založba
Univerze v Mariboru

8 Pripomočki

Pripomoček I: Tehnike zbiranja, analiziranja in predstavlja podatkov pri ocenjevanju ogroženosti/tveganja

Tehnike so predstavljene v tabelah 46–47. Deloma so povzete po standardu IEC 31010:2019.

Denotacija	Kategorija
T1	Tehnike za pridobivanje mnenj od deležnikov in strokovnjakov (**T1**)
T2	Tehnike za identifikacijo tveganj (**T2**)
T3	Tehnike za ugotavljanje virov, vzrokov in gonilnikov tveganja (**T3**)
T4	Tehnike za analizo kontrol (**T4**)
T5	Tehnike za razumevanje posledic in verjetnosti (**T5**)
T6	Tehnike za analizo odvisnosti in interakcij (**T6**)
T7	Tehnike, ki omogočajo meritve tveganja (**T7**)
T8	Tehnike za ocenjevanje pomembnosti tveganja (**T8**)
T9	Tehnike za izbiranje med možnostmi (**T9**)
T10	Tehnike za beleženje in poročanje (**T10**)

Tabela 46: Tehnike zbiranja podatkov

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T1	***Brainstorming***	Tehnika, ki se uporablja za spodbujanje razmišljanja.	pridobivanje mnenj	brez	kvalitativna	nizka	od nizka do srednja
T1	**tehnika Delfi**	Zbiranje mnenj strokovnjakov s pomočjo niza zaporednih vprašalnikov. Ljudje sodelujejo posamezno, vendar po vsakem prejmejo povratne informacije o odzivih drugih posameznikov. Mnenja se zbirajo do doseženega soglasja med udeleženci.	pridobivanje mnenj	brez	kvalitativna	srednja	srednja
T1	**Intervjuji**	Strukturirani ali polstrukturirani individualni pogovori s strokovnjaki ali drugimi deležniki za pridobivanje različnih mnenj.	pridobivanje mnenj	brez	kvalitativna	srednja	visoka
T1	**Temeljna skupinska tehnika (NGT)/tehnika nominalnih skupin**	Tehnika pridobivanja stališč skupine ljudi, pri kateri sprva udeleženci sodelujejo individualno – brez interakcije z drugimi, nato pa sledi skupinska razprava o idejah.	pridobivanje mnenj	brez	kvalitativna	nizka	srednja
T1	**Ankete**	Vprašalniki v papirnati ali elektronski obliki za pridobivanje mnenj in stališč.	pridobivanje mnenj	majhna	kvalitativna	visoka	srednja
T1	**Fokusne skupine**	Strukturirani ali polstrukturirani pogovori s skupino strokovnjakov z namenom pridobivanja mnenj skozi soglasje.	pridobivanje mnenj	brez	kvalitativna	srednja	visoka
T1	**Q-metodologija**	Raziskuje različna mnenja ljudi, ki zavzemajo različna stališča glede določene zadeve.	pridobivanje mnenj	brez	kvalitativna	srednja	visoka

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T1	**Spletno luščenje podatkov (*web scraping*)**	Tehnika prebiranja in iskanja podatkov po delno strukturiranih spletnih dokumentih.	identifikacija tveganja	velika	mešana	visoka	visoka
T2	**Študija nevarnosti in operativnosti (HAZOP)**	Strukturiran in sistematičen pregled načrtovanega ali obstoječega procesa za identifikacijo in vrednotenje težav, ki bi lahko predstavljale tveganje za osebje ali opremo.	identifikacija tveganja, analiza tveganja	srednja	kvalitativna	od srednja do visoka	od srednja do visoka
T2	**Analize scenarijev**	Identifikacija možnih scenarijev skozi izkušnje, domišljijo, ekstrapolacijo ali modeliranje. Tveganje je nato določeno za vsakega od scenarijev.	identifikacija tveganja	od majhna do srednja	kvalitativna	od nizka do srednja	srednja
T2	**Strukturirana »kaj, če?« tehnika (SWIFT)**	Poenostavljena verzija tehnike HAZOP, kjer se opredeljujejo deviacije od pričakovanega skozi »kaj, če?« analizo.	identifikacija tveganja	srednja	kvalitativna	od nizka do srednja	srednja
T2	**Analiza možnih napak in njihovih posledic (FMEA)**	Analiza načinov, kako lahko vsaka komponenta sistema odpove ter vzroke in posledice okvare.	identifikacija tveganja	odvisna od namena	mešana	od nizka do visoka	srednja
T2	**Kontrolni seznami klasifikacije, taksonomije**	Seznami, ki temeljijo na izkušnjah ali na konceptih in modelih, ki jih je mogoče uporabiti za pomoč pri prepoznavanju tveganj ali nadzora.	identifikacija tveganj ali kontrol	velika	kvalitativna	od nizka do srednja	od nizka do srednja
T3	**Cilindrični pristop**	Upošteva cilje, vrednote, pravila, podatke in modele deležnikov ter ugotavlja nedoslednosti, nejasnosti, opustitve in neznanje.	identifikacija povzročiteljev/ virov tveganja	majhna	kvalitativna	visoka	srednja

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T3	**Diagram vzrokov in rezultatov po Ishikawi (*fishbone analysis*)**	Opredeljuje dejavnike, ki prispevajo k določenemu izidu (želenemu ali neželenemu). Dejavniki so običajno razdeljeni v vnaprej določene kategorije in prikazani v drevesni strukturi ali diagramu ribje kosti.	analiza vzrokov	majhna	kvalitativna	nizka	od nizka do srednja

Tabela 47: Tehnike analiziranja podatkov

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T4	**Analiza plasti zaščite (LOPA)**	Analizira zmanjšanje tveganja, ki ga je mogoče doseči z različnimi plastmi zaščite.	analiza kontrol	srednja	mešana	od srednja do visoka	od srednja do visoka
T4	**Analiza tveganja in ugotavljanja kritičnih kontrolnih točk (HACCP)**	Analiza zmanjšanja tveganja, ki ga lahko dosežemo z različnimi plastmi zaščite.	analiza kontrol	srednja	kvalitativna	srednja	srednja
T4	**Analiza »*Bow tie*«**	Oblika opisa poti od virov tveganja do rezultatov in za pregled kontrol v obliki diagrama.	analiza tveganj in kontrol	majhna	mešana	nizka	nizka
T5	**Analiza vpliva na poslovanje**	Proces BIA (ang. *business impact analysis*) analizira posledice potencialnega incidenta na organizacijo, ki določa prioritete obnovitve izdelkov in storitev organizacije in s tem prednostne naloge dejavnosti in virov, ki jih zagotavljajo.	analiza posledic, analiza kontrol	srednja	mešana	srednja	nizka
T5	**Drevesna analiza dogodkov (ETA)**	Analiza frekvenc in verjetnosti različnih možnosti iz modela, ki izhaja iz začetnega dogodka.	analiza posledic, analiza kontrol	od majhna do srednja	mešana	srednja	srednja
T5	**Bayesova analiza**	Metoda za sklepanje o parametrih modela z uporabo Bayesovega teorema omogoča vključitev empiričnih podatkov v napovedovanje verjetnosti.	analiza verjetnosti	srednja	kvantitativna	srednja	visoka

