



REPUBLIKA SLOVENIJA
SLOVENSKA OBVEŠČEVALNO-VARNOSTNA AGENCIJA



AKTIVNOSTI SOVE v letu 2024

KAZALO

Predgovor direktorja Sove

1. SPREMENJENO MEDNARODNO VARNOSTNO OKOLJE
 - 1.1. Terorizem in ekstremizem
 - 1.2. Neregularne migracije
 - 1.3. Mednarodni organizirani kriminal
 - 1.4. Kršenje mednarodnih pogodb o prepovedi širjenja orožja za množično uničevanje in mednarodnih gospodarskih sankcij
 - 1.5. Obveščevalno delovanje tujih akterjev
 - 1.6. Kibernetske grožnje kritični infrastrukturi
 - 1.7. Hibridne grožnje
 - 1.8. Gospodarska varnost
2. IZPOSTAVLJENO
 - 2.1. Proruske hektivistične aktivnosti proti Sloveniji
 - 2.2. Tajnost
3. SOVA V ŠTEVILKAH

PREDGOVOR DIREKTORJA SOVE

Živimo v globalno prepredenem svetu, kjer je nadnacionalna dimenzija tveganj in groženj varnosti naše države in širšega mednarodnega prostora postala standard. V prepletenosti raznolikih in številnih dejavnikov postajajo razmerja med njimi zaradi multipolarizacije globalne varnostne ureditve izjemno zapletena, težko predvidljiva in nestabilna. Na varnostno okolje in



Joško Kadivnik, direktor Sove

občutek varnosti pri posamezniku vplivajo poleg konkretnih dogodkov tudi premiki v svetovni varnostni arhitekturi, ki odpirajo vprašanja stabilnosti, perspektive in predvidljivosti razmer v prihodnjih letih ter desetletjih. Zato je pri prizadevanjih za zgodnje prepoznavanje tveganj in groženj treba razmišljati v širših okvirjih, upoštevati številne in raznolike, med seboj vzročno-posledično povezane dejavnike ter prepoznati najzgodnejše simptome novih varnostnih dinamik.

Poseben izziv predstavljajo tveganja, ki izvirajo iz kibernetnega prostora, kjer se porajajo številne možnosti za povzročanje konkretne škode tako državnim ustanovam kot gospodarskim subjektom in za subtilno, ciljno usmerjeno vplivanje na družbo - na javno mnenje, splošno razpoloženje, dožemanje stvarnosti. Prav v povezavi s kibernetnimi grožnjami je posebej pomembno, da se prizadevanja usmerja v družbeno odpornost na tovrstne poskuse destabilizacije družbe, države in širše skupnosti, saj je to najučinkovitejši način preprečevanja vplivanja zlonamernih akterjev v kibernetnem prostoru.

V predstavitvi aktivnosti agencije v lanskem letu predstavljamo ob že omenjenih spremenjenih varnostnih razmerah v svetu in kibernetnih grožnjah še vsebine s področja terorizma in ekstremizma, neregularnih migracij, mednarodnega organiziranega kriminala, kršenja mednarodnih pogodb o prepovedi širjenja orožja za množično uničevanje in mednarodnih gospodarskih sankcijah, gospodarske varnosti, obveščevalnem delovanju tujih akterjev. Vse to so področja, ki pomembno oblikujejo naše varnostno okolje, zato jim v agenciji posvečamo posebno pozornost.

V Slovenski obveščevalno-varnostni agenciji pozorno spremljamo dejavnike tveganj in groženj za vitalne interese Republike Slovenije ter pridobivamo informacije o dogajanjih in dejanjih, ki izkazujejo elemente tveganja za varnost naše države in stabilnost širše

regije. O svojih ugotovitvah obveščamo odločevalce, ki so pristojni za sprejemanje odločitev in usmeritev na svojih delovnih področjih. Namen in cilj našega delovanja je, da s pridobljenimi informacijami omogočimo pravočasno in učinkovito odzivanje na varnostne dejavnike ter tako prispevamo k zaščiti in krepitvi nacionalne varnosti.

Za učinkovito izvajanje nalog agencije v danih varnostnih razmerah je nujno povezovanje z drugimi državnimi organi in ustanovami ter tujimi partnerji. Tvrno sodelovanje z vsemi deležniki je ključnega pomena za doseganje rezultatov, ki so podlaga za sprejemanje ustreznih odločitev na najvišji državni ravni in pravočasno odzivanje na sodobne varnostne izzive. Zato gre zahvala za uspešno opravljeno delo agencije tudi vsem tistim deležnikom, s katerimi smo se v agenciji ob izvajanju svojih nalog strokovno povezovali in dopolnjevali.

Z zavezo, da bo varnost prebivalcev in prebivalcev Republike Slovenije tudi v prihodnje prednostna skrb agencije,

A handwritten signature in white ink on a dark blue background. The signature is written in a cursive, flowing style and reads "Josko Kodrič".



1.

SPREMENJENO

MEDNARODNO

VARNOSTNO

OKOLJE

Republika Slovenija in celotna Evropa se soočata z bistveno slabšimi varnostnimi okoliščinami kot v zadnjih nekaj desetletjih, zato v Evropi narašča potreba po oblikovanju nove varnostne strategije ter vzpostavitvi samostojne kolektivne obrambe.

Trenutni globalni multilateralni red, ki temelji na mednarodnem pravu in neodvisnih mednarodnih organizacijah, je na preizkušnji. Nekatere tuje države ter njihova partnerstva in zavezništva si prizadevajo za vzpostavitev novega, multipolarnega svetovnega reda, v katerem Zahod ne bo več imel takšne vloge, kakršno ima sedaj. Za to si najbolj prizadevata Rusija in Kitajska, ki v ta namen vzpostavljata in favorizirata vzporedne multilateralne organizacije (npr. BRICS+ in Šanghajsko organizacijo za sodelovanje – SCO). Razmerje moči v svetu se spreminja zaradi različnih političnih, gospodarskih in varnostnih dejavnikov, kar vpliva tako na globalno kot regionalno politično in varnostno okolje ter se med drugim odraža v krepitvi avtorskih režimov ter zaostrovanju obstoječih in pojavljanjem novih kriznih žarišč po svetu.

