



SIGURNOSNO-OBAVJEŠTAJNA AGENCIJA

**JAVNO IZVJEŠĆE
2020./21.**



MISIJA

Prikupljanjem i analizom podataka od značaja za nacionalnu sigurnost, SOA prepoznaje, istražuje i razumijeva prijetnje i izazove nacionalnoj sigurnosti pružajući državnom vodstvu i ostalim tijelima pouzdanu podlogu u odlučivanju i djelovanju u zaštiti nacionalne sigurnosti, interesa i dobrobiti građana Republike Hrvatske.

VIZIJA

Moderna, učinkovita i odgovorna sigurnosno-obavještajna agencija, primjerena potrebama, usmjerena na ostvarivanje svoje misije i postizanje vrhunskih rezultata, sa značajnim nacionalnim utjecajem i učinkom te regionalnim dosegom koja je prepoznata po razvijenim sposobnostima, izvrsnim djelatnicima i snažnim partnerskim vezama.

SADRŽAJ

Uvodno obraćanje	1
O Sigurnosno-obavještajnoj agenciji	3
Pandemija bolesti COVID-19 ima posljedice i na globalnu sigurnost.....	7
Teroristička prijetnja Evropi i dalje je značajna	9
Ekstremizam jača u vrijeme pandemije	12
Strano obavještajno i informacijsko djelovanje stalno je prisutno	13
Državno sponzorirani kibernetički napadi sve su zastupljeniji u špijunaži.....	16
Kibernetička otpornost postaje ključ zaštite nacionalne sigurnosti	18
Gospodarska sigurnost važan je dio nacionalne sigurnosti	22
Korupcija nanosi štetu državnom proračunu i gospodarstvu RH.....	24
Pitanje ratnih zločina i nestalih u Domovinskom ratu i dalje je otvoreno	25
Globalna geopolitička i gospodarska nadmetanja su dinamična i neizvjesna	26
Zapadni Balkan u sporom je procesu stabilizacije.....	28
Europsko okruženje obilježava nestabilnost.....	30
Organizirani kriminal je postao transkontinentalan	32
Nezakonite migracije dugotrajni su društveni i sigurnosni izazov	34
Međunarodna suradnja važan je segment rada SOA-e.....	36
Izvješćivanje korisnika svakodnevna je zadaća SOA-e	38
Nadzor rada SOA-e dio je demokratske prakse	40
Posao u SOA-i jedinstveni je izazov	41



Uvodno obraćanje

Poštovani,

naša javna izvješća postala su izvrstan alat kojim se može pratiti u kakvom promjenjivom i dinamičnom svijetu sigurnosti živimo. Od 2014. godine, ovo nam je sedmo po redu izvješće i u ovom kratkom razdoblju bili smo svjedoci brojnih i ponekad neočekivanih sigurnosnih trendova i pojava.

Svjedočili smo stvaranju, brzom širenju i teritorijalnom porazu tzv. Islamske države, najveće terorističke organizacije na svijetu; pratili smo kako su širenje demokratskih vrijednosti u svijetu zamijenile autoritarne tendencije uz vraćanje hladnoratovskih napetosti, špijunaže, plasiranja lažnih vijesti i propagande; kibernetičke tehnologije omogućile su provođenje velikih kibernetičkih napada u cilju krađe državnih i industrijskih podataka; nezakonite migracije doživjele su ogromni rast na jugoistoku Europe preko kojeg su prošle stotine tisuća migranata; u našem jugoistočnom susjedstvu aktivni su nezapadni akteri, a reforme za dostizanje europskih standarda sporo napreduju; organizirani kriminal u ovom dijelu Europe dodatno je osnažen međusobnim vezama i širenjem nezakonitih poslova; krizna žarišta poput Sirije i Libije još od prvog javnog izvješća predstavljaju izvorišta nestabilnosti i prijetnji; pratili smo kako svijetom sve više dominiraju procesi geopolitičkih preslagivanja i nadmetanja, a jačaju ambicije gospodarskih, političkih i vrijednosnih izazivača liberalnim demokracijama u međunarodnom poretku; klimatske promjene sve više pokazuju svoje posljedice; talibani su unatoč 20 godina međunarodnih npora u demokratizaciji tamošnjeg društva zavladali Afganistanom i konačno, svjedočimo najvećoj pandemiji u modernoj povijesti koja je uzrokovala nezabilježene poremećaje u svakodnevnom životu i nanijela ogromne štete globalnom gospodarstvu.

U isto vrijeme, od našeg prvog javnog izvješća možemo pratiti i brojne pomake u sigurnosnoj sferi: članstvo u EU i NATO-u omogućilo nam je multipliciranje naših sposobnosti i jačanje naših sigurnosnih mehanizama i veza prema drugim demokratskim sigurnosno-obavještajnim sustavima; europske države sve su bliže u suprotstavljanju zajedničkim sigurnosnim prijetnjama; hrvatsko društvo i institucije potvrstile su stabilnost i učinkovitost u brojnim kriznim situacijama; novi infrastrukturni projekti ojačali su našu energetsku i nacionalnu sigurnost; razvoj tehnologije omogućio nam je nove sposobnosti i mogućnosti zaštite nacionalne sigurnosti; gradimo novu generaciju naših djelatnica i djelatnika koji nam se javljaju za posao slijedom naših javnih poziva.

Sve ove promjene i pomaci ukazuju da je sigurnosna dinamika u suvremenom svijetu izuzetno brza i često nepredvidiva, jačaju nove i netradicionalne sigurnosne prijetnje, a uloga pravodobnih i točnih informacija i procjena postaje ključna.

Posjedovanje informacija i točnog uvida u sigurnosne i političke procese postaje preduvjet uspješnog razvoja. I upravo u tome se vidi važnost sigurnosno-obavještajne djelatnosti u suvremenom svijetu. Takve okolnosti nama u Sigurnosno-obavještajnoj agenciji predstavljaju

profesionalni izazov, jer smo upravo mi državna institucija koja donositeljima odluka treba ukazati na sigurnosne trendove i scenarije, upozoriti na prijetnje i izazove nacionalnoj sigurnosti, objasniti njihovu pozadinu i moguće posljedice i, konačno, omogućiti im donošenje informiranih odluka u zaštiti nacionalnih interesa.

Kao i ranijih godina, i ovo Javno izvješće potvrđuje da se Republika Hrvatska sigurna i stabilna demokracija te da, i u ovako izazovnom vremenu i dinamičnom sigurnosnom okruženju, nema naznaka njezine značajnije destabilizacije.

Da bismo se nosili s promjenjivošću današnjeg svijeta, potrebno je imati sposobne i obučene profesionalce, modernu tehnologiju i fleksibilnu organizaciju. Kako bismo ispunili svoju iznimno odgovornu ulogu, Sigurnosno-obavještajna agencija stalno prilagođava svoje djelovanje i organizaciju rada, ulaže u profesionalni razvoj svojih djelatnica i djelatnika i izgrađuje svoje tehničke sposobnosti.

Kako bi sposobnosti koje danas razvijamo pružile najbolju moguću zaštitu u budućnosti, razvijamo ih planski i odgovorno prema javnom novcu kojeg hrvatski građani za naš rad izdvajaju. Pri tome u Sigurnosno-obavještajnoj agenciji nastojimo pažljivo razvijati one sposobnosti kojima možemo pokriti široki spektar djelovanja i učinkovito ih prilagođavati potrebama i zahtjevima zaštite nacionalne sigurnosti.

Na ovaj način, usmjerenošću na učinak u provedbi svojih zadaća, profesionalnim razvojem svojih djelatnica i djelatnika te ulaganjem u nove sposobnosti, Sigurnosno-obavještajna agencija i nadalje će biti prva državna institucija u zaštiti nacionalne sigurnosti, interesa, demokratskog ustavnog poretka i građana Republike Hrvatske.

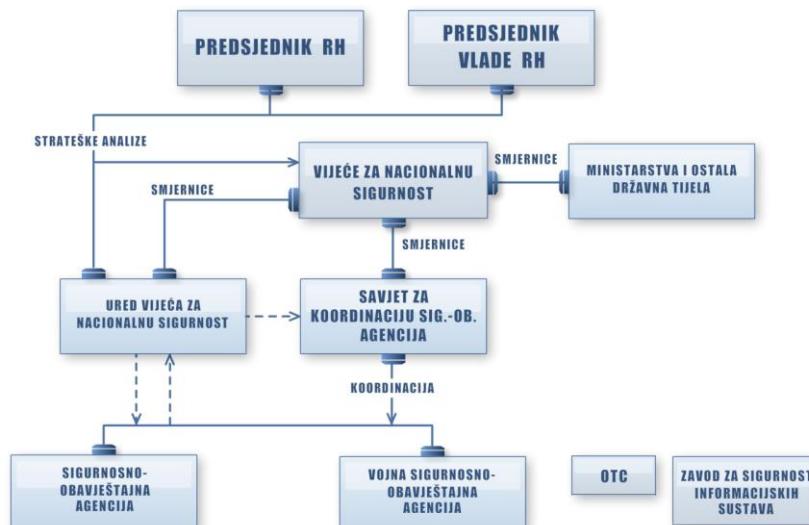
Ravnatelj

Daniel Markić

O Sigurnosno-obavještajnoj agenciji

Sigurnosno-obavještajni sustav Republike Hrvatske

Sigurnosno-obavještajni sustav u Republici Hrvatskoj (RH) definiran je 2006. godine Zakonom o sigurnosno-obavještajnom sustavu RH. U RH postoje dvije sigurnosno-obavještajne agencije: Sigurnosno-obavještajna agencija (SOA) bavi se civilnim dijelom zaštite nacionalne sigurnosti, a Vojna sigurnosno-obavještajna agencija (VSOA) se bavi vojnim i obrambenim dijelom sigurnosnih tema.



Rad sigurnosno-obavještajnih agencija usmjeravaju Predsjednik RH i Vlada RH kroz Vijeće za nacionalnu sigurnost (VNS). VNS, između ostalog, usmjerava rad sigurnosno-obavještajnih agencija, razmatra i procjenjuje prijetnje i rizike te donosi odgovarajuće smjernice i zaključke. Savjet za koordinaciju sigurnosno-obavještajnih agencija (Savjet) operativno usklađuje rad agencija, provodi odluke Predsjednika RH i Vlade RH o usmjeravanju rada SOA-e i VSOA-e te razrađuje odluke VNS-a koje se odnose na rad sigurnosno-obavještajnog sustava. Stručne i administrativne poslove za Vijeće za nacionalnu sigurnost i Savjet obavlja Ured Vijeća za nacionalnu sigurnost (UVNS). UVNS obavlja poslove koji Vijeću za nacionalnu sigurnost omogućavaju ocjenu rada i nadzor nad sigurnosno-obavještajnim agencijama.

Za poslove u tehničkim područjima sigurnosti informacijskih sustava i mreža državnih tijela nadležan je Zavod za sigurnost informacijskih sustava (ZSIS). Operativno-tehnički centar za nadzor telekomunikacija (OTC) aktivira i upravlja mjerom tajnog nadzora telekomunikacijskih usluga, djelatnosti i prometa, na zahtjev SOA-e i drugih zakonom ovlaštenih tijela uz odgovarajući nalog i odobrenje.

Uloga SOA-e

SOA prikuplja i analizira podatke u cilju otkrivanja i sprječavanja radnji pojedinaca ili skupina usmjerenih protiv opstojnosti, neovisnosti, jedinstvenosti i suvereniteta RH, ka nasilnom rušenju ustroja državne vlasti, ugrožavanju ljudskih prava i temeljnih sloboda te protiv osnova gospodarskog sustava RH. SOA prikuplja i analizira podatke političke, gospodarske, znanstveno-tehnološke i sigurnosne prirode koji se odnose na strane države, organizacije, političke i gospodarske saveze, skupine i osobe te ostale podatke od značaja za nacionalnu sigurnost.

SOA je zakonom ovlaštena prikupljati podatke sigurnosnog i obavještajnog značaja komunikacijom s građanima, potraživanjem službenih podataka od državnih i lokalnih tijela te pravnih osoba, primjenom tajnih mjera i postupaka te razmjenom podataka s partnerskim službama. SOA prikuplja podatke i iz javnih i otvorenih izvora.

Primjenu mjera tajnog prikupljanja podataka kojima se ograničavaju ustavna prava i slobode čovjeka i građanina odobravaju Vrhovni sud ili ravnatelj SOA-e, ovisno o vrsti mjere, a što je regulirano Zakonom o sigurnosno-obavještajnom sustavu RH.

O svojim saznanjima i procjenama od značaja za nacionalnu sigurnost SOA izvješćuje zakonom propisane korisnike informacija (državni vrh, ministarstva i ostala državna tijela).

Kao dio šireg sustava nacionalne i domovinske sigurnosti, SOA surađuje i dostavlja podatke i procjene drugim državnim tijelima poput Ministarstva unutarnjih poslova (MUP), Državnog odvjetništva, USKOK-a, Ministarstva vanjskih i europskih poslova (MVEP), Ministarstva obrane (MORH), Ministarstva finansija, Ministarstva gospodarstva i održivog razvoja i ostalih.

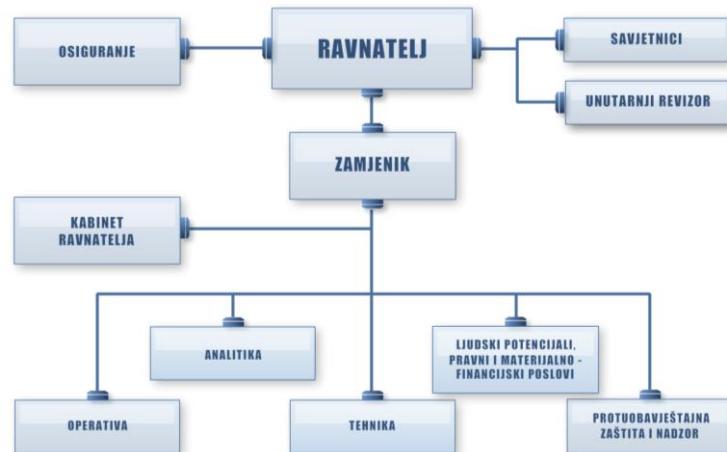


Organizacija i ustroj

Na čelu SOA-e je ravnatelj kojeg supotpisom imenuju Predsjednik RH i predsjednik Vlade RH. Dužnost ravnatelja SOA-e od 5. svibnja 2016. obavlja Daniel Markić, a 6. svibnja 2020. imenovan je na drugi mandat. Mandat ravnatelja SOA-e traje četiri godine.

