

ZBORNIK RADOVA

III. Naučno-stručni skup sa međunarodnim učešćem:

„ZAŠTITA KRITIČNE I KRITIČNE INFORMACIONE INFRASTRUKTURE – TRENUTNO STANJE I OBAVEZE DRŽAVA PREMA EU DIREKTIVI O OZNAČAVANJU I ZAŠTITI KI IZ 2008. GODINE I NIS1 I NIS2 DIREKTIVAMA IZ 2016. GODINE I 2022. GODINE"

Banja Luka, 12. Novembar 2022. godine

Zaštita kritične i kritične informacione infrastrukture – trenutno stanje i obaveze država prema EU Direktivi o označavanju i zaštiti KI iz 2008. godine i NIS1 i NIS2 Direktivama iz 2016. godine i 2022. godine

Organizacioni i programski odbor konferencije:
prof. dr Ljubinko Mitrović, Istraživački centar Banja Luka
doc. dr Dejan Kojić, Univerzitet PIM Banja Luka
Mr Dragana Kosić, Sector Security Banja Luka

Izdavač:
Istraživački centar Banja Luka
Aleja Svetog Save 7A, 78000 Banja Luka, Republika Srpska – BiH

Za izdavača:
doc. dr Gojko Pavlović

Glavna i odgovorna urednica:
doc. dr Nikolina Grbić Pavlović

Recenzentski odbor:
Akademik prof. dr Miodrag Simović (BiH), prof. dr Tunjica Petrašević (HRV), prof. dr Zoran Pavlović (SRB), prof. dr Velimir Rakočević (CG), prof. dr László István Gál (HU), prof. dr Marjan Gjurovski (MKD), doc. dr Damjan Podparić (SVN), doc. dr Armin Kržalić (BiH)

Prevod i lektura:
Jelena Gavranović

Kompjuterska priprema:
Aleksandar Jorgić

Štampa:
Markos Design & Studio, Banja Luka

Za štampariju:
Igor Jakovljević

Tiraž: *50 primjeraka*

ISBN Republika Srpska:

SADRŽAJ / CONTENT

Doc. dr Gojko Pavlović: DIREKTIVE EVROPSKE UNIJE U OBLASTI ZAŠTITE KRITIČNE I KRITIČNE INFORMACIONE INFRASTRUKTURE / EUROPEAN UNION DIRECTIVES ON CRITICAL AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION ***str. 1 – 10.***

Prof. dr Velimir Rakočević, Dr Aleksandra Jovanović: RANJIVOST SISTEMA ZAŠTITE KRITIČNE INFORMACIONE INFRASTRUKTURE U CRNOJ GORI I POSLEDICE NAPADA NA KOMPLETNU INFORMATIČKO-TEHNOLOŠKU MREŽU U 2022. GODINI / THE VULNERABILITY OF THE CRITICAL INFORMATION INFRASTRUCTURE PROTECTION SYSTEM IN MONTENEGRO AND THE CONSEQUENCES OF AN ATTACK ON THE COMPLETE IT AND TECHNOLOGY NETWORK IN 2022 ***str. 11 – 22.***

Prof. dr Tatjana Gerginova: PROTECTION OF CRITICAL INFRASTRUCTURE FROM HYBRID THREATS / ZAŠTITA KRITIČNE INFRASTRUKTURE OD HIBRIDNIH PRIJETNJI ***pp. 23 – 36.***

Prof. dr Ljubinko Mitrović, Vanja Mitrović: PREVOZ OPASNIH MATERIJA KAO ELEMENT KRITIČNE INFRASTRUKTURE / TRANSPORT OF HAZARDOUS MATERIALS AS AN ELEMENT OF CRITICAL INFRASTRUCTURE ***pp. 37 – 53.***

Mr Dragana Kosić, Dr Željko Zorić: PRIVATNA BEZBJEDNOST U ZAŠTITI KRITIČNE INFRASTRUKTURE REPUBLIKE SRPSKE / PRIVATE SECURITY IN PROTECTION OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SRPSKA ***pp. 54 – 63.***

Dr Gojko Šetka, Aleksandar Đekić, MA: KOMPARATIVNI PRIKAZ ULOGE POLICIJE U ZAŠTITI KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ I SRBIJI / COMPARATIVE OVERVIEW OF THE ROLE OF THE POLICE IN THE PROTECTION OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SRPSKA AND REPUBLIC OF SERBIA ***pp. 64 – 79.***

Márton András: PROMJENE U MAĐARSKOJ STRUKTURI KIBERNETIČKE OBRANE TOKOM PROVEDBE PROPISA EVROPSKE UNIJE / CHANGES IN THE HUNGARIAN CYBER DEFENSE STRUCTURE DURING THE IMPLEMENTATION OF EUROPEAN UNION REGULATIONS ***pp. 80 – 90.***

Uvodno izlaganje

DIREKTIVE EVROPSKE UNIJE U OBLASTI ZAŠTITE KRITIČNE INFRASTRUKTURE I KRITIČNE INFORMACIONE INFRASTRUKTURE[1]

Doc. dr Gojko Pavlović[2]
Pravni fakultet, Univerzitet PIM Banja Luka

DIREKTIVA O UTVRĐIVANJU I OZNAČAVANJU EVROPSKE KRITIČNE INFRASTUKTURE I PROCJENI POTREBE POBOLJŠANJA NJENE ZAŠTITE IZ 2008. GODINE

Neposredno sa usvajanjem Evropske strategije bezbjednosti iz 2003.g., u aprilu 2004. godine Evropski savjet je pokrenuo inicijativu za izradu cjelovite strategije kojom bi se zaštitila kritična infrastruktura. Kao odgovor na ovaj zahtjev Evropskog savjeta, Evropska komisija je 20. septembra iste godine usvojila *Komunikaciju o zaštiti kritične infrastrukture u borbi protiv terorizma*, u kojoj su izneseni prijedlozi koji bi evropi omogućili adekvatnije sprečavanje terorističkih napada kojima su direktno pogođeni objekti ili subjekti kritične infrastrukture. Ovim dokumentom se predviđalo unapređenje reakcije na takve situacije, te spremnost da se na njih odgovori. Takođe, Evropska komisija je 2005. godine usvojila *Zelenu knjigu o evropskom programu zaštite kritične infrastrukture*, u kojoj se nude moguća rješenja za uspostavljanje programa i informacione mreže za uzbunjivanje radi zaštite kritične infrastrukture. Iste godine je Savjet za pravosuđe i unutrašnje poslove zatražio od Evropske komisije izradu prijedloga *Evropskog programa zaštite kritične infrastrukture* kojim su se u obzir uzele sve opasnosti, pri čemu je primat dat suprotstavljanju terorističkim prijetnjama. Tako je Evropski savjet 2007. godine usvojio zaključke o ovom programu, a kojima se ponovno naglašava da je konačna

[1] Rad predstavlja nastavak istraživanja autora na naslovljenu temu i isti je uz neznatne izmjene izložen na Naučno-stručnoj konferenciji "*Zaštita kritične infrastrukture – obaveze država i mogućnosti privatnog sektora bezbjednosti"* i objavljen u istoimenom Zborniku radova sa navedenog skupa. Vidjeti: Gojko Pavlović, Direktive Evropske unije u oblasti zaštite kritične infrastrukture i kritične informacione infrastrukture – uvodni referat, Zbornik radova "*Zaštita kritične infrastrukture – obaveze država i mogućnosti privatnog sektora bezbjednosti"*, Istraživački centar Banja Luka, Sector Security, Banja Luka, 2021, str. 1-6.

[2] Docent na Katedri za međunarodno javno pravo, Pravni fakultet Univerzitet PIM Banja Luka.

odgovornost za upravljanje rješenjima za zaštitu kritičnih infrastruktura na državama članicama.

Konačno, Savjet donosi prvi dokument čiji je osnovni cilj upravo utvrđivanje i označavanje kritične infrastrukture i procjene njihove zaštite, a to je *Direktiva o utvrđivanju i označavanju evropske kritične infrastukture i procjeni potrebe poboljšanja njene zaštite iz 2008.godine*.[3]

Prema članu 2. Direktive „kritična infrastruktura je imovina, sistem ili njihov dio koji se nalazi u državama članicama i neophodan je za održavanje vitalnih društvenih funkcija, zdravlja, bezbjednosti, zaštite, ekonomije i socijalne dobrobiti ljudi, a čiji bi poremećaj rada ili čije bi uništenje, kao posljedica neuspjelog održavanja tih funkcija, moglo imati znatan učinak u državi članici“. S druge strane, definisano je i pitanje evropske kritične infrastrukture – tzv. EKI. EKI je kritična infrastruktura koja se nalazi u državama članicama, a čiji bi poremećaj u radu ili čije bi uništenje imalo znatan učinak na najmanje dvije države članice.

Direktivom Evropske unije data je i definicija zaštite kritične infrastrukture. Naime, pod zaštitom podrazumijevaju se sve djelatnosti koje imaju za cilj osigurati funkcionalnost, neprekidnost i cjelovitost kritičnih infrastruktura kako bi se odvratila, ublažila ili neutralisala prijetnja, rizik ili slabost.

Utvrđivanje kritične infrastrukture podrazumijeva da svaka država članica utvrđuje potencijalne EKI-je koji ispunjavaju međusektorska i sektorska mjerila, a koji odgovaraju definicijama „kritične infrastrukture“ i „evropske kritične infrastrukture“.

Međusektorska mjerila obuhvataju: a) broj žrtava (koji se procjenjuje s obzirom na mogući broj mrtvih i ranjenih); b) privredne posljedice (koje se procjenjuju s obzirom na značaj privrednog gubitka i/ili srozavanje kakvoće proizvoda ili usluga; uključujući mogući uticaj na okolinu) i v) uticaj na javnost (koji se procjenjuje s obzirom na uticaj na povjerenje javnosti, tjelesne patnje i remećenje svakodnevnog života; uključujući gubitak osnovnih usluga) (član 2. stav 3. Direktive).

Svakako da se ova mjerila moraju prilagoditi karakteristikama pojedinih sektora eki-ja. ukoliko na nivou unije ili u državama članicama već postoje određene sektorske mjere, a koje se već bave zaštitom kritične infrastukture i kojima se postižu pozitivni rezultati u toj oblasti, trebalo bi ih i dalje nastaviti sprovoditi, a direktivom ih samo dopuniti.

[3] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L, pp. 345-375, 23.12.2008.

Svaka država članica obavještava druge države članice čiji EKI bi mogao imati znatan nepovoljan učinak o njegovom postojanju i o njegovim razlozima za njegovo označavanje potencijalnim EKI-jem.

Država članica koja smatra da bi potencijalni eki na nju mogao imati znatan nepovoljni učinak, ali ga država članica na čijem se državnom području nalazi nije utvrdila kao takvog, može obavijestiti komisiju o svojoj želji da se uključi u bilateralne i/ili multilateralne rasprave o tom pitanju.

Važniji ciljevi direktive jesu uspostavljanje *bezbjednosnih planova (član 5. Direktive)* i postavljanje *službenika za bezbjednost (član 6. Direktive).* Bezbjednosnim planovima utvrđuje se važna imovina, zatim vrši procjena rizika, te u odnosu na prethodno utvrđuju i definišu prioriteti za primjenu adekvatnih mjera i postupaka za zaštitu. Svaka država članica ocjenjuje da li svaki označeni EKI koji se nalazi na njenom području ima svoj plan i da li postoje mjere kojima se već djeluje po pitanjima koja sačinjavaju navedeni plan. Ova pitanja utvrđena su u prilogu ii direktive.

Datim planom, najprije, potrebno je utvrditi imovinu kritične infrastrukture i bezbjednosna rješenja koja postoje ili se primijenjuju radi njihove zaštite.

