Sead Turčalo

Zaštita kritične infrastrukture BiH u doba (ruskih) hibridnih prijetnji

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK | BOSNIA & HERZEGOVINA
Detektor

Zaštita kritične infrastrukture BiH u doba (ruskih) hibridnih prijetnji

Sead Turčalo

Sarajevo, 2025.

Impressum

Autor:
Sead Turčalo

Urednik:
Semir Mujkić

Projekt menadžerica:
Aida Mahmutović

Lektura:
Nadira Korić i Amila Žunić

Design i DTP:
Jasmin Leventa

Izdavač:
BIRN BiH - Detektor

Za izdavača:
Denis Džidić

BIRN BALKAN INVESTIGATIVE REPORTING NETWORK | BOSNIA & HERZEGOVINA

Detektor

Sadržaj

Izvršni sažetak

Evropa se suočava s porastom hibridnih prijetnji koje uključuju subverziju i sabotaže kritične infrastructure povezane s ruskim djelovanjem. Nedavni događaji – poput razotkrivanja mreže ruskih instruktora za obuku provokatora u Moldaviji i sabotažnih operacija usmjerenih na infrastrukturu NATO zemalja – ukazuju na rastuću prijetnju. Bosna i Hercegovina (BiH) nije izolirana: na njenoj teritoriji u novembru 2024. uhapšen je ruski državljanin osumnjičen da je obučavao Moldavce za izazivanje nereda, a početkom 2025. BiH je izručila Poljskoj ruskog agenta povezanog sa sabotažama protiv evropskih zemalja.[1] Ovi incidenti potvrđuju sofisticiranost stranog uplitanja i ranjivost strateških resursa BiH.

Ključni sigurnosni izazovi BiH su međusobno povezani i zahtijevaju hitnu pažnju. Među najizraženijim slabostima su duboke etničke podjele koje otežavaju jedinstven odgovor na prijetnje, odsustvo koherentne državne strategije zaštite infrastrukture, značajni *cyber* propusti te prisutna institucionalna korupcija koja podriva provođenje sigurnosnih mjera. Ove slabosti, pogoršane kompleksnom administrativnom strukturom zemlje i nedovoljnim izdvajanjima za sektor sigurnosti, čine BiH podložnom hibridnim operacijama.

S ciljem jačanja odbrane, preporučuju se konkretne mjere usmjerene ka kratkoročnom i srednjoročnom djelovanju. Prioritet je razvoj državne strategije zaštite kritične infrastrukture uz usvajanje pratećeg zakonskog okvira, što bi jasno definiralo nadležnosti svih nivoa vlasti i standarde zaštite. Potrebno je zatim ojačati kapacitete obavještajno-sigurnosnih agencija (kadrovski i tehnološki) za rano otkrivanje i neutralizaciju prijetnji, te uspostaviti specijalizirani centar za hibridne prijetnje radi brze koordinacije odgovora. BiH treba intenzivirati i saradnju s EU i NATO partnerima – kroz razmjenu obavještajnih podataka, uključivanje u međunarodne treninge i primjenu najboljih praksi – kako bi podigla svoju otpornost na nivo zemalja koje su se već susrele s ruskim sabotažama. Konačno, pravne reforme osigurat će brži odgovor na prikrivene operacije ruskih službi. Proaktivno djelovanje u ovim oblastima smanjit će rizik od sabotaža i osigurati dugoročnu stabilnost BiH.

1 Service, R.B. (2024a) *Bosnia to expel Russian man suspected of training Moldovans to foment unrest, RadioFreeEurope/RadioLiberty.* Available at: https://www.rferl.org/a/bosnia-arrest-russian-national-training-camps-moldovans-unrests-sandu-election/33207761.html; (2025) *Russian suspected of sabotage against Poland, US, deported from Bosnia, Tusk says | Reuters.* Available at: https://www.reuters.com/world/europe/russian-suspected-sabotage-against-poland-us-deported-bosnia-tusk-says-2025-02-14/

1. Sigurnosni kontekst i relevantnost za BiH

Ruska agresija na Ukrajinu 2022. godine dovela je do intenziviranja ruskih hibridnih operacija širom Evrope. Umjesto otvorenog sukoba s NATO-om, Moskva pokušava destabilizirati evropske države prikrivenim metodama s ciljem podrivanja demokratskih procesa, poticanja unutrašnjih sukoba i sabotaže kritične infrastrukture. Primjer za to je Moldavija, gdje su ruski akteri tajno obučavali preko stotinu ljudi iz Moldavije i Balkana za izazivanje nereda nakon izbora. U sklopu te operacije identificirani su kampovi za obuku u Srbiji i BiH povezani s Wagner grupom, gdje su instruktori pokazivali polaznicima kako praviti eksplozive i upravljati dronovima.[2] Hapšenje jednog od tih ruskih instruktora na teritoriji BiH (Aleksandr Bezrukavy u Bosanskoj Krupi) direktno je potvrdilo uključenost BiH u širu sliku ruskih destabilizacijskih nastojanja.[3]

Istovremeno, sabotaže kritične infrastrukture postale su učestale u EU zemljama. Zapadni zvaničnici upozoravaju da je od početka 2023. zabilježen nagli porast incidenata, poput provala, požara i napada na energetska postrojenja, željezničke mreže i druge ključne objekte. Tokom 2023. paketi-bombe eksplodirali su u logističkim centrima u Britaniji, Njemačkoj i Poljskoj. Radi se o događajima za koje se sumnja da su bili proba za ruski plan napada na teretne avione ka SAD-u.[4] U Njemačkoj je otkrivena kampanja vandalskih napada na automobile koju su organizirali ruski operativci s ciljem uticaja na izbore. Počinioci su bili mladići iz Srbije,

2 Radio Slobodna Evropa (2024) *Moldavska Policija Uhapsila Više Osoba Zbog 'Pripremanja destabilizacije Nakon Obuka U Rusiji, bih I Srbiji', Radio Slobodna Evropa.* Available at: https://www.slobodnaevropa.org/a/moldavija-kampovi-srbija-bih-rusija/33162391.html#:~:text=U%20videu%20koji%20navodno%20prikazuje,izra%C4%91ivati%20eksploziv%20i%20koristiti%20dronove.

3 Service, R.B. (2024a) *Bosnia to expel Russian man suspected of training Moldovans to foment unrest, RadioFreeEurope/RadioLiberty.* Available at: https://www.rferl.org/a/bosnia-arrest-russian-national-training-camps-moldovans-unrests-sandu-election/33207761.html#:~:text=Authorities%20in%20Bosnia,trained%20young%20people%20to%20cause.

4 Reuters (2025) *Russian suspected of sabotage against Poland, US, deported from Bosnia, Tusk says | Reuters.* Available at: https://www.reuters.com/world/europe/russian-suspected-sabotage-against-poland-us-deported-bosnia-tusk-says-2025-02-14/.