SOA je ustrojstveno sastavljena od sljedećih cjelina:

- Operative koja se bavi prikupljanjem podataka,
- Analitike koja analizira podatke i izrađuje odgovarajuće analitičke uratke,
- Posebne tehnologije, informatike i komunikacija,
- Protuobavještajne zaštite i unutarnjeg nadzora i
- Ljudskih potencijala, pravnih i materijalno-finansijskih poslova.



Shema ustroja SOA-e

Usmjeravanje rada

Na provedbenoj razini, dokument kojim se usmjerava rad SOA-e su Godišnje smjernice za rad sigurnosno-obavještajnih agencija koje utvrđuje Vijeće za nacionalnu sigurnost. One su alat kojim Predsjednik Republike i Vlada RH usmjeravaju rad agencija te definiraju teme bitne za zaštitu i ostvarivanje nacionalne sigurnosti i interesa. Temeljem smjernica SOA planira svoj rad i izvješćuje korisnike. Godišnje smjernice ujedno su dokument koji služi kao okosnica za provedbu nadzora i ocjenjivanje ispunjavanja zadaća SOA-e.



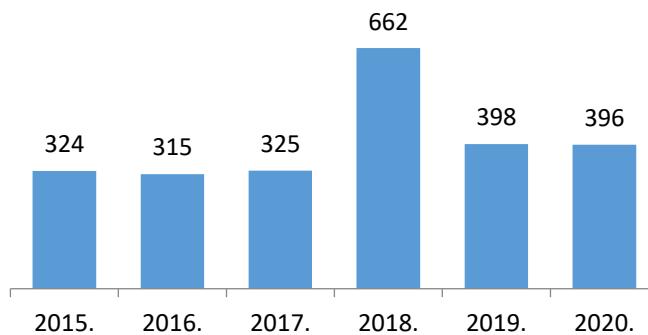
Grafički prikaz obavještajnog ciklusa

Uz Godišnje smjernice, rad SOA-e usmjeravaju strateški i dugoročni dokumenti poput Strategije nacionalne sigurnosti i Nacionalne strategije za prevenciju i suzbijanje terorizma.

Upravljanje proračunom

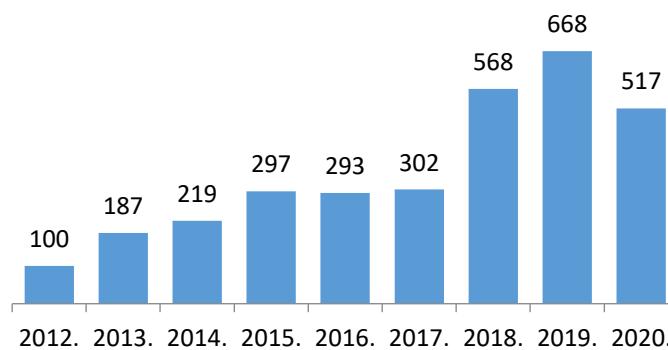
U 2020. godini proračun SOA-e iznosio je oko 396 milijuna kuna. Kao i ranijih godina, u strukturi proračuna SOA-e najveći udio čine izdaci za zaposlene, a potom tekući i kapitalni izdaci.

Struktura proračuna SOA-e je, slijedom zakonskih odredbi, tajna što je praksa i ostalih država članica EU-a i NATO-a. Unatoč tajnosti podataka, SOA u planiranju i izvršenju proračuna provodi sve propisane mjere usmjerene ka zakonitom i svrshishodnom korištenju proračunskih sredstava te izvješćuje nadležna državna tijela o proračunskim izdatcima.



Kretanje proračuna SOA-e po godinama, u milijunima kuna

Radi potreba rebalansa zbog pandemijskih uvjeta i pada gospodarske aktivnosti, proračun za 2020. godinu je smanjivan te su neki razvojni i modernizacijski projekti odgođeni ili je usporena njihova realizacija. Ipak, iznos uložen u razvoj i modernizaciju je i u 2020. godini bio značajan i osigurava SOA-i stalni napredak po pitanju izgradnje sposobnosti i tehnološkog razvoja. Sredstva za razvoj i modernizaciju ulažu se planski, kako bi se doabile sposobnosti kojima će SOA biti u mogućnosti odgovoriti na široki spektar sigurnosnih i tehnoloških izazova.



Indeks sredstava uloženih u razvoj i modernizaciju od 2012. do 2019. g. (2012. g. = 100)

Pandemija bolesti COVID-19 ima posljedice i na globalnu sigurnost

Uz sve javnozdravstvene i gospodarske posljedice, pandemija zarazne bolesti COVID-19 ima i značajan utjecaj na razvoj stanja sigurnosti u svijetu. Taj utjecaj kreće se u rasponu od osobne sigurnosti svakog pojedinca, stanja javne sigurnosti u pojedinim državama i regijama, do geopolitičkih promjena koje će utjecati na ukupni svjetski poredak i sigurnost.

Valovi pandemije uzrokovali su prenapregnutost zdravstvenih sustava. Države su, u pokušaju zaustavljanja širenja zaraze i očuvanja javnozdravstvenih sustava, ograničile kretanja ljudi, prometa roba i usluga uz zatvaranje dijela gospodarstava i društvenih djelatnosti, što je izazvalo globalni pad gospodarskih aktivnosti i jednu od najvećih gospodarskih kriza novijeg doba.

BDP Europske unije pao je 6% u 2020. godini, dok su posebno pogodjene bile države u kojima usluge i turizam čine značajan dio BDP-a, kao što su RH, Španjolska, Grčka i Italija. EU je na ovaj izazov odgovorila sveobuhvatnim paketom mjera za oporavak gospodarstava država članica.

Na gospodarsko-financijskom području pojačane su prijetnje europskim tvrtkama uzrokovanе nepoštenom konkurenциjom, krađom intelektualnog vlasništva, ali i pokušajima geopolitičkog preuzimanja visokotehnoloških tvrtki od strateške važnosti. Posebno se to odnosi na situacije kada europske strateške tvrtke, kojima je vrijednost dionica značajno pala nakon izbijanja pandemije, žele preuzeti strane kompanije u većinskom ili isključivom vlasništvu trećih država ili koje koriste prikrivene državne potpore u svojim državama. Pojedine članice EU već su predložile model državnog otkupa takvih dionica te usklađivanje tržišnih načela poslovanja s potrebom državne intervencije i uvođenja *protekcionističkih* mjera.

Države čija gospodarstva nisu u stanju prebroditi poteškoće uzrokowane gospodarskim i socijalnim poremećajima mogile bi biti suočene s rastom nezaposlenosti i siromaštva, a posljedično i s jačanjem kriminala, unutarnjim i vanjskim migracijama, socijalnim nemirima, ekstremizmom i nezadovoljstvom. U isto vrijeme, u pojedinim je državama pandemija usporila ili zaustavila rješavanje drugih društvenih i političkih pitanja.

Pandemija se svojom naglom pojmom i intenzitetom pojavila kao novi i dodatni pokretač repozicioniranja država u međunarodnim odnosima. Poremećaji u opskrbnim lancima, proizvodnji te ponudi i potražnji, posebice na početku pandemije, pokazali su ranjivosti globaliziranih gospodarskih procesa. Ovi poremećaji već pokazuju svoje posljedice u vidu nestaćice određenih proizvoda, usporenih proizvodnih procesa, poskupljenja repromaterijala i posljedičnih inflatornih pritisaka. Početkom pandemije došlo je do smanjenja, a ponegdje i do potpunog prekida proizvodnje, posebice repromaterijala i proizvoda u građevinskom sektoru. Nakon prvog vala pandemije i djelomičnog smirivanja situacije, gospodarske aktivnosti su ponovo pokrenute i potražnja je izuzetno naglo porasla. Proizvodni procesi nisu mogli pratiti tu dinamiku, što je utjecalo na smanjenu ponudu, nestaćicu sirovina, materijala i proizvoda,

uzrokovalo poremećaje na tržištu te izazvalo značajno povećanje cijene proizvoda i rada na europskom i svjetskom tržištu. Članice EU pojedinačno pokušavaju pružiti određene potpore i pomoći svojim gospodarstvima, ali se nameće potreba pronalaženja rješenja na razini EU.

Nestašica osnovnih namirnica i hrane u početku pandemije, čak i u visokorazvijenim zemljama, podigla je svijest o potrebi značajnije brige o prirodnim resursima, poput poljoprivrednog zemljišta i industrije hrane, kao jednom od prioriteta nacionalne sigurnosti.

Veliki broj europskih država suočio se s pokušajima korištenja zdravstvene i gospodarske krize za stjecanje nezakonitih prihoda. Manjak zaštitne opreme i sredstava na početku pandemije uzrokovao je nabavu tih roba alternativnim kanalima što je otvorilo mogućnost za različite manipulacije i nezakonita djelovanja pojedinaca i tvrtki s ciljem stjecanja protupravnih prihoda.



Pandemija je dodatno potaknula rast ekstremizma i radikalizma, pogotovo u okolnostima plasiranja dezinformacija i teorija zavjere oko europskog odgovora na krizu i učinkovitosti demokratskog i liberalnog političkog i društvenog uređenja. Pandemija je također iskorištena za nove informacijske aktivnosti u geopolitičkom nadmetanju, pa su tako pojedine države koristile medijski prostor za naglašavanje slabosti Zapada u suočavanju s pandemijom, dok su prikrivale vlastite nedostatke. Cilj ovakvih operacija utjecaja jest izazvati nepovjerenje javnosti u demokratske sustave vladavine i predstaviti autoritarne sustave kao učinkovitije u svim aspektima društvenog života. Jedno od područja ovih aktivnosti jest i Zapadni Balkan u čijem javnom prostoru su osobito zastupljene teorije zavjere i dezinformacije oko farmaceutske industrije, porijeklu virusa i svrsi cjepiva. S obzirom na bliskost južnoslavenskih jezika, dezinformacijama plasiranim u medijskom prostoru Zapadnog Balkana pokušava se utjecati i na percepciju javnosti u RH.

Rusija i Kina su *diplomaciju maski* s početka pandemije zamjenili *diplomacijom cjepiva*. *Diplomaciju cjepiva* podržavaju mediji pod državnom kontrolom uz cilj umanjivanja povjerenja javnosti u cjepiva proizvedena na Zapadu i institucije EU-a.

Pandemija je ukazala i na slabosti zdravstvenih sustava u kriznim situacijama što je u pojedinim državama dovelo do nabavke neodgovarajuće ili nekvalitetne medicinske opreme. Stoga se potvrdila važnost dostatnosti ljudskih i materijalnih resursa te otpornosti zdravstvenih sustava, kao i dostupnosti znanstveno-istraživačkih i proizvodnih kapaciteta u suočavanju s novim zdravstvenim izazovima.

Teroristička prijetnja Evropi i dalje je značajna

Trenutno nema utvrđenih izravnih terorističkih prijetnji hrvatskim institucijama, državljanima i interesima od strane terorističkih skupina/organizacija (neovisno o njihovoj ideologiji) te se teroristička prijetnja, odnosno prijetnja organiziranih napada terorističkih skupina i dalje procjenjuje niskom, ali se mogućnost provedbe terorističkog napada (prvenstveno samostalnih napadača) nikada ne može isključiti.

Iako su ISIL i Al Qaida znatno oslabljeni i smanjenih kapaciteta za provođenje vanjskih operacija/napada, i dalje predstavljaju prijetnju Evropi. U državama EU razina prijetnje od islamskičkog terorizma varira od niske u srednjoeuropskim i istočnoeuropskim državama do srednje ili visoke u većini zapadnoeuropskih država.

Države članice EU prijavile su Europolu 2020. godine ukupno 57 provedenih, neuspješnih i spriječenih terorističkih napada. Uz to, Ujedinjeno Kraljevstvo prijavilo je 62 teroristička incidenta i Švicarska dva vjerojatna napada. Ukupni broj terorističkih napada ostao je na približno istoj razini kao i u 2019. godini, uz povećanje broja uspješno provedenih napada. Tijekom 2020. u terorističkim napadima u EU ubijena je 21 osoba, troje je ubijeno u Ujedinjenom Kraljevstvu, a jedna osoba u Švicarskoj.

Kao i posljednjih godina, primarnu terorističku prijetnju u Evropi i dalje predstavljaju radikalizirani pojedinci inspirirani džihadističkom ideologijom. Radi se o samostalnim napadačima, tzv. usamljenim vukovima, nepredvidljivog djelovanja, bez izravnih kontakata s terorističkim organizacijama, ali koji su inspirirani pozivima terorističkih organizacija na počinjenje terorističkog čina. Zbog ovih osobina, ove je osobe vrlo teško prepoznati prije počinjenja terorističkog akta.

Pri tome se radi o pojedincima već prisutnima na teritoriju EU i koji napade provode lako dostupnim oružjem (hladno oružje, automobili). Također metodom počinjeni su svi teroristički napadi u 2020. godini uz iznimku terorističkog napada 2. studenoga 2020. vatrenom oružjem u Beču. Uz izuzetak ciljanog ubojstva nastavnika u Francuskoj, sve žrtve islamskičkih terorističkih napada su slučajni prolaznici te pripadnici snaga sigurnosti. Teroristički napadi u Francuskoj demonstriraju fanatizam i brutalnost ovakvih napadača (korištenje hladnog oružja i metoda odrubljivanja glave).

Sve islamske napade tijekom 2020. u Evropi proveli su samostalni napadači, većinom državljeni EU i simpatizeri ISIL-a, ali bez utvrđene stvarne povezanosti s terorističkim organizacijama. U RH je krajem 2020. godine zabilježen incident u kojem je psihički bolesna samoradikalizirana osoba bježeći iz psihijatrijske bolnice škarama napala prolaznike i policajce.

Uz nasilnu islamsku ideologiju, kao i u ostatku Europe, sigurnosni rizik za RH predstavljuju (samo)radikalizirani pojedinci ekstremno desne nasilne ideologije, najčešće vrlo mladi i iz disfunkcionalnih obitelji i okoline. U listopadu 2020. godine samoradikalizirani pojedinac izvršio oružani napad, s obilježjima terorističkog napada, na Markovu trgu na instituciju Vlade RH pri čemu je ranio policajca. Prikupljeni podaci ukazuju na psihički poremećaj disocijativne / bipolaritetne osobnosti kod napadača, što, između ostalog, ilustrira i njegovo samoubojstvo 20-ak minuta nakon napada.