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T5	**Markova analiza**	Izračun verjetnosti, da bo sistem, ki je sposoben biti v enem od številnih stanj, v točno določenem stanju ob točno določenem stanju v prihodnosti.	analiza verjetnosti	od srednja do velika	kvantitativna	srednja	visoka
T5	**Analiza dreves odpovedi (FTA)**	Analizira vzroke dogodkov z uporabo Booleove logike za opis kombinacije napak. Različice vključujejo drevo uspeha, kjer je potreben izvorni dogodek, in drevo vzrokov, ki se uporablja za raziskovanje preteklih dogodkov.	analiza verjetnosti in vzrokov	velika	mešana	od srednja do visoka	odvisna od kompleksnosti
T5	**Vzročno-posledična analiza (CCA)**	Kombinacija analize dreves odpoved (ang. *fault tree analysis*) in analiza dreves dogodkov (ang. *event tree analysis*).	analiza vzrokov in posledic	od srednja do velika	kvantitativna	od srednja do visoka	od srednja do visoka
T5	**Ocena učinkov v zvezi z varstvom podatkov (DPIA)**	Analizira, kako bi različni dogodki lahko vplivali na zasebnost posameznikov ter opredeljuje in kvantificira zmožnosti, ki bi bile potrebne za zagotavljanje zasebnosti.	analiza vzrokov in posledic	srednja	kvalitativna	srednja	od srednja do visoka
T5	**Analiza človeške zanesljivosti (HRA)**	Nabor tehnik za prepoznavanje možnosti človeških napak in ocenjevanje verjetnosti neuspeha.	analiza vzrokov in posledic	srednja	mešana	visoka	od srednja do visoka
T5	**Monte Carlo simulacija**	Izračun verjetnosti izidov z izvajanjem več simulacij z uporabo naključnih spremenljivk.	analiza vzrokov in posledic	srednja	kvantitativna	srednja do visoka	visoka

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T5	**Besedilno rudarjenje (ang. *text mining*)**	Imenovana tudi kakovostna analiza besedil je kvantitativna obdelava besedil z različnimi tehnikami, kot na primer kategorizacija besedila, združevanje besedil v skupine, ekstrakcija koncepta/entitet, izdelava granularnih taksonomij, analiza občutkov.	evalvacija tveganja	velika	kvantitativna	visoka	visoka
T5	**Bayesove mreže/ diagrami vpliva**	Grafični model spremenljivk in njihovih vzročno-posledičnih razmerij, izraženih z verjetnostmi. Osnovna Bayesova mreža ima spremenljivke, ki predstavljajo negotovosti. Razširjena različica, znana kot diagram vpliva, vključuje spremenljivke, ki predstavljajo negotovosti, posledice in dejanja.	identifikacija tveganj, ocena tveganj, odločanje	srednja	kvantitativna	od srednja do visoka	visoka
T6	**Analiza navzkrižnih vplivov**	Ocena spremembe verjetnosti nastanka določenega niza dogodkov, ki so posledica dejanskega nastopa enega od njih.	analiza verjetnosti in vzrokov	od majhna do srednja	kvantitativna	od srednja do visoka	od srednja do visoka
T6	**Vzročno mapiranje**	Mrežni diagram, ki predstavlja dogodke, vzroke in posledice ter njihove odnose.	analiza vzrokov in posledic	srednja	kvalitativna	srednja	srednja
T7	**CVaR (pogojni VaR – Value at Risk)**	Imenovana tudi pričakovani primanjkljaj je merilo pričakovane izgube iz	mera tveganja	velika	kvantitativna	srednja	visoka

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
		finančnega portfelja v najslabših N % primerov.					
T7	**Toksikološka ocena tveganja**	Sosledje korakov, ki prevedejo do pridobitve ocene tveganja za ljudi ali ekosistem zaradi izpostavljenosti kemikalijam.	mera tveganja	visoka	kvantitativna	visoka	visoka
T7	**Model »Value at Risk«**	Finančna mera tveganja, ki za izračun vrednosti izgub uporablja predvideno porazdelitev verjetnosti izgub v stabilnih tržnih razmerah.	mera tveganja	visoka	kvantitativna	visoka	visoka
T8	**Paretov diagram**	Paretovo načelo (pravilo 80–20) pravi, da za mnoge dogodke približno 80 % posledic izvira iz 20 % vzrokov.	določanje prioritet	srednja	mešana	nizka	srednja
T8	**ALARP/SFAIRP**	Merila za določanje resnosti tveganja in načini za evalvacijo tolerance tveganja.	evalvacija tveganja	velika	mešana	visoka	visoka
T8	**Diagrami frekvenca/število**	Poseben primer grafa kvantitativnih posledic/verjetnosti, ki se uporablja za upoštevanje tolerance tveganja za človeška življenja.	evalvacija tveganja	velika	kvantitativna	visoka	visoka
T8	**Podatkovno rudarjenje (ang. *data mining*)**	Podatkovno rudarjenje je proces iskanja anomalij, vzorcev in korelacije znotraj velikih podatkovnih nizov za napovedovanje rezultatov s pomočjo različnih metod, kot so nevronske mreže,	evalvacija tveganja	velika	kvantitativna	visoka	visoka

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
		odločitvena drevesa in K-najbližji sosedi.					
T8	**V zanesljivost usmerjeno vzdrževanje (RCM)**	Ocena tveganja, ki se uporablja za opredelitev ustreznih nalog za vzdrževanje sistema in pripadajočih komponent.	evalvacija tveganja, analiza kontrol	srednja	mešana	od srednja do visoka	od srednja do visoka
T8	**Indici tveganja**	Ocena pomembnosti posameznih tveganj na podlagi ocen dejavnikov, za katere se domneva, da vplivajo na obseg tveganja.	primerjava tveganj	srednja	semikvantitativna	nizka	od nizka do srednja
T9	**AHP (analitični hierarhični proces)**	Ocena pomembnosti posameznih meril ali alternativ na podlagi medsebojne primerjave. Rezultati omogoča razvrščanje v hierarhijo in uteževanje.	primerjava in vrednotenje alternativ	srednja	semikvantitativna	srednja	nizka
T9	**Analiza stroškov in koristi**	V analizi se uporablja denar kot enota na lestvici za ocenjevanje pozitivnih in negativnih, materialnih in nematerialnih posledic različnih možnosti.	primerjava možnosti	od srednja do velika	kvantitativna	od srednja do visoka	od srednja do visoka
T9	**Analiza z odločitvenimi drevesi**	Uporablja drevesno vizualizacijo ali model odločitev in njihovih možnih posledic. Rezultati so običajno izraženi v denarnih sredstvih ali uporabnosti.	primerjava možnosti	od majhna do srednja	kvantitativna	srednja	srednja
T9	**Teorija iger**	Strateško odločanje za modeliranje vpliva odločitev različnih udeležencev v »igri«. Primer področja uporabe je	primerjava možnosti	velika	kvantitativna	od srednja do visoka	visoka

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
		lahko določanje cen na podlagi tveganja.					
T9	**Večkriterijska analiza (MCA)**	Primerja možnosti na način, da so kompromisi eksplicitni. Predstavlja alternativo analizi stroškov in koristi, ki pa ne potrebuje denarnih vrednosti, ki bi bili dodeljeni vsem vložkom.	primerjava možnosti	majhna	kvalitativna	od nizka do srednja	srednja