BiH i Njemačke, regrutirani i plaćani putem aplikacija za poruke.[5] Sve ove aktivnosti dio su ruskog arsenala hibridnog rata kojim Kremlj nastoji posijati nepovjerenje u institucije, izazvati ekonomske poremećaje i skrenuti pažnju Zapada sa podrške Ukrajini.[6]

Za Bosnu i Hercegovinu, ova šira strategija destabilizacije itekako je relevantna. Rusija već dugo nastoji zadržati uticaj na Balkanu kako bi spriječila integraciju regiona u EU i NATO. BiH je posebno ranjiva zbog složene unutrašnje strukture. Republika Srpska (RS), kao entitet s jakim proruskim stavovima, može poslužiti kao poligon za ruske operacije. Moskva bi, koristeći svoje veze u RS-u, mogla BiH pretvoriti u sljedeću metu subverzije sa čitavom lepezom akcija, od poticanja političkih kriza do tajnih sabotaža usmjerenih na državne institucije ili infrastrukturu. Ekstremni scenarij bio rusko ohrabrivanje secesionističkih poteza RS-a koje ovih dana poduzima entitetsko rukovodstvo uz insceniran incident – npr. napad lažno predstavljen kao teroristički čin na kritični infrastrukturni objekat u RS – kako bi se stvorio izgovor za eskalaciju u postavljanje policijskih snaga na entitetsku granicu i proglašenje nezavisnosti. Posljedice odsustva strategije zaštite kritične infrastrukture u BiH u takvom slučaju bile bi katastrofalne. Nadležni organi bili bi zatečeni, reagiranje sporo ili nepostojeće, što bi dovelo do dugotrajnog prekida vitalnih usluga, panike među stanovništvom i ozbiljne političke nestabilnosti.[7]

Bosna i Hercegovina, uključujući i nivo Federacije BiH i kantone, usto nema sveobuhvatan plan ni zakon za zaštitu ključnih sistema, što povećava njenu ranjivost. Za razliku od mnogih evropskih zemalja koje su nakon 2022. unaprijedile mehanizme zaštite, BiH još uvijek nije definirala šta se smatra kritičnom infrastrukturom i kako je štititi. Zakon o kritičnoj infrastrukturi povučen je s dnevnog reda sjednice Vijeća ministara 24. septembra 2024., pa takav propis ne postoji na državnom nivou. Zbog toga dijelovi BiH ne mogu biti efikasno zaštićeni. Integrirani pristup na nivou države je neophodan kako bi se pokrile međuentitetske i međusektorske slabosti. Ova praznina u sistemu sigurnosti čini BiH "slabom karikom" koju protivnik može iskoristiti za potkopavanje šireg regiona i evroatlantske sigurnosti.

---

5 Lunday, C. (2025) *Russia supported sabotage spree in Germany to roil election campaign, report says, POLITICO.* Available at: https://www.politico.eu/article/germany-hit-by-suspected-russia-backed-sabotage-campaign/#:~:text=According%20to%20Spiegel%2C%20the%20perpetrators,via%20messaging%20apps%20like%20Viber.

6 *Reuters (2024) Russia's suspected sabotage campaign steps up in Europe | reuters.* Available at: https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/.

7 Irvin Pekmez, N.B. (2024) *Bomb hoax responses spotlight Bosnia and Herzegovina's cybersecurity weaknesses, Detektor.* Available at: https://detektor.ba/2024/10/04/cyber-bitka-koju-ne-znamo-voditi-reakcije-na-lazne-dojave-bombi-otkrile-slabosti-bih/?lang=en#:~:text=But%20Bosnia%20and%20Herzegovina%20does,on%-20September%2024%20this%20year.

2.
Ruska strategija hibridnog ratovanja i prijetnja BiH

Ruska strategija tzv. "hibridnog rata" obuhvata kombinaciju klasičnih obavještajnih operacija, *cyber* napada, propagande, političkog uticaja i fizičkih sabotaža. Cilj je postići geopolitičke interese bez formalne objave rata, iskorištavajući rupe u odbrani i pravnom okviru protivnika. Sabotaža i subverzivne aktivnosti zauzimaju sve istaknutije mjesto u tom arsenalu. Od jedinice GRU-a koja je organizirala eksplozije skladišta municije u inostranstvu (poput slučaja u Češkoj 2014. godine) do podmetanja požara i napada na infrastrukturu u zemljama NATO-a, ruske službe pokazale su spremnost da pribjegnu razornim prikrivenim akcijama.[8]

Šefovi američke CIA-e i britanskog MI6 upozorili su krajem 2024. da Moskva vodi "neobuzdanu kampanju sabotaže" širom kontinenta. Direktor MI5 Ken McCallum naveo je da ruska vojna obavještajna služba (GRU) sve češće koristi kriminalne grupe za izvođenje paljevina i sabotaža u Evropi.[9] Takve operacije, premda tajne, ostavljaju direktne posljedice, uključujući prekide saobraćaja i isporuke energije do stvaranja osjećaja nesigurnosti među građanima.

U regionu Zapadnog Balkana prisustvo i djelovanje ruskih obavještajnih struktura je dokumentirano. NATO je izrazio zabrinutost da protjerani ruski obavještajci pronalaze utočište u zemljama poput BiH i Srbije, odakle nastavljaju voditi operacije protiv interesa Zapada.[10] Drugim riječima, Balkan se koristi kao baza iz koje ruske službe mogu djelovati s manje

8 Reuters (2024) *Russia's suspected sabotage campaign steps up in Europe | reuters.* Available at: https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/.

9 Reuters (2024) *Russia's suspected sabotage campaign steps up in Europe | reuters.* Available at: https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/.; Robbie Gramer, A.M. (2024) *Russia ramps up sabotage operations in Europe, Foreign Policy.* Available at: https://foreignpolicy.com/2024/06/13/russia-sabotage-attacks-europe-espionage-hybrid-arson/ (Accessed: 02 March 2025).

10 *NATO to tackle Russian spying and sabotage operations, says Stoltenberg* (2024) *Cyber Security News | The Record.* Available at: https://therecord.media/nato-russia-sabotage-spies-stoltenberg (Accessed: 02 March 2025).

Nagrada

10.000 $

u kriptovaluti

za zadatke poput špijuniranja vojnih baza, paljenja vozila ili čak likvidacije mete (*Reuters*)

nadzora.[11] U BiH je prisutan ruski diplomatski kadar i tzv. kulturni centri, ali zapadne agencije sumnjaju da se među njima nalaze i "prikriveni operativci" koji koordiniraju obavještajne mreže. Mediji su izvještavali i o prisustvu proruskih paramilitarnih grupa u RS-u (npr. "Noćni vukovi" – motoklub blizak Kremlju, te pojedina veteranska udruženja) koje bi mogle biti iskorištene za lokalne operacije sabotaža ili nasilja. Takva infrastruktura na terenu predstavlja potencijalni kanal za ruske subverzivne planove u BiH.

Rusija se u hibridnom ratu oslanja i na digitalne platforme kako bi proširila doseg za vrbovanje pomagača.[12] Aplikacije poput *Telegrama* i sličnih postale su novi regrutni centri za sabotaže. Istrage su pokazale da anonimni ruski posrednici na *Telegram* kanalima oglašavaju potrebu za "evropskim patriotima" spremnim izvesti sabotaže u zamjenu za izdašne nagrade. U jednom takvom slučaju, novinari su otkrili oglas u kojem se nudi do 10.000 dolara u kriptovaluti za zadatke poput špijuniranja vojnih baza, paljenja vozila ili čak likvidacije mete.[13] Na prve pozive javljaju se često mladići s kriminalnom prošlošću ili finansijskim problemima, motivirani brzom zaradom). Ovakav model regrutacije znači da Rusija može mobilizirati mreže sabotera *ad hoc*, smanjujući tragove koji bi ukazali na direktnu umiješanost Moskve.