Spremembe mednarodnega varnostnega okolja so lahko nenadne ali dalj časa trajajoče, kompleksne in večplastne, kar otežuje ustrezno odzivanje na posamezne varnostne in krizne dogodke. Naloga Sove je budno spremljanje dinamike mednarodnega varnostnega okolja ter ugotavljanje, kakšen vpliv ima na varnost in interese Republike Slovenije, EU in Nata.

Od začetka ruske agresije na Ukrajino je minilo že tretje leto, zato bo ključnega pomena ohranjanje enotnosti evropskih držav za nadaljnje zagotavljanje vojaške in finančne pomoči Ukrajini ter s tem odvrčanje Rusije. Ob nastajanju novega multipolarnega ravnovesja v mednarodnih odnosih, se izrisujejo okrepljena ruska zavezništva z državami, ki Rusijo podpirajo z znatno materialno pomočjo in tudi pri spreminjanju svetovne ureditve ravnajo v skladu z njenimi interesi. Poleg tega je Rusija prešla na vojno gospodarstvo in za vojaško industrijo v letu 2025 namenja kar tretjino proračunskih sredstev. Obujanje globalne oboroževalne tekme, spodkopavanje mehanizmov za nadzor jedrskega orožja, odstop držav od sporazumov za nadzor jedrskega arzenala velesil, posledično tekma za razvoj tehnološkega orožja (Rusija, Kitajska, Iran, Severna Koreja) pomeni vse večji izziv za strateško stabilnost. Med drugim vojna v Ukrajini vpliva tudi na zamrznjene konflikte v njeni neposredni soseščini, kjer se povečuje strah pred obnovitvijo vojaških spopadov.

Konflikt v Gazi je v preteklem letu močno zaostila varnostne razmere na Bližnjem vzhodu, sovražnosti med Izraelom in Iranom so se okrepile, s tem pa se je zaustavil proces normalizacije odnosov na Bližnjem vzhodu, ki ga je naznanil podpis Abrahamovih sporazumov med Izraelom in več arabskimi državami leta 2020. Iran bo kljub izraelskim aktivnostim, zaradi katerih so se občutno zmanjšale vojaške zmogljivosti iranskih zaveznikov v regiji kot sta Hezbolah, Hamas in jemenski hutijevci, še naprej osrednja varnostna grožnja Izraelu in glavni dejavnik nestabilnosti na Bližnjem vzhodu. Možnosti

za obnovitev pogovorov o iranskem jedrskem programu so majhne, medtem pa Iran nadaljuje bogatenje urana in razvoj balističnega programa, ki bi ga ob nadaljnjem zaostrovanju napetosti lahko uporabil v vojaške namene. V Siriji so oblast po padcu režima Bašarja Al Asada prevzele islamistične uporniške skupine, ki sicer izražajo pripravljenost za oblikovanje vključujočih oblasti. Mednarodno skupnost skrbi predvsem usoda verskih in etničnih skupin v državi, posledično stopnjevanje napetosti in morebitna razširitev medsektaških spopadov. Padec sirskega režima sicer pomeni priložnost za vrnitev sirskih beguncev v domovino, vendar je nadaljnji razvoj dogodkov negotov in v veliki meri odvisen od sposobnosti novih oblasti za uravnoteženje interesov različnih verskih in etničnih skupin.

V Afriki se krepi vpliv in prisotnost Rusije ter Kitajske na račun zmanjšanja zahodnega vpliva in z izkoriščanjem politične nestabilnosti v posameznih državah. Rusija v zameno za dobave orožja, urjenja, varovanja vojaških oblasti in ostalih storitev, pridobiva gospodarske koristi, širi diplomatski vpliv in vzpostavlja vojaško prisotnost v zanj strateško pomembnih delih. S pomočjo afriških in drugih zavezniških držav zmanjšuje učinke zahodnih sankcij in dokazuje (tudi z njihovim glasovanjem v Generalni skupščini Združenih narodov), da ni mednarodno politično izolirana. Kitajska sodelovanje z afriškimi državami krepi z infrastrukturnimi projekti na področju transporta, energetike, informacijsko-telekomunikacijskih sistemov in industrije ter s sodelovanjem na področju varnosti, obrambe, kulture, politike in izobraževanja. V zameno pridobiva njihovo politično podporo in kritične surovine, potrebne za kitajsko industrijo ter kitajski gospodarski in tehnološki razvoj. S tovrstnim sodelovanjem pridobiva tudi naklonjenost afriških držav, ki jih združuje v okviru svojih globalnih pobud s ciljem, da bi postala voditeljica globalnega juga.

Kitajska prihaja v ospredje kot vedno bolj napredna in razvita država, ki krepi svojo prisotnost tako v Aziji kot drugod po svetu. S svojimi globalnimi pobudami za sodelovanje na področju gospodarstva, tehnološkega razvoja in varnosti širi svoj vpliv ter postopno uresničuje strateške interese oblasti in Komunistične partije Kitajske. Pospešeno razvija civilno in vojaško tehnologijo, s pomočjo katere si prizadeva postati vodilna globalna velesila na vseh področjih.

Indo-pacifiška regija postaja vedno pomembnejše območje, kjer Kitajska in Severna Koreja na eni strani ter ZDA in njene zaveznice na drugi strani razkazujejo svojo moč. Zaradi stopnjevanja napetosti med omenjenimi in drugimi akterji ima regija potencial, da v bližnji prihodnosti postane novo krizno žarišče z negativnim vplivom na ves svet. Krepitev severnokorejskih zmogljivosti na področju vojaške in vesoljske tehnologije, kar

vključuje tudi razvoj jedrskega in raketnega programa oziroma orožja, prav tako povečuje tveganje za eskalacijo napetosti v regiji.

1.1.

Terorizem in ekstremizem

Teroristične skupine v svoji propagandi izkoriščajo aktualne oborožene konflikte in tako neposredno vplivajo na vse pogostejše primere radikalizacije mladih in mladoletnih. Radikalizacija mladih prek svetovnega spleta predstavlja resen izziv za sodobno družbo.