Prema odredbama priloga iz direktive postupak izrade bezbjednosnog plana obuhvata najmanje: utvrđivanje važne imovine, zatim analizu rizika na osnovu glavnih prijetnji imovini, te u odnosu na prethodno obuhvata obavezu utvrđivanja i odabira prioriteta za primjenu adekvatnih mjera i postupaka za zaštitu. ove mjere i postupci mogu biti trajne bezbjednosne mjere kojima se utvrđuju neizostavna bezbjednosna ulaganja i sredstva za koja je važno da su trajno angažovana.

Na primjer, tehničke mjere - postavljanje sredstava za nadzor, kontrolu pristupa, zaštitu i sprečavanje; organizacione mjere - postupci za uzbunjivanje i upravljanje krizama; mjere za nadzor i provjeru; komunikaciju; podizanje svijesti i osposobljavanje, te bezbjednost informacionih sistema) i mogu biti privremene bezbjednosne mjere koje se koriste u zavisnosti od različitih stepena rizika i prijetnji.

Ukoliko država članica ustanovi da ne postoji ovakav bezbjednosni plan ili da nisu pripremljene adekvatne mjere za zaštitu, nastojaće da se osigura donošenje bezbjednosnog plana zaštite prema navedenim pitanjima iz priloga ii direktive.

Takođe, svaka država članica osigurava redovno preispitivanje plana i mjera u roku od jedne godine nakon što je kritična infrastruktura označena kao EKI taj se rok pod posebnim okolnostima može produžiti uz saglasnost nadležnog tijela države članice i uz obaviještenje Komisije.

Važna obaveza po direktivi jeste i određivanje *službenika za bezbjednost i vezu* kako bi se olakšala saradnja i komunikacija sa državnim

tijelima za zaštitu kritične infrastrukture. službenik za bezbjednost i vezu zadužen je za bezbjednost i djeluje kao kontakt tačka za bezbjednosna pitanja između vlasnika/operatera eki-ja i odgovarajućeg tijela države članice. takođe, svaka država članica uspostavlja odgovarajući mehanizam za komunikaciju između odgovarajućeg državnog tijela i službenika za bezbjednost, kao i vezu radi razmjene odgovarajućih informacija o utvrđenim rizicima i prijetnjama u odnosu na dotični EKI.

Kao važna karakteristika, koja bi svakako podrazumijevala dodatnu efikasnost u radu na zaštiti kritične infrastrukture, jeste ta da se u svakoj državi članici imenuje kontakt tačka koja bi koordinisala pitanjima koja su u vezi sa zaštitom evropske kritične infrastrukture u zemlji, ali i sa drugim državama članicama i Evropskom komisijom.

Direktivom je regulisana i zaštita podataka o zaštiti EKI-ja, koja podrazumijeva da svaka osoba, koja raspolaže informacijama u skladu s ovom direktivom, prolazi odgovarajuće bezbjednosne provjere. države članice, komisija i odgovarajuća nadzorna tijela osiguravaju da se informacije o zaštiti evropske kritične infrastrukture koje se podnose državama članicama ili komisiji ne koriste ni u koju drugu svrhu osim zaštite kritičnih infrastruktura. Ova pravila se odnose i na nepisane informacije koje se razmjenjuju na sastancima na kojima se raspravlja o osjetljivim temama.

Direktiva EU 2008/114/EC direktno se usmjerava na zaštitu kritične infrastrukture u sektorima energije i prevoza, ali se ne ograničava samo na ove sektore te se ističe da se mogu odrediti kritične infrastrukture i iz drugih sektora a daje se prednost informaciono komunikacionim tehnologija.
Iz ova dva sektora posebno su kao podsektori navedeni

SEKTOR	PODSEKTOR	
I. Energetika	1. Električna energija	Infrastruktura i objekti za proizvodnju i prenos električne energije vezano za snabdijevanje električnom energijom
	2. Nafta	Proizvodnja, rafinisanje, prerada, skladištenje i prenos nafte naftovodima
	3. Gas	Proizvodnja, rafinisanje, prerada, skladištenje i prenos gasa gasovodima
II. Prevoz	4. Drumski prevoz 5. Željeznički prevoz 6. Vazduhoplovni prevoz 7. Pevoz kopnenim plovnim putovima 8. Prekookeanski prevoz i pomorski prevoz na kratkim udaljenostima i lukama	

Definisanje i određivanje kritičnih infrastruktura, naročito izrada metodologije procjenjivanja rizika i njihove ugroženosti, u isključivoj je nadležnosti država članica Evropske unije.

DIREKTIVA O MJERAMA ZA VISOKI ZAJEDNIČKI NIVO BEZBJEDNOSTI MREŽNIH I INFORMACIONIH SISTEMA U EU – NIS 1 DIREKTIVA

Direktiva o mjerama za visoki zajednički nivo bezbjednosti mrežnih i informacionih sistema u EU - NIS Direktiva, je usvojena 2016. godine, a države članice su imale rok do 09. maja 2018. godine da transponuju odredbe direktive u nacionalna zakonodavstva, kao i da do 09. novembra 2018. godine identifikuju operatore sistema koji pružaju usluge od posebnog značaja[4].

U ovoj Direktivi se pozivaju sve države članice da propišu osnovne standarde bezbjednosti nacionalnih mrežnih i informacionih sistema, a posebno da: usvoje strategiju za mrežnu i informacionu bezbjednost (NIS); usvoje kooperacioni plan za NIS; uspostave kompetentni autoritet za NIS i uspostave tim nadležan za odgovore na bezbjednosne računarske incidente (*Computer Security Incident Response Team - CSIRT).*

Prema tome, NIS Direktivom najprije se propisuju obaveze državama članicama u oblasti uspostavljanja strateškog i pravnog okvira.

U tu svrhu, državama članicama je savjetovano da izrade nacionalne strategije koje će uključiti sve relevantne dimenzije društva i privrede.

Direktivom se takođe određuje i da bezbjednosne mjere treba da budu zasnovane na principu upravljanja na osnovu procjene rizika, što je kultura koja treba da bude razvijena kroz odgovarajuće regulatorne okvire, kao i na osnovu postojećih praksi u različitim branšama.

U pogledu kritične informacione infrastrukture, NIS Direktiva propisuje da su države članice odgovorne za utvrđivanje kritične infrastrukture u oblasti koju Direktiva uređuje. NIS Direktiva u stvari prepoznaje dvije vrste subjekata: operatore IKT sistema koji pružaju usluge od posebnog značaja (*eng. operators of essential services*) i pružaoce digitalnih usluga (*eng. digital services providers*).

Aneksi II i III sadrže spisak usluga koje spadaju u prvu grupu, na osnovu kojeg se može utvrditi da li određeni pružalac usluga spada u pružaoce usluga koje su posebno značajne za održavanje ključnih društvenih i ekonomskih

[4] Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union L 194/1.

aktivnosti (usluge od posebnog značaja). Spisak usluga zapravo izjednačava ovu grupu sa operatorima kritične infrastrukture u koju spada sljedeće: Energetski sektor (struja, nafta i gas); Sektor transporta (vazdušni, željeznički, vodni i drumski transport); Bankarski sektor; Infrastrukture finansijskog tržišta; Zdravstveni sektor (zdravstvene ustanove, uključujući bolnice i privatne klinike); Snabdijevanje i distribucija vode za piće i Digitalna infrastruktura (IXP, pružaoci usluga DNS i registri domena TDL) (Aneks II). Onlajn tržište; Onlajn pretraživač i Usluga računarstva u oblaku (*eng. cloud computing*) (Aneks III).

Države članice su dužne da redovno, a najmanje jednom u dvije godine, ažuriraju spisak identifikovanih pružalaca usluga od posebnog značaja na svojoj teritoriji, kao i metodologiju za identifikaciju i klasifikaciju navedenih pružalaca usluga po značaju, kao i da o tome obavijeste Evropsku komisiju.

Kompetentni autoritet je najznačajnija institucija sa obavezama da prati primjenu NIS Direktive na nacionalnom nivou, da sarađuje sa nacionalnim kompetentnim autoritetima drugih država članica, sa odgovarajućim bezbjednosnim službama i autoritetima za zaštitu podataka u svojoj zemlji i da prima i postupa po prijemu obavještenja o incidentima kod javne administracije i javnih operatora telekomunikacionih i informacionih usluga.

Pored kompetentnog autoriteta, predviđeno je da svaka država članica formira i sljedeće tijela:

- Autoritet za informacionu bezbjednost (IAA);
- Autoritet za tempest (TA);
- Autoritet za odobravanje kriptografskih rješenja (CAA) i
- Autoritet za distribuciju kriptografskih materijala (CDA).

Direktiva o mrežnoj i informacionoj bezbjednosti (NIS 1) je prvi dio zakona o sajber bezbjednosti širom EU, a njen specifični cilj je bio postizanje visokog zajedničkog nivoa sajber bezbjednosti u svim državama članicama. Međutim, iako je povećala kapacitete za sajber bezbjednost država članica, njena primjena se pokazala prilično teškom, a što je za rezultat imalo fragmentaciju na različitim nivoima na unutrašnjem tržištu.

NIS 2 DIREKTIVA - VISOK ZAJEDNIČKI NIVO SAJBER BEZBEJDNOSTI U EU

Kako bi odgovorila na rastuće prijetnje digitalizacije i porast sajber-napada, Komisija je podnijela prijedlog za zamjenu NIS 1 direktive da bi na taj način ojačala bezbjednosne zahtjeve, pozabavila se bezbjednošcću lanaca snabdjevanja, pojednostavila obaveze izvještavanja i uvela strože nadzorne

mjere i strožije zahtjeve za sprovođenje, uključujucći usklađene sankcije širom EU. U stvari, predloženo je proširenje djelokruga koji pokriva NIS 2.

U okviru Evropskog parlamenta, zadatak je dodjeljen Odboru za industriju, istraživanje i energetiku, a koji je usvojio svoj izvještaj 28. oktobra 2021. godine, nakon čega su započeli međuinstitucionalni pregovori. Sa svoje strane, Savjet je usaglasio stav 3. decembra 2021. godine, dok su kozakonodavci postigli privremeni dogovor o tekstu 13. maja 2022. godine. Politički sporazum je formalno usvojen u Parlamentu, a potom i u Savjetu u novembru 2022. godine i stupio je na snagu 16. januara 2023. godine, a države članice sada imaju 21 mjesec, odnosno do 17. oktobra 2024. godine da prenesu dogovorene mjere u nacionalno zakonodavstvo[5].

Direktiva NIS 2 uvodi pravilo ograničenja veličine za određivanje subjekata koji ispunjavaju kriterijume da bi se kvalifikovali kao operateri bitnih usluga i važnih subjekata. To znači da bi svi srednji i veliki subjekti koji posluju u okviru sektora obuhvaćenih direktivom ili koji pružaju usluge obuhvaćene direktivom, spadali u njen delokrug. Takvi subjekti bi bili pod jurisdikcijom države članice u kojoj su osnovani, a ne države članice u kojoj pružaju svoje usluge.

NIS 2 postavlja tri opšta cilja:

Prvi - povećati nivo sajber otpornosti - preduzeća koja posluju u Evropskoj uniji u svim relevantnim sektorima, postavljanjem pravila koja osiguravaju da svi javni i privatni subjekti na unutrašnjem tržištu, koji ispunjavaju važne funkcije za privredu i od društva u cjelini se zahtijeva da preduzmu adekvatne mjere sajber bezbjednosti. Na primjer, značajno se proširuje djelokrug trenutne Direktive dodavanjem novih sektora kao što su telekomunikacije, platforme društvenih medija i javna uprava. Njime se utvrđuje da bi svi srednji i veliki subjekti aktivni u sektorima obuhvaćenim NIS 2 okvirom stoga morali da se pridržavaju bezbjednosnih pravila;

Drugi - smanjiti nedosljednosti u otpornosti na unutrašnjem tržištu u sektorima koji su već obuhvaćeni direktivom.