---

11 Nermina Kuloglija-Zolj, N.B. (2023) *Expelled by other countries, Russian diplomats get accredited in Bosnia, Detektor.* Available at: https://detektor.ba/2023/09/06/expelled-by-other-countries-russian-diplomats-get-accredited-in-bosnia/?lang=en (Accessed: 02 March 2025).

12 *Following Russia's 'Oreshnik' missile strike on Ukrainian Aerospace plant, pro-war Russian telegram channels call for escalation, 'Real War' with the west* (2024) *MEMRI.* Available at: https://www.memri.org/reports/following-russias-oreshnik-missile-strike-ukrainian-aerospace-plant-pro-war-russian-telegram.

13 Reuters (2024) *Russia's suspected sabotage campaign steps up in Europe | reuters.* Available at: https://www.reuters.com/world/russias-suspected-sabotage-campaign-steps-up-europe-2024-10-21/.

3.
Stanje zaštite kritične infrastrukture u Bosni i Hercegovini

Kritična infrastruktura podrazumijeva sektore i objekte od ključnog značaja za funkcioniranje države i društva, energetsku mrežu (elektrane, dalekovodi, naftovodi, gasovodi), vodosnabdijevanje, transportne koridore (putevi, željeznice, mostovi, tuneli, luke, aerodromi), informacijske i komunikacijske sisteme, finansijski sistem, te ključne javne institucije i objekte sigurnosti. Zaštita ovih resursa u BiH je kompleksna zbog više nivoa vlasti i fragmentiranih nadležnosti.

Trenutno je institucionalna odgovornost za zaštitu kritične infrastrukture podijeljena između više subjekata. Na državnom nivou, Ministarstvo sigurnosti BiH formalno je zaduženo za koordinaciju sigurnosnih politika, uključujući zaštitu infrastrukture i civilnu zaštitu. Unutar Ministarstva djeluje Sektor za zaštitu i spašavanje koji se bavi planiranjem odgovora na vanredne situacije, ali ne postoji posebna agencija isključivo fokusirana na kritičnu infrastrukturu. Obavještajno-sigurnosna agencija (OSA) prati potencijalne prijetnje, uključujući kontraobavještajne aktivnosti vezane za sabotaže ili terorizam. OSA sarađuje s policijskim agencijama i tužilaštvima kada identificira prijetnje usmjerene na vitalne objekte. Na entitetskom nivou, MUP Republike Srpske i Federalno ministarstvo unutrašnjih poslova (FMUP) su s kantonalnim MUP-ovima u FBiH nadležni za javnu sigurnost i fizičku zaštitu objekata na svojim teritorijama. Oni osiguravaju policijsko obezbjeđenje ključnih objekata i reagiraju na incidente. SIPA (Državna agencija za istrage i zaštitu) i entitetske policije imaju antiterorističke jedinice koje bi bile angažirane u slučaju sabotaža ili napada na infrastrukturu. SIPA također štiti određene važne objekte na državnom nivou. Oružane snage BiH mogu, u vanrednim okolnostima i na zahtjev Predsjedništva BiH, biti angažirane na čuvanju važnih objekata (npr. skladišta naoružanja, objekti odbrambene infrastrukture) ili pružanju podrške civilnim vlastima – premda je njihova uloga u unutrašnjoj sigurnosti ograničena ustavnim okvirom i političkim saglasnostima. Operateri infrastrukture (komunalna preduzeća, elektroprivrede, telekomi, transportna preduzeća) imaju vlastite sigurnosne službe i protokole za zaštitu svojih postrojenja. Njihovi kapaciteti variraju i često ovise o saradnji s državnim organima u kriznim situacijama.

4.
Postojeći protokoli i planovi

BiH je u prošlosti razvijala određene strateške dokumente za upravljanje krizama (npr. strategije za borbu protiv terorizma i organiziranog kriminala), ali strategija posvećena zaštiti kritične infrastrukture još ne postoji na državnom nivou. Unutar entiteta su pokretane inicijative. U Federaciji BiH je izrađen Prednacrt zakona o zaštiti kritične infrastrukture, a u RS je 2019. godine usvojen Zakon o zaštiti kritičkih infrastruktura u RS-u.[14] Ne postoji ni krovni državni zakon koji bi uspostavio jedinstven okvir i obavezujuće standarde. Ovaj zakonski i strateški vakuum je ozbiljan problem. BiH je potreban državni zakon o kritičnoj infrastrukturi kako bi se jasno definirale nadležnosti i akcioni mehanizmi za zaštitu ključnih usluga. Bez takvog okvira, odgovor na sabotaže oslanja se na *ad hoc* mjere i ličnu inicijativu službenika, umjesto na uhodane procedure. Nedostatak specifičnih planova odbrane od sabotaža znači i da potencijalni incidenti možda neće biti pravovremeno prepoznati.

Koordinirani prekidi u elektroenergetskim sistemima ili komunikacijskim mrežama predstavljaju scenarij visokog sigurnosnog rizika, naročito kada postoje institucionalne nejasnoće ili, još opasnije, otvorena nesuradnja dijelova sigurnosnog aparata. U kontekstu Bosne i Hercegovine ovaj rizik eksponencijalno raste. Naime, kao što smo ranije opisali, sigurnosna i upravljačka složenost kritične infrastrukture u BiH temelji se na isprepletenosti nadležnosti između entiteta, kantona i državnih institucija. Takvo administrativno okruženje generira sistemsku nejasnoću o tome ko preuzima vođenje odgovora i istrage u kriznim situacijama poput koordiniranih *cyber* ili fizičkih napada na ključnu infrastrukturu. U prvim satima od nastanka incidenta, jasnoća i brzina reakcije predstavljaju ključne faktore ublažavanja štete i efikasnosti odgovora, ali upravo zbog ove složenosti može doći do opasnog kašnjenja ili potpune paralize sistema upravljanja krizom.

14 (2019) *Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj, NSRS.* Available at: https://www.narodnaskupstinars.net/?q=la%2Fakti%2Fusvojeni-zakoni%2Fzakon-o-bezbjednosti-kriti%C4%8Dnih-infrastruktura-u-republici-srpskoj

Ova strukturalna ranjivost Bosne i Hercegovine dodatno se zaoštrila u aktuelnom političko-sigurnosnom kontekstu. Posljednjih mjesec dana, kontinuirano djelovanje entitetskih vlasti RS-a na podrivanju ustavnog poretka Bosne i Hercegovine, kulminiralo je raspisivanjem centralne potjernice za političkim rukovodstvom tog entiteta. Uprkos tome, policija RS-a demonstrira otvorenu političku pristrasnost i ne izvršava mjere državnih pravosudnih institucija. Takvo postupanje upućuje na ozbiljne i zabrinjavajuće implikacije sigurnosne prirode. Policija, kao ključni institucionalni garant sigurnosti entiteta, pokazuje veću lojalnost bjeguncima od zakona, nego institucijama pravnog poretka države.