Zaostrene varnostne razmere na Bližnjem vzhodu, širjenje islamistične propagande po svetovnem spletu, pa tudi vojna v Ukrajini so v preteklem letu vplivali na povišano teroristično ogroženost evropskih držav, med njimi tudi Slovenije. Zaradi svojega specifičnega geostrateškega položaja in vloge pri zagotavljanju miru ter stabilnosti na kriznih območjih in v Jugovzhodni Evropi je Slovenija še naprej izpostavljena različnim vplivom, ki bi lahko posredno ali neposredno ogrozili njeno nacionalno varnost. Napadi in druga nasilna dejanja, ki so jih v Evropi izvedli radikalizirani posamezniki in manjše celice, ter številni preprečeni napadi so pokazali, da je teroristična grožnja še vedno realna in resna.

Teroristične skupine v svoji propagandi izkoriščajo aktualne oborožene konflikte, v katerih je tarča muslimansko prebivalstvo, s čimer neposredno vplivajo na vse pogostejše primere radikalizacije mladih in mladoletnih. Hitra digitalizacija družbe in vesplošna dostopnost interneta sta ekstremističnim skupinam omogočili, da na subtilne in učinkovite načine širijo svoje skrajne ideje, s čimer pomenijo resno grožnjo družbi. [Radikalizacija mladih prek svetovnega spleta predstavlja resen izziv za sodobno družbo.](#)

Kako se mladi radikalizirajo prek spleta?

V današnjem času mladi primarno uporabljajo za medsebojno komunikacijo in izmenjavo informacij družbena omrežja. Ekstremistične skupine pa ta omrežja izkoriščajo za širjenje svoje skrajne propagande, ustvarjanje zaprtih skupin in manipulacijo ter novačenja mladih za svoje politične in ideološke cilje. Podobno se za komunikacijo, novačenje in indoktrinacijo uporabljajo nekatere spletne video. Video platforme, kot sta npr. YouTube in TikTok ter druge omogočajo enostavno/ciljno širjenje video vsebin, ki promovirajo ekstremistične ideje in nasilje. Te vsebine so pogosto privlačne za mlade zaradi svoje dinamične in jasne oblike sporočil. Nenazadnje tudi forumi in druge spletne skupnosti omogočajo ekstremističnim skupinam, da vzpostavijo tesnejše stike z mladimi in jih postopoma radikalizirajo, tudi za izvajanje nasilnih dejanj.

Zakaj so mladi ranljivi za radikalizacijo?

Mladi v obdobju odraščanja iščejo svojo identiteto in vlogo v družbi. Ekstremistične skupine jim lahko ponudijo občutek pripadnosti določeni skupnosti ter njim jasne in razumljive odgovore na vprašanja o smislu življenja, kar je za mnoge mlade zelo privlačno, saj zapolnjuje vrzeli, ki se porajajo v času odraščanja in iskanja svojega mesta

in vloge v družbi. Mladi, ki se počutijo osamljeni ali izključeni iz družbe, se zatekajo po družbene stike na internet, ki je najenostavnejša pot do navezave stikov s številnimi podobno mislečimi. Takšni posamezniki so še posebej ranljivi za vpliv ekstremističnih skupin, ki jim ponujajo občutek povezanosti in sprejetosti. Človek je v mladosti pogosto odprt za različne družbene ideje, večina mladih pa je tudi nezadovoljnih z obstoječimi politikami in družbenim sistemom, kar lahko vodi k večji dovzetnosti za radikalne ideje, ki obljublajo spremembe v družbi.

Kako se lahko borimo proti radikalizaciji?

Pomembno je, da se mlade že v zgodnji mladosti s formalnimi in neformalnimi oblikami izobraževanja opremi z znanjem o različnih kulturah in religijah ter se jih nauči kritičnega mišljenja. Pri preprečevanju radikalizacije imajo izjemno pomembno vlogo starši in družina. Ti morajo biti pozorni na spremembe v vedenju svojih otrok in se z njimi odprto pogovarjati o njihovih pogledih na svet. Državne institucije, kot so šole, zdravstvo in socialne službe imajo pomembno vlogo pri preprečevanju radikalizacije v družbi. Učitelji, zdravniki in drugi državni uslužbenci morajo biti usposobljeni za prepoznavanje znakov radikalizacije pri mladih in za pravočasno ukrepanje ter nudenje ustrezne psihosocialne podpore. Nevladne organizacije imajo pri tem dopolnilno vlogo zagotavljanja alternativnih možnosti vključevanja posameznika v družbo in odvrčanja od ekstremističnih idej. Svojo odgovornost pri preprečevanju radikalizacije pa imajo tudi ponudniki spletnih storitev, ki morajo skrbeti, da se prek njihovih platform ne širijo ekstremistične in nasilne vsebine.

Za uspešno soočanje z radikalizacijo je nujno potrebno nadaljnje razvijanje programov, ki bodo posameznikom pomagali razviti odpornost na ekstremistične ideje, dezinformacije in teorije zarot. Pri tem je nujno sodelovanje vseh deležnikov ter okrepitev nadzora nad internetom, s ciljem omejitve širjenja ekstremistične propagande in pozivov k nasilju. Korak v to smer je bil storjen tudi z implementacijo Uredbe EU o obravnavanju razširjanja terorističnih spletnih vsebin v slovenski pravni red.