Sveukupno su u EU tijekom 2020. godine evidentirana četiri napada motivirana desnim ekstremizmom, od kojih je jedan bio uspješan, proveden u veljači 2020. u njemačkom gradu Hanau, pri čemu je samostalni napadač ubio 9 osoba. Sprječeni su planirani napadi u Njemačkoj, Belgiji i Francuskoj.

Svi planirani napadi inspirirani lijevom ekstremističkom i anarhističkom ideologijom u EU bili su sprječeni, gotovo svi (24) u Italiji uz jedan u Francuskoj.

Izvori prijetnje za europske državljane i interese izvan Europe i dalje su krizna žarišta, prvenstveno na područjima djelovanja ISIL-a, Al Qaide i njima bliskih islamskih skupina (Bliski istok, sjeverna Afrika, Sahel, rog Afrike, Arapski poluotok, srednja i jugoistočna Azija). Teroristički napad ISIL-a kod zračne luke u Kabulu 26. kolovoza 2021. u kojem je poginulo više od 100 osoba, uključujući i 13 američkih vojnika, pokazuje da je ISIL, unatoč vojnem porazu u Siriji i Iraku, i dalje aktivna na kriznim žarištima i sposoban izvesti velike terorističke napade.



Ravnatelj SOA-e održao je 21. lipnja 2021. izlaganje o hrvatskom doprinosu u borbi protiv terorizma na 2. visokoj konferenciji čelnika protuterorističkih agencija članica Ujedinjenih naroda (High-level Conference of Heads of Counter-Terrorism Agencies of Member States)

Sigurnosna prijetnja za RH i dalje proizlazi od islamskog radikalizma unutar zapadnobalkanskih zajednica, odnosno sljedbenika terorističkih organizacija među kojima su i oni koji se nisu uspjeli pridružiti ISIL-u/Al Qaidi na kriznim ratištima, kao i džihadisti-povratnici i osobe osuđena za djela povezana s terorizmom, od kojih su neki već na slobodi ili uskoro izlaze iz zatvora. Više od 200 osuđenika za djela povezana s džihadističkim terorizmom izaći će do 2023.

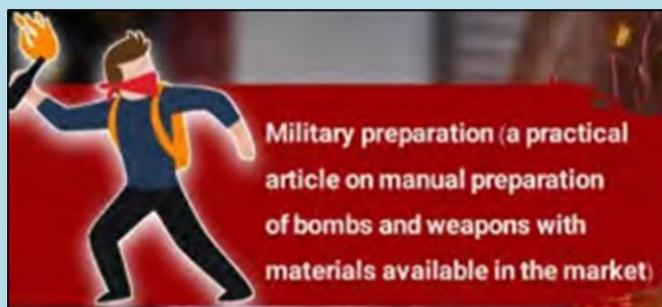
iz zatvora u zapadnoj Europi. Osuđenici za terorizam rijetko se deradikaliziraju te predstavljaju potencijalnu sigurnosnu prijetnju i nakon izlaska iz zatvora.

Očekuje se nastavak repatrijacije boraca ISIL-a, njihovih žena i djece u države Zapadnog Balkana, nakon što je proces zastao zbog pandemijskih uvjeta. Do sada se u zapadnobalkanske države (od oko 1.000 osoba koji su otišli u Siriju i Irak) vratio njih oko 450. Oko 300 osoba još uvijek se nalazi na području Sirije.

Iz RH nije otišla niti jedna osoba, ali je utvrđeno nekoliko osoba koje kao drugo imaju i državljanstvo RH (osim jedne osobe), a koje se i dalje nalaze u zarobljeničkim kampovima pod kontrolom snaga sirijskih Kurda. U tim kampovima boravi više tisuća djece i žena koje su u velikoj većini visokoradikalizirane i lojalne ISIL-u, dok njihova djeca odrastaju u takvom okruženju.

U susjedstvu i dalje djeluju tzv. paradžemati koji propovijedaju radikalno tumačenje islama, uključujući i nepriznavanje službenih islamskih zajednica u svojim državama, kao i opravdavanje nasilja u cilju navodne zaštite islama. Preko teritorija RH tranzitiraju sljedbenici radikalnog islama iz država Zapadnog Balkana s boravištem u zapadnoeuropskim državama.

Kontinuirani sigurnosni rizik predstavlja mogućnost korištenja balkanske migracijske rute od strane terorističkih skupina.



ISIL i Al Qaida neprestano pozivaju sljedbenike na izvođenje terorističkih napada, kojima bi dodatno sigurnosno ugrozili pandemijom pogodjena zapadna društva. Primjerice, jedan časopis povezan s Al-Qaidom je krajem 2020. godine, u dijelu koji se bavi metodama napada na Zapadu, najviše pažnje posvetio otrovima i podmetanju požara.

Čitateljima se sugerira da razdoblje pandemije COVID-19 na Zapadu iskoriste za razne oblike terorističkog djelovanja - od korištenja maski s ciljem skrivanja identiteta prilikom ubojstava i pljački do dijeljenja prolaznicima maski natopljenih otrovom. Navode da prazne ulice tijekom restriktivnih mjera treba iskoristiti za podmetanje požara.

Središnji operativni dio časopisa odnosi se na upute za izradu poboljšane varijante *molotovljevog koktela* koje bi, ako se pažljivo slijede, rezultirale smrtonosnjom inačicom nego standardna naprava izrađena samo na bazi benzina.

Časopis ističe kako muslimanski hakeri moraju iskoristiti oslanjanje Zapada na umjetnu inteligenciju i potiče Al Qaidinu *cyber vojsku* na hakiranje računalnih sustava obrambene industrije, banaka i nuklearnih postrojenja. U završnom dijelu najavljuju se sljedeća izdanja časopisa, a postoje i poveznica preko koje mogu komunicirati s čitateljima.

Ekstremizam jača u vrijeme pandemije

Hrvatska je i dalje društvo u kojem ekstremizam, ni po jednoj osnovi, vjerskoj, ideološkoj ili nacionalnoj, nema značajnije uporište, kao ni potporu u javnosti, a time ni snagu ili potencijal za destabilizaciju nacionalne sigurnosti.

U okolnostima pandemije, društvena izolacija i povećanje vremena provedenog na internetu povećavaju rizik pristupa ekstremističkim sadržajima i samoradikalizacije pojedinaca. Pritom, najveći rizik za samoradikalizaciju predstavljaju psihički nestabilne osobe koje su posebno ranjive na negativne učinke pandemije. Takve se osobe, opsjednute ekstremističkim stavovima, mogu odlučiti i na teroristički čin.

Uz islamski i ideološki ekstremizam, pandemija COVID-19 je sama po sebi izvor teorija zavjere čiji pobornici postaju podložni i drugim radikalnim idejama. Gospodarska i društvena nesigurnost pogoduju razvoju svih oblika radikalizma u društvu. Samostalni počinitelji terorističkih napada često su osobe s marginje društva čije su društvene i poslovne perspektive dodatno ograničene posljedicama pandemije.

Iako islamski ekstremizam i dalje predstavlja najveći sigurnosni rizik u Europi, u pojedinim europskim državama sve više pojavljuju i slučajevi tzv. desnog terorizma, odnosno oružanih napada usmjerenih primarno protiv manjinskih skupina i nedomicilnog stanovništva. Ova pojava u Europi se, kao i drugi sigurnosni izazovi, preslikava i na stanje sigurnosti u RH, te je i oružani napad samostalnog napadača u listopadu 2020. na Markovu trgu na Vladu RH imao obilježja terorističkog napada s ekstremno desnih ideoloških polazišta.

U pojedinim europskim državama, primarno Italiji i Grčkoj, djeluju lijeve i anarhističke nasilne ekstremističke skupine i pojedinci.

Koristeći mogućnosti internetskih tehnologija, ekstremistički akteri se sve više umrežavaju. To ne vrijedi samo za islamske ćelije, nego i za radikalnu europsku desničarsku i ljevičarsku scenu.

Aktivnosti malobrojnih osoba s ekstremističkim opredjeljenjem u RH ponajviše se ogledaju kroz promicanje neofašističke ideologije uz sukobljavanje (zasad u virtualnom prostoru) s pripadnicima i skupinama suprotnih ideoloških polazišta. Povećana online prisutnost virtualnih ekstremističkih grupa i pojedinaca koji promoviraju nasilje povećava rizik od radikalizacije. Tako je unutar manje online aktivne skupine mlađih osoba prisutan trend promoviranja nasilne neonacističke ideologije iz zapadnih ekstremističkih krugova.

I dalje su prisutne pojave velikosrpskog ekstremizma u pojedinim državama susjedstva, a velikosrpska ideologija očituje se u poricanju teritorijalnog integriteta RH i susjednih država, pozivanju na obnovu tzv. Republike Srpske Krajine te netrpeljivosti prema drugim narodima ili negiranju njihova identiteta. Ovakve velikosrpske i ekstremističke poruke ponekad javno upućuju političke i medijske osobe iz susjednih država koristeći društvene mreže ili javne nastupe.

U većini ekstremističkih poruka i objava, neovisno o ideološkom predznaku, radi se uglavnom o djelovanju u virtualnom prostoru, pri čemu često osobe koji objavljuju ekstremističke sadržaje ne žive u RH.

Nastavila se pojava nasilnih sukoba između ekstremnih pripadnika navijačkih skupina. Ovi sukobi narušavaju javni red i mir, ali i destabiliziraju lokalne sigurnosne prilike, osobito jer poprimaju karakter međunacionalnih sukoba kada se radi o navijačima klubova iz Hrvatske i Srbije.



Napad na Markovu trgu 12. listopada 2020. pokazao je svu kompleksnost i nepredvidljivost fenomena samoradikaliziranih pojedinca, tzv. vukova samotnjaka. Radi se o pojedincima koji su, neovisno o ideologiji, potencijalno opasne osobe spremne provesti teroristički napad, samostalno indoktrinirane većinom online, često uz prisutna neliječena psihička stanja, introvertirana i nasilna prema svojoj najbližoj okolini.

Pri tome najveći izazov predstavljaju pojedinci koji su "nevidljivi" sigurnosnim službama, jer ne ostvaruju kontakte s istomišljenicima i ne objavljuju ekstremističke sadržaje, zbog čega mogu ostati neidentificirani do trenutka provođenja napada. Njihova pojava osobito je opasna u kontekstu dostupnosti oružja zaostalog iz rata.

Sukladno iskustvima zapadnoeuropskih država, proces radikalizacije vrlo je složen i slojevit, ali zna biti iznenađujuće brz i učinkovit. Radikalizaciji u društvu pogoduje nezadovoljstvo pojedinih slojeva društva, loši socioekonomski uvjeti, niža obrazovna razina, psihički poremećaji, disfunkcionalna obitelj i disfunkcionalna društvena okolina.

Važan faktor (samo)radikalizacije je ekstremistička propaganda preko interneta i društvenih mreža. Internet je najvažniji medij komunikacije, regrutacije i radikalizacije sljedbenika (bez obzira na ideologiju), a čiji je utjecaj još veći u uvjetima izoliranosti zbog mjera ograničavanja kretanja u vezi s pandemijom COVID-19.

Suprotstavljanje radikalizaciji općedruštveno je pitanje koje zahtijeva multidisciplinarni pristup uz aktivno uključivanje obitelji, najbliže okoline, odgojno-obrazovnih ustanova, državnih institucija, socijalnih službi, znanstvenih ustanova, medija i drugih društvenih i političkih aktera kako bi se problem dijagnosticirao u ranoj reverzibilnoj fazi. Uloga SOA-e u prevenciji radikalizacije je u ranom upozoravanju, odnosno na prepoznavanju procesa i nositelja radikalizacije te izvješćivanju nadležnih o tome.

Strano obavještajno i informacijsko djelovanje stalno je prisutno

Obavještajno djelovanje, iako uglavnom nevidljivo javnosti, stalno je prisutno. Republika Hrvatska predmet je obavještajnog interesa pojedinih država koje RH vide kao sigurnosnog, gospodarskog ili političkog suparnika, pojedinačno ili kao dijela NATO-a i Europske unije.

Prema RH se obavještajno djeluje prikupljanjem podataka koji su od interesa za pojedinu stranu obavještajnu službu, ali i aktivnim djelovanjem kojim se želi utjecati na javno mnjenje, međunarodni položaj RH te na procese donošenja odluka u RH.

Pri tome se osobito ističe informacijsko djelovanje, odnosno plasiranje lažnih vijesti u kojima se RH želi prikazati kao nevjerodostojna članica NATO-a i EU, kao čimbenik koji destabilizira susjedne države i onemogućuje daljnje euroatlantske integracije. U isto vrijeme obavještajnim djelovanjem želi se unijeti razdor unutar euroatlantskih organizacija kojih je RH članica.

Prilikom informacijskog djelovanja prema RH zlorabe se novinski portalni, internetske društvene platforme, a pojedine informacijske operacije se odvijaju plasiranjem zlonamjernih teza o SOA-i i RH pod krinkom znanstvenih instituta, čime se želi lažnim vijestima i tezama dati vjerodostojnost, poput teze da je Republika Hrvatska „njiveća kočnica i faktor ugrožavanja mira na Zapadnom Balkanu“.

Osobitu sigurnosnu težinu imaju zlonamerne i lažne objave koje manipuliraju naporima u prevenciji i suzbijanju međunarodnog terorizma, kao što je bio slučaj s lažnim medijskim objavama u kojima se SOA-u i RH optuživalo za naoružavanje terorista u BiH.

U smislu prikupljanja podataka, strano obavještajno djelovanje prema RH usmjерeno je prema prikupljanju podataka o sigurnosnim, političkim i gospodarskim procesima u RH, a osobito onima koja su povezani s međusobnim otvorenim pitanjima, kao i hrvatskoj politici prema državama Zapadnog Balkana.

Strano obavještajno djelovanje usmjерeno je i na prikupljanje podataka u sklopu hrvatskog članstva u EU i NATO-u. U ovom kontekstu, RH predmet je obavještajnog djelovanja država koje NATO i EU smatraju sigurnosnim izazovom ili prijetnjom.

Obavještajno djelovanje usmjерeno je i na strateško pozicioniranje u RH u novim i razvojnim sektorima, kao što su nove tehnologije i obnovljivi izvori energije, kao i projektima koji su od strateškog značaja za regiju, poput velikih infrastrukturnih projekata.