NIS 2 uključuje listu od sedam ključnih elemenata koje sve kompanije moraju da adresiraju ili implementiraju kao dio mjera koje preduzimaju, uključujući reagovanje na incidente, bezbjednost lanca snabdjevanja, šifrovanje i otkrivanje ranjivosti. Osim toga, predviđa se dvostepeni pristup izvještavanju o incidentima. Pogođene kompanije imaju rok od 24 sata od kada prvi put saznaju za incident da podnesu početni izvještaj, nakon čega slijedi konačni izvještaj najkasnije mjesec dana kasnije.

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Što se tiče sankcija utvrđuje se minimalna lista administrativnih sankcija kada god subjekti prekrše pravila u vezi sa upravljanjem rizikom od sajber bezbjednosti ili svoje obaveze izvještavanja propisane Direktivom o NIS. Ove sankcije obuhvataju obavezujuća uputstva, nalog za sprovođenje preporuka bezbjednosne revizije, nalog za usklađivanje bezbjednosnih mjera sa zahtjevima NIS-a i administrativne kazne (do 10 miliona evra ili 2% ukupnog prometa entiteta u svijetu, u zavisnosti od toga koji je viši).

Treći - poboljšati nivo zajedničke situacione svjesti i kolektivne sposobnosti za pripremu i reagovanje, a) preduzimanjem mjera za povećanje nivoa povjerenja između nadležnih organa; b) dijeljenjem više informacija; i v) utvrđivanje pravila i procedura u slučaju incidenata ili krize velikih razmjera.

Revidiranom Direktivom se uspostavlja upravljanje krizama u EU okvir, koji zahtijeva od država članica da usvoje plan i odrede nacionalne nadležne organe odgovorne za učešće u odgovoru na incidente i krize u sajber bezbjednosti na nivou EU. Direktivom se uspostavlja mreža organizacija za vezu između EU i sajber kriza (e*u-ciclone*) kako bi se podržalo koordinisano upravljanje incidentima sajber bezbjednosti širom EU, kao i da bi se osigurala redovna razmjena informacija.

Od država članica se i dalje zahtijeva da usvoje nacionalnu strategiju sajber bezbjednosti i da odrede jedan ili više nacionalnih nadležnih organa koji će nadgledati poštovanje direktive; kao i da odrede *CSIRT*-ove da obrađuju obavještenja o incidentima i da odrede jedinstvene kontaktne tačke (SPOC) da djeluju kao tačka za vezu sa drugim državama članicama.

Kako je savjet zahtijevao, direktiva se neće primjenjivati na subjekte koji obavljaju djelatnost u oblastima kao što su odbrana i nacionalna bezbjednost, javna bezbjednost, sprovođenje zakona i pravosuđe. Parlamenti i centralne banke su takođe isključeni iz djelokruga.

Međutim, prema zahtjevima skupštine, primenjivaće se na subjekte javne uprave na centralnom i regionalnom nivou. Pored toga, države članice mogu takođe odlučiti da se to odnosi na subjekte na lokalnom nivou.

ZAKLJUČNA RAZMATRANJA

Imajući u vidu značaj usklađivanja domaćih pravnih propisa sa propisima Evropske unije, sa aspekta zaštite kritične i kritične informacione infrastukture neophodno je najprije na normativnom, a potom i na institucionalnom nivou, u skladu sa najboljim uporednim rješenjima pristupiti izradi strateških dokumenata u Republici Srpskoj i na drugom nivoima vlasti u BiH, kao i akcionih planova, te donošenju adekvatnih bezbjednosnih planova

kojima bi se detaljno regulisalo pitanje zaštite kritične i kritične informacione infrastrukture.

LITERATURA

1. Gojko Pavlović, Direktive Evropske unije u oblasti zaštite kritične infrastrukture i kritične informacione infrastrukture – uvodni referat, Zbornik radova "*Zaštita kritične infrastrukture – obaveze država i mogućnosti privatnog sektora bezbjednosti*, Istraživački centar Banja Luka, Sector Security, Banja Luka, 2021, str. 1-6.
2. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union L, pp. 345-375, 23.12.2008.
3. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning the measures for a high common level of security of network and information systems across the Union. 19.7.2016. Official Journal of the European Union L 194/1.
4. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

EUROPEAN UNION DIRECTIVES ON CRITICAL AND CRITICAL INFORMATION INFRASTRUCTURE PROTECTION[6]

Asst. prof. Gojko Pavlović, PhD[7]
Faculty of Law, PIM University Banja Luka

CONCLUDING REMARKS

Bearing in mind the importance of harmonizing domestic legal regulations with the European Union regulations in terms of protection of critical and critical information infrastructure, it is necessary to start drafting strategic documents in the Republic of Srpska and other levels of government in Bosnia and Herzegovina first at the normative, and then at the institutional level in accordance with the best comparative solutions, as well as action plans, and appropriate security plans that would regulate in detail the protection of critical and critical information infrastructure.

[6] The paper is a follow-up of the author's research on the topic and it was presented, with minor changes, at the Scientific and Professional Conference "*Protection of Critical Infrastructure - Obligation of States and Opportunities of the Private Security Sector*" and published in the Proceedings of the same conference. See: Gojko Pavlović, Directives of the European Union in the field of protection of critical infrastructure and critical information infrastructure - introductory report, Proceedings "*Protection of critical infrastructure - obligations of states and opportunities of the private security sector*", Research Center Banja Luka, Sector Security, Banja Luka, 2021, p. 1-6

[7] Ass.prof. at the Department of Public International Law, Faculty of Law, University of PIM Banja Luka

Originalni naučni članak

RANJIVOST SISTEMA ZAŠTITE KRITIČNE INFORMACIONE INFRASTRUKTURE U CRNOJ GORI I POSLEDICE NAPADA NA KOMPLETNU INFORMATIČKO-TEHNOLOŠKU MREŽU U 2022. GODINI

Prof. dr Velimir Rakočević[1]
Pravni fakultet Univerziteta Crne Gore

Dr Aleksandra Jovanović[2]
Više državno tužilaštvo, Podgorica

Apstrakt: U cilju usklađivanja nacionalnog zakonodavstva u oblasti kritične infrastrukture sa standardima Evropske unije, Crna Gora je u decembru 2019. godine donijela Zakon o određivanju i zaštiti kritične infrastrukture kojim je definisala sisteme, mreže i objekte kritične infrastrukture i odredila aktivnosti i mjere njihove zaštite. Usvajanje ovog dokumenta predstavljalo je solidnu normativnu osnovu koju je bilo neophodno implementirati u optimalnom vremenskom periodu. Do toga očigledno nije došlo budući da su sajber napadi na informacionu mrežu Vlade CG počeli sredinom avgusta tekuće godine i trajali više sedmica a saniranje posledica trajaće zasigurno duži vremenski period. Hakerski napadi onemogućili su pristup sajtovima i mejlovima većeg broja ministarstava kao i drugim važnim državnim organima kao što su sudovi, tužilaštva, Uprava prihoda i carina, Uprava za nekretnine i slično. U vrijeme pisanja ovoga rada učinioci ovih krivičnih djela nijesu identifikovani a država čini sve da prevaziđe posledice sajber napada na državne institucije. Predmet istraživanja u ovom radu je analiza kompatibilnosti crnogorskog zakonodavstva sa relevantim aktima EU o ovoj oblasti, kao i eksplanacija inkriminacija protiv bezbjednosti računarskih podataka i drugih krivičnih djela kod kojih su objekti napada informaciono komunikacione tehnologije, sa posebnim osvrtom na metodiku otkrivanja i dokazivanja ovih delikata.

Ključne riječi: kritična informaciona infrastruktura, sajber napadi, kompjuterski kriminalitet.

[1] Prof. dr Velimir Rakočević, redovni profesor Pravnog fakulteta Univerziteta Crne Gore, e-mail: *veljorakocevic@yahoo.com*

[2] Dr Aleksandra Jovanović, savjetnica u Višem državnom tužilaštvu, Podgorica, e-mail: *aleksandrajovanovic417@gmail.com*

UVOD

Brojni izazovi sa kojima se svijet suočava u XXI vijeku ukazali su na neophodnost poklanjanja mnogo više pažnje na ključne kapacitete svake države čije bi ugrožavanje neminovno dovelo do paralize obavljanja vitalnih državnih funkcija. U najvažnije potencijale države bez sumnje spada kritična infrasturuktura koja osigurava redovno funkcionisanje sistema i servisiranje potreba građana. Svaki napad na ovo državno dobro dovodi do brojnih materijalnih i kombinovanih posledica, zbog čega je država obaveza da kreira optimalan normativni okvir za efikasno suzbijanje i prevenciju napada na kritičnu infrasturukturu u skladu sa međunarodnim standardima.

Kako ističu pojedini autori nakon razornih terorističkih napada na SAD ovo državno dobro postalo je esencijalni segment bezbjednosti države i spada u najviše prioritete zaštite.[3] Generalno posmatrano ovaj termin se odnosi na sve ono što je potrebno za neometano odvijanje bazičnih društvenih funkcija pri čemu je fokus na imovinu u širem smislu. Radi se o onim sredstvima koja obezbjeđuju egzistiranje više posebnih segmenata od političkih do ekonomskih u okviru jedinstvenog sistema a svaki prekid u obavljanju fuinkcija dovodi do nenadoknadivih gubitaka. Jedan od najvažnijih segmenata kritične infrastutukture su informaciono komunikacione tehnologije i njihovo stavljanje van funkcije ugrožava najvažnije potencijale svake države.

Ukoliko analiziramo determinaciju kritične infrastutruktire u aktima EU vidjećemo da je sadržaj definicije šire postavljen i obuhvata imovinu i sistem pojedine države bez koga nema odvijanja bitnih funkcija društva. Tu se u prvom redu misli na bezbjednost, ekonomiju, zdravstvo i slično. S pravom se ukazuje na faktor međuzavisnosti kao unutar pojednih nacionalnih sektora tako i na prelivanje negativnih implikacija sa jedne države na drugu.[4]

ZAŠTITA KRITIČNE INFRASTRUKTURE U CRNOJ GORI I USKLAĐENOST SA STANDARDIMA EU

Crna Gora je u decembru 2019. godine donijela Zakon o određivanju i zaštiti kritične infrastrukture[5] koji je napisan u skladu sa međunarodnim ugovorima i standardima EU. U članu 2 ovog dokumenta kritična infrastruktura definisana je na način da obuhvata:“ siisteme, mreže i objekte, odnosno njihove

[3] Škero M.Ateljević V. (2015). Zaštita kritične infrastrukture i osnovni elementi usklađivanja sa Direktivom SE 2008/114ES, Vojno delo,3/2015. str.192.

[4] Council Directive 2008/114/EC, Official Journal of the European Union pp.345-357.