1.2. Neregularne migracije



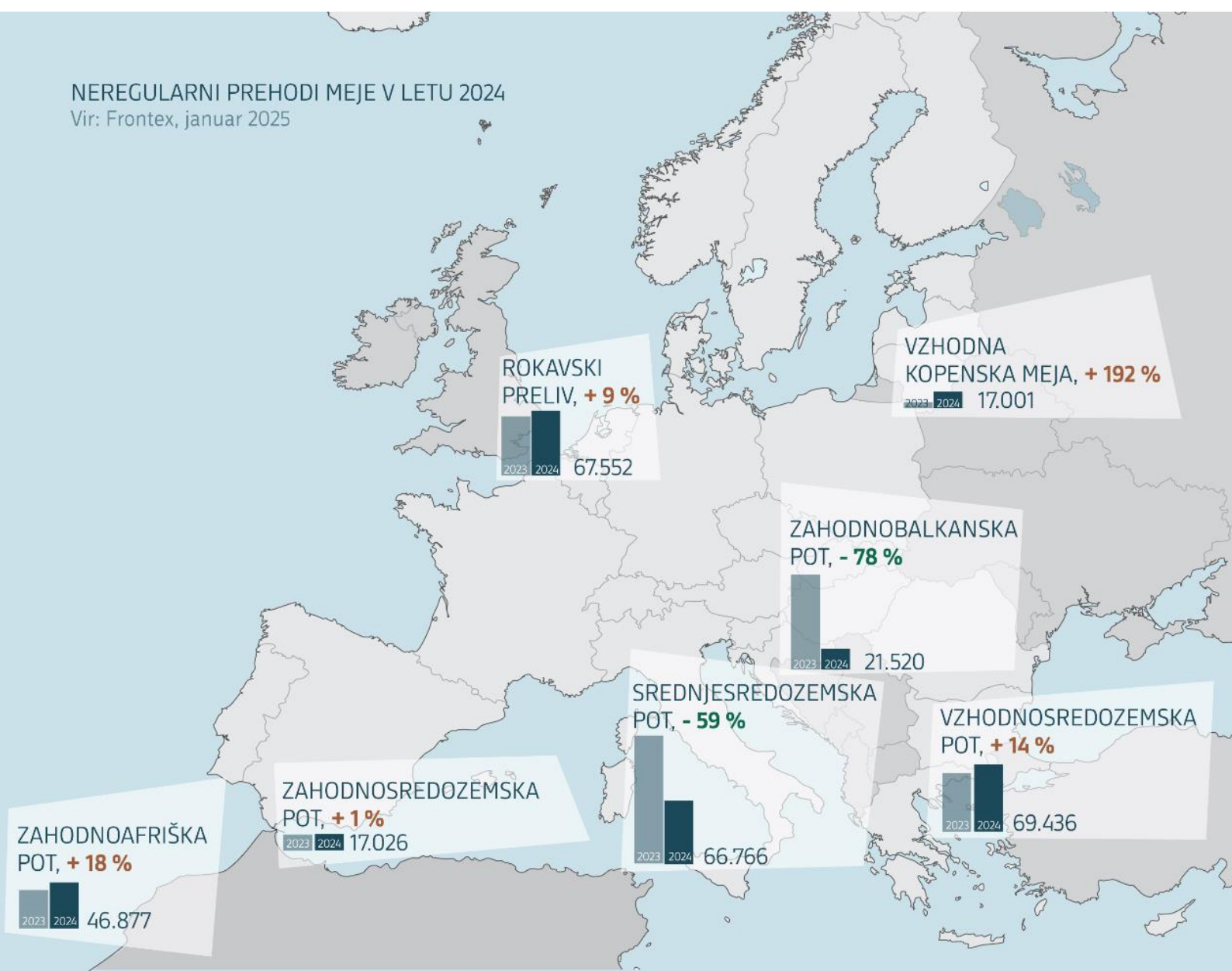
Migracije proti Evropi so v letu 2024 upadle. Slovenija ostaja pretežno tranzitna država za neregularne migrante.

V migrantskih tokovih proti Evropi, ki jih najpogosteje narekujejo varnostno-politične in ekonomske razmere v izvornih državah migrantov, je za Republiko Slovenijo najpomembnejša t. i. zahodnobalkanska pot, katere del poteka tudi preko naše države. Z njimi je v veliki meri povezano tudi delovanje kriminalnih tihotapskih združb, ki težke življenjske razmere migrantov zlorablajo za lastno korist in dobiček, hkrati pa dodatno ogrožajo nacionalno varnost ciljnih držav zaradi možnosti infiltracije radikaliziranih posameznikov v migrantske tokove.

Migracije proti Evropi so v letu 2024 upadle. Po podatkih Frontexa je zunanje meje EU nezakonito prestopilo 239.000 oseb, kar je 38 odstotkov manj kot leto prej. Po oceni Frontexa je k upadu najbolj prispevalo sodelovanje EU in partnerskih držav v boju proti tihotapskim omrežjem. Največji upad so zabeležili na osrednjesredozemski in zahodnobalkanski poti, medtem ko se je število prihodov preko vzhodnosredozemske, atlantske in vzhodnoevropske poti povečalo. Intenzivnost delovanja kriminalnih tihotapskih združb je še vedno visoka.

NEREGULARNI PREHODI MEJE V LETU 2024

Vir: Frontex, januar 2025



Na migracijska gibanja so vplivali različni dejavniki, med njimi slabšanje gospodarskih razmer, politična nestabilnost, oboroženi konflikti ter posledice podnebnih in demografskih sprememb v izvornih državah, delovanje tihotapskih omrežij in razširjena uporaba družabnih omrežij. Velik vpliv je imela tudi migracijska politika ključnih tranzitnih držav, predvsem Turčije, Libije, Tunizije, Libanona in zahodnoafriških držav. Najštevilnejši so bili prebežniki iz Sirije, Afganistana, Bangladeša, Turčije, Maroka in Podsaharske Afrike.

[Slovenija ostaja pretežno tranzitna država za neregularne migrante.](#) Po podatkih Slovenske policije je v letu 2024 notranje schengenske meje nedovoljeno prestopilo 46.186 oseb, kar je 23,8 odstotka manj kot leto prej. Velika večina jih je vstopila v Slovenijo iz Hrvaške, med njimi pa so prevladovali državljani Sirije, Afganistana, Turčije, Maroka in Bangladeša. Migranti so večinoma potovali po kopenskih poteh iz Turčije preko Grčije in Severne Makedonije ali Bolgarije v Srbijo, od tam pa proti BiH, Hrvaški, Sloveniji in Italiji ali proti Madžarski in Avstriji. Nekateri so za zakonit prihod na Balkan izkoristili tudi brezvizumske režime ali pridobili delovno dovoljenje, kasneje pa so se odpravili v ciljne evropske države. Na zahodnobalkanski poti delujejo dobro organizirana in prilagodljiva tihotapska omrežja, ki migrantom ponujajo številne možnosti potovanja. Cene tihotapskih storitev so se v minulem letu zvišale.