Tabela 48: Tehnike predstavljanja podatkov

Kategorija	Tehnika	Opis	Namen	Količina podatkov	Metoda	Zahtevnost	Znanja
T10	**Matrika »posledica/ verjetnost«**	Uporabljena za primerjavo posameznih tveganj na načina, da se izbere par posledica/verjetnost in jih prikaže na matriki s posledicami na eni osi in verjetnostjo na drugi.	Poročanje o tveganjih, evalvacija	srednja	mešana	nizka	od nizka do srednja
T10	**Registri tveganj**	Sredstva za beleženje informacij o tveganjih.	Poročanje o tveganjih, nadzorovanje in pregledovanje	od srednja do velika	mešana	srednja	od nizka do srednja
T10	**S-krivulje**	Sredstva za prikaz razmerja med posledicami in verjetnostjo njihove uresničitve.	Evalvacija in vizualizacija tveganj	od srednja do velika	mešana	srednja	od srednja do visoka

Pripomoček II: Ocenjevanje kakovosti

Postopek ocenjevanja varnostne ogroženosti/tveganj mora, v podporo razumevanju končnih rezultatov oz. ocen in odločanju, zajeti tudi oceno kakovosti podatkov in njihovih virov. Za presojanje kakovosti podatkov in virov so na voljo različni standardi in priporočila, med uveljavljene pa sodijo usmeritve NATO, ki se sicer primarno uporabljajo na obveščevalno-varnostnem področju in pri delu z obveščevalnimi informacijami, pogosto pa so upoštevane tudi na drugih področjih. Pri analiziranju in ocenjevanju varnostne ogroženosti/tveganj so namreč pogosto vključene tudi obveščevalne informacije, prav tako se pogosto pojavljajo podobne razmere kompleksnosti in nepredvidljivosti groženj in scenarijev.

Skladno z usmeritvami zavezništva NATO (STANAG 2511 iz leta 2003, NATO AJP 2.1 iz leta 2016) je treba kakovost informacij presoditi na osnovi dveh ločenih meril, in sicer: kredibilnosti in zanesljivosti (tabela 49).

Zanesljivost vira je konceptualno povezana z zaupanjem v vir informacij na osnovi preteklih izkušenj, medtem ko se *kredibilnost informacij* nanaša na to, koliko so nove informacije skladne s preteklimi poročili. Obe merili se presojata na petstopenjskih kvalitativnih lestvicah, pri vsaki pa je dodana možnost, da kakovosti ni mogoče oceniti (zadnja stopnja). Po oceni vsakega merila se poda končna, kombinirana ocena informacije, sestavljena iz obeh vrednosti.

Tabela 49: Usmeritve NATO za ocenjevanje kakovosti podatkov (prilagojeno po Irwin in Mandel, 2019)

Ocena	*Kredibilnost informacije*	*Opis*
1	Popolnoma kredibilna	Če je z zanesljivostjo mogoče trditi, da obstoječa informacija o isti zadevi izvira tudi iz drugega vira.
2	Verjetno resnična	Če neodvisnosti vira informacije ni mogoče zanesljivo potrditi, vendar sta kakovost in količina preteklih poročil lahko potrjeni.
3	Lahko je resnična	Čeprav ni mogoče zanesljivo potrditi visoke verjetnosti, nova informacija ne nasprotuje preteklim poročilom glede vzorcev oz. trendov.
4	Dvomljiva	Informacija se nagiba k nasprotnim ugotovitvam preteklih poročil glede vzorcev oz. trendov.
5	Neverjetna	Informacija pozitivno nasprotuje preteklim informacijam ali nasprotuje ugotovitvam preteklih poročil glede vzorcev oz. trendov.
6	Resnice ni mogoče oceniti	Nove informacije ni mogoče primerjati s preteklimi poročili o vzorcih oz. trendih.

Ocena	*Zanesljivost informacije*	*Opis*
A	Popolnoma zanesljiva	Informacija se nanaša na preizkušen in zaupanja vreden vir, na katerega se lahko prepričano zanesemo.
B	Navadno je zanesljiva	Informacija se nanaša na vir, ki se je v preteklosti izkazal za uspešnega, kljub temu pa v posamičnem primeru obstaja element dvoma.
C	Pretežno zanesljiva	Informacija se nanaša na vir, ki je bil v preteklosti občasno uporabljen in v katerega smo lahko v določeni meri prepričani.
D	Navadno ni zanesljiva	Informacija se nanaša na vir, ki je bil v preteklosti že uporabljen, ampak se je pogosto izkazal za nezanesljivega.
E	Nezanesljiva	Informacija se nanaša na vir, ki je bil v preteklosti že uporabljen in se je izkazal kot nevreden zaupanja.
F	Zanesljivosti ni mogoče oceniti	Informacija se nanaša na vir, ki v preteklosti še ni bil uporabljen.

Opisan pristop k ocenjevanju kakovosti informacij poda določen vpogled v njeno vrednost, vendar so s takšnim vrednotenjem povezani tudi določeni izzivi. Težava je v denimo v primerljivosti ocen (npr. kako se ocena A3 primerja z oceno B2) ali v nedefinitivnih pojasnilih k ocenam, kar prepušča ocenjevalcem veliko prostora za različne in subjektivne ocene. Izziv je tudi v tem, da sta zanesljivost in kredibilnost informacij lahko tudi multidimenzionalna konstrukta, ki sta odvisna od mnogih podmeril. Tako se v praksi pogosto uporablja zgolj ena ocena k vrednotenju kakovosti, kar lahko odpravi določene omenjene izzive; pojavljajo pa se tudi kompleksnejše razlage dimenzij oz. karakteristik, ki vplivajo na kakovost podatkov (za več informacij glej Irwin in Mandel, 2019).

V nadaljevanju sledi predstavitev kompleksnejše razčlembe dimenzij in atributov, povezanih z ocenjevanjem kakovosti informacij in virov na področju kriznega managementa (za več informacij glej Rogova, 2016).

Kakovost informacij je povezana z uporabno vrednostjo informacij za uporabnika in je rezultat kombinacije treh povezanih kategorij:

a) Kakovost informacijskega vira;
b) Kakovost vsebine informacij;
c) Kakovost predstavitve informacij.

Vsaka izmed teh kategorij je nadalje sestavljena iz več atributov.

a) Atributi **Kakovosti vsebine informacij** so:

1. **Razpoložljivost** (DA/NE – najpomembnejše merilo; če je informacija nerazpoložljiva, ostali atributi niso pomembni)
2. **Dostopnost** (stroški, povezani z dostopanjem, oz. pridobitve informacije)
3. **Pravočasnost** (uporabnost informacije v času dostopa)
4. **Pomembnost** (pomembnost informacije za dosego cilja npr. oceno grožnje)
5. **Integriteta** (stopnja popolnosti informacije):
   - 5.1 Negotovost (stopnja prepričanosti v resnično vrednost informacije):
     - 5.1.1 zanesljivost (točnost, stabilnost), ki je odvisna tudi od:
     - 5.1.2 kredibilnosti (stopnja, do katere je informacija zaupanja vredna) in
     - 5.1.3 verjetnosti (ponovljivost informacije v drugih virih).
   - 5.2 Nenatančnost:
     - 5.2.1 podatki z napako:
       - 5.2.1.1 nedorečenost (informacija je neotipljiva);
       - 5.2.1.2 nepopolnost (informacija ni celovita);
       - 5.2.1.3 nejasnost (informacija ni jasno opisana);
       - 5.2.1.4 pomanjkljivost (informaciji primanjkujejo pomembni elementi).
     - 5.2.2 Podatki brez napake:
       - 5.2.2.1 kontradiktornost (nasprotovanje podatkov, ki tvorijo informacijo);
       - 5.2.2.2 natančnost (do kolikšne mere informacija odraža značilnosti analiziranega področja);
       - 5.2.2.3 konsistentnost (skladnost ob primerjavi s preteklimi informacijami).