Uz klasično obavještajno djelovanje i prikupljanje podataka, posljednjih godina je sve intenzivnije korištenje kibernetičkih napada na informacijsku infrastrukturu državnih tijela radi špijuniranja i krađe podataka.

Iako se obavještajne operacije provode u tajnosti, veliki broj slučajeva se zadnjih godina javno eksponirao, pri čemu se medijski najekspoziraniji slučajevi u Europi posljednjih godina odnose na djelovanje ruskih obavještajnih službi u državama članicama EU i NATO-a. Tako su časnici ruske vojne obavještajne službe GRU osumnjičeni za eksplozije skladišta oružja u Češkoj 2014. godine te u Bugarskoj u razdoblju od 2011. do 2020. godine. Ranije su pripadnici GRU-a bili osumnjičeni za pokušaje ubojstva bivšeg časnika GRU-a Sergeja Skripalja i njegove kćeri u Engleskoj (2018.) i bugarskog trgovca oružjem Emilijana Gebreva (2015.). U travnju 2018. godine nizozemske vlasti su uhitile i protjerale četvoricu pripadnika GRU-a koji su pokušavali hakirati sjedište Organizacije za zabranu kemijskog oružja. U neposrednom okružju RH, pripadnici GRU-a povezivani su s pokušajem državnog udara u Crnoj Gori 2016. godine neposredno prije parlamentarnih izbora i ulaska Crne Gore u NATO.



U svibnju 2020. godine ukrajinska služba SBU je uhitila svog generala Valerija Šaitanova zbog suradnje s ruskim obavještajnim službama. Ukrajinska služba je objavila da je suradnja obuhvaćala organizaciju atentata u Ukrajini te da se Šaitanov s ruskim obavještajcima sastao i na teritoriju RH.

Pored aktivnog rada na suzbijanju prikrivenog djelovanja stranih obavještajnih službi, zadaća SOA-e je kontinuirano djelovanje na jačanju protuobavještajne zaštite i širenju sigurnosne kulture kod osoba koje bi mogle biti predmet stranog obavještajnog djelovanja.

Državno sponzorirani kibernetički napadi sve su zastupljeniji u špijunaži

Državno sponzorirane kibernetičke napade organiziraju nalogodavci iz pojedinih država, a pri tome posredno ili neposredno koriste različite organizirane aktere za provođenje napada. Ovi napadi su usmjereni prema pažljivo odabranim ciljevima, koji su prethodno dobro proučeni, a izvršavaju ih državno sponzorirane kibernetičke APT (*Advanced Persistent Threat*) grupe koje su usko povezane sa sigurnosno-obavještajnim sustavima pojedinih država. Ovakvi kibernetički napadi u prvom redu ciljuju države članice EU-a i NATO-a.

Republika Hrvatska je zadnjih godina bila cilj više desetaka državno sponzoriranih kibernetičkih napada. O karakteru tih napada najbolje govori podatak da se najveći broj odnosio na pokušaje probroja u informacijske i komunikacijske sisteme Ministarstva vanjskih i europskih poslova te Ministarstva obrane.

Pored toga, ovakvi kibernetički napadi u svijetu se koriste i s ciljem onesposobljavanja i oštećenja mrežnih i informacijskih sustava od važnosti za ključne društvene i gospodarske procese (kritična infrastruktura), čime se nanosi šteta ugledu države ili velikim nacionalnim kompanijama, odnosno onemogućava se funkcioniranje procesa važnih za društvo u cjelini.

Države koje sponzoriraju kibernetičke napade usklađuju ciljeve kibernetičkih napada sa svojim nacionalnim strategijama gospodarskog razvoja te profiliraju pojedine kibernetičke APT grupe za napade na određena državna tijela ili gospodarske sektore, poput energetike ili zrakoplovne industrije, a ukradene podatke koriste za vlastite političke ciljeve ili industrijski razvoj i neovlašteno kopiranje proizvoda. Tako je i tijekom pandemije COVID-19, u procesu razvoja cjepiva, uočen niz kibernetičkih napada na zapadne farmaceutske korporacije.

Atribucija kibernetičkog napada je proces pridjeljivanja odgovornosti za izvršenje kibernetičkog napada koji je uzrokovao kibernetički incident ili kibernetičku krizu, i koji je rezultat niza tehničkih i analitičkih aktivnosti koje nadležna tijela provode na tehničkoj i sigurnosno-obavještajnoj razini. Cilj je otkrivanje i utvrđivanje činjenica, njihovo povezivanje i procjena vjerojatnosti, kako bi se omogućilo razmatranje i donošenje političke odluke o atribuciji kibernetičkog napada, zajedno s odabirom diplomatskih instrumenata koji će se primijeniti u svakom pojedinom slučaju javne atribucije. Pri tome kontekst atribucije može biti nacionalni, EU ili NATO.

Tijekom 2020. godine EU je započela proces javne atribucije niza kibernetičkih napada atribuiranih akterima iz Ruske Federacije, Kine i Sjeverne Koreje, što je uključilo i rusku vojnu obavještajnu službu te niz povezanih pojedinaca i više državno sponzoriranih APT grupa iz Rusije, Kine i Sjeverne Koreje, kojima su uvedene odgovarajuće sankcije.

Kao odgovor na rastuće izazove u kibernetičkom prostoru, SOA je 2019. godine uspostavila Centar za kibernetičke tehnologije s ciljem zaštite nacionalnog kibernetičkog prostora. Centar za kibernetičke tehnologije putem sustava SK@UT svakodnevno registrira nekoliko stotina tisuća sigurnosno indikativnih događaja.

Tijekom 2020. godine Centar za kibernetičke tehnologije potvrdio je 12 državno sponzoriranih kibernetičkih napada na ciljeve u RH. Uz trend rasta broja napada, povećan je i broj APT grupa koje napadaju ciljeve u RH. Primarni razlozi ovog trenda su hrvatsko predsjedanje Vijećem EU u prvoj polovici 2020. godine, kao i iskoristavanje pandemije COVID-19 za provedbu kibernetičkih napada, ali i značajno povećana vidljivost nacionalnog kibernetičkog prostora ostvarena širenjem opsega sustava SK@UT.

[SK@UT]

Vlada RH je 1. travnja 2021. donijela Odluku o mjerama i aktivnostima za podizanje nacionalnih sposobnosti pravovremenog otkrivanja i zaštite od državno sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza. Odlukom se, u cilju dodatne zaštite nacionalnog kibernetičkog prostora, omogućava uključenje u sustav SK@UT operatorima ključnih usluga, davateljima digitalnih usluga, operatorima kritične nacionalne infrastrukture te drugim pravnim osobama registriranim u RH.

Sustav SK@UT izgradili su SOA i Zavod za sigurnost informacijskih sustava u cilju podizanja nacionalnih sposobnosti za pravovremeno otkrivanje i zaštitu od kibernetičkih napada.

SK@UT predstavlja središnji sustav za otkrivanje, rano upozorenje i zaštitu od državno sponzoriranih kibernetičkih napada, APT kampanja te drugih kibernetičkih ugroza, koji se sastoji od distribuirane mreže senzora u ključnim državnim tijelima i pravnim osobama.

SK@UT omogućuje otkrivanje sofisticiranih kibernetičkih napada u najranijim fazama napada i u bilo kojem segmentu kibernetičkog prostora koji pokriva mreža senzora. Ovakav pristup povezuje najsloženije tehničke sustave za zaštitu kibernetičkog prostora i sigurnosno-obavještajne sposobnosti, čime se bitno smanjuje rizik kompromitacije ključnih nacionalnih informacijskih resursa.

Očekuje se daljnji trend rasta državno sponzoriranih kibernetičkih napada, osobito u okviru globalnih procesa vezanih uz uvođenje 5G tehnologije te uz aktualno stanje pandemije COVID-19. Pri tome se taktike, tehnike i procedure državno sponzoriranih kibernetičkih APT grupa kontinuirano pokušavaju prilagoditi reakciji svojih ciljeva kako bi i dalje ostale učinkovite.

Državno sponzorirane kibernetičke APT grupe u pripremi i provedbi napada ponajviše ciljaju na nedovoljnu sigurnosnu svijest i edukaciju korisnika, kao i na nedovoljno razvijene kibernetičke sigurnosne politike tijela i pravnih osoba. To znači da preventivne mjere u svim tijelima (sigurnosne politike upravljanja zaporkama, ažuriranje programske podrške, dvofaktorske

autentifikacije za pristup sustavu e-pošte, korištenje VPN-a za vanjski pristup korisnika računalnim poslužiteljima) uvelike smanjuju mogućnosti kibernetičkih napada i vjerovatnost kompromitacije informacijskih sustava. Rad Centra za kibernetičke tehnologije usmjeren je između ostalog i prema prepoznavanju najboljih praksi kao odgovoru na detektirane državno sponzorirane kibernetičke napade.

Tijekom 2020. i 2021. godine odvijali su se izuzetno sofisticirani globalni kibernetički napadi na proizvođače poslovnih programskih rješenja, s ciljem kompromitacije velikog broja njihovih korisnika. U prosincu 2020. godine otkriven je globalni kibernetički napad korištenjem lanca nabave programske podrške tvrtke *SolarWinds*. Kompromitacija programske podrške *SolarWinds*, koju koristi oko 18 tisuća poslovnih korisnika u svijetu, provedena je između ožujka i svibnja 2020. godine, a otkrivena je tek šest mjeseci kasnije što potvrđuje visoku sofisticiranost samog napada.

Jedan od primjera globalnih kibernetičkih napada je i iskorištavanje kritičnih i nepoznatih (*0-day*) ranjivosti *Microsoft Exchange* sustava koje je tvrtka *Microsoft* objavila u ožujku 2021. godine. Napad je ugrozio više od 100.000 poslovnih korisnika u svijetu.

Kibernetički APT napadi korištenjem lanca nabave programske podrške *Solarwindsa* i nepoznatih ranjivosti *Microsofta* pokazuju visoku sofisticiranost državno sponzoriranih kibernetičkih APT grupa te nužnost sustavne primjene mjera kibernetičke sigurnosti na široj nacionalnoj razini.

Zabrinjava ubrzani trend prijenosa sofisticiranih taktika, tehnika i procedura državno sponzoriranih APT grupa u područje organiziranog kibernetičkog kriminala i njihova primjena u kibernetičkim napadima sa zlonamjernim programskim kôdovima (*Malware*) koji ciljaju finansijski sektor ili zlonamjernim ucjenjivačkim kôdovima (*Ransomware*) koji ciljaju gospodarske subjekte.

Ovakvi napadi usmjeravaju se na strateške i velike kompanije koje se u slučaju uspješnog napada blokira u radu i dostupnosti podataka, nanose im se veliki finansijski gubitci te ih se dodatno ucjenjuje prijetnjom objave ukradenih poslovnih podataka. U svibnju 2021. godine zlonamjernim ucjenjivačkim kôdom napadnuta je tvrtka *Colonial Pipeline* koja gorivom opskrbljuje istočnu obalu SAD-a. Zbog poteškoća u opskrbi gorivom, vlasti SAD-a uvele su izvanredno stanje. U srpnju 2021. godine napadnut je lanac nabave programske podrške tvrtke *Kaseya*, a posljedica ove kompromitacije bio je napad zlonamjernim ucjenjivačkim kôdom na oko 1500 tvrtki koje koriste programska rješenja *Kaseya*.

Početkom 2020. godine kibernetički napad zlonamjernim ucjenjivačkim kôdom pretrpjela je hrvatska naftna kompanija INA. Napadi na gospodarske subjekte, uz gospodarsku štetu tim kompanijama, imaju i obavještajnu dimenziju, s obzirom da neke kompanije, u sklopu svojih poslova, raspolažu podacima od obavještajnog značenja, poput industrijskih i poslovnih tajni, osobnih i finansijskih podataka svojih klijenata, nacionalnih analiza i pregleda stanja u svom području djelovanja i slično.

Kibernetička otpornost postaje ključ zaštite nacionalne sigurnosti

Ravnatelj SOA-e održao je 6. travnja 2021. izlaganje o ulozi SOA-e u zaštiti nacionalnog kibernetičkog prostora na globalnoj konferenciji Cybertech Global 2021 koja se održavala u Dubaiju, Ujedinjeni Arapski Emirati. Cybertech Global je platforma kibernetičke industrije koja služi za uspostavljanje poslovnih kontakata i raspravu o tehnološkim inovacijama, izazovima i rješenjima u suzbijanju globalnih kibernetičkih prijetnji. Radi se o jednoj od najvećih konferencija ove vrste na svijetu. Na konferenciji su sudjelovali čelnici iz kibernetičke industrije, donositelji odluka iz brojnih država, tehnološki stručnjaci, poduzetnici i drugi.



Daniel Markić

Director General, Security and Intelligence Agency (SOA), Croatia

Izlaganje ravnatelja se u cijelosti nalazi u nastavku:

Kao ravnatelj jedne obavještajne službe čiji je posao ukazivati na trendove, moram filmsku industriju upozoriti na jednu veliku promjenu na koju se trebaju pripremiti!

Operativce tajnih službi u svim onim blokbasterima koji su skakali po krovovima, jurili po ulicama svjetskih velegradova, izbjegavali metke strojnica loših dečki i spašavali svijet od zlih znanstvenika, morat će zamijeniti s pametnim mladim curama i dečkima koji taj isti svijet spašavaju koristeći tipke miša, iz svojih ergonomskih stolica ispred velikih monitora.

Operativci hrvatske tajne službe su, naravno, sposobni i spremni kao oni iz blokbastera, ali zadnjih godina sve više izgrađujemo i ove koji klikom miša spašavaju svijet.

Razvoj tehnologije prisilo nas je da iz zatvorenog nevidljivog svijeta obavještajnih službi izađemo na javni otvoreni prostor. I to je dobro: naši građani moraju znati da postoje ljudi i službe koji se brinu o njihovoј sigurnosti i u kibernetičkom prostoru.

Kibernetička otpornost postaje ključni cilj nacionalne sigurnosti u digitalnoj eri. Međutim, potrebna je uključenost svih dionika društva u izgradnji kibernetički otporne zajednice. Zato je važno da i mi javno govorimo o našoj ulozi u jačanju kibernetičke otpornosti. Jer vjerujemo da smo upravo mi okosnica oko koje će se ta otpornost graditi.

2020. godinu u SOA-i smo počeli vrlo ambiciozno. U siječnju smo u Tel Avivu po prvi put predstavili naš Centar za kibernetičke tehnologije svjetskoj javnosti, a Hrvatska je po prvi put preuzeila predsjedanje Vijećem Europske unije. Naši ambiciozni planovi kibernetičke otpornosti poklopili su se s predsjedanjem, za koje smo procjenjivali da će izazvati pojačani interes malicioznih državno sponzoriranih kibernetičkih APT grupa.