1.3.

Mednarodni organizirani kriminal

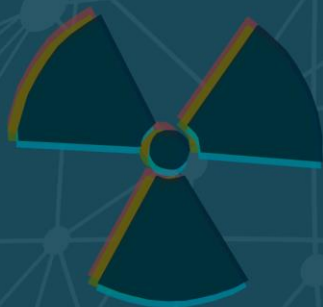


Mednarodne kriminalne združbe predstavljajo tveganje tako zaradi svojih nezakonitih dejavnosti kot notranjih obračunov – oboroženi incidenti, naročeni umori na javnih mestih.

Aktivnosti mednarodnih kriminalnih združb pomenijo stalno grožnjo in varnostno tveganje za Slovenijo in njene državljane. Te združbe izrabljajo ozemlje Slovenije večinoma za tranzitno območje pri tihotapljenju prepovedanih drog v države EU, v manjši meri pa je Republika Slovenija tudi ciljno območje. Ukvarjajo se tudi z organiziranjem in izvajanjem ilegalnih migracij, nezakonito trgovino z orožjem in razstrelivom, izdelavo in trgovanjem s ponarejenimi dokumenti ter pranjem denarja, pridobljenega s kriminalnimi aktivnostmi. Pri izvajanju teh nezakonitih aktivnosti so najbolj aktivne kriminalne združbe z Zahodnega Balkana, ki delujejo vzdolž balkanske tihotapske poti, ter iz vzhodnoevropskih in azijskih kot tudi držav Bližnjega vzhoda in Severne Afrike.

V Sloveniji živeti tujci in slovenski državljani, ki so povezani s kriminalnimi združbami, za slednje prenašajo denar iz držav Evropske unije v različne države Južne Amerike, v nasprotni smeri pa organizirajo tihotapljenje drog na območje EU. [Mednarodne kriminalne združbe z območja Zahodnega Balkana so bile v zadnjih letih odgovorne tudi za izvedbo večjega števila oboroženih incidentov in umorov po naročilu \(v državah Zahodnega Balkana, pa tudi v Sloveniji in v drugih državah EU\), ki so jih večinoma na javnih mestih izvedli pripadniki konkurenčnih klanov.](#) V napadih je bilo uporabljeno strelno orožje in/ali eksplozivne naprave, ranjenih ali ubitih pa večje število ljudi. Finančna sredstva pridobljena s kriminalnimi aktivnostmi pa člani kriminalnih združb legalizirajo z vlaganjem v nepremičnine.

Pri nelegalnih dejavnostih tihotapljenja migrantov delujejo na zahodnobalkanski poti tudi člani sirskih, afganistanskih, iraških in kurdskih mednarodnih kriminalnih in tihotapskih združb. Ti delujejo med Pakistanom oz. Afganistanom, Turčijo ter vzdolž zahodnobalkanske migrantske poti in organizirajo nezakonite prevoze tujcev preko tranzitnih držav Zahodnega Balkana, Hrvaške in Slovenije do ciljnih držav EU. Kot organizatorji in prevozniki ilegalnih migrantov delujejo tudi tuji državljani, ki prebivajo v Sloveniji in sodelujejo z državljani Slovenije, pa tudi tujci, ki za ta dejanja že prestajajo zaporne kazni v Sloveniji, ter različni tuji državljani z urejenim statusom v Sloveniji, kakor tudi prosilci za mednarodno zaščito. V Sloveniji močno narašča število obsojencev zaradi izvajanja kaznivih dejanj tihotapljenja ljudi in droge.



1.4.

Kršenje mednarodnih pogodb
o prepovedi širjenja orožja
za množično uničevanje
in mednarodnih gospodarskih
sankcij



Sova skupaj z drugimi državnimi organi in tujimi partnerskimi varnostno-obveščevalnimi službami aktivno sodeluje pri preverjanju in pridobivanju podatkov o morebitnih kršitvah mednarodnih konvencij in pogodb proliferacijsko spornih držav in podjetij. Pri tem je pozorna predvsem na preprečevanje njihovih aktivnosti preko slovenskega ozemlja ter morebitne kršitve mednarodnih konvencij in pogodb, ki so obvezujoče za Republiko Slovenijo na področju proliferacije oz. preprečevanja širjenja orožja, sredstev in opreme za množično uničevanje ter blaga za t. i. dvojno rabo. Posebna pozornost je namenjena tudi spremljanju domnevnih proliferacijskih aktivnosti slovenskih podjetij in podjetij v lasti tujih državljanov v Sloveniji ter njihovim poskusom izogibanja mednarodnim sankcijam proti državam, za katere veljajo omenjene sankcije, in aktivnostim drugih proliferacijsko spornih posredniških podjetij v tretjih državah.

V Sloveniji se zaradi njenega statusa regionalnega transportno-logističnega vozlišča vsako leto obravnavajo obsežne količine uvoznih in izvoznih pošiljk, med katerimi so tudi raznovrstni strateško pomembni materiali in izdelki za dvojno rabo, ki se uporabljajo tako v civilne kot vojaške namene in so zato podvrženi strogemu kontrolnemu režimu.

Tudi v letu 2024 smo tudi zaznali poskuse tujih podjetij za nabavo posameznih komponent pri slovenskih proizvajalcih, ki sodijo v kategorijo blaga z dvojno rabo – to pomeni, da se jih lahko uporabi za sestavljanje naprav za civilno rabo kot tudi za oborožitveno industrijo.

1.5.

Obveščevalno
delovanje
tujih
akterjev

Tuje obveščevalne aktivnosti, usmerjene proti slovenskim interesom, ugotovljene tudi v letu 2024.

Sova v okviru protiobveščevalne dejavnosti odkriva in preprečuje tuje obveščevalno delovanje proti interesom slovenske nacionalne varnosti. Pomemben pa je tudi prispevek Sove pri zagotavljanju protiobveščevalne zaščite Nata in Evropske unije.