b) Atributi **Kakovosti informacijskih virov** so naslednji:

Atributi **subjektivnih virov** (informacije izvirajo od opazovalcev, odločevalcev, strokovnjakov, odprti podatkov):

1. **Objektivnost**
2. **Usposobljenost/strokovnost**
3. **Poštenost**

4. **Ugled**
5. **Prepričanost**

Atributi **objektivnih virov** (informacije izvirajo iz senzorjev, modelov, podatkovnih baz, strojnih procesov):

1. **Zanesljivost**
2. **Verodostojnost**
3. **Ustreznost**
4. **Pomembnost**

c) Atributi **Kakovost predstavitve informacij** so:

1. **Interpretativnost** (razumljiva predstavitev)
2. **Razumljivost** (sposobnost slediti logike predstavitve)
3. **Popolnost** (informacija predstavlja vse pomembne elemente za razumevanje dejanskega stanja)
4. **Pravočasnost** (informacija odraža dejansko stanje in je predstavljena v času, ko je potrebna)

Takšna celostna ocena kakovosti informacij skozi posamezne atribute v končni fazi zahteva tudi končno oceno. Odvisno od konteksta in potreb uporabnika se kakovost informacij oceni na osnovi ene ali več kategorij in atributov. V primeru kombinacije je nujno določiti prioritete med pomembnostjo posameznih kategorij in atributov znotraj skupin, prav tako pa določiti medsebojne povezave oz. vplive ocen (npr. kakovost vira vpliva na kakovost vsebine ali zanesljivost vsebine vpliva na njeno verjetnost). Tudi v takem primeru je odločitev glede vključenih atributov odvisna od odločevalca, npr. v ocenah groženj se lahko upoštevajo merila, kot so kredibilnost, zanesljivost, pravočasnost; resničnost, pomembnost; popolnost, razumljivost ali popolnost in pravočasnost. Za izračun končne ocene kakovosti informacije se denimo lahko uporabi uteževanje atributov glede na njihov pomen in nato izvede povprečenje ocene, medtem ko so posamezne ocene lahko binarne (0–1), kategorične-opisne.

Pripomoček III: Register groženj in tveganj

Tabela 50: Register groženj

Kategorija groženj	Grožnja/ scenarij	Dobrina/ tarča	Splošen opis (indici, trendi)	Indikatorji							Ocena dobrin	Ocena verjetnosti	Stopnja ogroženosti	Ocena zanesljivosti ali kakovosti
				Vir	Zmogljivosti	Preteklost	Razsežnost	Prisotnost	Metode	Okoliščine				
Kategorija 1	*[grožnja 1]*	[dobrina]	[opis]	[opis]	[opis]	[opis]	[opis]	[opis]	[opis]	[opis]	[ocena]	[ocena]	[stopnja]	[stopnja]
	[grožnja 2]													
	[grožnja 3]													
Kategorija 2	*[grožnja 4]*													
	[grožnja 5]													
Kategorija 3	*[grožnja 6]*													
	[grožnja 7]													
	[grožnja 8]													
	[grožnja 9]													
	[grožnja 10]													

Tabela 51: Register tveganj

Kategorija groženj	Grožnja/ Scenarij	Dobrina/ Tarča	Ocena elementov				Izračun tveganj	Stopnja tveganja	Obstoječi ukrepi	Odločitev	Ukrepi naslavljanja	Odgovornost	Časovnica	Ocena zanesljivosti ali kakovosti
			Dobrina	Verjetnost	Vpliv	Ranljivost								
Kategorija 1	*[grožnja 1]*	[dobrina]	[ocena]	[ocena]	[ocena]	[ocena]	[ocena]	[ocena]	[popis]	[vrsta]	[popis]	[subjekti]	[roki]	[stopnja]
	[grožnja 2]													
	[grožnja 3]													
Kategorija 2	*[grožnja 4]*													
	[grožnja 5]													
Kategorija 3	*[grožnja 6]*													
	[grožnja 7]													
	[grožnja 8]													
	[grožnja 9]													
	[grožnja 10]													

Ker lahko za vsako grožnjo prepoznamo več vplivov, ranljivosti in ogroženih dobrin, je (v takem primeru) treba za vsako grožnjo pripraviti register vseh ogroženih dobrin, posledic in potencialnih vplivov (tabela 50). V končnem registru (predstavljen v tabeli 51) pa so podane zgolj končne oz. združene ocene.

Univerzitetna založba
Univerze v Mariboru

9 Zaključek

Ocenjevanje nacionalnovarnostne ogroženosti je ključni mehanizem oz. proces v zagotavljanju nacionalne varnosti, ki omogoča ustrezno pripravljenost družbe na najnevarnejša tveganja, ki ogrožajo blaginjo, stabilnost, suverenost in zaščito ključnih vrednot in temeljnih funkcij družbe. Nacionalna ocena tveganja je zahteven proces in za vsako državo predstavlja resen izziv (tako z vidika časa, financ in kompleksnosti, saj zahteva sodelovanje med raznimi področji, subjekti in disciplinami).

S ciljem izboljšanja pristopov k ocenjevanju je EU v svojih strateških usmeritvah zastavila cilj sistematičnega razvoja in poenotenja metodologij med državami članicami. Pri tem je poudarek predvsem na poenotenju dobrih praks, metodologij in terminologije. EU je zato zaostrila zahteve za pripravo nacionalnih ocen tveganja za vse države članice. Z zakonodajo, ki je bila sprejeta leta 2013 (in kasneje večkrat posodobljena), je vsaka država članica primorana Evropski komisiji oddati povzetek ocene tveganja na nacionalni ali primerni regionalni ravni vsaka tri leta. Intenzivnejši razvoj tovrstnih metodologij in sistematično izvajanje postopkov ocenjevanja v evropskih državah lahko zato zasledimo predvsem v zadnjem desetletju. Čeprav se pristopi med državami še vedno nekoliko razlikujejo, države, ki smo jih zajeli v pregled, pri razvoju svojih metodologij večinoma sledijo evropskim priporočilom in strokovnim usmeritvam (kot so mednarodni standardi ISO).

Da bo ocena tveganj na nacionalni ravni uspešna, je pomembno zagotoviti predvsem sistematičen in vse družbeni oz. vse vključujoč pristop, ki zajema posvetovanja z vsemi pomembnimi interesnimi in strokovnimi skupinami, je transparenten in zagotavlja ustrezno ravnovesje med uporabnostjo in znanstveno utemeljenostjo. Kakovostna informacijska podlaga, razumevanje morebitnih nezanesljivosti v ocenah in upoštevanje možnosti medsebojnega vplivanja tveganj ter njihovega vpliva na lokalno, regionalno in globalno skupnost so prav tako ključnega pomena. V sodobnem varnostnem okolju, ki je nepredvidljivo in zaznamovano s številnimi spremembami v naravi ogrožanj, pa je še posebej pomembno, da se tovrstne analize izvajajo periodično, kar omogoča stalno izpopolnjevanje ocene, spremljanje tveganj in zagotovitev ustrezne obveščenosti različnih javnosti.

Da bi v prihodnje lahko ustrezno naslovili omenjene izzive in pomanjkljivosti, smo razvili t. i. Model za ocenjevanje ogroženosti/tveganja na področju javne varnosti, ki omogoča praktično nadgradnjo aktualnih pristopov. Predlagane rešitve so tako strateške in operativne narave ter uporabne za vse zainteresirane organizacije, ki posredno ali neposredno delujejo na področju javne varnosti.