Ako bi hipotetički scenarij koordiniranog napada na kritičnu infrastrukturu došao iz krugova ili država bliskih aktuelnom rukovodstvu RS-a, osnovano je pretpostaviti da bi sigurnosne institucije u ovom entitetu pokazale vrlo ograničen stepen saradnje. Drugim riječima, uslijed evidentne politizacije i lojalnosti političkom, a ne pravnom poretku, može se očekivati izostanak pravovremenog dijeljenja vitalnih informacija, usporavanje ili direktna opstrukcija istrage, te slaba ili potpuno izostala reakcija u ključnim prvim satima krize. Takav scenarij ima ozbiljne posljedice po ukupnu sigurnost građana, energetsku stabilnost i stratešku otpornost države.

Dodatnu opasnost predstavlja moguće iskorištavanje ovakvih ranjivosti od strane vanjskih aktera, prije svega aktera s jakim uticajem na rukovodstvo RS-a, poput Rusije koja posjeduje sofisticirane *cyber* kapacitete i historiju korištenja energetike kao oruđa geopolitičke prisile. Nezavisno od nivoa formalne uključenosti, takve sile mogle bi biti u iskušenju da iskoriste institucionalnu nejasnoću i političke slabosti Bosne i Hercegovine za destabilizaciju i vršenje dodatnog pritiska, produbljujući postojeću polarizaciju i političke tenzije. Ovakve dileme i nejasnoće usporavaju ne samo adekvatnu reakciju u kritičnim satima, već i prethodno planiranje odgovora. Postoje planovi za vanredne situacije (poput prirodnih katastrofa) koji bi se mogli primijeniti i kod sabotaža, ali oni uglavnom ne uključuju preventivne mjere specifične za prijetnje od organizirane ljudske akcije.

5.
Saradnja s međunarodnim partnerima

Iako BiH nije članica NATO-a, sarađuje kroz program Partnerstvo za mir i MAP, a NATO štab u Sarajevu djeluje kao savjetodavno tijelo u oblasti odbrane i sigurnosti. U zaštiti infrastrukture i suzbijanju hibridnih prijetnji ta saradnja podrazumijeva obuke i razmjenu informacija. Sigurnosne agencije BiH održavaju kontakte s obavještajnim službama partnerskih zemalja. Primjer efikasne saradnje zabilježen je početkom 2025., kada su vlasti BiH postupile po zahtjevu Poljske te locirale i izručile ruskog državljanina osumnjičenog za sabotaže protiv NATO zemalja. Ovakvi potezi pokazuju spremnost BiH da bude konstruktivan partner. Također, EU kroz svoje programe (IPA fondovi, instrumenti za vladavinu prava) pomaže jačanju kapaciteta policije i pravosuđa u BiH, što uključuje i domene relevantne za zaštitu kritične infrastrukture (npr. obuke za *cyber* odbranu energetskih mreža, forenziku eksplozivnih naprava).

Međutim, saradnju bi trebalo unaprijediti formalnijim kanalima. BiH još nije integrirana u sve evropske mreže za razmjenu obavještajnih podataka o hibridnim prijetnjama, što bi bilo korisno s obzirom na prekograničnu prirodu ovih izazova. Također, postoji prostor za dublju saradnju sa susjednim zemljama – Hrvatskom i Srbijom, po pitanju zaštite zajedničkih infrastrukturnih sistema (npr. prekograničnih energetskih vodova ili komunikacijskih mreža). U praksi, dosadašnja saradnja najviše je funkcionirala u oblasti reakcije na incidente, dok bi cilj ubuduće trebao biti preventivno dijeljenje informacija i usklađivanje planova zaštite.

Trenutno stanje zaštite kritične infrastrukture u BiH karakteriziraju fragmentiranost i reaktivnost. Postoji svijest o potrebi unapređenja – što pokazuju inicijative za zakone na entitetskom nivou – ali potrebno je to podići na državni nivo i operativno provesti. Dok se to ne desi, BiH ostaje ranjiva u slučaju ozbiljnije kampanje sabotaža ili koordiniranog napada na kritičnu infrastrukturu.

6.
Uporedna analiza: Kako druge države odgovaraju na rusku prijetnju?

Evropske zemlje na prvoj liniji ruske hibridne ofanzive preduzele su niz mjera za jačanje otpornosti svojih infrastruktura. Iskustva Poljske, Češke i Estonije posebno su relevantna jer su ove države kombinacijom političkih, sigurnosnih i pravnih koraka podigle nivo zaštite i mogu poslužiti kao model za BiH.

Kao susjed Ukrajine i logistički centar za pomoć Kijevu, Poljska je rano prepoznala da će biti meta ruskih obavještajnih i saboterskih aktivnosti. Od početka rata u Ukrajini, poljske vlasti su pojačale kontraobavještajne napore i uspjele razotkriti jednu od najvećih špijunskih mreža u novijoj historiji zemlje. U decembru 2023. poljski sud je osudio 14 stranih državljana (uglavnom iz susjedstva) za špijunažu i pripremu sabotaža po nalogu Rusije.[15] Istraga je utvrdila da su planirali izazvati željezničku nesreću, izbacivanja iz šina voza koji je prevozio pomoć za Ukrajinu, te su prikupljali podatke o ključnim objektima (aerodromima, vojnoj fabrici, lukama) povezanim s isporukama pomoći. Ovakve presude neutraliziraju neposrednu prijetnju i djeluju odvraćajuće na buduće sabotere. Uz pravosudne mjere, Poljska je posegla i za diplomatijom. U oktobru 2024. zatvorila je ruski konzulat u Poznanju, navodeći dokaze o umiješanosti ruskog osoblja u saboterske aktivnosti.[16] Poljski ministar vanjskih poslova Radosław Sikorski izjavio je da postoji čvrst dokaz da je ruska obavještajna služba stajala iza pokušaja sabotaže u Poljskoj i drugim savezničkim državama.[17] Time je poslana poruka da će se svaki čin subverzije povezane

15 Service, R.R. (2023) *Polish court convicts 14 foreigners of spying for Russia, RadioFreeEurope/RadioLiberty.* Available at: https://www.rferl.org/a/polish-court-convicts-foreigners-spying-russia/32740122.html#:~:text=A%20court%20in%20Poland%20convicted,13%20months%20to%20six%20years.

16 *Minister of foreign affairs decides to close Russian consulate in Poznań - Ministry of Foreign Affairs Republic of poland - gov.pl website* (2024) *Ministry of Foreign Affairs Republic of Poland.* Available at: https://www.gov.pl/web/diplomacy/minister-of-foreign-affairs-decides-to-close-russian-consulate-in-poznan.

17 Reuters (2024) *Poland to close Russian consulate in Poznan, citing alleged sabotage attempts | Reuters.* Available at: https://www.reuters.com/world/europe/poland-close-russian-consulate-poznan-2024-10-22/.