Dinamika odnosov med svetovnimi velesilami, tudi na primeru vojne v Ukrajini, v določeni meri vpliva na obseg in načine tujega obveščevalnega delovanja. Tuje obveščevalne službe lahko ob svojih osnovnih nalogah pridobivanja podatkov izvajajo tudi druge sovražne aktivnosti v okviru tujega zlonamernega hibridnega delovanja. Povečana mednarodna vidnost in aktivnost naše države, kot je aktualni dvoletni mandat v Varnostnem svetu OZN, samo še krepi tuje obveščevalne interese za Republiko Slovenijo.

Avgusta 2024 se je z izmenjavo zapornikov med Rusijo in zahodnimi državami po intenzivnih pogajanjih dokončno zaključila aktivnost agencije na protiobveščevalnem področju, ki je privedla do aretacije dveh pripadnikov ruske obveščevalne službe v Sloveniji. Obe osebi, ki sta v Sloveniji delovali pod skrbno izgrajeno krinko, sta bili skupaj z drugimi zamenjani za državljane EU, ZDA in Ruske federacije, ki jim je bila v Ruski federaciji neupravičeno odvzeta prostost in so bili obsojeni zgolj zaradi svojih političnih prepričanj, novinarske dejavnosti ali na opozarjanja na kršitve človekovih pravic in temeljnih svoboščin.

1.6.

Kibernetske grožnje kritični infrastrukturi

Sova pridobiva predvsem podatke o morebitnem obveščevalnem ozadju tujih groženj slovenski digitalni infrastrukturi, ki bi lahko imele škodljive posledice za nacionalno varnost in interese Republike Slovenije.

Kibernetski prostor ostaja pomembna domena v mednarodnem varnostnem okolju, kjer medsebojno konkurenčne države še naprej izkoriščajo svoje tehnične kapacitete za izvedbo kompleksnih kibernetskih operacij vohunjenja in vplivanja, v primerih vojaških konfliktov tudi uničevanja, z namenom doseganja lastne prevlade in pridobivanja strateške prednosti pred tekmicami. Tovrstne napredne in vztrajne kibernetske grožnje (angl. *Advanced Persistent Threat* ali *APT*) povezujemo predvsem z vojaškimi silami ali obveščevalnimi službami, ki delujejo v skladu z usmeritvami in interesi tujih držav.

Gre za napredne kibernetske akterje z obsežnimi tehničnimi in finančnimi sredstvi, ki iščejo možnosti dolgoročnega dostopanja do informacijsko-komunikacijskih sistemov tuje kritične infrastrukture, v katerih bi lahko nato izvajali organizirane, prikrite in dolgoročne operacije pridobivanja obveščevalnih in drugih strateško pomembnih podatkov. Dostop do ciljnih omrežij lahko izkoriščajo tudi za druge oblike zlonamernih aktivnosti, kot so informacijsko, propagandno ali uničevalno delovanje. Pri tem lahko delujejo pod krinko drugih, navadno manj sofisticiranih zlonamernih kibernetskih akterjev, kot so finančno motivirani kibernetski kriminalci ali ideološko motivirani haktivistični kolektivi, kar jim v primeru razkritja omogoča zanikanje odgovornosti in izogibanje posledicam svojih dejanj.

Republika Slovenija je v trenutnih varnostnih razmerah kot država članica EU in Nata ter nestalna članica Varnostnega sveta Organizacije združenih narodov predmet interesa geostrateško konkurenčnih držav in cilj delovanja tujih obveščevalnih služb, kar se pogosto odraža tudi v kibernetskem prostoru. Sova pridobiva predvsem podatke o morebitnem obveščevalnem ozadju tujih groženj slovenski digitalni infrastrukturi, ki bi lahko imele škodljive posledice za nacionalno varnost in interese Republike Slovenije.

1.7.

Hibridne grožnje

Destabilizacija družbenih in varnostnih razmer - eden izmed osrednjih strateških ciljev tujega hibridnega delovanja.

Dinamika odnosov med svetovnimi velesilami, generira razmere, v katerih se lahko hibridne grožnje znajdejo v ospredju varnostnih in obveščevalnih zaznav. V teh razmerah lahko tuje obveščevalne službe poleg pridobivanja obveščevalnih podatkov izvajajo tajne hibridne operacije, s ciljem vplivanja na določeno javnost, vnašanja razdora, povzročanja nezaupanja v demokratične procese ali dvomov v učinkovitost delovanja nacionalno-varnostnih sistemov. [Destabilizacija družbenih in varnostnih razmer je tako eden izmed osrednjih strateških ciljev tujega hibridnega delovanja.](#)

V preteklem letu je bilo mogoče tudi preko javne razprave slediti več varnostno relevantnim pojavom iz opisane kategorije groženj. Ob nekaterih podatkih in ocenah, da bi lahko bile tuje obveščevalne službe v ozadju načrtovane sabotaže vojaške pomoči Ukrajini v Nemčiji ter nekaterih sabotažnih aktivnosti proti telekomunikacijski in prometni infrastrukturi ob zadnjih olimpijskih igrah v Franciji, je postajala teza o spremenjeni in bolj agresivni naravi tujega hibridnega delovanja bolj verjetna. K temu so dodatno prispevali podatki o dogodkih, v katerih so bili v Baltskem morju poškodovani podvodni telekomunikacijski tokovi, zaznani primeri samovžigov tovornih paketov na nekaterih linijah letalskega transportnega prometa in v večjih logističnih skladiščih, načrtovanje atentata na direktorja nemškega orožarskega podjetja ter sabotaža večjega števila avtomobilov v Nemčiji. Tovrstni pojavi so bili v širšem smislu varnosti letalskega prometa še posebej resno obravnavani. Pojavile so se dokaj relevantne ocene, da so nekatere države in njihove tajne službe v omenjenem tekmovanju med velesilami pripravljene sprejeti visoko ceno civilnih kolateralnih dogodkov in žrtev za doseg ciljev svojega hibridnega delovanja.