Univerzitetna založba
Univerze v Mariboru

Viri in literatura

Anželj, D. (2011). Predstavitev Resolucije o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje. V T. Pavšič Mrevlje (ur.), *Zbornik prispevkov: 12. slovenski dnevi varstvoslovja*. Fakulteta za varnostne vede.

Aurer-Jezerčić, I. (2017). Sigurnost i zaštita na radu: Procjena rizika od katastrofa za Republiku Hrvatsku. *Kemija u industriji : Časopis kemičara i kemijskih inženjera Hrvatske*, *66*(11–12), 716–718.

Australian Institute for Disaster Resilience. (2020). *National Emergency Risk Assessment Guidelines*. Australian Disaster Resilience Handbook Collection. https://www.aidr.org.au/media/7600/aidr_handbookcollection_nerag_2020-02-05_v10.pdf

Aven, T. (2015). *Risk Analysis*. John Wiley & Sons.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, *253*(1), 1–13.

Banka Slovenije. (2019). *Smernice o oceni tveganja pranja denarja in financiranja terorizma*. https://www.bsi.si/ckfinder/connector?command=Proxy&lang=sl&type=Files&currentFolder=%2FFinan%C4%8Dna%20stabilnost%2FPredpisi%2FPPDFT%2F&hash=6ce6c512ea433a7fc5c8841628e7696cd0ff7f2b&fileName=Smernice%20o%20oceni%20tveganja%20pranja%20denarja%20in%20financiranja%20terorizma%20(1).pdf

Bela knjiga o obrambi Republike Slovenije. (2020). Ministrstvo za obrambo Republike Slovenije. https://www.gov.si/assets/ministrstva/MO/Dokumenti/BK2020.pdf

Brecelj Anderluh, M., Brecelj-Kobe, M., Cvetežar, I. Š., Gregorič Kumperščak, H., Kocmur, M., Lokovšek, N., Mihevc Ponikvar, B., Mlakar, J., Rus-Makovec, M. in Širaj Mažgon, K. (2015). *Strokovne smernice za obravnavo nasilja v družini pri izvajanju zdravstvene dejavnosti*. Ministrstvo za zdravje. http://www.prepoznajnasilje.si/docs/default-source/zakonodaja/strokovne-smernice-za-obravnavo-nasilja-v-dru%C5%BEini-pri-izvajanju-zdravstvene-dejavnosti.pdf?sfvrsn=0

Britovšek, J. (2019). Predlog modela ocen ogroženosti in ocen tveganj za področje obveščevalnovarnostne dejavnosti v Republiki Sloveniji. *Varstvoslovje*, *21*(1), 73–86.

Cherkaoui, A. in Lopez, P. (2009). CO ₂ storage risk assessment: feasibility study of the systemic method MOSAR. *WIT Transactions on The Built Environment*, 108, 173–184. https://doi.org/10.2495/SAFE090171

Coleman, T. G. (2012). *A model for improving the strategic measurement and management of policing: The police organisational performance index (popi)*. https://ourspace.uregina.ca/bitstream/handle/10294/3775/Coleman_Terence_197703880_PhD_PLST_Fall2012.pdf?sequence=1&isAllowed=y

Commission notice: Reporting guidelines on disaster risk management, Art. 6(1)d of Decision No 1313/2013/EU. (2019). *Official Journal of the European Union*, (C 428), 8–33. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019XC1220(01)&from=ES

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise Risk Management: Integrating with Strategy and Performance. Executive Summary*. https://www.coso.org/Shared%20Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Council of the European Union. (2011). *Council conclusions on further developing risk assessment for disaster management within the European Union*. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/121462.pdf

Council of the European Union. (2015). *Serious and Organised Crime Threat Assessment 2017 (SOCTA): Updated methodology*. Europol. https://www.statewatch.org/media/documents/news/2015/dec/eu-council-socta-2017-methodology-14913-15.pdf

Council of the European Union. (2020). *Implementation of the Renewed EU Internal Security Strategy: joint Presidency paper*. https://data.consilium.europa.eu/doc/document/ST-5618-2020-REV-1/en/pdf

Council of the European Union. General Secretariat of the Council. (2010). *Internal security strategy for the European Union : towards a European security model*. Publications Office. https://data.europa.eu/doi/10.2860/87810

Cox, Jr, L. A. (2008). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, *28*(6), 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x

Danish Emergency Management Agency (DEMA). (2022). *National Risk Profile 2022*. https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2022/-national-risk-profile-2022-.pdf

Decision (EU) 2019/420 of the European Parliament and of the Council of 13 March 2019 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism. (n. d.). *Official Journal of the European Union*, (L 77I).

Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance. (n. d.). *Official Journal of the European Union*, (L 347).

Deng, Y. (2015). A Threat Assessment Model under Uncertain Environment. *Mathematical Problems in Engineering*, *2015*, 1–12.

Deutscher Bundestag. (2013). Bericht zur Risikoanalyse im Bevölkerungsschutz 2012 Inhaltsverzeichnis. *Drucksache*, *17/12051*. https://dserver.bundestag.de/btd/17/120/1712051.pdf

Direktorat za informacijsko družbo. (2018). *Ocena kibernetskih tveganj*.

Državna uprava za zaštitu i spašavanje. (2009). *Procjena ugroženosti Republike Hrvatske od prirodnih i tehničko-tehnoloških katastrofa i velikih nesreća*. Zagreb. https://civilna-zastita.gov.hr/UserDocsImages/DOKUMENTI_PREBACIVANJE/PLANSKI%20DOKUMENTI%20I%20UREDBE/Procjena%20ugrozenosti%20RH.pdf

European Commission. (n. d.). *Risk & recovery mapping: Product portfolio – Emergency Management Service*. https://emergency.copernicus.eu/mapping/sites/default/files/files/CopernicusEMS-Service_Portfolio-Risk_and_Recovery_Mapping.pdf

European Commission. (2009). *Principles of multi-risk assessment : interaction amongst natural and man-induced risks*. Publications Office. https://data.europa.eu/doi/10.2777/30886

European Commission. (2010). *Commission staff working paper: Risk assessment and mapping guidelines for disaster management - SEC(2010) 1626 final*. https://ec.europa.eu/echo/files/about/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

European Commission. (16. 4. 2016*). Security: EU strengthens response to hybrid threats*. https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1227

European Commission. (2019). *Report from the commission to the European parliament and the council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities {SWD(2019) 650 final} -COM/2019/370*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0370

European Commission. (2020). *Communication from the commission on the EU Security Union Strategy (COM(2020) 605 final)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605

European Commission in Royal HaskoningDHV. (2021). *Current practice in flood risk management in the European Union: September 2021*. Publications Office. https://data.europa.eu/doi/10.2779/235272

European Parliament. (13. 3. 2019). *Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism Text with EEA relevance, 2013;* https://eur-lex.europa.eu/legal-content/EN-SL/TXT/?uri=CELEX%3A32019D0420

Europol. (2021a). *European Union Serious and Organised Crime Threat Assessment (SOCTA) – A Corrupting Influence: the Infiltration and Undermining of Europe's Economy and Society by Organised Crime*. https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf

Europol. (2021b). *European Union Terrorism Situation and Trend Report 2021 (TE-SAT)*. Publications Office. https://data.europa.eu/doi/10.2813/677724

Europol. (2022). *EU Policy Cycle - EMPACT*. Europol. https://www.europol.europa.eu/crime-areas-and-statistics/empact