14

stranih državljana (uglavnom iz susjedstva) poljski sud je, u decembru 2023. osudio za **špijunažu i pripremu sabotaža** po nalogu Rusije

s Rusijom direktno vezivati uz rusku državu i da će uslijediti posljedice (diplomatske sankcije, protjerivanje osoblja). Poljska je također značajno pojačala fizičko osiguranje strateških objekata – vojna i policijska prisutnost povećana je oko željezničkih pruga, skladišta goriva i transportnih čvorišta. Uvedene su dodatne provjere radnika i tereta na kritičnim rutama kako bi se preveniralo postavljanje eksploziva ili uređaja za ometanje signalizacije. Kao rezultat, uprkos učestalim pokušajima, do sada nije zabilježen uspješan veći akt sabotaže u Poljskoj. Svaki sumnjivi incident (npr. požari u fabrikama, ometanje željezničkih signala) istražuje se s pretpostavkom mogućeg stranog uticaja.

Češka ima iskustvo ruskog subverzivnog djelovanja. Tek 2021. otkriveno je da su dvije velike eksplozije u skladištima municije 2014. bile djelo ruskih agenata, što je izazvalo diplomatski skandal i masovno protjerivanje ruskih "diplomata" iz Praga. Ova spoznaja bila je katalizator da Češka revidira pristup sigurnosti infrastrukture. Već 2022. češka vlada je počela pojačano čuvanje strateških objekata, angažirajući i vojsku u tu svrhu.[18] Ministrica odbrane Jana Černochová izjavila je da su vojnici raspoređeni na zaštiti objekata važnih za odbranu države, poput energetskih postrojenja, izvorišta pitke vode, važnih mostova i skladišta naoružanja.[19] Ta praksa, ranije rezervirana za vanredna stanja (elementarne nepogode, terorizam), postala je nova norma uslijed prijetnje ruskih sabotaža. Istovremeno su češke sigurnosne agencije pojačale nadzor i obavještajno praćenje potencijalnih meta. Prema riječima ministrice, u izvještajima obavještajne službe redovno se detektiraju pokušaji izviđanja tih objekata od strane sumnjivih aktera. Češka je reagirala i pravnim reformama. Iako joj krivični zakon

18 *Czechs beefing up defence over threat of Russian terror* (2022) *Radio Prague International.* Available at: https://english.radio.cz/czechs-beefing-defence-over-threat-russian-terror-8763798#:~:text=Speaking%20on%20Czech%20Television%20on,invasion%20of%20Ukraine%20in%20February.

19 *Czechs beefing up defence over threat of Russian terror* (2022) *Radio Prague International.* Available at: https://english.radio.cz/czechs-beefing-defence-over-threat-russian-terror-8763798.

potiče još iz 1961. i formalno nema poseban zakon o terorizmu, uvode se novi mehanizmi za procjenu rizika – četverostepeni sistem terorističkih prijetnji od 2025.godine, te omogućava fleksibilnije djelovanje policije i tajnih službi u sivoj zoni hibridnih prijetnji.[20] Nastavljen je i obračun s ruskom špijunskom mrežom. Češka je među zemljama koje su najviše smanjile rusko diplomatsko prisustvo (protjerane desetine osumnjičenih obavještajaca). Kao rezultat, kapacitet ruskih operativaca na terenu u Češkoj bitno je smanjen. Odbrambeni fokus proširen je i na *cyber* domen. Češka agencija NÚKIB upozorila je na sve učestalije *cyber* napade na energetski i transportni sektor, očito koordinirane sa fizičkim prijetnjama.[21] Najbolje prakse iz Češke pokazuju važnost kombinacije mjera – od fizičkog obezbjeđenja i obavještajnog praćenja do diplomatskog pritiska i prilagođavanja zakonskog okvira – kako bi se odgovorilo na novu vrstu rata.

Kao baltička zemlja s dugim iskustvom suočavanja s ruskim pritiscima i sabotažama, Estonija je razvila robustan sistem otpornosti koji obuhvata i državne i društvene kapacitete. Još 2007. pretrpjela je masivan ruski *cyber* napad, nakon čega je postala pionir u kibernetičkoj sigurnosti. Estonija je postala sjedište NATO centra za *cyber* odbranu. U aktuelnom kontekstu pojačanih sabotaža u Evropi, Estonija nastavlja prednjačiti u proaktivnom pristupu. Godine 2024. estonske vlasti uhapsile su grupu od 10 osoba osumnjičenih za provođenje sabotaža i akcija zastrašivanja u korist Rusije.[22] Ovo hapšenje uslijedilo je nakon otkrivanja zavjere čiji je cilj bilo ometanje estonskih isporuka vojne pomoći Ukrajini. Ovo potvrđuje da i Estonija, iako geografski udaljenija od sukoba, nije poštеđena pokušaja ruskog subverzivnog djelovanja. Nakon nedavnih incidenata oštećenja podmorskih kablova i gasovoda u Baltičkom moru, za koje postoji sumnja na sabotažu, NATO je rasporedio pomorsku patrolnu grupu uz obale Estonije radi pojačanog nadzora podmorske infrastructure.[23] Vlada Estonije je otvoreno pozvala stručnjake iz savezničkih zemalja da pomognu u istragama takvih incidenata, pokazujući transparentnost i spremnost na međunarodnu saradnju. Estonija ulaže značajne napore u civilnu odbranu i svijest javnosti. Redovno informira građane o procedurama za vanredne situacije, bilo da je riječ o *cyber* napadu ili nestanku struje uslijed sabotaže, čime smanjuje prostor za paniku i dezinformacije. Također, KAPO (Estonska služba unutrašnje sigurnosti)

20 *Safety in Czechia: Officials outline what to watch for as new threats loom* (2025) *Prague, Czech Republic.* Available at: https://www.expats.cz/czech-news/article/safety-in-czechia-police-outline-what-to-watch-for-as-new-dangers-loom#:~:text=Czechia%27s%20new%20terrorist%20threat%20system.

21 *Czech minister tells Financial Times Russia trying to sabotage critical infrastructure* (2024) *Radio Prague International.* Available at: https://english.radio.cz/czech-minister-tells-financial-times-russia-trying-sabotage-critical-8813329#:~:text=The%20EU%20Agency%20for%20Cybersecurity,areas%20of%20energy%20and%20transportation.

22 RFERL (2024) *Estonia detains 10 people suspected of committing sabotage on orders from Russia, RadioFreeEurope/RadioLiberty.* Available at: https://www.rferl.org/a/estonia-detains-10-sabotage-russia/32828650.html#:~:text=Estonia%E2%80%99s%20domestic%20security%20agency%20said,society%2C%20the%20security%20service%20said.

23 *NATO flotilla assembles off Estonia to protect undersea cables in Baltic Sea* (2025) *The Guardian.* Available at: https://www.theguardian.com/world/2025/jan/19/nato-flotilla-assembles-off-estonia-protect-undersea-cables-baltic-sea.

10

osoba osumnjičenih za **provođenje sabotaža i akcija zastrašivanja** u korist Rusije uhapsile su estonske vlasti 2024. godine

godinama javno objavljuje godišnje izvještaje o prijetnjama[24] u kojima otvoreno imenuje ruske obavještajne aktivnosti i upozorava ključne sektore na mjere opreza. Rezultat je da je estonsko društvo izgradilo visok prag otpornosti. Svaki sumnjiv događaj se odmah ispituje, a građani su podstaknuti da prijavljuju neobične aktivnosti oko infrastrukturnih objekata. Najbolje prakse Estonije naglašavaju značaj uključivanja cijelog društva u odbranu, od vrha države do lokalne zajednice, te stalnog inoviranja odbrambenih metoda kako se prijetnje razvijaju.