Kako je u međuvremenu pandemija COVID-19 zaustavila procese u fizičkom svijetu, svi važni procesi počeli su se odvijati u kibernetičkom prostoru. Bio je to znak da će očekivanja od našeg Kibernetičkog centra iznimno porasti.

Centar za kibernetičke tehnologije uspostavljen 2019. godine u okviru naše Agencije dokazao je svoju učinkovitost u brzo promijenjenim nacionalnim i globalnim okolnostima u 2020. godini.

Naše procjene pokazale su se točnima: u 2020. godine se udvostručio broj državno sponzoriranih APT napada na hrvatski kibernetički prostor. Jednako tako, udvostručio se broj APT grupa koje su targetirale Hrvatsku.

Tehnike, taktike i procedure (TTP) APT grupa su se promijenile te se koriste i tradicionalne i moderne TTP. Namjera napadača jest minimizirati digitalni trag kojeg ostavljaju te tako onemogućiti mogućnost atribucije napada u ciljanim državama, odnosno spriječiti diplomatske i gospodarske sankcije koje su sve neugodnije za države koje sponzoriraju APT kibernetičke napade.

O ovom problemu govori podatak da je Europska unija prošle godine, po prvi put, uvela sankcije zbog kibernetičkih napada. Sankcije se odnose na šest pojedinaca i tri institucije iz Rusije, Kine i Sjeverne Koreje, među njima i Glavni centar za posebne tehnologije Glavne uprave Glavnog stožera oružanih snaga Ruske Federacije (GU/GRU).

Naše članstvo u Europskoj uniji može nam pomoći da taj cilj lakše ostvarimo, iako su brojni izazovi pred nama.

Novi paket EU-a od 16. prosinca 2020. – Direktiva NIS2, Kibernetička strategija EU, Direktiva o otpornosti kritičnih entiteta – još je jedan izazov za nacionalnu sigurnost glede daljnje prilagodbe nacionalnih kibernetičkih organizacija i koordinacijskih sposobnosti.

Strateški i tehnološki rizici povezani s 5G pojavljuju se u već započetoj implementaciji nove generacije mobilne mreže spajajući prethodno razdvojene svjetove telekomunikacija i Interneta u jedinstveni kibernetički prostor.

Pred nama je četvrta industrijska revolucija s kibernetičko-fizičkim pristupom koji će bitno preoblikovati naše ekonomije u narednoj digitalnoj eri.

Nedavni globalni državno-sponzorirani kibernetički napadi, kompromitacija Solarwinda, kao najteži napad na globalni lanac nabave te četiri 0-day ranjivosti Microsoft Exchange Servera, pokazuju izazove s kojima ćemo se morati suočavati u narednoj eri.

Posao moje službe je zaštita nacionalne sigurnosti, a otpornost na prijetnje je naš zajednički nacionalni cilj. Kibernetički prostor je već odavno sastavni dio nacionalne sigurnosti. I kao što razvijamo otpornost u fizičkom svijetu, tako smo posvećeni cilju izgradnje kibernetičke otpornosti. Zato ćemo i dalje razvijati naš Centar prema zaštiti nacionalnog kibernetičkog prostora.

Mi kao sigurnosna i obavještajna agencija tu imamo nekoliko prednosti: mi imamo te mlade i pametne cure i dečke koji su u stanju klikom miša zaštititi nacionalnu sigurnost, spremni smo prihvatići tehnološke platforme za zaštitu, razvili smo mrežu nacionalnih i međunarodnih partnerstava kojom možemo proširiti naše spoznaje i sposobnosti i konačno, imamo ono što nas izdvaja od drugih, imamo informacije (*intelligence*).

Dakle, imamo sve sastojke za uspjeh. Sad ih trebamo sjediniti zajedno i veselim se što ćemo biti na prvoj liniji obrane našeg nacionalnog kibernetičkog prostora.



Gospodarska sigurnost važan je dio nacionalne sigurnosti

Snažno i otporno gospodarstvo čini temelj zaštite nacionalne sigurnosti, pa je za svaku državu iznimno važna gospodarska sigurnost i okvir koji će omogućiti gospodarski razvoj i napredak.

SOA prati nacionalne, regionalne i globalne gospodarske procese i kretanja koja mogu utjecati na gospodarsku sigurnost, položaj i interese RH. U sklopu ove zadaće SOA kontinuirano prati aktivnosti brojnih aktera, državnih i nedržavnih, u gospodarskom području, čije aktivnosti se mogu negativno odraziti na interes hrvatskog gospodarstva u zemlji i inozemstvu. Pri tome se posebno sagledavaju rizici obavještajnog i hibridnog djelovanja protiv hrvatskih ili zajedničkih europskih interesa pod krinkom legitimnih gospodarskih aktivnosti. Radi se o mogućim aktivnostima špijuniranja, preuzimanja intelektualnog vlasništva, stvaranja gospodarske ovisnosti, mogućnosti medijskih manipulacija i utjecaja i slično.

Situacije gospodarske i finansijske krize povećavaju rizik da sumnjivi investitori i kriminalne skupine pod legendom otvaranja tvrtki i novih radnih mjesta pokušaju uložiti nelegalno stečeni kapital. Stoga se intenzivnije koriste raspoloživi nacionalni mehanizmi s ciljem provjere ulaganja i sprječavanja sumnjivih ulaganja.

Gospodarska kriza izazvana pandemijskim uvjetima dovela je u poteškoće brojne europske strateške kompanije te EU poduzima mjere za zaštitu tržišnog natjecanja, odnosno sprječavanje preuzimanja europskih gospodarskih i infrastrukturnih subjekata od strane gospodarskih aktera izvan EU koji dobivaju nelegalne i prikrivene državne potpore ili su u državnom vlasništvu.

Jedan od važnih segmenata ovih aktivnosti jest i praćenje kibernetičke sigurnosti u gospodarskoj sferi, gdje SOA svojim sposobnostima može pomoći u zaštiti strateški važnih hrvatskih gospodarskih subjekata od naprednih kibernetičkih napada.

SOA prati gospodarske i finansijske procese koji mogu utjecati na pozicioniranje hrvatskih gospodarskih subjekata u inozemstvu, kao i trendove i procese koji bi mogli ugroziti sigurnost hrvatskih gospodarskih subjekata, poglavito u nestabilnim područjima u svijetu.

Energetska sigurnost sastavni je dio nacionalne i međunarodne sigurnosti. Stoga je SOA uključena i u praćenje procesa u energetskom sektoru, a energetska sigurnost važno je europsko i globalno sigurnosno pitanje.

Europska unija osobito je osjetljiva na pitanje sigurnosti opskrbe prirodnim plinom. Od gotovo 500 milijardi prostornih metara prirodnog plina koliko EU potroši godišnje (u pandemiji je potrošnja pala na oko 400 milijardi), 90% dolazi iz uvoza. Od toga je oko 40% uvezenog ruskog plina, a raste uvoz iz SAD-a i čini oko 7% europske potrošnje.

Ipak, iako asimetrična, ovisnost Europske unije i Rusije po pitanju prirodnog plina je obostrana, jer postoji značajna ovisnost Rusije o kupcima iz Europske unije. Zato bi ekološka transformacija EU i manje oslanjanje na fosilna goriva u budućnosti, kao i uvođenje poreza na ugljik, mogli biti izazov za rusko gospodarstvo.

Puštanje u rad LNG terminala na Krku predstavlja značajan čimbenik energetske neovisnosti i diverzifikacije izvora plina za RH, ali i za države susjedstva. Tako su započele aktivnosti na izgradnji Južne interkonekcije kojom će se s hrvatskim povezati plinski sustav Bosne i Hercegovine. Na ovaj način otporniji hrvatski plinski sustav ima izravne pozitivne učinke i na jačanje energetske sigurnosti i stabilnosti susjednih država.



Dana 29. siječnja 2021. pušten je u rad Plutajući LNG terminal u Omišlju i spojni plinovod Zlobin-Omišalj kojim će se ukapljeni prirodni plin otpravljati u hrvatski transportni plinski sustav, čime su Hrvatska i Europa dobili novi i konkurentan dobavni pravac prirodnog plina (Foto: Vlada RH)

Korupcija nanosi štetu državnom proračunu i gospodarstvu RH

Sukladno zakonskim rješenjima u RH, suzbijanjem korupcije primarno se bave specijalizirana tijela policije i Državnog odvjetništva (DORH) kao državna tijela koja provode kazneni postupak (uz sudove koji su zasebna grana vlasti).

Ipak, zbog svog negativnog utjecaja na državni proračun, gospodarstvo, povjerenje građana u institucije države kao i na procese političkog odlučivanja, korupcija i gospodarski kriminal potencijalno ugrožavaju i nacionalnu sigurnost. Stoga u njihovoj prevenciji i suzbijanju SOA ima važnu ulogu u suradnji s drugim državnim tijelima. U isto vrijeme, SOA kroz svoj operativni rad može doći do podataka koji mogu ukazivati na koruptivne pojave i kriminal te u tom slučaju SOA izvješćuje druga nadležna tijela (MUP, DORH, USKOK, Ministarstvo financija, Porezna uprava).

Korupcija, uz sve negativne društvene posljedice, predstavlja značajnu prijetnju za gospodarski razvitak RH te ugrožava pošteno tržišno natjecanje, smanjuje gospodarski rast, oštećeće državni proračun i javne financije. Dugoročno, korupcija smanjuje povjerenje građana u ustavni poredak i učinkovitost državnih tijela.

Korupcija se, kao iskorištavanje javnih i državnih dobara za privatnu korist, ponajviše vezuje za zloporabu položaja i ovlasti u javnoj upravi, državnim institucijama i tijelima te javnim tvrtkama.

U koruptivnom djelovanju kriminalne skupine i pojedinci pokušavaju na nezakonite načine utjecati na predstavnike vlasti i voditelje javnih tvrtki na raznim razinama kako bi ostvarili nezakonitu dodatnu zaradu ili stekli nezakonite pogodnosti. Pri tome su osobito zabrinjavajući pokušaji koruptivnog utjecaja na političke, pravosudne, gospodarske i druge procese te na procese u kojima se donose odluke od javnog interesa.

Posebno rizično područje na području suzbijanja korupcije i gospodarskog kriminala predstavljaju procesi javne nabave i njihova zloporaba, posebice u segmentu velikih infrastrukturnih projekata.

U sferu koruptivnog djelovanja i gospodarskog kriminala spada i interes za ulaganjem kapitala nepoznatog porijekla u RH, pri čemu postoji rizik da se radi o „pranju“ nezakonito stečenog novca. Posebno složeni oblici korupcije, zloporabe i malverzacije u trgovačkim društvima, izvlačenja i pranja novca imaju i svoju međunarodnu dimenziju.

Rizici od pranja novca, finansijskih malverzacija i drugih oblika gospodarskog kriminala rastu u slučajevima gospodarskih kriza kakvu je uzrokovala pandemija COVID-19.

Pitanje ratnih zločina i nestalih u Domovinskom ratu i dalje je otvoreno

Nakon Domovinskog rata, u trenutku pisanja javnog izvješća još uvijek je nepoznata soubina 1458 osoba te mjesto ukopa posmrtnih ostataka 400 smrtno stradale osobe, što ukupno čini 1858 neriješenih slučajeva. SOA kontinuirano, u suradnji s drugim nadležnim tijelima (Ministarstvo hrvatskih branitelja, MUP, VSOA), sudjeluje u rasvjetljavanju soubine i mjesta ukopa nestalih osoba.

Radi se o izrazito osjetljivom humanitarnom pitanju, ali i pitanju čije rješavanje ima utjecaj na međunarodne i međudržavne odnose.

SOA je također usmjerena na počinjenja ratnih zločina i utvrđivanju njihovih počinitelja, okolnosti i svjedoka. Aktivnosti SOA-e usmjerene su i na utvrđivanje mjesta boravka osoba za kojima je RH raspisala tjeralice i nalaze se u bijegu od kaznene odgovornosti, a u cilju njihovog procesuiranja pred pravosudnim tijelima.



Foto: MORH

Globalna geopolitička i gospodarska nadmetanja su dinamična i neizvjesna

Globalne geopolitičke prilike obilježava jačanje regionalnih rivalstava u situaciji u kojoj globalizirano gospodarstvo uzrokuje takvu međusobnu gospodarsku isprepletenost i međuovisnost koja nadilazi gospodarske odnose zabilježene kroz povijest. Tijekom Hladnog rata Zapad i SSSR bili su odvojeni ekonomski sustavi koji međusobno skoro nisu ni trgovali. Danas, Kina, Rusija, SAD i EU imaju značajne trgovinske veze, a Kina, EU i SAD su međusobno najveći trgovinski partneri. U isto vrijeme, između zapadnih država i Kine postoji neslaganje oko brojnih gospodarskih i trgovinskih pitanja, a odnosi s Rusijom opterećeni su brojnim političko-gospodarskim temama poput sankcija zbog ruske aneksije Krima.

Gospodarske prilike u svijetu obilježava značajan pomak gospodarskih aktivnosti prema azijsko-pacifičkoj regiji. Tako su gospodarstva današnjih država EU i Ujedinjenog Kraljevstva 1989. godine činila oko 28% globalnog BDP-a, SAD 22%, a Kina tek 4%. Nakon 30 godina, EU i Ujedinjeno Kraljevstvo čine 16%, SAD oko 15%, a Kina 18% globalnog BDP-a.

S političke strane, vidljivo je nadmetanje zapadnog liberalnog u odnosu na istočni autoritarni pogled na razvoj političkih i društvenih sustava vrijednosti. U tom je smislu EU Kinu označila kao ekonomskog takmaka i sistemskog suparnika koji promiče alternativni model vladavine.

U okruženju EU postoje brojna neriješena krizna žarišta, a otvorena su pitanja daljnog odnosa EU-e s Rusijom i Kinom, kao i pitanja energetske sigurnosti EU, zaštite tržišnog natjecanja i europskih kompanija od nelojalne konkurenциje. EU je, uz nastavak oslanjanja na NATO i euroatlantsko partnerstvo, nastavila jačati vlastite obrambene sposobnosti kroz više vojno-obrambenih inicijativa.