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA)*. Europol. https://www.europol.europa.eu/publications-events/main-reports/iocta-report

EXCIMAP. (2007a). *Atlas of flood maps*. https://open.rijkswaterstaat.nl/publish/pages/19689/383224.pdf

EXCIMAP. (2007b). *Handbook on good practices for flood mapping in Europe*. http://www.pcn.minambiente.it/mattm/wp-content/uploads/2017/03/direttiva_alluvioni/linee_guida_e_specifiche_tecniche/linee_guida_europee/handbook_goodpractice.pdf

FATF. (2021). *National money laundering and terrorist financing risk assessment*. https://www.fatf-gafi.org/en/documents/news/nationalmoneylaunderingandterroristfinancingriskassessment.html

Federal Office for Civil Protection FOCP. (2020). *National risk analysis methodology - disasters and emergencies in Switzerland 2020*. https://www.babs.admin.ch/content/babs-internet/en/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/_jcr_content/contentPar/tabs/items/fachunterlagen/tabPar/downloadlist/downloadItems/38_1461911615743.download/knsmethode2020-en.pdf

Frontex. (2013). *Skupni integrirani model analize tveganja*. https://frontex.europa.eu/assets/CIRAM/sl_CIRAM_brochure_2013.pdf

Glavna radna skupina Hrvatske platforme za smanjenje rizika od katastrofa. (2019). *Procjena rizika od katastrofa za Republiku Hrvatsku*. https://civilna-zastita.gov.hr/UserDocsImages/CIVILNA%20ZA%C5%A0TITA/PDF_ZA%20WEB/Procjena_rizika%20od%20katastrofa_2019.pdf

Government of Ireland. (2021a). *A National risk assessment for Ireland 2020*. https://assets.gov.ie/128544/e3cf811b-8fc9-4fc6-ab4e-a70bd1fd423c.pdf

Government of Ireland. (2021b). *Draft national risk assessment: Overview of strategic risks 2021/2022*. https://assets.gov.ie/179806/9e43b897-b6d9-49a1-810b-37095ef0ebb7.pdf

Hilton, S. in Baylon, C. (2020). *Risk management in the UK: What can we learn from COVID-19 and are we prepared for the next disaster?* The Centre for the Study of Existential Risk, University of Cambridge. https://www.cser.ac.uk/media/uploads/files/Risk_management_in_the_UK___What_can_we_learn_from_COVID-19_and_are_we_prepared_for_the_next_disaster___FINAL_VERSION___2.pdf

Hirsch Ballin, E., Dijstelbloem, H. in De Goede, P. (2020). The Netherlands and the extended concept of security: The rise of security strategies. V E. Hirsch Ballin, H. Dijstelbloem, in P. De Goede (ur.), *Security in an Interconnected World* (str. 65–85). Springer International Publishing.

Home Office Government. (2015). *The strategic policing requirement*. Home Office. https://www.sussex-pcc.gov.uk/media/1079/strategic-policing-requirement-march-2015.pdf

Hrovat Svetičič, T., Horvat, D. in Hrovatič, D. (2008). *Strokovna izhodišča za delo z odraslimi žrtvami in povzročitelji nasilja v družini za strokovne delavce na centrih za socialno delo*. https://www.drustvo-dnk.si/images/dokumenti/smernice-zenske.pdf

Hrovat Svetičič, T., Horvat, D., Hrovatič, D. in Premzel, F. (2010). Rezultati iskanja Strokovna izhodišča za delo z odraslimi žrtvami in povzročitelji nasilja v družini za strokovne delavce centrov za socialno delo. *Kaljenje: Bilten Skupnosti CSD Slovenije*, *10*(5), 38–95.

IEC 31010:2019. (1. 7. 2019). https://www.iso.org/standard/72140.html

IMPRODOVA. (2021). *Nacionalna platforma*. https://www.fvv.um.si/improdova/

Irwin, D. in Mandel, D. R. (2019). Improving information evaluation for intelligence production. *Intelligence and National Security*, *34*(4), 503–525.

ISO 31000:2018. (4. 2. 2022). https://www.iso.org/standard/65694.html

ISO/IEC 27005:2018. (16. 12. 2020). https://www.iso.org/standard/75281.html

Joint Task Force Transformation Initiative. (2012). *Guide for conducting risk assessments* (NIST Special Publication (SP) 800-30 Rev. 1). National Institute of Standards and Technology.

Kuipers, S., Grieken, B. in Asselt, M. (2018). Risk, hazards and crisis in research: What risks get researched, where and how? *Risk, Hazards & Crisis in Public Policy*, *9*.

Lin, L. (2018). Integrating a national risk assessment into a disaster risk management system: Process and practice. *International Journal of Disaster Risk Reduction*, *27*, 625–631.

Meško, G. in Sotlar, A. (2012). Preprečevanje kriminalitete v lokalnih skupnostih –med ad hoc pristopi in na znanju temelječih preventivnih dejavnostih. *Revija za kriminalistiko in kriminologijo*, *63*(2), 229–239

Ministarstvo unutarnjih poslova Republike Hrvatske. (2021). *Ustroj*. mup.gov.hr. https://mup.gov.hr/ustroj/201

Ministrstvo za infrastrukturo. (2013). *Medresorska delovna skupina za spremljanje in izvajanje Resolucije o nacionalnem programu varnosti cestnega prometa za obdobje od 2013 do 2022*. GOV.SI. https://www.gov.si/zbirke/delovna-telesa/medresorska-delovna-skupina-za-spremljanje-in-izvajanje-resolucije-o-nacionalnem-programu-varnosti-cestnega-prometa-za-obdobje-od-2013-do-2022/

Nacionalna strategija za preprečevanje terorizma in nasilnega ekstremizma št 22100-2/2019/4. (2019).

Navodilo o pripravi ocen ogroženosti. (1995). *Uradni list RS,* (39/95).

Navodilo za ocenjevanje tveganj za delovanje kritične infrastrukture Republike Slovenije. (2019). *Uradni list RS*, (7/19).

Obrambna strategija Republike Slovenije. (2013). Republika Slovenija, Ministrstvo za obrambo. https://www.gov.si/assets/ministrstva/MO/Dokumenti/Obrambna_strategija_RS_2012_slo_eng.pdf

OECD. (2018). *National risk assessments: A cross country perspective*. https://doi.org/10.1787/9789264287532-en

Office of the Director of National Intelligence. (2021). *Annual threat assessment of the us intelligence community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

Ostrom, L. T. in Wilhelmsen, C. A. (2012). *Risk assessment: Tools, techniques, and their applications* (2nd edition). Wiley.

Poljansek, K., Casajus, V. A., Marin, F. M., De, J. A., Dottori, F., Galbusera, L., Garcia, P. B., Giannopoulos, G., Girgin, S., Hernandez, C. M. A., Iurlaro, G., Karlos, V., Krausmann, E., Larcher, M., Lequarre, A. S., Theocharidou, M., Montero, P. M., Naumann, G., Necci, A., … Wood, M. (8. 5. 2019). *Recommendations for national risk assessment for disaster risk management in EU*. JRC Publications Repository.

Pravilnik o dejavnikih neznatnega in povečanega tveganja za pranje denarja ali financiranje terorizma. (2018, 2020, 2022). *Uradni list RS*, (6/18, 152/20, 48/22).

Pravilnik o fizičnem varovanju jedrskih objektov, jedrskih in radioaktivnih snovi ter prevozov jedrskih snovi. (2013, 2017). *Uradni list RS*, (17/13, 76/17).