Iz primjera ovih zemalja mogu se izvući zajedničke odrednice uspješnog odgovora na rusku prijetnju:

a) *Snažno kontraobavještajno djelovanje i pravosudni progon mreža povezanih s Rusijom – hapšenje, procesuiranje i javno obznanjivanje slučajeva radi odvraćanja budućih aktera.*
b) *Pojačana fizička i cyber zaštita ključne infrastrukture, uz korištenje svih raspoloživih sredstava (policije, vojske, tehnologije) za nadzor i odbranu.*
c) *Međunarodna saradnja i koordinacija, od razmjene obavještajnih podataka do zajedničkih vježbi i patrola, poput angažmana NATO-a na Baltiku.*
d) *Diplomatske mjere protiv zloupotrebe ruskog prisustva. Ograničavanje broja "diplomata", zatvaranje sumnjivih objekata, nadzor nad ruskim investicijama u kritičnim sektorima.*
e) *Prilagođavanje zakonodavstva kako bi hibridne prijetnje bile eksplicitno obuhvaćene. Donošenje novih zakona ili strategija koji sabotaže, dezinformacije i sl. tretiraju kao vid agresije.*

Sve ove lekcije iz zemalja centralne Evrope i postsovjetskog prostora su primjenjive i na BiH, uz prilagođavanje lokalnim okolnostima.

---

24 KAPO (2024) *Annual Review 2023-2024*. Available at: https://kapo.ee/sites/default/files/content_page_attachments/Annual%20review%202023-2024.pdf.

7.
Ključni izazovi i slabosti BiH u kontekstu ruske prijetnje

Uprkos svijesti o opasnosti, BiH se suočava s nizom unutrašnjih izazova koji otežavaju uspostavljanje efikasne odbrane od ruskih hibridnih prijetnji. Komplicirana ustavna struktura znači da nema jedinstvene politike u oblasti sigurnosti. Vlasti entiteta Republika Srpska često blokiraju ili usporavaju državne inicijative koje percipiraju kao prijetnju entitetskoj autonomiji ili kao suprotstavljanje Rusiji. Politički lideri RS-a, poput entitetskog predsjednika Milorada Dodika i predsjednika Narodne skupštine Nenada Stevandića, otvoreno njeguju veze s Moskvom i nerijetko negiraju ili umanjuju rusku prijetnju, nazivajući je zapadnom propagandom. Zbog toga BiH nema jedinstvenu strategiju. Dok politički akteri sa sjedištem u Sarajevu prepoznaju potrebu jačanja zaštite kritičke infrastrukture i sigurnosti u cjelini, Banja Luka to osporava. Rezultat je paraliza po pitanju ključnih odluka, kao što je usvajanje državnog zakona o kritičnoj infrastrukturi ili nove strategije sigurnosti, što ostaje zarobljeno u političkim nesuglasicama. Unutrašnja nejedinstvenost upravo je ono što hibridni napadač poput Rusije može iskoristiti. Bilo podržavanjem jedne strane (RS) da prkosi drugoj (FBiH), bilo izazivanjem incidenata koje državni vrh neće moći jednoglasno adresirati. Teoretski, vlasti RS-a bi nakon incidenta protiv kritične infrastrukture mogle odbiti pomoć državnih institucija ili NATO partnera, što bi dovelo do haotične situacije. Čak bi i stvarna sabotaža od strane treće strane mogla biti iskorištena za politička prepucavanja unutar BiH, umjesto za koordiniranu reakciju. Time bi se multiplicirale posljedice štetnog događaja.

Institucionalne slabosti i nedostatak strateškog okvira predstavljaju još jedan značajan izazov za razvoj otpornosti Bosne i Hercegovine na potencijalno ugrožavanje kritičke infrastrukture. Sigurnosne institucije BiH su fragmentirane po entitetskim linijama i često kadrovski vođene političkom podobnošću, što potkopava profesionalizam. OSA već godinama trpi unutrašnje pritiske. Ako OSA ne funkcionira optimalno, rano otkrivanje ruskih prikrivenih operacija može zakazati. SIPA i policijske agencije imaju ograničene kapacitete za proaktivno praćenje sofisticiranih hibridnih prijetnji. Njihove istrage uglavnom reagiraju *post festum*. Problem je i zastarjela/neadekvatna pravna regulativa. Krivični zakoni BiH i entiteta inkriminiraju terorizam,

špijunažu i diverziju, ali postupci dokazivanja mogu biti spori i kompleksni. Ne postoji u zakonu eksplicitna kategorija "hibridnog djelovanja" ili "stranog malignog uticaja" koja bi olakšala sankcioniranje domaćih lica koja za račun strane sile učestvuju u subverziji. BiH je ranije usvojila zakon kojim je zabranila građanima odlazak na strana ratišta, ciljajući ekstremiste koji su išli u Siriju, a poslije i Ukrajinu, što pokazuje da su pravne inovacije moguće, ali uz međunarodni pritisak koji proizvede političku volju. No takva volja zasad izostaje u suprotstavljanju ruskoj prijetnji. Odsustvo državne strategije zaštite kritične infrastrukture znači i da nema jasno definiranih procedura ni namjenskog budžeta za ovu oblast. Posljedično, ulaganja u sigurnosnu opremu, obuku specijaliziranih jedinica i otpornost infrastrukture ostaju *ad hoc* i nedovoljna.

Tu su i ekonomske prepreke i ograničenja resursa, koji su ozbiljna slabost. BiH je zemlja skromnih finansijskih mogućnosti i višegodišnjih socio-ekonomskih problema. Budžetski prioriteti često su usmjereni na osnovne socijalne potrebe i održavanje glomaznog javnog sektora, dok su izdvajanja za sektor sigurnosti minimalna. Osim toga, institucije na državnom nivou su godinama imale zamrznut nivo budžeta zbog odbijanja političkih aktera iz entiteta Republika Srpska da se taj budžet uvećava. Modernizacija opreme policije i agencija ide sporo. Za nadzor kritične infrastrukture potrebne su savremene kamere, dronovi, senzori i cyber-sistemi, što zahtijeva značajna sredstva i kontinuirano održavanje. Čak i kada postoji svijest o potrebi, javne nabavke ovih sistema se odugovlače ili su kompromitirane korupcijom. Korupcija je veliki izazov. Nije nezamisliv scenarij gdje saboter "kupi" pristup kontrolnoj sobi postrojenja ili dođe do internih planova obezbjeđenja u okruženju gdje integritet kadrova nije osiguran. Ekonomska situacija utiče i na društvenu sferu. Visoka nezaposlenost mladih i osjećaj besperspektivnosti čine dio populacije podložnim uticaju proruskih narativa, ili čak spremnim da za novac učestvuju u rizičnim aktivnostima. Ovo se uklapa u obrazac korištenja lokalaca s margina društva za prljave poslove sabotaže, kao što je rađeno u zemljama centralne Evrope i postsovjetskog prostora. Dakle, socijalna ranjivost prelijeva se u sigurnosnu ranjivost.