Vanjsku sigurnosnu politiku SAD-a obilježavaju nastavak napetosti s Rusijom, nadmetanje s Kinom, pitanje odnosa s Iranom i njegovim nuklearnim programom te povlačenje snaga iz Afganistana, gdje je vojna nazočnost SAD-a pružala stabilnost širem srednjoazijskom prostoru. Nova predsjednička administracija najavila je obnovu mreže savezništava koje SAD gradi po cijelom svijetu.

Kina dovodi u pitanje globalnu dominaciju SAD-a i ima ambiciju postati vodeća svjetska sila. Svoj model vladavine Kina promovira kao alternativu liberalnoj demokraciji. Unatoč pandemiji Kina je zadržala veliki gospodarski rast, a nakon pandemije mogla bi izaći kao prvi gospodarski partner brojnim državama.

Uz jačanje svojih vojnih kapaciteta, Kina i dalje u globalnim okvirima koristi gospodarsku politiku, pri čemu joj odgovara sve veća oslonjenost globalnih opskrbnih lanaca na Kinu. Glavni projekt kineske gospodarske politike je inicijativa Pojas i put koja od 2013. objedinjuje projekte kojim se gradi trgovinska i infrastrukturna mreža između Kine i više od 60 država u Aziji, Africi i Europi. U sklopu te inicijative kineske državne banke sudjeluju u financiraju izgradnje infrastrukture u

zemljama u razvoju davanjem kredita. Kina je postala najveći svjetski uvoznik nafte, a naftom iz država Perzijskog zaljeva pokriva 40% svojih potreba, dok SAD više ne ovisi o uvozu nafte iz Perzijskog zaljeva.

U odnosima Kine sa Zapadom, kao otvorena pitanja ističu se ukupni odnosi sa SAD-om, status Tajvana, pitanje razvoja prometnih i vojnih kapaciteta u Južnokineskom moru, kineska politika prema Hong Kongu te politika prema manjinskom narodu Ujgurima, trgovinske teme poput zaštite intelektualnog vlasništva, širenja novih tehnologija, državnih subvencija i vlasništva nad poduzećima, tržišnog natjecanja i druga.

Rusija je i dalje primarno orijentirana na unutarnju stabilnost te na zadržavanje svog dominantnog utjecaja na prostoru svog bližeg susjedstva, odnosno državama nekadašnjeg SSSR-a koje smatra svojom interesnom sferom. Ipak, ta dominacija je pod pritiskom poput rasta kineskog utjecaja u Srednjoj Aziji ili turskog utjecaja na Kavkazu nakon azerbajdžansko-armenskog rata te u Srednjoj Aziji. Iako su tursko-ruski odnosi, posebice gospodarski, stabilni, na pojedinim kriznim žarištima poput Libije i Sirije njihovi se interesi sukobljavaju. Rusija se u svojoj politici i dalje oslanja na veliku vojnu moć u čiju modernizaciju stalno ulaže značajne resurse. Sporazum o prodljenju ugovora START (Novi START) sa SAD-om o ograničavanju nuklearnog oružja je stupio na snagu i vrijedi do 2026. godine.

Rusija kontinuirano nastoji ograničiti utjecaj NATO-a i EU te njihovo daljnje širenje na jugoistok i istok Europe. Većina država Zapada i dalje prema Rusiji održava režim sankcija zbog aneksije Krima, a odnose sa Zapadom dodatno opterećuju optužbe o fizičkoj eliminaciji političkih protivnika, ruskom hibridnom i obavještajnom djelovanju prema Zapadu i kibernetičkim napadima koji dolaze s ruskog teritorija.

Nakon što je EU uveo gospodarske sankcije zbog aneksije Krima, Rusija se gospodarski pokušava okrenuti Aziji, međutim to je dugoročan i izazovan projekt, pogotovo u odnosu prema Kini koja gospodarski sve više nadilazi rusko gospodarstvo, posebice jer se Kina i Rusija gospodarski nadmeću u pojedinim područjima.

U međusobnim odnosima, Rusija i Kina su se nastavile približavati, međutim, istodobno, među njima postoje izazovi koji ih udaljavaju, kao što je kinesko potiskivanje ruskih gospodarskih interesa u Srednjoj Aziji. Kopneni dio inicijative Pojas i put ide upravo preko tog područja. U 2020. godini se željeznički promet između Kine i Europe preko Srednje Azije gotovo udvostručio. Također, Kina je ruski prvi trgovачki partner, dok Rusija Kini nije niti među prvih 10.

Na globalne sigurnosne prilike utječu i dugoročni procesi poput sve snažnijeg utjecaja klimatskih promjena i njihovih posljedica, prekomjernog iscrpljivanja resursa i uništavanje prirode, gubitka poljoprivrednih površina i biološke raznolikosti, širenja zaraznih i drugih bolesti. Ovi procesi uzrokuju ili multipliciraju druge sigurnosne izazove kao što su migracije stanovništva, društvene napetosti, unutardržavni i regionalni sukobi, kriminal, raspad društvenih i državnih institucija u nestabilnim državama i slično.

Zapadni Balkan u sporom je procesu stabilizacije

Hrvatsko jugoistočno susjedstvo, odnosno Zapadni Balkan i dalje je opterećeno nedovršenim stabilizacijskim procesima. Radi se o području koje obilježavaju neriješena međudržavna i međunacionalna pitanja, uz teškoće vezane uz iskazanu namjeru za europskim integracijama zbog nedovoljne provedbe reformi. Nepovoljni politički i gospodarski uvjeti stvaraju podlogu za jačanje radikalnih i ekstremnih tendencija, kao i društvenih rascjepa u tim krhkim društвима.

Iseljavanje iz država Zapadnog Balkana dodatno utječe na razvojne perspektive ovog područja. Ovaj trend će se nastaviti, a uz ostale, može imati i sigurnosne posljedice, koje su se već pokazale tijekom pandemije kroz nedostatak medicinskog osoblja.

Društvene i međunacionalne tenzije mogu dovesti do međusobnih napetosti i incidenata, posebno u sredinama u kojima postoje neriješeni međunacionalni odnosi.

Političke prilike u BiH i dalje obilježava unutarnja politička nestabilnost uzrokovanu prvenstveno različitim pogledima konstitutivnih naroda oko budućeg ustavnopravnog uređenja BiH, posebice pitanja daljnje centralizacije države, vanjskopolitičkih prioriteta te neriješenog pitanja ustavom zajamčene jednakopravnosti konstitutivnih naroda. Nastavak tendencija postupnog ukidanja temeljnih načela Daytonskog mirovnog sporazuma, poput umanjivanja konstitutivnih prava Hrvata u BiH, mogao bi negativno utjecati na položaj Hrvata kao najmalobrojnijeg naroda u BiH, političku stabilnost i međunacionalni balans unutar BiH, kao i umanjiti demokratsku legitimaciju društvenog uređenja BiH.

Nepostizanje srpsko-albanskog dogovora oko Kosova i dalje pridonosi nestabilnosti u regiji, a posebnu neizvjesnost na Zapadnom Balkanu uzrokuje društveni rascjep u Crnoj Gori u kojoj značajan dio političke moći zauzimaju stranke s protu-NATO, prosrpskom i proruskom orijentacijom nasuprot tzv. suverenističke prozapadne opcije.

U regionalnom kontekstu, pojedini nositelji državne politike u Srbiji promoviraju koncept „srpskog svijeta“ kao jedinstvenog srpskog političkog naroda, odnosno jedinstvene političke i državne zajednice svih Srba na jugoistoku Europe u kojoj svi Srbi trebaju slijediti jedan politički smjer, onaj službenog Beograda. Promoviranje ovakvih ideja s vrha srbijanske vlasti dodatno destabilizira osjetljive međunacionalne i međudržavne odnose na jugoistoku Europe, posebice prema BiH i Crnoj Gori.

Kroz medije i javne nastupe istaknutih pojedinaca, u pojedinim državama susjedstva nastavilo se plasiranjem narativa kojim se želi osporiti legitimnost i zakonitost oslobođilačkih vojno-redarstvenih operacija tijekom Domovinskog rata, a Republiku Hrvatsku se iskrivljavanjem činjenica sustavno pokušava prikazati kao državu nastalu na zločinima te kao sljednicu politike i postupaka kvislinške NDH iz Drugog svjetskog rata.

Organizirani kriminal koji potječe s područja Zapadnog Balkana i dalje je vrlo snažan, a dodatni poticaj daju mu ukorijenjenost u društvenim strukturama, kao i koruptivno-interesne veze prema nositeljima političkih funkcija.

Na ovom području svoje političke, vojne i gospodarske interese žele promovirati i nezapadni akteri. Ovi akteri nastoje prepoznati i iskoristiti institucionalne i društvene slabosti država Zapadnog Balkana za svoje interese te korištenjem instrumenata tzv. meke moći žele ojačati svoj utjecaj, destabilizirati euroatlantske procese, a ponekad i utjecati na promjenu etničke i vjerske strukture stanovništva pojedinih područja.

Prijetnja širenja radikalnog islamizma ostaje konstantna, dok se rizik od terorizma povećava zbog povratka u matične države *džihadista* zarobljenih u Siriji i Iraku, posebice u slučaju izostanka njihove uspješne deradikalizacije. U pojedinim državama Zapadnog Balkana i dalje su aktivni salafitski džihadistički paradžemati u kojima se ne priznaju službene islamske zajednice i demokratski poredak matične države, odobrava terorističko djelovanje i potiče na mržnju i nasilje prema svim *nevjernicima*, uključujući i neistomišljenike muslimane.

Stanje na Zapadnom Balkanu dodatno otežava značajan priljev migranata koji je osobito velik unutar BiH, iz koje migranti nastoje nezakonito ući u RH, odnosno dalje u EU.

Europsko okruženje obilježava nestabilnost

Pojas nestabilnosti koji se proteže južnim i istočnim okruženjem Europske unije i dalje predstavlja sigurnosni izazov. Primarni izvor nestabilnosti predstavljaju oružana krizna žarišta poput Sirije i Libije na kojima se prelamaju i interesi regionalnih sila. Neriješeni zamrznuti sukobi predstavljaju izvor političkih napetosti uz stalnu mogućnost izbijanja i oružanih sukoba, poput onog na području Gorskog Karabaha u jesen 2020. godine ili u pojasu Gaze u proljeće 2021. godine.

Nakon povlačenja međunarodnih snaga iz Afganistana talibani su nakon 20 godina gerilskog ratovanja ponovo zauzeli glavni grad Kabul i cijeli prostor Afganistana. Afganistske institucije i oružane snage su se raspale, a talibani su došli u posjed velikih količina modernog naoružanja i vojne opreme. Slučaj Afganistana pokazuje brzinu i dinamiku sigurnosnih promjena u svijetu, a daljnji razvoj situacije u Afganistanu ovisit će o unutarnjim procesima u Afganistanu, politikama talibanskih vlasti, uključujući i njihove stavove o ljudskim pravima i međunarodnom terorizmu, kao i o djelovanju međunarodnih aktera (regionalnih i globalnih) prema talibanskom režimu. Pogoršanje sigurnosnih prilika u Afganistanu utjecat će i na druge sigurnosne izazove, poput migracijskog pritiska prema Evropi i regionalne stabilnosti u Srednjoj Aziji.

Na području Donbasa u istočnoj Ukrajini povremeno se bilježi jačanje napetosti između sukobljenih strana i češća razmjena vatre koja rezultira vojnim i civilnim žrtvama na obje strane. U isto vrijeme pregovarački proces između sukobljenih strana stagnira.

EU je od listopada 2020. uvela niz mjera ograničenja protiv Bjelorusije kao odgovor na nepravilnosti tijekom predsjedničkih izbora, represiju prilikom mirnih prosvjeda te nakon prisilnog prizemljenja leta tvrtke Ryanair u Minsku i pritvaranja novinara koji je bio u avionu.

Europska unija zainteresirana je i za rješavanje otvorenih pitanja na svojim granicama i u okruženju, poput pitanja razgraničenja i iskorištanja resursa istočnog Sredozemlja, rješavanja aktivnih i zamrznutih sukoba u državama okruženja, pitanja iranskog nuklearnog programa, nezakonitih migracija i druga.

Stanje u dugogodišnjim kriznim žarištima u Siriji i Libiji se u vojnom smislu stabiliziralo te se u tim državama trenutno ne odvijaju značajniji oružani sukobi. S političke strane, nema značajnijeg napretka u rješavanju unutarnjih prilika koji su doveli do građanskih ratova, tako da su obje države i dalje podijeljene između suprotstavljenih strana, iako je u Libiji nakon višemjesečnih intenzivnih oružanih sukoba potpisano primirje i, pod okriljem UN-a, formirana i privremena vlada.

Rog Afrike ostaje krizno područje. U Etiopiji je sukob centralne vlasti s lokalnima u regiji Tigray prerastao u oružani sukob u kojem je federalna vojska zauzela regiju, ali su se sukobi nastavili. Ovaj sukob mogao bi imati destabilizacijski učinak i na susjedne države, Sudan i Eritreju koje su

ionako opterećene brojnim sigurnosnim i gospodarskim izazovima. U Somaliji traju stalni sukobi centralne vlade, uz potporu vojne misije Afričke unije, protiv militantne terorističke organizacije Al Shabab, povezane s Al Qaidom. U državama Sahela poput Malija, Burkine Faso i Nigerije, aktivne su islamiški terorističke skupine, povezane s ISIL-om i Al Qaidom i predstavljaju stalnu prijetnju širem okruženju.

Pojedini procesi u europskom okruženju mogu imati i stabilizacijske učinke, poput normalizacije odnosa Države Izrael s više arapskih država.

Države ovog prostora su, uz sve sigurnosne izazove kojima su opterećene, dodatno pogodjene posljedicama pandemije COVID-19, koja multiplicira sve one društvene i gospodarske poteškoće s kojima se tamošnja društva suočavaju. To znači da tamošnje ionako oslabljene institucije i društva mogu još više gubiti na svojoj stabilnosti.

Društveni i sigurnosni procesi koji će se nastaviti preljevati na Evropu i dalje će biti rast ekstremizma koji može prerasti u terorizam, širenje siromaštva i nezaposlenosti, veći migracijski pritisak prema Europskoj uniji, jačanje organiziranog kriminala i drugi.