Pravilnik o metodologiji za izradu procjena ugroženosti i planova zaštite i spašavanja. (2008). *Narodne novine*, (38/2008).

Prislan, K. in Bernik, I. (2019). *Informacijska varnost in organizacije*. Univerzitetna založba Univerze v Mariboru. https://press.um.si/index.php/ump/catalog/book/400

Prislan, K. in Lobnikar, B. (2019). Modern trends in policing: public perceptions of the preferred policing models in Slovenia. *Revija za kriminalistiko in kriminologijo*. *70*(5), 483–500

Pritchard, C. L. (2014). *Risk management: Concepts and fuidance* (5th edition). Auerbach Publications.

Pursiainen, C. in Rød, B. (2021). National disaster risk assessments in Europe. How comparable are they and why? *Risk, Hazards & Crisis in Public Policy*, *12*(2), 194–214.

Ravnateljstvo civilne zaštite. (2021). *Hrvatska platforma za smanjenje rizika od katastrofa*. civilna-zastita.gov.hr. https://civilna-zastita.gov.hr/hrvatska-platforma-za-smanjenje-rizika-od-katastrofa/80

Regulation (EU) 2021/836 of the European Parliament and of the Council of 20 May 2021 amending Decision No 1313/2013/EU on a Union Civil Protection Mechanism. (n. d.). *Official Journal of the European Union*, (L 185).

Republika Slovenija. (2016). *Strategija kibernetske varnosti*. https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske- varnosti.pdf

Resolucija o dolgoročnem razvojnem programu policije do leta 2025 – »Kakovostna policija za varno Slovenijo«. (2015). *Uradni list RS,* (75/15).

Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2019–2023. (2019). *Uradni list RS*, (43/19).

Resolucija o nacionalnem programu preprečevanja nasilja v družini 2009–2014. (2009). *Uradni list RS*, (41/09).

Resolucija o nacionalnem programu varnosti cestnega prometa za obdobje od 2013 do 2022. (2013). *Uradni list RS*, (39/13).

Resolucija o nacionalnem programu varstva pred naravnimi in drugimi nesrečami v letih od 2016 do 2022 (ReNPVNDN16–22). (2016). *Uradni list RS*, (75/16).

Resolucija o preprečevanju korupcije v Republiki Sloveniji. (2004). *Uradni list RS*, (85/04).

Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do leta 2035. (2022). *Uradni list RS*, (16/22).

Resolucija o strategiji nacionalne varnosti Republike Slovenije (2010). *Uradni list RS*, (27/10).

Resolucija o strategiji nacionalne varnosti Republike Slovenije. (2019). http://pisrs.si

Rogova, G. L. (2016). Information quality in information fusion and decision making with applications to crisis management. V G. Rogova in P. Scott (ur.), *Fusion methodologies in crisis management* (str. 65–86). Springer International Publishing.

Russell Vastveit, K. (2011). *The use of national risk assessments in the Netherlands and the UK*. Faculty of social sciences, University of Stavanger. https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/184618/Russell%20Vastveit%20Kirsti.pdf?sequence=1

Strategija Vlade RS na področju migracij. (2019). https://www.gov.si/assets/ministrstva/MNZ/SOJ/STR17072019.pdf

Šimenc, J. (2015). *Prepoznava in obravnava žrtev nasilja v družini: priročnik za zdravstveno osebje*. Zdravniška zbornica Slovenije. https://www.prepoznajnasilje.si/docs/default-source/default-document-library/priro%C4%8Dnik-za-zdravstveno-osebje.pdf?sfvrsn=0

Šooš, T., Lautar, K., Urbančič, H., Kobe Logonder, N., Kmet Zupančič, R. in Fajić, L. (ur.). (2017). *Strategija razvoja Slovenije 2030*. Služba Vlade Republike Slovenije za razvoj in evropsko kohezijsko politiko.

The Swedish Civil Contingencies Agency (MSB). (2016). *A summary of risk areas and scenario analyses 2012–2015*. https://www.msb.se/siteassets/dokument/publikationer/english-publications/a-summary-of-risk-areas-and-scenario-analyses-20122015.pdf

United Nations Department of Economic and Social Affairs. (2015). *Transforming our world: the 2030 Agenda for Sustainable Development | Department of Economic and Social Affairs*. https://sdgs.un.org/2030agenda

United Nations Office for Disaster Risk Reduction. (2017). *National disaster risk assessment*. https://www.unisdr.org/files/52828_nationaldisasterriskassessmentwiagu.pdf

Uprava Republike Slovenije za zaščito in reševanje. (2018). *Državna ocena tveganj za nesreče*. https://www.gov.si/assets/organi-v-sestavi/URSZR/Datoteke/Ocene-tveganja-za-nesrece/drzavna-ocena-tveganj-za-nesrece-2.0_2018_za-splet.pdf

Uprava Republike Slovenije za zaščito in reševanje. (2021). *Ocenjevanje tveganj za nesreče*. GOV.SI. https://www.gov.si/teme/ocenjevanje-tveganj-za-nesrece/

Urad RS za preprečevanje pranja denarja. (2015). *Povzetek poročila o izvedbi nacionalne ocene tveganja Republike Slovenije za pranje denarja in financiranje terorizma*. https://www.gov.si/assets/organi-v-sestavi/UPPD/Dokumenti/Mednarodno-sodelovanje/Povzetek-porocila-o-izvedbi-nacionalne-ocene-tveganja-Republike-Slovenije-za-pranje-denarja-in-financiranje-terorizma.pdf

Urad RS za preprečevanje pranja denarja. (2016). *Posodobljeno poročilo o izvedbi nacionalne ocene tveganja Republike Slovenije za pranje denarja in financiranje terorizma s podatki za leti 2014 in 2015*. https://www.gov.si/assets/organi-v-sestavi/UPPD/Dokumenti/Mednarodno-sodelovanje/Posodobljeno-porocilo-o-izvedbi-nacionalne-ocene-tveganja-Republike-Slovenije-za-pranje-denarja-in-financiranje-terorizma-s-podatki-za-leti-2014-in-2015.pdf

Urad RS za preprečevanje pranja denarja. (2021). *Povzetek poročila o izvedbi nacionalne ocene tveganja Republike Slovenije za pranje denarja in financiranje terorizma*. https://www.gov.si/assets/organi-v-sestavi/UPPD/Dokumenti/Mednarodno-sodelovanje/NRA-2021/Povzetek-porocila-o-izvedbi-nacionalne-ocee-tveganja-Republike-Slovenije-za-pranje-denarja-in-financiranje-terorizma.docx

Urad Vlade RS za komuniciranje. (2022). *Ocena teroristične ogroženosti Slovenije*. GOV.SI. https://www.gov.si/teme/ocena-teroristicne-ogrozenosti-slovenije/

Uredba o informacijski varnosti v državni upravi. (2018, 2020). *Uradni list RS*, (29/18, 131/20).

Uredba o izvajanju Sklepa o mehanizmu Unije na področju civilne zaščite. (2014). *Uradni list RS*, (62/14, 13/17).

Uredba o obveznem organiziranju službe varovanja na javnih prireditvah. (2010). *Uradni list RS*, (22/10, 17/11, 52/16).

Uredba o vsebini in izdelavi načrtov zaščite in reševanja. (2012). *Uradni list RS*, (24/12, 78/16, 26/19).