[5] Zakon o određivanju i zaštiti kritične infrastrukture, Službeni list CG br. 72/2019 od 26.12.2019. koji je stupio na snagu 3.1.2020.

djelove koji se nalaze na teritoriji CG čiji prekid funkcionisanja, kao i prekid isporuka roba ili usluga preko tih sistema, mreža i objekata može imati ozbiljne poledice po nacionalnu bezbjednost, život i zdravlje ljjudi, imovinu i slično.“[6] Naznačena determinacija kritične infrastrukture u bitnom sadrži ključne elemente iz definicije EU iz 2008. godine uz razliku koja se odnosi na prelivanje bezbjednosnih prijetnji na najmanje dvije članice EU kako je sadržano u definiciji EU. Ukoliko analiziramo sadržaj ovog pojma na drugim kontinentima vidjećemo da on obuhvata ili širok dijapazon sredstava, odnosno imovine u cilju omogućavanja funkcionisanja društveno ekonomskog sistema[7] ili objekte, sisteme snabdijevanja, informacione tehnologije i mreže čije uništenje bi moglo dovesti u pitanje odbranu i bezbjednost države.[8]

U poglavlju II koje se bavi određivanjem kritične infrastrukture utvrđeni su kriterijumi za determinaciju kao i sektorski i međusektorski kriterijumi za određivanje kritične infrastrukture. Kriterijumi sadrže procjenu posledica poremećaja u radu ili prekida rada kritične infrastrukture u vitalnim oblastima od javnog interesa. U skladu sa pozitivnim propisima Vlada CG propisuje sektorske kriterijume za određivanje kritične infrastrukture na bazi analize rizika i karakteristika svakog sektora pri čemu se posebno ima u vidu uticaj jednog sektora na drugi. Sektori naznačene infrasturukture obuhvataju energetiku, saobraćaj, vodosnabdijevanje, finansije, zdravstvo, IT tehnologije, komunikacije, životnu sredinu i funkcionisanje državnih organa, propisano je u članu 9. citiranog zakona.[9] Slična situacija je i u drugim državama koje gotovo bez izuzetka pod kritičnom infrastrukturom podrazumijevaju energiju, informaciono komunikacione tehnologije, zdravstvo, finansije, transport, hitne službe, vodosnabdijevanje, odbranu, policiju i slično[10]. Pojedini autori ističu da između sektora telekomunikacija i drugih sektora postoji uzročna povezanost zbog čega ovaj sektor treba da ima prioritet u svrhu povećanja stepena sigurnosti.[11]

Zaštita kritične infrastrukture regulisana je u poglavlju III koje obuhvata modele zaštite, bezbjednosni plan, plan zaštite kao bezbjednosni plan kao i poslove koordinacije i postupanje sa tajnim podacima. Modeli zaštite kritične infrastrukture obuhvataju primjenu fizičke i tehničke zaštite na način

---

[6] Zakon o određivanju i zaštiti kritične infrastrukture, Službeni list CG br. 72/2019 od 26.12.2019, član 2.

[7] Murray T.(2012). Critical Infrastructure Protection; The Vulnerability Conudrun, telemastics and Informatics, 1/29, p.33.

[8] Murray T. op..cit. str.34.

[9] Zakon o određivanju i zaštiti kritične infrastrukture CG član 9.

[10] Škero M. Ateljević V. op. cit. str.193-194.

[11] Rinaldi S..M.(2004). Modeling and Simulating Critical Infrastructures and Their Interdependencis, p.19.

sličan obezbjeđenju lica i imovine, odnosno objekata i prostora. Posebnim zakonom regulisani su načini zaštite kritične informatičke infrastrukture koju koristi vojska, policija i Agencija za nacionalnu bezbjednost. Shodno članu 14. citiranog akta operatori kritične infrastrukture dužni su da izrade bezbjednosni plan koji sadrži opis sistema, mreža, objekata i njihovih djelova koji označavaju kritičnu infrastrukturu, analizu rizika i druge aktivnosti i mjere. Trajne mjere bezbjednosti su tehničke, organizacione, komunikacione i mjere ranog upozoravanja i jačanja svijesti koje se permanentno realizuju. Osim njih predviđene su i mjere bezbjednosti koje se preduzimaju u zavisnosti od stepena rizika i prijetnji po funkcionisanje kritične infrastrukture. Koordinator obavlja poslove zaštite krtične infrastrukture putem praćenja nacionalnih i međunarodnih propisa, praćenja primjene i revizije bezbjednosnog plana, odnosno posredovanja u komunikaciji između operatora i organa uprave i td. U slučajevima nastanka poremećaja u radu kritične infrastrukture formira se koordinacioni tim obrazovan u skladu sa zakonom iz oblasti zaštite i spašavanja.Na sličan način regulisana je i zaštira kritične infrastrukture EU na teritoriji Crne Gore.

ANALIZA NAPADA NA INFORMATIČKO - TEHNOLOŠKU MREŽU CRNE GORE U 2022. GODINI

Država Crna Gora je 20.08.2022. godine bila izložena do sada najvećem sajber napadu na ovu državu koji je trajao više sedmica. Ono što je do sada utvrđeno jeste da je prvobitna procjena vrijednosti virusa kojim je napadnut informatički sistem Vlade na dark vebu iznosila od 100.000 do 2,5 miliona dolara, a nakon dodatnih istraživanje se utvrdilo da se radi o cifri od 10 miliona dolara. Još uvijek nije bilo zahtjeva za otkup kompromitovanih podataka. Utvrđeno je da je do sada zaraženo 150 stanica u deset državnih institucija. Kontaminirane stanice su isključene sa mreže i sa njih su izuzeti hard diskovi radi vještačenja. Zvaničnici su izašli sa stavom da iza napada ne stoji pojedinac već se radi o precizno planiranom napadu koji je dobro finansijski pripremljen. Iz Agencije za nacionalnu bezbjednost je saopšteno odmah nakon napada da iza napada stoje strane službe. Ova institucija je upozorila Elektroprivredu Crne Gore da može biti predmet sajber napada, zbog čega su elektrane prešle na manuelni sistem upravljanja. Međutim, deset dana kasnije se oglasio ministar javne uprave i saopštio da iza sajber napada stoji poznata kriminalna grupa iz oblasti sajber terorizma Kuba ransomver. U pitanju je vrsta štetnog softvera koji ograničava pristup kompjuterskom sistemu, odnosno podacima i zahtijeva otkup od žrtve. Pojedine vrste ransomvera imaju sposobnost da blokiraju kompjuter jer se ucjenjivačka poruka ne može ukloniti

ukoliko se ne plati otkupnina. Neke vrste ransomvera mogu da šifriraju datoteke. U takvim slučajevima vlasnik inficiranog računara mora da plati novčani iznos u zamjenu za dešifrovanje podataka sa diska.

Ova hakerska grupa tvrdila je da je došla do podataka iz Skupštine Crne Gore kako su naveli pojedini mediji specijalizovani za informacije o sajber bezbejdnosti koji su objavili fotografije sa sajta ove hakerske grupe. Ovdje je očigledno da se virus ne može formirati za mjesec dana. Prema odredjenim izvorima nije do sada nigdje korišćen u ovom formatu. Još uvijek traje remedijacija odnosno popravka mreže i pojedinih servera a opasnost od hakerskog napada nije prošla. Pronađene su pojedine malicioznosti na radnim stanicama i sistemu pa se morala očistiti kompletna mreža da ne bi došlo do ponavljanja napada. Jedan broj radnih stanica je kriptovan zbog čega se računari ne mogu koristiti. S druge strane, zvaničnici su istakli da postoji bekap sistema zbog čega bi šteta bila reducirana. Međutim više je nego očigledno da nije izgrađen dovoljno dobar bekap sistem. Državne institucije nakon napada koriste alternativne mejlove za komunikaciju putem gmail servisa ili privatnih naloga što je suprotno zakonskim odredbama koje predviđaju da se oficijelne adrese moraju nalaziti na informacionoj infrastrukturi u Crnoj Gori. Posledice sajber napada na CG manifestuju se u prouzrokovanoj šteti koja može biti finansijska, zatim nematerijalna kao što je otkrivanje tajnih podataka, ili kombinovana.

U poslednjih nekoliko mjeseci bilo je više sličnih napada u ovom regionu. Nakon napada na infrastrukturu Albanije ova država je smatrala Iran odgovornim za napad i prekinula diuplomatske odnose sa Teheranom. Napadi su registrovani i u Sjevernoj Makedoniji, odnosno jednom broju ministarstava te države.

KRIVIČNA DJELA PROTIV BEZBJEDNOSTI RAČUNARSKIH PODATAKA U CRNOGORSKOM KRIVIČNOM ZAKONODAVSTVU

U glavi XXVIII Krivičnog zakonika CG sistematizovana su krivična djela iz oblasti kompjuterskog kriminaliteta. Ovaj oblik inkriminacija manifestuje se u različitim formama zloupotrebe računarske tehnologije. Nosioci kriminalnih aktivnosti ugrožavaju protok i distribuciju podataka nanoseći štetu vitalnim vrijednostima društva. Crnogorsko zakonodavstvo propisuje šest krivičnih djela protiv bezbjednosti računarskih podataka. Najčešći pojavni oblici su: oštećenje računarskih podataka i programa, ometanje računarskog sistema, pravljenje i unošenje računarskih virusa, računarska prevara, neovlašćeni pristup računarskom sistemu i zloupotreba uređaja i programa.

Osnovni oblik krivičnog djela oštećenje računarskih podataka i programa propisan je u članu 349 KZ CG.[12] i obuhvata neovlašćeno brisanje, izmjenu, oštećenje, prikrivanje ili na drugi način činjenje neupotrebljivim računarskog podatka ili programa. Objekt ovog delikta je računarski podatak ili program. Radnja izvršenja je alternativno postavljena i sastoji se u neovlašćenom brisanju, izmjeni, oštećenju, prikrivanju i sl. Posledica se manifestuje u destrukciji računarskih podataka i programa. Krivično djelo je dovršeno preduzimanjem bilo koje naznačene radnje. Učinilac može biti svaka osoba a u pogledu krivice potreban je umišljaj koji obuhvata svijest o bitnim elementima djela. Ako se prema istom objektu napada preduzima više radnji ostvaruju se elementi jednog krivičnog djela.[13] Teži oblici ovog krivičnog djela kvalifikovani su težom posledicom, odnosno visinom nastale štete pri čemu je u pogledu krivice kod učiinioca osim umišljaja moguć i nehat. Zakonik predviđa obaveznu mjeru bezbjednosti oduzimanja uređaja i sredstava kojima je delikt izvršen.

Krivično djelo ometanje računarskog sistema (osnovni oblik) sastoji se u unošenju, brisanju, izmjeni, oštećenju, prikrivanju ili na drugi način činjenju neupotrebljivim računarski podatak ili sistem pri čemu je namjera učinioca da omete rad računarskog sistema.[14] Objekt krivičnog djela je računarski podatak ili računarski sistem. Radnja izvršenja je određena putem posledične norme kako je navedeno u opisu bića inkriminacije. Unošenje kao prvi oblik radnje izvršenja podrazumijeva smještanje podataka ili programa u kompjuter. Brisanje znači uništenje računarskih podataka iili programa. Oštećenje računarskog podatka ili programa znači njihovo činjenje neupotrebljivim u propisane svrhe. Mijenjanje računarskog programa ili podatka znači izmjenu sadržaja digitalne informacije koja ga konstituiše. Prikrivanje podatka ili programa znači njihovo činjenje nedostupnim za ovlašćene korisnike. Posledica inkriminacije sastoji se u uništenju ili oštećenju objekta zaštite. Namjera ometanja rada računarskog sistema čini subjektivni element krivičnog djela .Za krivicu je potreban umišljaj a izvršilac može biti svaka osoba.[15] Teži oblik ovog krivičnog djela postoji ako je ometanje računarskog siistema učinjeno u odnosu na podatke i programe značajne za državne organe, javne službe, provredna društva i td.

Krivično djelo pravljenje i unošenje računarskih virusa obuhvata dva oblika radnje izvršenja. Prvi oblik se sastoji u kreiranju računarskog virusa

[12] Krivični zakonik Crne Gore, „Sl. List RCG“ br.70/2003 i „Sl list CG“ br. 40/2008. čl.349.
[13] Lazareviić Lj. Vučković B. Vučković V. (2004).Komentar Krivičnog zakonika Crne Gore, Cetinje, str.817.
[14] Krivični zakonik CG, član 350.
[15] Rakočeviić V.(2014). Krivična djela sa elementiima organizovanog kriminaliiteta-specijalne istražne metode, Podgorica, str.203.

određenom kompjuterskom procedurom. Drugi oblik obuhvata ubacivanje podataka koji sadrže viruse korišćenjem kompjuterske tehnologije. Poznato je da računarski virus ima mogućnost reprodukcije i kontaminacije drugih programa. Posledice ovog deliikta se manifestuju u nastanku imovinske štete, gubitku podataka, zastoju u radu kompjutera i slično. U pogledu krivice potreban je direktni umišljaj koji obuhvata posebnu namjeru. I kod ovog krivičnog djela predviđena je mjera bezbjednostii oduzimanja računara i programa.