Organizirani kriminal je postao transkontinentalan

Europska unija procjenjuje da su prihodi od kriminala na glavnim tržištima kriminala u 2019. godini iznosili 1% BDP-a EU, odnosno 139 milijardi eura. Glavne kriminalne aktivnosti u Evropi su trgovina drogom, kibernetički kriminal, provale i krađe, poslovne i financijske prijevare, kriminal povezan s gospodarenjem otpadom i zagađenjem, nezakonita trgovina oružjem i eksplozivima, namještanje sportskih rezultata i prijevare s klađenjem, krijumčarenje migranata i trgovina ljudima, izrada krivotvorenih dokumenata i novca, krađa intelektualnog vlasništva i krivotvorene proizvoda. Organizirane kriminalne skupine u Evropi djeluju prekogranično, a raste korištenje nasilja kod kriminalnih skupina u smislu učestalosti i ozbiljnosti.

Poseban izazov na području organiziranog kriminala predstavlja pranje novca, odnosno legalizacija sredstava stečenih kriminalnim aktivnostima. Organizirane kriminalne skupine stalno traže nove načine za legalizacijom novca stečenog kriminalom, a pranje novca razvilo se u složene sheme koje kriminalcima, uz naknadu, obavljaju specijalizirane skupine – profesionalne mreže za pranje novca.

Pandemija COVID-19 još je jednom dokazala veliku prilagodljivost organiziranih kriminalnih skupina novim okolnostima. Tijekom pandemije organizirane kriminalne skupine u Evropi su prebacile svoje aktivnosti prema krivotvorenju i distribuciji traženih dobara, kibernetičkom kriminalu, provalama i različitim vrstama prijevara.

Potražnju i nedostatak određenih vrsta roba, posebice zdravstvene opreme (zaštitne maske, rukavice, dezinfekcijska sredstva), kriminalne skupine su brzo iskoristile i zloupotrijebile preusmjerivši dio svojih aktivnosti na to tržište. Pritom su često akutnu potražnju za navedenom robom iskoristivali za nerazmjerno podizanje cijene i ostvarivanje enormnog profita, ali i plasirali krivotvorene proizvode koji ne zadovoljavaju osnovne standarde.

Organizirane kriminalne skupine su tijekom pandemije koristile okolnost da većina ljudi u izolaciji provodi više vremena na internetu, što otvara nove mogućnosti za kibernetičke napade i razne oblike online prijevara. Isto tako, stalno iznalaze načine za korištenje novih tehnologija za kriminalne aktivnosti, kao što je korištenje kriptovaluta za pranje novca i isplatu ucjena.

U kontekstu ublažavanja restriktivnih epidemioloških mjera određene kriminalne aktivnosti će se postupno vraćati na razinu prije pandemije.

Po procjenama Europola više od 50% svih prijavljenih osumnjičenih pripadnika organiziranog kriminala u EU nisu državlјani EU. Polovica njih podrijetlom su iz država susjedstva EU: Zapadnog Balkana, istočne Europe i sjeverne Afrike.

Organizirani kriminal je postao značajan faktor nestabilnosti u državama Zapadnog Balkana, a u pojedinim državama takav kriminal ima značajan utjecaj i na političke prilike i donošenje odluka. Organizirani kriminal s ovog prostora preljeva se i na RH.

Posebno istaknutu destabilizacijsku ulogu pri tome imaju srpsko-crnogorske organizirane kriminalne skupine. Radi se o skupinama koje obilježava visoki stupanj organizacije, brojnost, međunarodno djelovanje i spremnost na provođenje svih oblika kaznenih djela. S njima su povezane i tamošnje navijačke skupine koje se, između ostalog, koriste i za distribuciju narkotika. Neke od tamošnjih navijačkih skupina su, nakon višegodišnjeg nezakonitog djelovanja na nižoj organizacijskoj razini, prerasle u kriminalne organizacije s ustrojenom hijerarhijom i razgranatim lancem za distribuciju narkotika te uspostavljenom i razvijenom suradnjom sa značajnijim kriminalnim skupinama iz regije.

Organizirane kriminalne skupine uspostavile su transkontinentalnu suradnju i nabavljaju velike količine kokaina iz Južne Amerike kojeg morskim putem dopremaju u luke na jugoistoku Europe prikrivene u kontejnerima na prekoceanskim brodovima.

Tako je u travnju 2021. godine policija u Luci Ploče zaplijenila oko 574 kg kokaina koji je dopremljen u kontejneru banana iz Južne Amerike. Uz to, Balkan je ostao glavni tranzitni pravac preko kojeg se heroin doprema u države EU-a.

Veliki broj migranata na području Zapadnog Balkana, odnosno veliki interes za nezakonitim prelaskom granice, organizirane kriminalne skupine koriste za krijućarenje ljudi preko granica u kojem ostvaruju velike profite.

Preko teritorija RH organizirane kriminalne skupine i pojedinci pokušavaju prokrijumčariti oružje, uglavnom zaostalo iz ratova 90-tih na prostoru jugoistočne Europe, prema zapadnoj Europi. To oružje može se koristiti za oružane kriminalne aktivnosti, terorističke napade, a postoji stalni rizik da se preko teritorija RH pokušaju krijumčariti robe koje mogu poslužiti kao komponente oružja za masovno uništavanje.

Nezakonite migracije dugotrajni su društveni i sigurnosni izazov

Područje jugoistočne Europe i dalje je pravac kojim migranti nezakonito žele doći do razvijenih zapadnoeuropskih država. Unatoč smanjenju broja nezakonitih ulazaka migranata iz Turske u Grčku, intenzitet nezakonitih migracija u jugoistočnoj Europi je u porastu, ali je došlo do promjena na pojedinim pravcima na tzv. balkanskoj ruti. Dio migrantskih skupina preusmjero je rutu kretanja iz Srbije prema Rumunjskoj i dalje prema Mađarskoj i zapadnoj Europi. Međutim, ova promjena nije smanjila pritisak na hrvatske granice koji je konstantan i kontinuirano raste u ljetnim mjesecima, pošto je u BiH i dalje stacioniran značajan broj migranata uz stalni priljev novih zapadnobalkanskog rutora.



Po podacima Frontexa tijekom pandemiske 2020. godine zabilježeno je 124.000 nezakonitih prelazaka granice duž vanjske granice EU-a, što je 13% manje nego 2019. godine. Pri tome je na zapadnomediteranskoj ruti zabilježeno 16.969 prelazaka (28% manje u odnosu na 2019. godinu), središnjoj mediteranskoj ruti 35.628 (povećanje od 154% u odnosu na 2019. godinu) te 19.681 prelazak na istočnomediteranskoj ruti (pad od 76% u odnosu na 2019. godinu). Međutim, iako je istočnomediteranska ruta zabilježila veliki pad nezakonitih migracija u 2020. godini, broj nezakonitih migranata na zapadnobalkanskoj ruti porastao je na 26.928, odnosno 78% više nego u 2019. godini.

Najveći broj migranata dolazio je iz Sirije, Maroka, Tunisa i Alžira. Pri tome muškarci čine više od 90% migranata, a oko 10% migranata su maloljetnici.

Iako migrantska kriza u Turskoj trenutno stagnira, nepovoljna sigurnosna i gospodarska situacija u zemljama ishodišta u nadolazećem razdoblju može inicirati novi val migracija na balkanskoj ruti. Uz to, politika Turske prema EU znatno će utjecati na priljev migranata prema jugoistoku

Europe. Razvoj sigurnosne situacije u pojedinim državama, poput Afganistana, utjecat će na daljnji razvoj migracijskog pritiska preko jugoistočne Europe. Pogoršanje situacije s pandemijom COVID-19 i posljedično uvođenje restriktivnijih mjera kretanja u državama utjecalo bi na ponovno usporavanje migrantskih kretanja, kao što se dogodilo u ožujku i travnju 2020. godine.

Nakon što je EU uvela sankcije Lukašenkovom režimu, u Bjelorusiji je registriran značajno veći migracijski pritisak (ponajviše iz Iraka, Konga i Kameruna) na litvansko-bjeloruskoj granici.

Nezakonite migracije predstavljaju značajan društveni izazov s kompleksnim uzrocima i posljedicama. U okolnostima pandemije nezakonite migracije mogu predstavljati javnozdravstveni izazov.

Sa sigurnosnog stajališta, nezakonite migracije su značajan izazov u smislu prepoznavanja pojedinaca s terorističkim namjerama. Više terorističkih napada u Europi posljednjih godina izvele su osobe koje su nezakonito pristigle u zapadnoeuropejske države (napadi u Francuskoj i Njemačkoj), što pokazuje da terorističke skupine koriste nezakonite migracije za prebacivanje svojih pripadnika ili simpatizera u Europu. Isto tako, ovi teroristički napadi pokazuju da je migrantsku populaciju, često traumatiziranu prilikama u zemlji porijekla i poteškoćama u integraciji u zemlji primateljici, moguće radikalizirati.



Pravci nezakonitih migracija u Europi i na jugoistoku Europe

Međunarodna suradnja važan je segment rada SOA-e

Međunarodna suradnja predstavlja izuzetno važan segment sigurnosno-obavještajnog djelovanja. Kroz međunarodnu suradnju sigurnosno-obavještajne zajednice štite zajedničke vrijednosti i interes, razmjenjuju podatke, upozorenja i procjene te iskustva i prakse.

U suvremenom svijetu ni jedna sigurnosna tema više nema samo nacionalno značenje ili učinak. Stoga je međunarodna dimenzija prisutna u svim temama kojima se bave sigurnosne i obavještajne agencije.

SOA ima vrlo razvijenu međunarodnu sigurnosno-obavještajnu suradnju s brojnim sigurnosnim i obavještajnim službama, s kojima surađuje po različitim zajedničkim temama, ovisno o specifičnostima pojedinih država i njihovih sigurnosnih prilika i interesa.

Kao sigurnosno-obavještajna agencija države članice NATO-a i EU-a, SOA razvija snažna međunarodna partnerstva u ovom krugu u kojem se štite zajedničke vrijednosti i interesi. Isto tako, SOA daje osobiti doprinos odgovarajućim tijelima EU-a i NATO-a koja se bave sigurnosnim i obavještajnim temama.



Izlaganje ravnatelja SOA-e povodom potpisivanja Pisma namjere o uspostavi Obavještajnog koledža u Europi 26. veljače 2020. u Zagrebu

U isto vrijeme, SOA je vrlo aktivna u svim multilateralnim forumima u kojima se doprinosi nacionalnoj i međunarodnoj sigurnosti, posebice onim platformama koje djeluju u kontekstu EU i NATO-a, odnosno europskog i euroatlantskog kruga vrijednosti.

U skladu s općim trendom sve veće otvorenosti prema građanima, i u europskoj sigurnosno-obavještajnoj zajednici nastoji se, koliko to sigurnosne i zakonske mogućnosti dopuštaju, više otvoriti svoje djelovanje prema javnosti. I javna izvješća su jedan od takvih alata.

U europskom kontekstu, jedan od najvećih projekata otvaranja europskih sigurnosno-obavještajnih zajednica predstavlja Obavještajni koledž u Europi (*Intelligence College in Europe - ICE*) koji je pokrenut 26. veljače 2020. potpisivanjem Pisma namjere u Zagrebu. Koledžu su pristupile 23 europske države. Koledž je platforma za dijalog između europskih obavještajnih zajednica, donositelja odluka i akademske zajednice kako bi se poticalo strateško razmišljanje, povećalo zajedničko znanje i razvila zajednička europska obavještajna kultura. SOA je tijekom 2020. predsjedavala Koledžom.

Pojedine multilateralne platforme osnovane su s ciljem suprotstavljanja zajedničkih sigurnosnim prijetnjama. Jedna takva iznimno važna i uspješna platforma je Protuteroristička skupina (*Counter Terrorism Group – CTG*) koja okuplja sigurnosne službe država članica EU-a i drugih zapadnoeuropskih država. SOA je u prvoj polovici 2020. godine predsjedala Protuterorističkom skupinom.

SOA je od 2018. do 2020. godine bila partner Agenciji za unutarnju sigurnost (ABW) Republike Poljske u provedbi projekta za učinkovitije identificiranje i suzbijanje terorističkih i asimetričnih prijetnji kod javne uprave. Projekt se sufinancirao iz Europskog socijalnog fonda. ABW je kao partnera u realizaciji projekta izabrala SOA-u zbog aktivnosti SOA-e, mogućnosti doprinosa cilju partnerstva i iskustva SOA-e u međunarodnim projektima slične vrste.



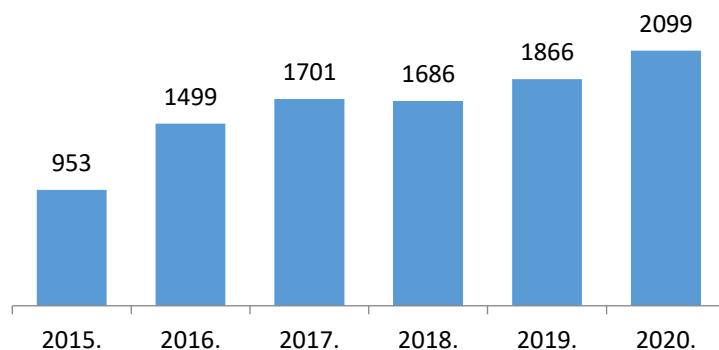
U sklopu projekta ABW-a i SOA-e, 19. i 20. siječnja 2021. održana je online konferencija o podizanju svijesti u prevenciji terorizma. Domaćin konferencije bio je Centar izvrsnosti za prevenciju terorizma ABW-a. Na konferenciji su sudjelovali predstavnici sigurnosnih službi i institucija drugih država te međunarodnih i akademskih organizacija.

SOA je svoj doprinos u projektu dala kroz prikupljanje i razmjenu praksi i iskustava na nacionalnim sastancima, kroz susrete stručnjaka i međunarodne sastanke s brojnim stranim službama i institucijama te je aktivno sudjelovala u izradi edukativnih materijala temeljem kojih su poljski partneri provodili nacionalne treninge za zaposlenike poljskih državnih i javnih službi.

Izvješćivanje korisnika svakodnevna je zadaća SOA-e

O svim relevantnim podacima prikupljenim u okviru svog djelovanja SOA je izvješćivala državni vrh: Predsjednika Republike, predsjednika Hrvatskog sabora i predsjednika Vlade RH. Njima je SOA tijekom 2020. godine dostavila po oko 530 različitih analitičkih uradaka.