Izazov predstavlja i sposobnost prepoznavanja prikrivenih operacija. Hibridne operacije su često teške za prepoznati. Bosna i Hercegovina se posljednjih godina suočava sa sve kompleksnijim sigurnosnim izazovima, među kojima posebno mjesto zauzimaju hibridne prijetnje i *cyber* operacije.[25] Jedan od ključnih problema predstavlja sposobnost države da prepozna prikrivene aktivnosti usmjerene na destabilizaciju kritične infrastrukture i državnih institucija. U tom kontekstu, posebno zabrinjava činjenica da su hibridne operacije po svojoj prirodi teško uočljive i lako se mogu prikriti iza naizgled slučajnih događaja ili tehničkih kvarova.

Požar u trafostanici se lako može pripisati običnom tehničkom kvaru, pad IT sistema rutinskoj greški, a kvar željezničke signalizacije uobičajenim tehničkim problemima. Međutim, iza ovakvih događaja često može stajati ciljano djelovanje vanjskih aktera ili unutrašnjih saboterskih grupa. Upravo zato je od suštinske važnosti sposobnost državnih agencija da identificiraju obrasce

25 Zorić;, T. (2022, October 14). *Tvrtke nezaštićene, U BiH 4,7 Milijuna cyber Napada U MJESECU.* Bloomberg Adria. https://ba.bloombergadria.com/politika/vijesti/12080/tvrtke-nezasticene-u-bih-47-milijuna-cyber-napada-u-mjesecu/news

takvih incidenata i povežu ih u širu sliku koja bi mogla ukazati na koordiniranu neprijateljsku aktivnost.

Jasan dokaz nedovoljne spremnosti institucija Bosne i Hercegovine za prepoznavanje i pravovremeno reagiranje na ovakve prijetnje predstavljaju događaji iz septembra 2022. godine, kada je Parlamentarna skupština BiH[26] bila žrtva ozbiljnog *ransomware cyber* napada. Ovaj napad paralizirao je rad institucije na duže od dvije sedmice, tokom kojih je nekoliko hiljada zaposlenih bilo onemogućeno izvršavati svakodnevne radnih zadataka. Napad je potpuno blokirao pristup zvaničnoj internet stranici Parlamenta[27] i internom informacijskom sistemu, pri čemu su blokirani svi podaci pohranjeni na serverima. Istovremeno su pogođeni i sistemi Vijeća ministara BiH te nekolicina ministarstava, što je dovelo do djelimičnog kolapsa sistema e-uprave. Nikada nije objavljeno odakle je napad došao, niti je provedena transparentna i detaljna istraga koja bi javnosti pružila jasan uvid u motive, metode i potencijalne nalogodavce.[28] Nedostatak transparentnosti i jasne reakcije dodatno potiču percepciju ranjivosti države, te šalje poruku potencijalnim akterima da se slične aktivnosti mogu ponoviti bez značajnih posljedica. Imajući ovo u vidu, pitanje je koliko su agencije u BiH spremne prepoznati obrazac i povezati tačke koje ukazuju na neprijateljsku akciju.

Zapadne zemlje su se suočavale s ovim problemom, ali su ga prevazišle uspostavom koordinacijskih centara za hibridne prijetnje, gdje se informacije brzo razmjenjuju među sektorima. BiH zasad nema takvo operativno tijelo. Ako bi se desili simultani incidenti (npr. istovremeni nestanak struje u više gradova i požar u telekom čvorištu), postoji rizik da bi se posmatrali izolirano, umjesto kao potencijalno povezani čin. Također, širenje dezinformacija može zamagliti sliku. Ruski mediji ili lokalni akteri bi u času incidenta mogli plasirati lažne narrative tako što bi, primjerice, okrivili neku domaću grupu ili zapadne službe, što bi zbunilo javnost i otežalo vlastima komunikaciju tačnih informacija. Institucije BiH nemaju razrađenu strategiju krizne komunikacije za hibridne napade – što je dodatna slabost.

Najveća slabost BiH je nedostatak jedinstvenog, proaktivnog fronta pred prijetnjom koja je multidimenzionalna. Sve dok domaći politički akteri ne postignu konsenzus da je ruska ili neka druga hibridna prijetnja realna i ozbiljna, i dok se ne izgrade institucije i planovi sposobni djelovati brzo i usklađeno, BiH će ostati ranjiva. Ta ranjivost ne znači nužno da je napad neminovan, ali znači da bi njegove posljedice bile znatno teže. Prevazilaženje navedenih izazova ključno je da bi preporuke iz narednog poglavlja imale puni efekat.

---

26 Hina. (2022, September 23). *Hina: Bosnia's state IT systems disabled for two weeks now due to Cyber Attack.* N1. https://n1info.ba/english/news/hina-bosnias-state-it-systems-disabled-for-two-weeks-now-due-to-cyber-attack/

27 Sladojević, D. (2022, September 16). *Haker Izazvao Haos U Parlamentu Bih.* Nezavisne novine. https://www.nezavisne.com/novosti/bih/Haker-izazvao-haos-u-parlamentu-BiH/736003

28 Kurtic, A. (2022, October 20). *Bosnia remains silent on Hacker Attack on Parliament.* Balkan Insight. https://balkaninsight.com/2022/09/28/bosnia-remains-silent-on-hacker-attack-on-parliament/

8.
Preporuke za jačanje zaštite kritične infrastrukture od ruskih hibridnih prijetnji

1. *Usvojiti državnu strategiju* – to podrazumijeva pokretanje inicijative u Vijeću ministara BiH za izradu državne strategije za zaštitu kritične infrastrukture, koja će identificirati vitalne sektore, procijeniti rizike, uključujući hibridne prijetnje, te odrediti mjere zaštite. Strategija treba jasno definirati uloge svih nivoa vlasti u prevenciji i reakciji na sabotaže.

2. Paralelno, *ubrzati donošenje zakona o kritičnoj infrastrukturi BiH* koji će stvoriti obavezu za operatere i institucije da primjenjuju sigurnosne standarde, razmjenjuju informacije o incidentima i izrađuju vlastite planove zaštite. Taj zakon bi nadogradio postojeće propise o sigurnosti i civilnoj zaštiti, popunjavajući praznine. U zakon treba uvrstiti i odredbe o redovnom ažuriranju liste kritičnih objekata i obaveznoj procjeni rizika od sabotaže za svaki od njih.

3. Uspostaviti *međuresorni centar za odbranu od hibridnih prijetnji* pri Ministarstvu sigurnosti BiH, koji bi uključivao predstavnike OSA-e, SIPA-e, Ministarstva odbrane, entitetskih MUP-ova, te po potrebi eksperte iz sektora telekomunikacija, energetike, transporta i dr. Ovaj centar bi pratio indikatore mogućih hibridnih napada, objedinjavao informacije iz različitih izvora i koordinirao brzi odgovor. Služio bi i kao kontakt-tačka za saradnju s NATO/EU centrima za hibridne prijetnje. U praksi, takvo tijelo može izdavati rana upozorenja nadležnim institucijama. Naprimjer, može upozoriti elektroprivredu na povećan rizik sabotaže dalekovoda u određenoj regiji, a na osnovu obavještajnih saznanja. Također, centar bi sprovodio zajedničke analize nakon incidenata, kako bi utvrdio ima li elemenata hibridnog napada i predložio poboljšanja.