Kada je riječ o krivičnom djelu računarska prevara ono sadrži poseban oblik prevare pri čemu je radnja izvršenja alternativno postavljena i obuhvata uticanje na rezultate elektronske obrade, odnosno transfera podataka, unošenjem netačnih podataka ili propuštanjem unošenja tačnog podataka. Radnja sadrži i prikrivanje ili lažno prikazivanje računarskog podatka i ometanje računarskog sistema u namjeri da učinilac sebi ili drugom pribavi protivpravnu imovinsku korist ili drugom prouzrokuje imovinsku štetu. Posledica krivičnog djela je izmjena rezultata elektronske obrade podataka. Da bi postojalo krivično djelo potrebno je da su podaci koji se unose natačni ili da se propusti unošenje tačnog podatka. Teži oblici ovog krivičnog djela određeni su visinom pribavljene imovinske koristi, dok lakši oblik postoji ako se ovo krivično djelo učini samo u namjeri da se drugo lice ošteti a ne da se pribavi protivpravna imovinska korist pri čemu nije neophodno da je namjera realizovana.

Prvi osnovni oblik krivičnog djela iz člana 353 KZ CG sastoji se u neovlašćenom pristupu računarskom sistemu kao cjelini ili pojedinom njegovom dijelu. Pristup kompjuterskom sistemu znači potpuno ili djelimično korišćenje kompjuterskog siistema bez pravnog osnova. Drugi oblik obuhvata neovlašćeni pristup računarskom sistemu kršenjem mjera zaštite, odnosno pristup računarskom sistemu koji je od značaja za državne organe, organe lokalne samouprave i ustanove kojima je povjereno vršenje javnih ovlašćenja. Kod ovog oblika učinilac postupa suprotno mjerama zaštite koje su propisane zakonom. Sljedeći oblik obuhvata neovlašćeno presrijetanje kompjuterskih podataka, bez obzira na način njihovog prenosa, koji nijesu javne prirode ka računarskom sistemu, od njega i unutar samog sistema uključujući i elektromagnetnu emisiju. Četvrti oblik postoji ukoliko učinilac upotrijebi podatak dobijen putem neovlašćenog pristupa računarskom siistemu, kršeći mjere zaštite ili neovlašćenim presrijetanjem računarskih podataka. Teži obliik ovog krivičnog djela postoji ako su nastupile teške posledice za drugog što se mora utvrditi u svakom konkretnom slučaju. U pogledu krivice potreban je umišljaj koji obuhvata svijest o neovlašćenom pristupu računarskom sistemu.

Poslednje krivično djelo iz ove grupe je zloupotreba uređaja ili programa propisano u članu 354 KZ CG. Ovo krivično djelo sastojii se u

proizvodnji, prodaji, nabavljanju radi upotrebe, uvozu, distribuciji ili na drugi način stavljanju na raspolaganje uređaja ili računarskih programa projektovanih ili prilagođenih izvršenja krivičnih djela kompjuterskog kriminaliteta, kao i računarskih šifri ili sličnih podataka putem kojih se može pristupiti sistemu u cjelini ili djelimično radi izvršenja naznačenih krivičnih djela. Inkriminisano je i posjedovanje uređaja ili programa u namjeri da se koriste za izvršenje krivičnih djela iz ove oblasti. Objekt radnje su uređaji ili programi projektovani i prilagođeni za izvršenje kompjuterskog kriminaliteta. Učinilac svih oblika može biti svako lice a u pogledu krivice potreban je umišljaj.

STANJE I KRETANJE KOMPJUTERSKOG KRIMINALITETA U CRNOJ GORI ZA PERIOD 2017.-2021. GODINE

Krivičnim pravom štiti se korišćenje informacionih tehnologija u zakonite svrhe što predstavlja djjelotvornu zaštitu funkcionisanja IT tehnologija. Danas se prilikom izvršenja krivičnih djela u značajnom obimu koriste računari i nove tehnologije a osim toga kompjuteri vrlo često predstavljaju objekt protivpravnog napada. To su očigledne negativne implikacije korišćenja računara.

Tabela 1: Prijavljena lica zbog izvršenja krivičnih djela protiv bezbjednosti računarskih podataka

Godina	2017	2018	2019	2020
Broj prijavljenih lica	5	2	7	9
Ukupno	23			

U posmatranom periodu prijavljena su ukupno 23 lica. Najviše prijavljenih lica bilo je 2020. godine 9 ili 39,1%, zatim 2019 kada je prijavljeno 7 ili 30,4%. Zbog izvršenja krivičnog djela računarska prevara u 2020. godini prijavljeno je 1 lice. U 2019. godini za ovo krivično djelo prijavljena su 4 lica, u 2018. godini 2 lica, a u 2017. godini 4 lica. Zbog izvršenja krivičnog djela neovlašćeni pristup računarskom sistemu u 2020. godini prijavljeno je 5 lica a u 2019. godini 2 lica.

Tabela 2: Optužena i osuđena lica zbog izvršenja krivičnih djela protiv bezbjednosti računarskih podataka u 2020. godini

Optužena lica	Osuđena lica	Vrsta kazne	Neriješeno optuženja
3	1	zatvor	15

U 2020. godini podignuta je optužnica protiv 3 lica. Protiv 1 lica sud je donio osuđujuću presudu-kaznu zatvora. Na kraju ove godine ostalo je neriješeno optuženja protiv 15 osoba.[16] Ovi podaci pokazuju da je digitalna transformacija dovela do porasta sajber napada i njegove multiplikacije.

METODIKA OTKRIVANJA KRIVIČNIH DJELA KOMPJUTERSKOG KRIMINALITETA

Brojne kriminalne aktivnosti u ovoj oblasti su napad na hardver što podrazumijeva uništenje, oštećenje ili otuđenje računarskog sistema ili njegovih komponenti. Ista je situacija sa napadom na softver koji osim prethodnih oblika sadrži i neovlašćenu izmjenu, objavljivanje ili korišćenje softvera. Slična je inkriminacija napad na program, zatim napad na podatke, napad na zaštitu sistema i napad na usluge.

Metodika otrivanja ovih oblika visokotehnološkog kriminaliteta je bitno različita u odnosu na rješavanje drugih tipologija kriminalnog ispoljavanja. Sutuaciju otežava i deficit standarda i specijalizovanih službi koje bi se ozbiljnije bavile ovom problematikom. Kriminalni događaj u sajber prostoru u fizičkom smislu ostavlja minumum tragova i to isključivo elektronskih u formi elektromagnetnih impulsa. Kriminalističku obradu i kasnije istragu usložnjava i to što učinioci ovih delikata koriste opremu koja je naprednija od one koju posjeduju oficijelne strukture, dok je većina vurusa kreirana na novim konceptima.

Nakon saznanja za izvršeno krivično djelo iz ove grupe policija u saradnji sa državnim tužilaštvom primjenjuje određene kriminalističke metode i tehnike.U prvoj fazi kriminalističke obrade računar se isključuje sa sistema i vrši integralna analiza svih segmenata funkcionisanja kompjuterskog sistema u smislu utvrđivanja vremena, načina i sredstava izvršenja uz pomoć ekeperata za ovu oblast. Nakon toga slijedi kriminalistički pregled, uvidu u odgovarajući dokumentaciju i vještačenje radi obezbjeđenja materijalnih dokaza. Od osumnjičenih osoba i njihovih provajdera se vrši oduzimanje računara sa

[16] Tužilački savjet Crne Gore (2021). Izvještaj o radu Tužilačkog savjeta i Državnog tužilaštva za 2020. godinu, Podgorica, str.120.

diskovima, fleš memorijama i slično. Vrši se kopiranje svih nosilaca kriminalistički relevantnih informacija kako bi se utvrdilo da li u njima postoje tragovi koji ukazuju na destruktivne programe i pravce napada.Važno je utvrditi kauzalnu vezu između delikta i učinioca i pravilno vrednovati utvrđene činjenice. Najefikasniji način dokazivanja ovih krivičnih djela je kombinacija materijalnih i ličnih dokaza.[17]

ZAKLJUČAK

Ne postoji država u svijetu danas koja je sposobna da se samostalno suprotstavi najtežim oblicima kriminaliteta uključujući i kompjuterski. Crna Gora na tom planu ne može biti izuzetak i ona mora djelovati udruženim aktivnostima sa drugim državama pošto se radi o prekorganičnom transnacionalnom kriminalitetu. Poslednji sajber napad više nego ikada ranije je ukazao na neophodnost adekvatne zaštite kritične kompjuterske iinfrastrukture budući da su kapaciteti sajber odbrane pokazali neefikasnost. Hakerska grupa je u ovom slučaju pronašla slabosti u sistemu posredstvom kojih je izvršila upad i uticaj na sistem da on funkcioniše na način koji hakerima odgovara. Ovaj slučaj je pokazao da kapaciteti sajber odbrane još uvijek nijesu dovoljno osnaženi i ažurirani, što je posebno izraženo u kriznim situacijama. U uslovima asimetričnih bezbjednosnih prijetnji potreban je integralni pristup i intenzivna saradnja ključnih subjekata. Što je veća otpornost kritične infrastrukture to je veća spremnost svake države za digitalno doba.

Veoma je važno istaći posvećenost EU rješavanju problema u oblasti sajber bezbjednosti kao uslova očuvanja i unapređenja digitalne povezanosti starog kontinenta izdvajanjem značajnih finansijskih sredstava. Upravo Strategija sajber bezbjednosti EU za period 2020-2025. godine u prvi plan stavlja izgradnju evropske rezistentnosti, samostalnosti i operativnih kapaciteta koji bi omogućili uspješno i efikasno suzbijanje opasnosti po mrežne informacione sisteme. Crna Gora u okviru procesa pristupanja EU, odnosno pregovaračkih poglavlja 10 i 24 ima obavezu da svoje zakonodavstvo prilagodi pravnoj tekovini EU. U prošlogodišnjem izvještaju za Crnu Goru EK je naglasila da ova država pojačava kapacitete u oblasti sajber kriminaliteta ali da sistem u cjelini nije na nivou koji garantuje uspješno suprotstavljanje ovim izazovima.

Ovoj državi je potrebno odgovorno, djelotvorno i efikasno upravljanje sajber bezbjednošću u okviru sektora bezbjednosti. Potrebno je razmisliti o proširenju nadležnosti državnih organa na sva krivična djela kod kojih se kao

[17] Rakočeviić V.(2012). Kriminalistička metodika, Podgorica, str.284.

sredstvo izvršenja ili objekt napada javljaju kompjuteri, kompjuterske mreže i podaci, odnosno njihovi produkti u digitalnom ili materijalnom vidu što bi omogućilo efikasniju identifikaciju učinilaca i njihov krivično pravni progon. Najvažnije je preduzeti preventivne mjere koje bi imale za cilj da eliminišu izvore opasnosti u ovoj oblasti, što bi podrazumijevalo eliminaciju napada ili ukoliko je do njega došlo minimizirati posledice. Neophodno je sačiniti planove i strategije koje su kompatibilne sa najvišim standardima u ovoj oblasti i pojačati mjere integralne bezbjednosti kao i pristup računarskom sistemu čemu treba da prethodi studiozna procjena ugroženosti računarskog sistema.

LITERATURA

1. Zakon o određivanju i zaštiti kritične infrastrukture, Službeni list CG br. 72/2019.
2. Krivični zakonik Crne Gore, „Sl. list RCG“ br.70/2003 i „Sl. list CG“ br. 40/2008.
3. Lazarević LJ. Vučković B. Vučković V.(2004). Komentar Krivičnog zakonika Crne Gore, Cetinje.
4. Murray T.(2012). Critical Infrastructure Protection; The Vulnerability Conudrun, telemastics and Informatics, 2012, 1/29.
5. Rakočević V.(2012). Kriminalistička metodika, Podgorica.
6. Rakočević V. (2014). Krivična djela sa elementiima organizovanog kriminaliteta- specijalne istražne metode, Podgorica.
7. Rinaldi S..M. (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencis.
8. Tužilački savjet Crne Gore,(2021). Izvještaj o radu Tužilačkog savjeta i Državnog tužilaštva za 2020.godinu, Podgorica.
9. Council Directive 2008/114/EC, Official Journal of the European Union.
10. Škero M.Ateljević V. (2015). Zaštita kritične infrastrukture i osnovni elementi usklađivanja Sa Direktivom SE 2008/114ES, Vojno delo,3/2015.