Van Den Born, A., Van Witteloostuijn, A., Barlage, M., Sapulete, S., Van Den Oord, A., Rogiest, S., Vallet, N., Reguli, Z., Vit, M., Mouhanna, C., Cassa, D., Binder, H., Blumenthal, V., Christe-Zeyse, J., Giljohann, S., Gruschinske, M., Pautz, H., Stein-Müller, S., Bisogni, F., … Pólos, L. (2013). Policing opportunities and threats in Europe. *Journal of Organizational Change Management*, *26*, 811–829.

Van Duyne, P. C. (2010). Organised crime (threat) as a policy challenge: A tautology. *Varstvoslovje*, *12*(4), 355–366.

Vlada Republike Hrvatske. (n. d.). *Procjena rizika od katastrofa za Republiku Hrvatsku*. https://civilna-zastita.gov.hr/UserDocsImages/DOKUMENTI_PREBACIVANJE/PLANSKI%20DOKUMENTI%20I%20UREDBE/Procjena%20rizika%20od%20katastrofa%20za%20RH.pdf

Vlada Republike Slovenije. (2022). *Srednjeročni obrambni program Republike Slovenije 2022–2026 (SOPR2022–2026)*. https://www.gov.si/assets/ministrstva/MO/Dokumenti/SOPR_2022_2026.pdf

World Bank Group. (2015). *National risk assessment tool: Guidance manual – Module 1: Money laundering threat assessment*. https://documents1.worldbank.org/curated/en/753831593423608028/pdf/National-Risk-Assessment-Tool-Guidance-Manual-Module-1-Money-Laundering-Threat-Assessment.pdf

World Bank Group. (2016). *Risk Assessment Support for Money Laundering/Terrorist Financing* [Text/HTML]. World Bank. https://www.worldbank.org/en/topic/financialsector/brief/antimoney-laundering-and-combating-the-financing-of-terrorism-risk-assessment-support

Zakon o informacijski varnosti (ZInfV). (2018, 2021). *Uradni list RS*, (30/18, 95/21).

Zakon o javnih zbiranjih (ZJZ). (2011). *Uradni list RS*, (64/11).

Zakon o kritični infrastrukturi (ZKI). (2017, 2021). *Uradni list RS*, (75/17, 189/21).

Zakon o občinskem redarstvu (ZORed). (2006, 2017). *Uradni list RS*, (139/06, 9/17).
Zakon o preprečevanju nasilja v družini (ZPND). (2008, 2016, 2017, 2021). *Uradni list RS*, (16/08, 68/16, 54/17, 196/21).
Zakon o preprečevanju pranja denarja in financiranja terorizma (ZPPDFT-1). (2016, 2019, 2020, 2021, 2022). *Uradni list RS*, (68/16, 81/19, 91/20, 2/21, 48/22).
Zakon o varstvu pred naravnimi in drugimi nesrečami (ZVNDN-UPB1). (2006, 2010, 2018). *Uradni list RS*, (51/06, 97/10, 21/18).
Zoutendijk, A. J. (2010). Organised crime threat assessments: a critical review. *Crime, Law and Social Change*, *54*(1), 63–86.

DOI
https://doi.org/
10.18690/um.fvv.1.2024

ISBN
978-961-286-802-4

KO SE SREČATA ZNANJE IN ODLOČANJE: PRISTOPI K OCENJEVANJU VARNOSTNIH TVEGANJ

KAJA PRISLAN MIHELIČ ET AL.

Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
kaja.prislan@um.si

Ocenjevanje varnostnih tveganj predstavlja temelj strateškega upravljanja varnosti razvitih držav. V monografiji je predstavljen širok pregled različnih usmeritev in pristopov za ocenjevanje varnostnih tveganj in ogroženosti. Predstavljamo tako nacionalne strateške in zakonodajne podlage kot tudi ključne strokovne vire, mednarodne standarde in smernice. Poleg splošnih usmeritev monografija prikazuje nekatere prakse tujih držav ocenjevanja varnostnih tveganj in ogroženosti. Osrednji doprinos tega dela predstavlja predlagani model za ocenjevanje ogroženosti in tveganj na področju javne varnosti, ki je primarno namenjen organizacijam, ki delujejo na področju javne varnosti. Gre za model, ki je v svoji osnovi celovit, enovit in praktično uporaben. Model predstavlja vodilo in orodje za izvajalce (analitike) ter je zasnovan v obliki navodila, ki omogoča izvedbo ocene skozi analitično in sistematično zasnovan proces, skozi katerega se odločevalcem zagotovi ustrezna informacijska podpora za odločanje. Zaradi specifičnih pričakovanj in zahtev je model predlagan v polni in skrajšani različici.

Ključne besede:
ocenjevanje tveganj,
ocenjevanje ogroženosti,
nacionalna varnost,
analiza ogroženosti,
varnostne organizacije

Univerzitetna založba
Univerze v Mariboru

DOI
https://doi.org/
10.18690/um.fvv.1.2024

ISBN
978-961-286-802-4

When Knowledge and Decision-making Meet: Approaches to Security Risk Assessment

Kaja Prislan Mihelič et al.
University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
kaja.prislan@um.si

Keywords:
risk assessment,
threat assessment,
national security,
threat analysis,
security organizations

Assessing security risks is the cornerstone of strategic security management in developed nations. This monograph provides a broad overview of various orientations and approaches to assessing security risks and vulnerabilities. It encompasses national strategic and legislative frameworks, essential professional resources, international standards, and guidelines. In addition to general orientations, the monograph presents selected practices of foreign countries in assessing security risks and threats. The central contribution of this work lies in the proposed model for assessing threats and risks in the realm of public security, primarily intended for organizations operating in the field of public security. The model is fundamentally comprehensive, cohesive, and practically applicable. Serving as a guiding tool, it is designed for analysts to conduct assessments through an analytical and systematic process, thereby providing decision-makers with appropriate informational support. Due to specific expectations and requirements, the model is presented in both full and short versions.

University of Maribor Press

Znanstvena monografija *Ko se srečata znanje in odločanje: Pristopi k ocenjevanju varnostnih tveganj* predstavlja dragocen vir znanja in smernic za vse, ki se ukvarjajo s strateškim upravljanjem varnosti in ocenjevanjem tveganj. S svojo v znanosti utemeljeno celovitostjo ter usmerjenostjo k prektičnem delovanju lahko postane nepogrešljiv vir podpore in navdiha pri oblikovanju učinkovitih strategij strokovnjakom za zagotavljanje javne varnosti ter nepogrešljiv učni pripomoček na področjih, ki obravnavajo zagotavljanje varnosti.

Prof. dr. Iztok PODBREGAR
Unvierza v Mariboru

Znanstvena monografija *Ko se srečata znanje in odločanje: Pristopi k ocenjevanju varnostnih tveganj* avtorjev Kaje Prislan Mihelič, Maje Modic, Branka Lobnikarja, Boštjana Slaka in Anžeta Miheliča predstavlja dragocen vir znanja za študente in akademike. Prav tako ponuja dobrodošle smernice za vse, ki se ukvarjajo s strateškim in operativnim upravljanjem varnosti in ocenjevanjem tveganj. Zaradi odlično združene znanstvene relevantnosti in neposredne uporabnosti lahko torej postane nepogrešljiv pripomoček vsem, ki želijo uspešno, učinkovito in kakovostno delovati na področju zagotavljanja javne varnosti.

Dr. Andrej BENEDEJČIČ
Kabinet predsednika Vlade Republike Slovenije

Univerza v Mariboru
Fakulteta za varnostne vede