V kontekstu hibridnih groženj je potrebno omeniti tudi moč družbenih omrežij in množičnih spletnih platform, ki lahko odločilno vplivajo na razvoj javnega mnenja in posledično tudi na procese demokratičnega odločanja. Tovrstna razprava se je še okrepila ob lanskih predsedniških volitvah v Romuniji. V Sloveniji smo bili zaradi podpore Ukrajini v preteklem letu priča tujemu hibridnemu delovanju v obliki večkratnih kibernetских aktivnosti proti spletnim stranem predsednice republike in drugih slovenskih organov, agencij in podjetij. Pri tem je šlo predvsem za poskus psihološkega vplivanja na slovensko javnost preko objav na družbenih omrežjih in posledičnega medijskega poročanja o incidentih, ki niso imeli resnejših posledic za delovanje slovenske digitalne infrastrukture.



1.8. Gospodarska varnost

Različni dejavniki tveganja v spremenjenem mednarodnem varnostnem okolju vnesli precejšnjo negotovost v ustaljene globalne dobavne verige, posledice občutilo tudi slovensko gospodarstvo.

V razmerah nenehnega prilagajanja novim kriznim razmeram, gospodarskega ohlajanja in prihajajoče recesije je rasel pomen zelenega prehoda, digitalizacije in razvoja tehnologij prihodnosti. Spreminjajoča se mednarodna dinamika in posledično zaostreno gospodarsko okolje sta države prisilila v večjo angažiranost pri zagotavljanju konkurenčne prednosti in privilegiranega položaja v odnosu do drugih držav, predvsem na področju strateško pomembnih panog in tehnološkega razvoja.

Zaostreni odnosi med Zahodom in Rusijo, negotov razvoj vojne v Ukrajini, nestabilne razmere na Bližnjem vzhodu in posledična blokada trgovskih poti čez Sueški prekop so vnašali nemir v mednarodne trgovinske odnose in vzbujali skrb pred prekinitvijo, motnjami in spremembami logističnih poti, pomembnih za dostop do strateško pomembnih surovin, materialov in energentov. Ti dejavniki tveganja so v mednarodno skupnost vnašali precejšnjo negotovost glede ohranjanja stabilnosti ustaljenih globalnih dobavnih verig, posledice pa je občutilo tudi slovensko gospodarstvo.

Na povečane potrebe po boljši obveščeni v zvezi z omenjenimi tveganji je odgovorila tudi Sova, ki je bila pozorna na aktivnosti tujih držav in akterjev, ki bi lahko pomembno vplivali na gospodarsko stabilnost Republike Slovenije, predvsem na področjih kritične infrastrukture in tehnologije, strateško pomembnih industrijskih panog, logistike, dostopa do ključnih informacij ter varovanja podatkov države in njenih prebivalcev. Slednje je pomembno predvsem z vidika potencialnih tveganj, ki izhajajo iz nezaželenih posledic tovrstnih aktivnosti, ki posledično lahko vodijo v zmanjšanje gospodarske konkurenčnosti domačih podjetij in nacionalne blaginje ter ustvarjajo neenake pogoje na trgu.

ice.svet24.si/clanek/novice/ slovenija /66044e6f3119f/ruski-
badli-spletno-stran-predsednice-pirc-musar
ji, slava predsedniku Putinu

om/novice/ slovenija /ruski-hekerji-napovedali-nov-
html
osilo in nadaljujemo
lovenije - hvala za podporo, mi smo z vami, vi ste z nami!!!
li v naši prijazni in topli ekipi

o izvedli vrsto kibernetičkih napadov na spletna mesta kritične
e v Slovenija v povezavi s podporo njene vlade ukrajinskemu režimu, ki
zločinskega, na čelu z Zelenskim. Prebivalci Slovenija so večkrat izrazili
vo nad dejstvom, da ukrajinske oblasti uporabljajo svoja davčna sredstva
privržencem Bandere, namesto da bi reševale notranje probleme.

zagotovo ni všeč, da proukrajinske oblasti zaradi hvaljenja Stoltenberga
zapravljajo za pitanje Banderovih privržencev – pred kratkim Slovenija se
češki pobudi za nakup topniških granat za teroriste Zelenskoga
zi slovensko internetno infrastrukturo in nismo pustili neprevrnjenega kamna

2. IZPOSTAVLJENO

2.1

Proruske
haktivistične
aktivnosti
proti
Sloveniji

... /ruski-hekerji-napadi-
predsednica-spletna-
... /ruski-hekerji-napadi-
urad-

MMC
Znanost in tehnologija Zdravje Okolje Lokalne novice Številke Planica 27. 3. 2024 | 21:27
Kibernetički napad na spletno stran predsednice republike.
Hakerji napovedujejo še več napadov.
SI-CERT: Ne gre za vdor v sistem
27. marca 2024 ob 17:34 | Objavljeno - MMC RTV SLO
Al. Ma.
Hakerji so napadli uradno spletišče predsednice republike, ki je bilo popoldne
nedosegljivo. SI-CERT je potrdil, da ni šlo za vdor v sistem, temveč zgolj za upočasnitev
delovanja in da so podatki varni.
Dragi kibernetički borci! Naša pobuda za napad na vladna spletna mesta Slovenija
opazili skoraj vsi vodilni novičarski portali v državi, še posebej pa o njem piše državna
televizija Slovenija : <https://www.rtvslo.si/znanost-in-tehnologija/kibernetiski-napad-na-spletno-stran-predsednice-republike-hekerji-napovedujejo-se-vec-napadov/703077>

Spreminjajoče mednarodno varnostno okolje je v zadnjih letih sprožilo porast zlonamernih kibernetских aktivnosti, povezanih s haktivizmom (angl. *hacking + activism*). Pojem označuje vrsto aktivističnega delovanja v nasprotnikovem kibernetickem prostoru z namenom dostopanja do občutljivih podatkov ali povzročanja motenj v delovanju informacijskih sistemov, pri čemer so glavni motivi haktivistov zastopanje lastnih stališč, zasledovanje določenih političnih ali družbenih interesov in diskreditacija nasprotne strani. Verjetno najbolj prepoznaven predstavnik tovrstnega gibanja je mednarodni kolektiv Anonymous.