THE VULNERABILITY OF THE CRITICAL INFORMATION INFRASTRUCTURE PROTECTION SYSTEM IN MONTENEGRO AND THE CONSEQUENCES OF AN ATTACK ON THE COMPLETE IT AND TECHNOLOGY NETWORK IN 2022

Full prof. Velimir Rakočević, PhD
Full professor of the Faculty of Law, University of Montenegro

Aleksandra Jovanović, PhD
Higher State Prosecutor's Office, Podgorica

Abstract: In order to harmonize the national legislation in the field of critical infrastructure with the standards of the European Union, in December 2019, Montenegro submitted the Law on the Determination and Protection of Critical Infrastructure, which defined the systems, networks and objects of critical infrastructure and determined the activities and measures of their protection. The adoption of this document represented a solid normative basis that had to be implemented in an optimal period of time. This obviously did not happen, since the cyber attacks on the information network of the Government of Montenegro started in the middle of August of the current year and lasted for several weeks, and the remediation of the consequences will certainly take a longer period of time. Hacker attacks disabled access to the websites and e-mails of a number of ministries as well as other important state bodies such as courts, prosecutor's offices, the Revenue and Customs Administration, the Real Estate Administration et cetera. At the time of writing this paper, the perpetrators of these crimes have not been identified, and the state is doing everything to overcome the consequences of cyber attacks on state institutions. The subject of research in this paper is the analysis of the compatibility of Montenegrin legislation with the relevant EU acts in this area, as well as the explanation of incriminations against the security of computer data and other criminal offenses in which the objects of the attack are information and communication technologies, with special review to the methodology of detecting and proving these crimes.

Key words: critical information infrastructure, cyber attacks, computer crime

PROTECTION OF CRITICAL INFRASTRUCTURE FROM HYBRID THREATS

Assoc. prof. Tatjana Gerginova, PhD[1]

Abstract: Security of citizens, protection of sovereignty and territorial integrity, principles of democracy and the rule of law are some of the main concepts and basic principles of modern democratic society in every country, including in the Republic of North Macedonia. The prevention of dangers from hybrid threats is basically an interdisciplinary, interdepartmental and long-term project that aims to help achieve the goals of democracy, good security management and economic priorities. Achieving the protection of critical infrastructure is one of the components of national security. The need to achieve protection of critical infrastructure is related to the need to build resilience of the Republic of North Macedonia in efficient and effective dealing with hybrid threats in order to achieve protection of national interests and create national resilience of society. In order to achieve effective protection of critical infrastructure, the emphasis needs to be placed on the following aspects: assessment, detection, rejection and response to threats. The new era of hybrid threats requires a new starting point in creating changes in the approach to protecting critical infrastructure. In the paper, the author establishes a new approach to the protection of critical infrastructure, and sets the following as priorities: adoption of the Law for the Protection of Critical Infrastructure; creation of an effective strategy for the protection of critical infrastructure; application of multiple early warning models; successful prevention, which can contribute to the reduction of risks, which will directly affect the increase of the security of the critical infrastructure; continuous training and training of human resources to deal with attacks on critical infrastructure.

Key words: critical infrastructure, hybrid threats, assessment, detection, rejection and response to threats

[1] Associate professor, Faculty of Security-Skopje, University "Sv. Kliment Ohridski"-Bitola, Macedonia. E-mail: *tanjagerginova@gmail.com*

INTRODUCTION

Today's security environment is unpredictable. Threats can come from state and non-state actors in the form of terrorist attacks but also cyber attacks and hybrid warfare, which can blur the lines between conventional and unconventional forms of conflict. They can also come from climate change and natural disasters such as floods, fires and earthquakes and from biohazards such as the COVID-19 pandemic. The challenge of adapting to and responding to these different types of threats is compounded by trends that have radically transformed the security environment.

There are various definitions of the term "critical infrastructure" in the scientific literature. Critical infrastructure is the basic physical and organizational structure that society and the state need to function. Critical infrastructure is defined as the sum of all facilities, systems, networks and functions, vital for the survival of the state, the destruction of which will negatively affect security, national security, public health and the like.

The term critical infrastructure includes all national capacities, services and information systems that are vital to the state and because of the impossibility of their operation or damage may endanger national security, national economy, public safety, public health, and government efficiency.[2] The European Union defines critical infrastructure through Directive 2008/114 / EC, which calls on member states to identify and design European critical infrastructure, as well as to assess the need to improve their protection. All Member States have implemented the Directive by establishing a process for identifying and designating critical European infrastructure in the energy and transport sectors. According to the Directive, critical infrastructure is defined as: "an asset, system or part thereof located in the Member States which is essential for the maintenance of vital social functions, health, safety, economic or social well-being of the people and whose disruption or destruction would significant impact in the Member State as a result of failure to maintain those functions".[3]

Achieving the protection of critical infrastructure is one of the components of national security. The need to achieve protection of critical

[2] About the definitions of critical infrastructure, see more at Gerginova, Tatiana., (2021). "Need for protection of critical infrastructure" – the paper was published in the Proceedings of the International Scientific Conference on the topic "Harmonization of legal regulations with legal currents (Acquis Communautaire) of the European Union - Situation in Bosnia and Herzegovina and experiences of others in Banja Luka" organized of the Research Center in Banja Luka and in cooperation with the Institute for Comparative Law in Belgrade.

[3] According to DIRECTIVE 2008/114/EC - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013

infrastructure is related to the need to build resilience of the Republic of North Macedonia in efficient and effective dealing with hybrid threats in order to achieve protection of national interests and create national resilience of society.

At the 2016, the Warsaw Summit was held where the allied leaders decided to strengthen NATO's resilience to the full spectrum of threats and continue to develop individual and collective capacity to counter any form of armed attack. They agreed on seven basic requirements for national resilience against which member states can measure their level of preparedness. These requirements reflect the essential functions of continuity of government, essential services to the population and civilian support of the military which must be maintained under the most challenging circumstances.

These seven basic requirements determine the following contents:[4]

- Continuity of government and critical government services ensured: for example the ability to make decisions, communicate and implement them in crisis conditions;

- Flexible energy supply: back-up plans and electricity networks, internal and cross-border;

- Ability to effectively deal with the uncontrolled movement of people and to deconflict these movements from NATO military deployments;

- Resilient food and water resources: ensuring these supplies are safe from disruption or sabotage;

- Ability to deal with mass casualties: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secured;

- Resilient civil communications systems: ensuring that telecommunications and cyber networks function even in crisis conditions with sufficient backup capacity. These requirements was updated in November 2019 by NATO Defense Ministers who highlighted the need for reliable communications systems including 5G, robust options for restoring these systems, priority access to national authorities in times of crisis and thorough assessments of all risks to communication systems; Resilient transport systems: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis.

Implementing this commitment is a top priority for Allies. Since 2016, the resilience of Allied members has improved, but challenges and shortfalls remain. At the same time, Allies are confronted with new challenges, including economic pressures that could undermine the assured access of essential critical infrastructures by national governments and the military in times of crisis.

[4]https://www.nato.int/nato-on-the-map/#lat=51.72673918960763&lon=4.84911701440904&zoom=0&layer-1
https://www.nato.int/cps/en/natolive/topics_37356.htm
https://www.nato.int/cps/en/natohq/topics_133127.htm

NATO updated its baseline requirements in 2020 to reflect the challenges presented by emerging communications technologies, such as 5G, as well as the impact and implications of the COVID-19 pandemic.

BUILDING NATIONAL RESISTANCE ACCORDING TO THE STRATEGY OF THE EUROPEAN UNION FROM 2020

In 2020, the European Union adopted a new Security Union Strategy and this strategy foresees activities for the period from 2020 to 2025. Through this strategy, the European Union provides guidance for strengthening security, by preventing and detecting hybrid threats. The comprehensive approach of the European Union in dealing with hybrid threats, as well as the established cooperation between the European Union and NATI in the field of hybrid threats, (EU-NATO Joint Declaration -2016 and 2018) - cyber defense and capacity building, have been taken into account in the development of this national Strategy. Within NATO, in 2016, guidelines for building resilience were defined, as well as evaluation criteria to support the seven basic needs/requirements for building national resilience - Seven Baseline Requirements for National Resilience.[5]

The proposal for a new strategy defines four priorities for action at European Union level. The first priority refers to the future security environment that focuses on protecting and increasing the resilience of key physical and digital infrastructure. The second priority recognizes the problem of rapidly evolving threats and the need for the European Union to adapt to it in order to combat them. This primarily refers to the growing cybercrime and the need to improve the capacity of digital investigations, but also to combat hybrid threats aimed at disrupting social cohesion and trust in institutions. The third priority is the fight against terrorism and organized crime. Regarding the fight against terrorism, the strategy emphasizes the importance of eliminating the causes of radicalization, prosecuting terrorists and foreign terrorist fighters and cooperating with non-EU countries and international organizations. As far as organized crime is concerned, the measures will focus on combating human trafficking, especially migrants, drug trafficking and illegal weapons. The fourth priority refers to building a strong security ecosystem, which means cooperation and exchange of information, strong external borders, strengthening research capacities and improving skills and raising awareness in security issues.

[5] See more about this https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO AND THE STRATEGIC CONCEPT OF 2010 AND 2016

NATO Heads of State and Government approved a new Strategic Concept for the Alliance in Madrid on 29 June 2022, setting out the Alliance's priorities, core tasks and approaches for the next decade.[6] The Strategic Concept is a key document for the Alliance. It reaffirms NATO's values and purpose and provides a collective assessment of the security environment. It also drives NATO's strategic adaptation and guides its future political and military development. The Strategic Concept is reviewed and updated regularly. Since the end of the Cold War, it has been updated approximately every 10 years to take account of changes to the global security environment and to make sure the Alliance is prepared for the future. The previous Strategic Concept was adopted at the NATO Lisbon Summit in 2010. The new The Strategic Concept describes the new security reality facing the Alliance, reaffirms NATO's values and spells out NATO's key purpose of ensuring Allies' collective defense. The document defines Russia as the "most significant and direct threat" to Allies' security, while addressing China for the first time and the challenges that Beijing poses toward Allies' security, interests and values. The documents also states that climate change is "a defining challenge of our time". The Strategic Concept is updated roughly every decade and is NATO's second most important document. It reaffirms the values of the Alliance, provides a collective assessment of security challenges and guides the Alliance's political and military activities. The previous version was adopted at the NATO Lisbon Summit in 2010.[7]

The 2010 Strategic Concept - The 2010 Strategic Concept "Active Engagement, Modern Defense" is a very clear and resolute statement on NATO's core tasks and principles, its values, the evolving security environment and the Alliance's strategic objectives. This document defines NATO as "a unique community of values committed to the principles of individual freedom, democracy, human rights and the rule of law", and presents the three essential core tasks of NATO - collective defense, crisis management and cooperative security. It also emphasizes the solidarity of the Alliance, the importance of transatlantic consultation and the need to engage in a continuous process of reform. The document then describes the 2010 security environment and identifies the capabilities and policies needed to ensure that NATO's deterrence and defense, as well as crisis management abilities, are equipped to face today's threats. These threats include, for instance, the proliferation of ballistic missiles

[6] https://www.nato.int/cps/en/natohq/news_196144.htm
[7] https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

and nuclear weapons, terrorism, cyber attacks and fundamental environmental problems. The Strategic Concept also affirms how NATO aims to promote international security through cooperation. It will do this by reinforcing arms control, disarmament and non-proliferation efforts, emphasizing NATO's open door policy for all European countries, and significantly enhancing its partnerships in the broad sense of the term. Additionally, it affirms that NATO will continue its reform and transformation process.