4. *Ojačati kapacitete obavještajnih i sigurnosnih agencija*. Uložiti u kadrovsko i tehničko jačanje OSA-e i policijskih agencija da mogu pratiti nove oblike prijetnji. To uključuje specijalizirane obuke analitičara za prepoznavanje hibridnih obrazaca; zapošljavanje IT stručnjaka za praćenje *dark web* komunikacija i šifriranih aplikacija (poput *Telegrama*) koje koriste saboterske mreže; nabavku opreme za tehničko osmatranje (dronovi, senzori, kamere) i forenziku napada. Rano prepoznavanje je ključno. Potrebno je ohrabriti zaštićene dojave unutar kritičnih preduzeća kako bi se sumnjive aktivnosti odmah prijavile. Već sada zapadne agencije dijele informacije o ruskim operativcima. Te podatke iskoristiti za praćenje i po potrebi protjerivanje sumnjivih osoba iz BiH. NATO je najavio povećanje razmjene informacija i nadzora infrastrukture zbog ruskih sabotaža. BiH mora biti spremna da te informacije apsorbira i djeluje po njima. Također, unutar policije oformiti specijalne timove za brzi odgovor na sabotaže, po uzoru na antiterorističke jedinice. Trebaju biti opremljene za deminiranje eksplozivnih naprava, sanaciju posljedica napada na npr. elektroenergetska postrojenja i osiguranje mjesta događaja radi istrage.

5. *Unaprijediti saradnju s EU i NATO u obavještajnom domenu i obukama*. BiH bi trebala proaktivno tražiti status posmatrača ili pridruženog člana u relevantnim evropskim inicijativama za borbu protiv hibridnih prijetnji, poput Evropskog centra za suzbijanje hibridnih prijetnji (Hybrid CoE) u Helsinkiju. Kroz takve forume, bh. stručnjaci mogu učiti iz tuđih iskustava i brže razmjenjivati informacije. Pojačati bilateralnu saradnju s državama koje su direktno iskusile ruske sabotaže – kao što su Poljska, Češka, Estonija, Litvanija – kroz sporazume o razmjeni operativnih podataka i stručnjaka.

6. Obuka kadra je prioritet te je potrebno *organizirati seminare i simulacijske vježbe scenarija sabotaže s NATO timovima*. EU i NATO već imaju razvijene trening module za zaštitu energetskih mreža, transporta i dr., a BiH treba iskoristiti te alate. Također, razmotriti traženje NATO savjetnika koji bi privremeno pomogli uspostavu sistema zaštite. U kontekstu EU integracija, prioritetno se uskladiti s Direktivom EU o otpornosti kritičnih subjekata iz 2022., koja zahtijeva od članica identifikaciju nacionalne kritične infrastrukture i mehanizme njene zaštite. Pripreme za provođenje te direktive, iako BiH nije članica, podigle bi spremnost institucija na EU nivo.

7. *Pojačati pravne mehanizme za brzu reakciju*. Izmijeniti krivično zakonodavstvo radi boljeg adresiranja sivih zona hibridnog ratovanja. Uvesti odredbe koje kažnjavaju učešće državljana BiH u sabotažnim ili obavještajnim aktivnostima za stranu silu, analogno postojećim kaznama za odlazak na strana ratišta. Također, olakšati proceduru protjerivanja stranih državljana koji predstavljaju prijetnju nacionalnoj sigurnosti – primjer ruskog agenta deportiranog iz BiH u Poljsku pokazuje da BiH može djelovati brzo, i tu praksu treba ozakoniti za buduće slučajeve. U okviru zakona o kritičnoj infrastrukturi ili posebnog propisa *predvidjeti mogućnost privremenog preuzimanja kontrole nad privatnim ili entitetskim resursima u vanrednoj situaciji*, to jest da državni organi mogu izdati obavezujuća uputstva operaterima mreža ili lokalnim vlastima radi odbrane od koordiniranog napada. Ovo je osjetljivo zbog decentralizacije, ali se može riješiti jasnim definiranjem uslova. Pored toga, *uspostaviti pravila za medije u krizama*, odnosno omogućiti da Regulatorna agencija za komunikacije (RAK) i druge nadležne institucije mogu brzo reagirati na širenje opasnih dezinformacija koje prate sabotaže, bilo demantijima ili privremenim blokiranjem izvora, kako bi se spriječila panika i manipulacija javnošću.

8. *Podizanje svijesti i uključivanje privatnog sektora*. Državne institucije trebaju pokrenuti program javne edukacije o važnosti zaštite kritične infrastrukture. To uključuje informativne kampanje, bez nepotrebnog širenja straha, koje građanima objašnjavaju da prijava sumnjivih aktivnosti – u blizini elektroenergetskih postrojenja, mostova i slično – može spriječiti katastrofu. Paralelno, *raditi s privrednim subjektima, posebno u energetici, transportu i telekomunikacijama na javno-privatnom partnerstvu za sigurnost*. To znači održavanje redovnih sastanaka sa sigurnosnim službama, izvođenje zajedničkih simulacija napada na njihove objekte, provjeru planova kontinuiteta poslovanja u slučaju sabotaže. Privatni sektor treba ohrabriti da ulaže u vlastite sigurnosne sisteme, uz mogućnost subvencija za takve investicije, jer time rasterećuje državu.

Implementacija ovih preporuka zahtijeva političku volju na najvišem nivou i razumijevanje da se radi o ulaganju u sveobuhvatnu sigurnost i budućnost. Donosioci odluka trebaju ove mjere posmatrati kao paket za jačanje otpornosti koji će, čak i ako se najgori scenariji nikada ne ostvare, donijeti korist – kroz modernizaciju, bolje upravljanje krizama i snažnije međunarodne veze.

9. Zaključak

Bosna i Hercegovina se nalazi u složenom sigurnosnom okruženju u kojem se klasične prijetnje prepliću s nekonvencionalnim, hibridnim izazovima. Zaštita kritične infrastrukture postala je preduslov ekonomske i političke stabilnosti svake države, jer moderne društvene funkcije mogu biti paralizirane jednim uspješnim aktom sabotaže. Za BiH posljedice strateške neaktivnosti u ovom polju mogu biti posebno teške. Ignoriranje znakova upozorenja – poput otkrivanja ruskih mreža za subverziju u regionu i učestalih sabotaža širom Evrope – moglo bi dovesti do toga da BiH bude zatečena i nespremna u trenutku krize. Time bi bila ugrožena ne samo sigurnost građana i imovine, već i međunarodni položaj BiH. S druge strane, jačanje institucionalnog odgovora na ruske hibridne prijetnje donosi višestruke koristi. Proaktivnim djelovanjem, počevši od usvajanja strategija, jačanja kapaciteta i saradnje sa saveznicima, BiH može umanjiti rizik od sabotaža i ujedno se bolje pripremiti i za druge vrste kriza, poput prirodne nepogode, tehnološke havarije, terorizma. Vrijeme je ključni faktor. BiH više nema luksuz da odgađa pripreme. Svaki mjesec bez strategije, zakona i obuke povećava prostor za one koji bi iskoristili rupe u sistemu. Nasuprot tome, pravovremena akcija – prije nego se desi ozbiljan incident – može osujetiti planove onih koji vrebaju.

BIRN
BALKAN INVESTIGATIVE REPORTING NETWORK
BOSNIA & HERZEGOVINA

Detektor