V evropskem kibernetickem prostoru trenutno najbolj izstopajo proruski haktivistični akterji, ki so po začetnem fokusu na ukrajinske cilje svoje delovanje sčasoma razširili tudi proti drugim evropskim državam, članicam EU in Nata. [Najpogosteje izvajajo manj sofisticirane aktivnosti začasnega onemogočanja spletnih mest na daljavo z ustvarjanjem množičnega prometa \(angl. *Distributed Denial of Service* ali na kratko *DDoS*\), ki jih skupaj s svojimi propagandnimi sporočili redno promovirajo na družbenih omrežjih.](#) V preteklem letu, ko je število tovrstnih incidentov proti evropskim državam skokovito naraslo, je njihovo pozornost pritegnila tudi Republika Slovenija.

Konec marca so naši državi v objavi na družbenih omrežjih napovedali povračilne ukrepe za podporo ukrajinskim prizadevanjem v vojni z Rusijo, ki so se v naslednjih dnevih, tednih in mesecih odražali predvsem v obliki DDoS aktivnosti proti uradnim spletnim stranem predsednice dr. Nataše Pirc Musar in drugih državnih organov, agencij ter gospodarskih družb v Sloveniji. Po ugotovitvah pristojnih organov pri tem poleg začasne nedosegljivosti spletnih strani ni prišlo do resnejših groženj za slovensko omrežno infrastrukturo.

Kaj so proruski haktivisti pridobili s ciljanjem slovenskega spletišča?

Zagotovili so si predvsem medijsko odmevnost in posledično pozornost javnosti, kar je njihov osnovni cilj in s čimer se radi pohvalijo. S prikazovanjem svojih navidezno visokih zmogljivosti in vzbujanjem strahu med drugače mislečimi želijo psihološko vplivati na nasprotno stran, pri tem pa pri poudarjanju svojega vpliva neredko pretiravajo. Pogosto nagovarjajo ideološko podobno usmerjeno lokalno prebivalstvo in jih vabijo k

sodelovanju. Vse naštetu je bilo iz njihovih objav na spletu razvidno tudi v primeru delovanja proti Sloveniji.

Kljub relativno omejenim škodljivim posledicam najpogostejših oblik haktivističnih kibernetских aktivnosti pa tovrstnih groženj ne gre prehitro odpisati. Treba je upoštevati dejstvo, da se različni kolektivi med seboj razlikujejo po tehničnem znanju, sposobnostih in kapacitetah, kar lahko privede do različnih oblik ofenzivnega kibernetičnega delovanja. Tako so ideološko motivirani akterji v preteklosti že izvajali resnejše kibernetične aktivnosti z izsiljevalsko programsko opremo (angl. *ransomware*) in vdore v omrežja z zaupnimi podatki, ki jih navadno pripisujemo tehnično bolj podkovanim skupinam. V teh primerih lahko gre za medsebojno povezovanje in sodelovanje različnih akterjev, prav tako pa niso izključene niti povezave s tujimi obveščevalno-varnostnimi strukturami, ki bi lahko haktivistične aktivnosti izkoriščale predvsem za prikrivanje lastnega operativnega delovanja in interesov.

2.2.

Tajnost



Za učinkovitost vsake obveščevalne službe je tajnost delovanja eden osnovnih postulatov – tudi za Sovo. Na ta način zaščitimo svoje vire, ukrepe in dejavnosti, ki so nujni potrebni za pravočasno pridobivanje kakovostnih varnostno relevantnih podatkov. Pridobljene podatke metodološko ovrednotimo in posredujemo prejemnikom informacij agencije.

Razkrivanje podatkov agencije, ki se nanašajo na izvajanje njenih nalog, opredeljenih v 2. členu Zakona o Slovenski obveščevalno-varnostni agenciji, nepoklicanim osebam bi za agencijo pomenilo vsaj tveganje za nadaljnje izvajanje aktivnosti, krnitev njihove učinkovitosti in tudi nevarnost za posameznike – tako tajne sodelavce kot zaposlene v agenciji. Posledično bi se krepila tveganja in grožnje za varnostne, politične in gospodarske interese države, nacionalno varnost in ustavno ureditev Republike Slovenije.

Formalnopravno je tajnost v Sloveniji urejena v Zakonu o tajnih podatkih in povezanih predpisih. Glede na možne škodljive posledice razkritja nepoklicanim osebam se tajnim podatkom lahko določijo štiri stopnje tajnosti:

- INTERNO
- ZAUPNO
- TAJNO in
- STROGO TAJNO.

Zakonsko je urejeno tudi ravnanje s tajnimi podatki – označevanje, hramba, prenašanje, omejitve glede seznanitve in razmnoževanja, posredovanja.

Do tajnih podatkov smejo dostopati le osebe, ki imajo veljavno dovoljenje za dostop do tajnih podatkov ustrezne stopnje tajnosti in se z določenim tajnim podatkom morajo seznaniti zaradi izvajanja svojih delovnih nalog. Najvišji državni predstavniki dovoljenja za dostop do tajnih podatkov ne potrebujejo. Vsak, ki se s tajnim podatkom seznanil, je dolžan varovati ta tajni podatek, ne glede na to, kako se je z njim seznanil.

Tajnost delovanja agencije in pridobljenih ali posredovanih podatkov je uravnotežena s številnimi notranjeorganizacijskimi ukrepi in nadzornimi mehanizmi ter oblikami zunanjega nadzora – vladnega, parlamentarnega, finančnega, nadzora javnosti preko Varuha človekovih pravic, Informacijskega pooblaščenca in splošne ali strokovne javnosti v skladu z določbami Zakona o dostopu do informacij javnega značaja. S temi varovalkami se kljub siceršnji tajnosti zagotavlja transparentnost delovanja agencije in sistemsko urejeno ravnanje s tajnimi podatki.

3.

SOVA

V ŠTEVILKAH



KADRI

42% žensk | **58%** moških

47,9 let | povprečna starost zaposlenih

71% zaposlenih s VII. stopnjo izobrazbe

24,8 let | povprečna delovna doba



PRORAČUN

21.473.743,70 EUR

veljavni proračun agencije na dan 31. 12. 2024