In accordance with the Warsaw Summit Declaration (2016), in the event of a hybrid threat to a member state, NATO may request the activation of Article 5 of the Washington Treaty. Accordingly, NATO member states should build resilience capabilities against hybrid threats as part of their collective defense commitment. Resilience is a fundamental element of NATO's concept of deterrence and defense.

Resilience and Article 3 - Each NATO member country needs to be resilient to resist and recover from a major shock such as a natural disaster, failure of critical infrastructure, or a hybrid or armed attack. Resilience is a society's ability to resist and recover from such shocks and combines both civil preparedness and military capacity. Civil preparedness is a central pillar of Allies' resilience and a critical enabler for the Alliance's collective defense, and NATO supports Allies in assessing and enhancing their civil preparedness.

- The principle of resilience is anchored in Article 3 of the Alliance's founding treaty: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."
- Article 3 helps to give NATO the means to fulfill its core tasks, in particular, that of collective defense.
- The individual commitment of each and every Ally to maintaining and strengthening its resilience reduces the vulnerability of NATO as a whole.
- Resilience is first and foremost a national responsibility. Each Ally needs to be sufficiently robust and adaptable to deal with and address the entire spectrum of crises envisaged by the Alliance.
- NATO has agreed seven baseline requirements for national resilience against which Allies can measure their level of preparedness; these requirements reflect the core functions of continuity of government, essential services to the population and civil support to the military.
- Military efforts to defend Alliance territory and populations need to be complemented by robust civil preparedness to reduce potential vulnerabilities and the risk of attack in peacetime and during war.

- Military forces, especially those deployed during crises and war, heavily depend on the civilian and commercial sectors for transport, communications and even basic supplies such as food and water, to fulfill their missions.

REPUBLIC OF NORTH MACEDONIA AND BUILDING NATIONAL RESILIENCE OF SOCIETY

Taking into account the fact that modern threats have a complex content, the need to respond to the entire society is also imposed. This implies thee need to build national capacities to improve resilience to these threats through a broader, more integrated and better coordinated approach at the national level.

According to the Defense Strategy of Macedonia,[8] Macedonia is included in the collective security systems and aims to: increase the system's resilience in dealing with risks and threats and improving the existing and developing new capabilities that are necessary for the effective and efficient functioning of the system.

In order to achieve effective protection of critical infrastructure, the emphasis needs to be placed on the following aspects: assessment, detection, rejection and response to threats.

- Assessment, taking into account the risks and vulnerability, as well as the expected results of the possible consequences. This is achieved by the methods of analysis, modeling and simulation.

- Prevention, i.e. risk reduction by forecasting the effects of threats. This dimension is achieved through intimidation, as well as with other "passive" countermeasures.

- Detection – it is the ability to promptly recognize abnormal conditions and behavior. This aspect is realized with active sensors and other technological devices.

- Response – more precisely, quick reaction to threats. This aspect is realized with the method of early warning, situation monitoring and decision support systems.[9]

[8] According to Defense Strategy of the Republic of North Macedonia "Official Gazette No. 75" from March 2020.

[9] Flammini, F.,Critical Infrastructure Security: Assessment, Prevention, Detection, Response, 2012, p.9.

In its preventive action, the security services in Macedonia uses the following three methods: detection, rejection and response.[10]

Detection of the threat – A key moment in the emergence of hybrid threats is the detection. As a way to manage hybrids, the detection standard has the ability to obtain relevant and timely information on potential cost intentions from all areas and carriers.[11]

The method to be used to successfully detect threats includes identifying critical national vulnerabilities, linking vulnerabilities to possible scenarios and assumptions about an attacker's goals and capabilities and identifying vulnerability – related indicators and measures to be taken to deal with hybrids threats. Institutions that are primarily responsible for the detection of hybrid threats are the intelligence and security services of the Republic of North Macedonia and they are obliged to develop an efficient method of collecting relevant and timely information and detection of hybrid threats. Practicing this method requires the use of expertise and information from all entities of the Government, holders of individual areas in the legislative, judicial and executive branches. Creating and developing a detection capability is a priority activity, because without threat detection it is not possible to plan a response to effectively counter it.

Rejection of the threat - The ability to repel a threat is a method aimed at building resilience, building the capacity to withstand stress and the ability to overcome the damage caused by threats, as well as the ability to retaliate against an attacker. Resilience is needed, above all. In areas targeted for hybrid attack, such as politics, economics, the defense and security sectors, the information sector, civil society and critical infrastructure.

Response to the threat – Responding to hybrid threats means having an effective decision-making process at the strategic level. The body responsible for directing, drawing conclusion and proposing measures to respond to hybrid threats as a threat to national security is the Intelligence-Security Coordination Council.[12]

---

[10] See more about this https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf) accessed on 15.11.2022).

[11] Gerginova, Tatiana., (2022). "National security of the Republic of North Macedonia in a modern global security environment", Paper published in Proceedings of the 13th International Scientific Conference - 45 YEARS HIGHER EDUCATION IN THE AREA OF SECURITY - EDUCATIONAL CHALLENGES AND SECURITY PERSPECTIVES, organized by the Faculty of security, Skopje and the German Friedrich Ebert Stiftung.

[12] See more about this https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf accessed on 15.11.2022

A key factor in this process is having a credible assessment of the situation and determining the level of threat tolerance, the overcoming of which would indicate that the country is subject to attack using hybrid methods. It is therefore necessary to realize effective inter-institutional communication and cooperation, coordination of intelligence services and a fast and efficient political decision-making process. Availability of credible and timely information on hybrid threats against the Republic of North Macedonia will assist the descision-making process, as well as the process of activating the assistance mechanisms of the European Union and NATO's collective defense system. Various mechanisms can be used in response to a hybrid attack, such as economic sanctions against countries, companies and individuals, expulsion of diplomats, intelligence operations and other activities to neutralize hybrid threats. However, it is essential that the response be modeled in a way that does not cause the threat to escalate, but will force the attacker to discontinue hybrid activities due to their ineffectiveness, as the damage they will suffer from such activities will outweigh the potential benefits.

Building resistance to hybrid threats is the responsibility of society as a whole. All state institutions have roles, responsibilities and tasks in dealing with these threats, within their competencies. These institutions are also directed towards cooperation with the private and civil sector.

ACCORDING TO THE NATO – STRATEGIC CONCEPT OF 2022

NATO Heads of State and Government approved a new Strategic Concept for the Alliance in Madrid on 29 June 2022, setting out the Alliance's priorities, core tasks and approaches for the next decade. NATO's deterrence and defense posture is based on an appropriate mix of nuclear, conventional and missile defense capabilities, complemented by space and cyber capabilities. It is defensive, proportionate and fully in line with international obligations. According to this concept, NATO undertakes to use military and non-military tools in a proportionate, coherent and integrated manner to be able to respond to all security threats at the national and global level.[13] Proportionate to the threats faced, NATO determines an approach credible, flexible, adapted and sustainable, deterrence and defensive posture will be implemented. Furthermore, the concept states that NATO will continue to strengthen its Collective readiness, responsibility, deploy ability and integration of national forces. NATO is committed to providing a resilient and integrated command structure and will increase the coherence of NATO's national and defense plans

[13] https://www.nato.int/cps/en/natohq/news_196144.htm

and strengthen and modernize NATO's force structure. It will strengthen training and exercise, adapt and streamline decision-making processes, improve planning and improve the effectiveness of the crisis response system. NATO also undertakes activities in the direction of accelerating the digital transformation, towards adapting NATO's command structure for the information age and will improve cyber defense, networks and infrastructure. Through this concept, NATO will pursue a more robust, integrated and coherent approach to building national and Alliance-wide resilience against military and non-military threats and challenges to our security, as a national responsibility and collective obligation rooted in Article 3 of North Atlantic Treaty. It will work to identify and mitigate strategic vulnerabilities and dependencies, including in relation to critical infrastructure, supply chains and health systems and to improve energy security and invest in stable and reliable energy supplies and sources.

NATO will also invest in advancing capabilities and skills to prepare for deter and defend against the coercive use of political, economic, energy, information and other hybrid tactics by states and non-state actors. Hybrid operations against allies could reach the level of an armed attack and could prompt the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty. The primary purpose of NATO's nuclear capability is to preserve the peace, prevent coercion and deter aggression. Any use of nuclear weapons against NATO would fundamentally change the nature of the conflict.

NATO will take all necessary steps to ensure the credibility, effectiveness and security of the nuclear deterrence mission. The Alliance is committed to ensuring greater integration and coherence of capabilities and activities across all domains and the spectrum of conflicts, while affirming the unique and distinct role of nuclear deterrence. NATO will continue to maintain credible deterrence, strengthen its strategic communications, enhance the effectiveness of its exercises and reduce strategic risks. Strategic stability, ensured through effective deterrence and defense, arms control and disarmament and meaningful and reciprocal political dialogue, remains an essential priority for the security of the European Union. Arms control, disarmament and non-proliferation contribute strongly to the Alliance's goals. Allies' arms control, disarmament and non-proliferation efforts aim to reduce risk and improve security, transparency, verification and compliance – building and predictability through dialogue, increasing understanding and establishing effective tools for crisis management and prevention.[14]

[14] https://www.nato.int/cps/en/natohq/news_196144.htm

NATO will pursue all elements of strategic risk reduction, including promoting confidence-building and predictability through dialogue, increasing understanding and establishing effective tools for crisis management and prevention.

NATO will be used as a platform for in-depth discussion and close consultation on arms control efforts. The concept establishes and strengthens coordination and cooperation with the United Nations and the European Union, as well as with other regional organizations such as the Organization for Security and Cooperation in Europe and the African Union. The concept establishes that the European Union is a unique and essential partner for NATO. NATO allies and EU members share the same values. NATO and the EU play complementary, coherent and mutually reinforcing roles in supporting international peace and security. Based on the long-term cooperation, the strengthening of the NATO-EU strategic partnership, strengthening political consultation and increasing cooperation on issues of mutual interest, such us military mobility, resilience, the impact of climate change on security, new and disruptive technologies, human security, the women's technologies, human security, the women's agenda, peace and security, as well as countering cyber and hybrid threats etc.

CONCLUSION

Macedonia is not a direct target of hybrid threats, but this security issue must not be underestimated, given its effects, which can penetrate deeply into all spheres of social life, contribute to undermining trust in the system and gradually lead to its disintegration, in a situation where the state is not yet at the level to guarantee an adequate level of security from such actions. Increasing awareness of their occurrence and exchange of experiences and knowledge through international cooperation are key to achieving protection against hybrid threats. In terms of defense against such attacks, our country is not yet at the level to guarantee an adequate level of security. In order to create conditions for protection, it is first necessary to raise the level of knowledge and exchange experiences about threats with countries that have a built-in system of identification measures and countermeasures. The conclusion is that it is necessary to urgently analyze the situation by organs and institutions independent of political influence, to continue cooperation with external non-governmental and governmental institutions and to take measures to protect the social fabric as soon as possible. Otherwise, the consequences can be far-reaching and dangerous. The term hybrid threats was invented in order to cover a set of illegal actions by persons who for different reasons and motives, take

actions to achieve their intended goals. Some of them deliberately and others spontaneously, thus definitely working to destroy the social system of the state. In such situations, gaps are created in the system, which will gradually and in the long run be fatal for security, economic, political and overall social life.

Such "deformations" will gradually acquire unfathomable proportions and the people will in time understand that the system does not work, will lose faith in the institutions and will eventually demand a change of government, which will have to bear the burden of mistrust in the overall relations. In such situations, the so-called colorful revolutions, coups, sabotage, terrorism and separatism, etc. It is noticeable that there is an increased risk of intensification of hybrid threats when there are important political developments in Macedonia and the reason for their frequency can be regional and global crises of a wider scale.