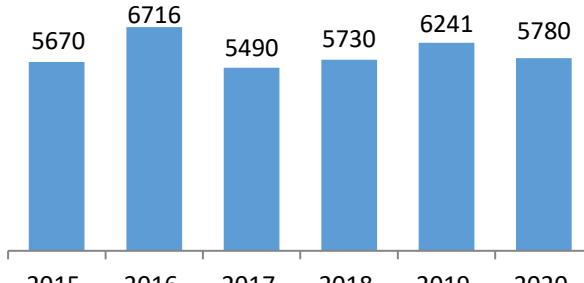
Temeljni oblici izvješćivanja državnih dužnosnika i nadležnih tijela bile su sigurnosno-obavještajne informacije i analize te druga izvješća s obavještajnim podacima. SOA je tijekom 2020. godine izvršila dodatne napore kako bi se izvješćivanje s obavještajnim podacima dodatno intenziviralo tijekom pandemije.



Broj sigurnosno-obavještajnih informacija i analiza te izvješća s obavještajnim podacima po godinama

SOA je dio šireg sustava nacionalne i domovinske sigurnosti te kontinuirano surađuje i dostavlja podatke i procjene drugim nadležnim tijelima, ovisno o tematici i sadržaju podataka. SOA tako dostavlja podatke MUP-u, MVEP-u, Državnom odvjetništvu RH, USKOK-u, MORH-u, Ministarstvu gospodarstva i drugima. SOA je u 2020. godini ukupno uputila oko 9300 različitih sigurnosno-obavještajnih informacija drugim državnim tijelima, što je manje nego 2019. godine kada ih je upućeno 12200. Manji broj podataka u odnosu na ranije godine rezultat je otkazivanja društvenih, gospodarskih, političkih i ostalih aktivnosti sa sigurnosnim implikacijama tijekom 2020. godine zbog pandemije.

U sklopu svog preventivnog rada i jačanja informacijske sigurnosti SOA obavlja sigurnosne provjere (temeljne sigurnosne provjere i one za pristup klasificiranim podacima). Kao i za ostala područja, zbog pandemije broj zahtjeva za provedbom sigurnosnih provjera u 2020. godini bio je manji nego godinu ranije. Ipak, unatoč ograničenjima SOA je u 2020. godini obavila ukupno 5780 sigurnosnih provjera, što je više nego 2017. i 2018. godine.



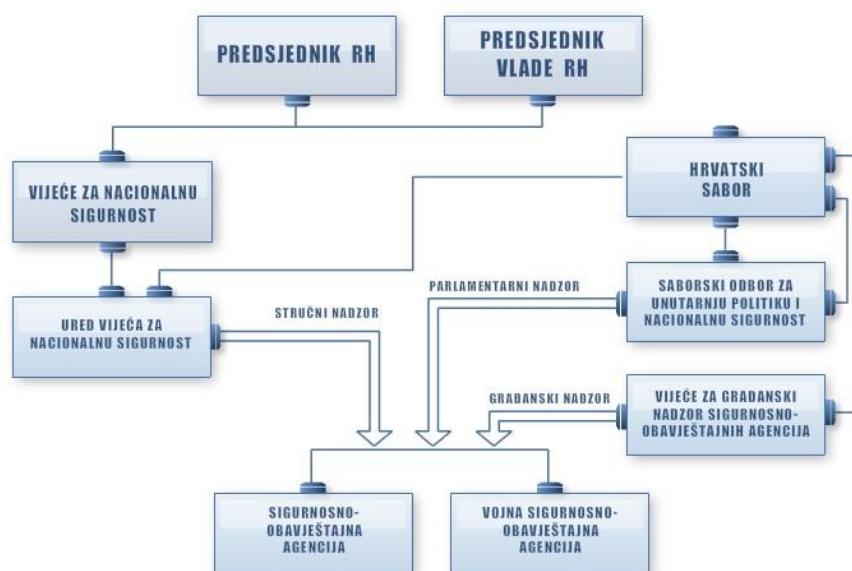
Broj provedenih sigurnosnih provjera po godinama

Pandemija je u brojčanom smislu imala najveći utjecaj na izradu sigurnosnih prosudbi vezanih uz kretanje i boravak štićenih osoba te štićene objekte. SOA je tijekom 2020. godine izradila 300 sigurnosnih prosudbi vezanih uz kretanje i boravak štićenih osoba te štićene objekte, što je manje nego 2019. godine kada ih je izrađeno 565. Provedeno je i oko 23.000 sigurnosnih provjera za osobe koje su imale mogućnost neposrednog pristupa štićenim osobama, objektima i prostorima, što je na razini 2019. godine.

Sigurnosna pitanja stranaca i državljanstava posljednjih godina angažiraju sve značajnije kapacitete SOA-e, pri čemu se posebno ističe problematika tražitelja azila u RH. 2020. godinu obilježio je značajan pad broja provjera u postupku rješavanja statusnih pitanja stranaca i državljanstava koji je uzrokovan zatvaranjem granica među državama tijekom pandemije. Ipak, zbog općih migracijskih trendova, očekuje se porast ovih zadaća u budućnosti. Tako je broj ovih provjera u 2020. godini iznosio 18.825, dok je godinu ranije bio 76.637. U rješavanju zahtjeva za međunarodnom zaštitom (azil i supsidijarna zaštita), na traženje MUP-a, sudjeluje i SOA koja MUP-u daje mišljenje o zahtjevu. SOA svakom predmetu pristupa individualno i obavlja razgovore s podnositeljima zahtjeva za međunarodnom zaštitom.

Nadzor rada SOA-e dio je demokratske prakse

U skladu s praksom u razvijenim demokratskim državama, radi osjetljivosti rada SOA-e i potrebe zaštite zakonitosti i očuvanja ljudskih prava, SOA podliježe stalnom nadzoru rada. U RH postoje tri razine nadzora: parlamentarni nadzor provodi Hrvatski sabor neposredno ili posredstvom Odbora za unutarnju politiku i nacionalnu sigurnost, stručni nadzor provodi Ured Vijeća za nacionalnu sigurnost, dok građanski nadzor provodi Vijeće za građanski nadzor sigurnosno-obavještajnih agencija. Građanski nadzor je pokazatelj demokratske razvijenosti hrvatskog društva jer se radi o rijetkom institutu civilnog nadzora u svijetu, čak i u razvijenim zapadnim demokracijama.



Ilustracija vanjskog nadzora nad zakonitošću rada SOA-e

S obzirom da Vrhovni sud odobrava mјere kojima se privremeno ograničavaju neka ustavna ljudska prava i temeljne slobode te da je zakonitost rada SOA-e podložna sudskoj kontroli, može se govoriti i o četvrtoj, tzv. sudscoj razini nadzora SOA-e.

Nadzorna tijela u obavljanju nadzora imaju široke mogućnosti utvrđivanja činjenica poput uvida u dokumente SOA-e, obavljanja razgovora s ravnateljem i zaposlenicima SOA-e i drugo. Prema dostavljenim rezultatima provedenih nadzora tijekom 2020. nije utvrđeno nezakonito postupanje SOA-e tijekom obavljanja svojih aktivnosti.

Osim vanjskog nadzora rada, unutar SOA-e djeluje tzv. unutarnji nadzor, posebna ustrojstvena jedinica zadužena za nadzor zakonitosti rada ustrojstvenih jedinica i zaposlenika SOA-e, zaštite tajnosti podataka i protuobavještajne zaštite.

Posao u SOA-i jedinstveni je izazov

Unatoč tehnološkom napretku i sve moćnijim alatima za prikupljanje i obradu podataka, ljudska dimenzija sigurnosno-obavještajne djelatnosti ostaje nezamjenjiva, a ljudski čimbenik je i dalje ključan u uspješnosti organizacija. Stoga kvaliteta i učinak rada ponajviše ovise o sposobnostima, znanjima i vještinama zaposlenika.

Broj zaposlenika SOA-e je klasificiran podatak, a sličan je broju zaposlenika sigurnosno-obavještajnim agencijama usporedivih država članica EU-a i NATO-a. Najveći dio zaposlenika SOA-e su službene osobe, a znatno manji dio čine namještenici.

S obzirom na specifičnost posla koji obavljaju, ali i rizike i moguće opasnosti kojima su izloženi, SOA je dužna štititi identitet svojih zaposlenika.

Obrazovna struktura zaposlenika SOA-e je široka te je uvjetovana širinom potreba organizacijske strukture SOA-e. U SOA-i tako rade osobe koje su stekle obrazovanje iz područja ekonomije, računarstva, elektrotehnike, kriminalistike, prava, politologije, psihologije, stranih jezika i drugih područja. Tri četvrtine zaposlenika SOA-e ima neku od razina visokog obrazovanja.

Zaposlenici u SOA-i rade kao operativci, analitičari, informatički stručnjaci, finansijski stručnjaci, pravnici, stručnjaci za ljudske potencijale i kao osobe zadužene za osiguranje, administrativne, arhivske i druge poslove.

U ukupnom broju zaposlenih oko 40% su žene koje obavljaju iste poslove kao i njihovi muške kolege. Dob SOA-inih zaposlenika se uglavnom kreće u rasponu od 30 do 50 godina starosti.

Postupak prijma u SOA-u

Za prijam u SOA-u ne provodi se javni natječaj. SOA na svojim internetskim stranicama (www.soa.hr) ima prostor posvećen zapošljavanju.

Više podataka o zapošljavanju u SOA-i može se pronaći na poveznici www.soa.hr/hr/posao-u-soa-i/, a sve zainteresirane osobe mogu se prijaviti za posao u SOA-u putem web obrasca koji se nalazi na poveznici www.soa.hr/hr/posao-u-soa-i/prijavi-se/#prijava-body.

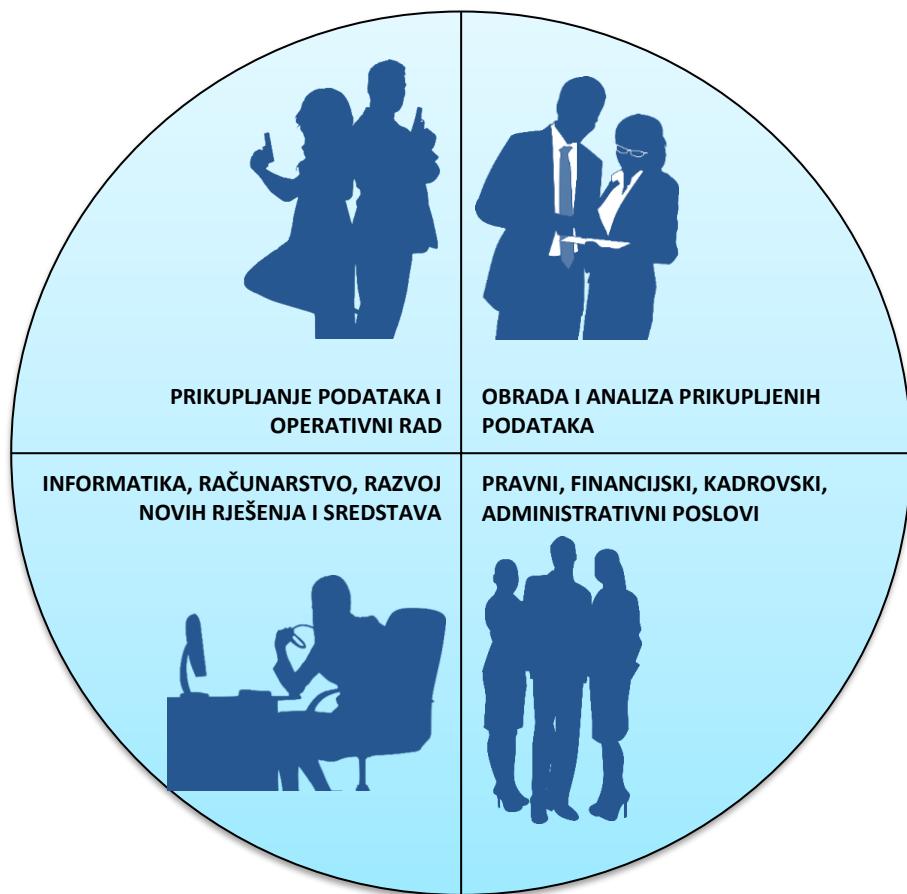
Postupak prijma u SOA-u vrlo je važan u odabiru najboljih kandidata za rad u SOA-i. SOA nastoji privući mlade i obrazovane osobe koje posjeduju znanja, vještine i motivaciju za modernim sigurnosno-obavještajnim radom i koji žele raditi na zaštiti nacionalne sigurnosti Republike Hrvatske.

Sukladno trenutnim potrebama SOA-e, sve zaprimljene prijave se uzimaju u razmatranje te se kontaktiraju one prijavljene osobe koje imaju stečena zvanja i zanimanja te osobine potrebne za konkretna radna mjesta. Svi takvi kandidati se pozivaju da pristupe postupku prijma pod jednakim uvjetima.

Kandidacijski postupak, između ostalog, uključuje sigurnosnu provjeru, razna testiranja znanja i vještina, psihološku procjenu i zdravstveni pregled. Tijekom postupka odabiru se oni kandidati čiji rezultati najviše odgovaraju potrebnom profilu djelatnika.

SOA i ovim putem poziva sve osobe koje smatraju da svojim obrazovanjem i vještinama mogu odgovoriti na izazov rada u sigurnosno-obavještajnom okruženju te žele raditi na dobrobit Republike Hrvatske i njezinih građana, da se prijave za posao u SOA-i. SOA im jamči ravnopravan i pošten, ali i zahtjevan postupak prijma.

Radna mjesta u SOA-i su raznovrsna, a ovdje smo izdvojili četiri najzastupljenije kategorije: radna mjesta operativnih službenika koji rade na prikupljanju podataka i zapošljavaju se uglavnom u centrima SOA-e na cijelom teritoriju RH, radna mjesta na poslovima analize i obrade podataka, radna mjesta na poslovima informatike i računarstva te radna mjesta pravnih, finansijskih, ljudskih potencijala, administrativnih i sličnih poslova.



Ilustracija skupina radnih mјesta u SOA-i

Ovaj dokument vlasništvo je Sigurnosno-obavještajne agencije i objavljen je s namjerom informiranja građana o radu SOA-e i sigurnosnim izazovima i prijetnjama. Dokument je izrađen za javno objavljivanje, dostupan je u elektronskom obliku na internetskim stranicama www.soa.hr i njime se može svatko koristiti.

Fotografije: SOA, MORH, Vlada RH, Pixabay
Karte: SOA

Sigurnosno-obavještajna agencija
Savska cesta 39/1
10000 Zagreb

KONTAKT:

telefon: 01/ 377 22 22
e-pošta: informiranje@soa.hr

www.soa.hr