When facing hybrid threats, negative propaganda, defamation of some of the state and international institutions, as well as distortion of the legitimate interests of the state have been observed in Macedonia. That is why efforts should be made at the state level to increase resistance to such security risks. that directly or indirectly refer to the protection of the critical infrastructure, creation of an efficient strategy for the protection of the critical infrastructure; application of multiple early warning models; successful prevention, which can contribute to risk reduction, which will directly affect the increase in the safety of critical infrastructure; continuous training and training of human resources to deal with attacks on critical infrastructure.

REFERENCES

1. Gerginova, T., (2021). "Need for protection of critical infrastructure" – the paper was published in the Proceedings of the International Scientific Conference on the topic "Harmonization of legal regulations with legal currents (Acquis Communautaire) of the European Union - Situation in Bosnia and Herzegovina and experiences of others in Banja Luka" organized by the Think Tank Banja Luka in cooperation with the Institute for Comparative Law in Belgrade.

2. Gerginova, T., (2022). "National security of the Republic of North Macedonia in a modern global security environment", Paper published in Proceedings of the 13th International Scientific Conference - 45 YEARS HIGHER EDUCATION IN THE AREA OF SECURITY - EDUCATIONAL CHALLENGES AND SECURITY PERSPECTIVES, organized by the Faculty of security, Skopje and the German Friedrich Ebert Stiftung.

3. DIRECTIVE 2008/114/EC - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0013
4. Defense Strategy of the Republic of North Macedonia "Official Gazette No. 75" from March 2020.
5.Flammini, F.,Critical Infrastructure Security: Assessment, Prevention, Detection, Response, 2012.
6.https://www.nato.int/nato-on-the-map
7.https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
8.https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
9. https://www.nato.int/cps/en/natohq/topics_132722.htm
10. https://www.mod.gov.mk/storage/2021/12/Nacionalna-Strategija-za-gradene-otpornost-i-spravuvane-so-hibridni-zakani-april-2021.pdf) accessed on 15.11.2022).

ZAŠTITA KRITIČNE INFRASTRUKTURE OD HIBRIDNIH PRIJETNJI

Prof. dr Tatjana Gerginova
Fakultet bezbjednosti, Skoplje

Apstrakt: Bezbjednost građana, zaštita suvereniteta i teritorijalnog integriteta, principi demokratije i vladavine prava su neki od glavnih pojmova i osnovnih principa savremenog demokratskog društva u svakoj zemlji, pa i u Republici Severnoj Makedoniji. Prevencija opasnosti od hibridnih prijetnji je u osnovi interdisciplinarni, interresorni i dugoročni projekat koji ima za cilj da pomogne u ostvarivanju ciljeva demokratije, pri dobrom upravljanju bezbjednošću i kod ekonomskih prioriteta. Ostvarivanje zaštite kritične infrastrukture jedna je od komponenti nacionalne bezbjednosti. Potreba za postizanjem zaštite kritične infrastrukture povezana je sa potrebom izgradnje otpornosti Republike Severne Makedonije kako bi se efikasno i efektivno suočavala sa hibridnim prijetnjama u cilju postizanja zaštite nacionalnih interesa i stvaranja nacionalne otpornosti društva. Da bi se postigla efikasna zaštita kritične infrastrukture, akcenat treba staviti na sljedeće aspekte: procjenu, otkrivanje, odbacivanje prijetnji i odgovor na prijetnje. Nova era hibridnih prijetnji zahtijeva novu polaznu osnovu za kreiranje promjena u pristupu zaštiti kritične infrastrukture. U radu autor uspostavlja novi pristup zaštiti kritične infrastrukture, a kao prioritete postavlja: donošenje Zakona o zaštiti kritične infrastrukture; kreiranje efikasne strategije za zaštitu kritične

infrastrukture; primjena više modela ranog upozoravanja; uspješna prevencija, koja može doprinijeti smanjenju rizika, što će direktno uticati na povećanje bezbjednosti kritične infrastrukture; kontinuirana obuka i obuka ljudskih resursa za suočavanje sa napadima na kritičnu infrastrukturu.

Ključne riječi: kritična infrastruktura, hibridne prijetnje, procjena, detekcija, odbacivanje prijetnje i odgovor na prijetnje

Pregledni naučni članak

PREVOZ OPASNIH MATERIJA KAO ELEMENT KRITIČNE INFRASTRUKTURE

Dr Ljubinko Mitrović[1]
Vanja Mitrović[2]

Apstrakt: Savremeno društvo je prosto nemoguće zamisliti bez transporta roba, pri čemu je od posebnog značaja bezbjedan prevoz jedne posebne vrste roba - opasnih materija. Opasne materije, na čiju opasnost i sam njihov naziv ukazuje, jesu materije opasne po život građana, zdravlje ljudi, njihovu životnu sredinu, bezbjednost saobraćaja, imovinu, odnosno materijalna dobra pojedinaca, preduzeća i drugih pravnih lica. Prema najvećem broju poznavalaca ove oblasti, pod opasnim materijama podrazumijevaju se eksplozivne materije i predmeti; zbijeni gasovi, gasovi pretvoreni u tečnost i gasovi rastvoreni pod pritiskom; zapaljive tečnosti; zapaljive čvrste materije; materije sklone samopaljenju; materije koje u dodiru sa vodom razvijaju zapaljive gasove; oksidirajuće materije; organski peroksidi; otrovi; zagađujuće i zarazne materije; radioaktivne materije; korozivne, odnosno nagrizajuće materije i ostale opasne materije. Postupanje sa opasnim materijama, upravo zbog njihove opasnosti mora se odvijati u strogo kontrolisanom, standardizovanom i zakonom normiranom procesu.

Upravo o opasnim materijama i posebno eksplozivnim materijama i zapaljivim tečnostima i gasovima i njihovom prevozu u drumskom saobraćaju uopšte i u Republici Srpskoj biće riječi u ovom referatu.

Ključne riječi: drumski prevoz, opasne materije, eksplozivne materije i predmeti, ADR.

UVODNE NAPOMENE

Opasne materije (na čiju opasnost i sam njihov naziv ukazuje), jesu materije opasne po život, zdravlje i imovinu ljudi, bezbjednost saobraćaja,

[1] Ljubinko Mitrović, redovni profesor na Panevropskom univerzitetu APEIRON u Banjoj Luci, naučni saradnik, Banja Luka, *ljubinko58@gmail.com*

[2] Vanja Mitrović, diplomirani pravnik, viši stručni saradnik, Okružni sud u Banjoj Luci, *vmitroviceva85@gmail.com*

materijalna dobra društvene zajednice i sl.. S druge strane, opasnim materijama smatraju se sve one materije koje u toku proizvodnje, transporta, skladištenja ili rukovanja mogu da izazovu posljedice štetne po zdravlje ili čovjekovu okolinu. Stoga je shvatljivo zbog čega je oblast koja se odnosi na promet, držanje, prevoz i promet ovim materijama uopšte i stavljena u isključivu nadležnost države i njenih institucija. To je bio sasvim dovoljan razlog i za zakonodavca u Republici Srpskoj da ovu važnu oblast djelovanja čovjeka uredi posebnim Zakonom o prometu eksplozivnih materija i zapaljivih tečnosti i gasova[3], dok se Zakonom o prevozu opasnih materija Republike Srpske[4] uređuju uslovi pod kojima se u Republici Srpskoj prevoze opasne materije u pojedinim granama saobraćaja (prevoz opasnih materija u drumskom i željezničkom saobraćaju, te saobraćaju na unutrašnjim plovnim putevima), prava i obaveze lica koja učestvuju u prevozu, uslovi koji se tiču ambalaže i vozila, izdavanje odobrenja za prevoz, uslovi za imenovanje savjetnika za bezbjednost, nadležnost i uslovi za osposobljavanje lica koja učestvuju u prevozu, nadležnost ministarstava u vezi s tim prevozom u Republici Srpskoj, te nadzor nad sprovođenjem ovog zakona. Uz ova dva, najvažnija zakona, tu je i niz drugih propisa koji se u većoj ili manjoj mjeri dotiču pitanja koja se odnose na promet, prevoz, čuvanje, držanje i sl. opasnih materija, svakako uz opasku da se prevoz radioaktivnih materija obavlja u skladu sa propisima o radijacijskom i nuklearnom bezbjednosti u BiH.

Kako smo već istakli, opasne materije mogu štetno djelovati na život i zdravlje čovjeka, njegovu životnu sredinu, bezbjednost saobraćaja, imovinu, odnosno materijalna dobra pojedinaca, preduzeća i drugih pravnih lica[5]. Zbog toga je onda sasvim razumljivo da se bilo kakva manipulacija njima, a posebno njihov transport moraju odvijati u strogo kontrolisanom, standardizovanom i zakonom normiranom procesu[6].

---

[3] Službeni glasnik Republike Srpske, br. 78/2011 i 58/2016. Ovim zakonom regulišu se promet, proizvodnja i korišćenje eksplozivnih materija, zapaljivih tečnosti i gasova na teritoriji Republike Srpske.

[4] Službeni glasnik Republike Srpske, broj 15/2016.

[5] Prema statističkim podacima iz 2004. godine u SR Njemačkoj, koja ima izuzetno razvijen transportni sistem, drumski prevoz u ukupnom transportu opasnih materija prelazi preko 50%. Prema istom izvoru, od ukupne količine svih roba u transportu u SR Njemačkoj, oko 18% bile su opasne robe. Ovi podaci potvrđuju dominantnu ulogu drumskog saobraćaja razvijenih zemalja u svijetu, u odnosu na druge vidove prevoza (više u: F. Islamović, H. Kofrc, R. Šahinović, B. Bajrić, Sigurnosni propisi i osiguranje transporta opasnih materija, *Bosna i Hercegovina i Euroatlanske integracije*, Bihać, 2014. godine, str. 793-812.

[6] Lj. Mitrović, *Policijsko pravo – pravo unutrašnjih poslova*, Defendologija centar za bezbjednosna, sociološka i kriminološka istraživanja Banja Luka, Banja Luka, 2008. godine, str. 181-209.

Moguće nepravilnosti u postupanjima sa opasnim materijama su mnogobrojne, počev od faze same proizvodnje materije, ispitivanja njenog kvaliteta, pakovanja, označavanja, stavljanja u promet, kupovine, nabavke, prodaje, transporta, prevoza, istovara, utovara, pretovara, pregleda, uvoza, izvoza, skladištenja, držanja u posjedu, korišćenja i uništenja opasne materije i dr. To su sve i razlozi posebno pažljivog postupanja sa opasnim materijama u skladu sa propisima i tehničkim normativima, odnosno pravilima struke[7].

Upotreba opasnih, posebno eksplozivnih materija je nezamjenjiva za privredu, te bez ozbira na potencijalno štetno dejstvo po okolinu, opasne materije su, pogotovo u pojedinim granama privrede, nezamjenjive u radu, zbog čega se moraju koristiti, a što svakodnevno povlači mogućnost zloupotrebe i potencijalnu havariju, izazvanu kako nestručnim radom i nepažnjom, tako i namjernim subverzivnim ili diverzantskim namjerama[8].

Posebno značajnom čini se sama proizvodnja opasnih, posebno eksplozivnih materija, odnosno proizvodnja na način da se u toku procesa proizvodnje proizvedena materija dobije u skladu sa normama kvaliteta[9].

POJAM I VRSTE OPASNIH MATERIJA

Pod pojmom opasnih materija smatraju se one materije koje mogu ugroziti zdravlje ljudi, izazvati zagađivanje okoline ili nanijeti materijalnu štetu, koje imaju opasna svojstva za ljudsko zdravlje i okolinu, koje su kao takve definisane zakonima, drugim propisima, te međunarodnim ugovorima, koje na osnovu njihove prirode ili svojstava i stanja, a u vezi sa prevozom mogu biti opasne za javnu bezbjednost ili red ili koje imaju dokazane toksične, nagrizajuće, nadražujuće, zapaljive, eksplozivne ili radioaktivne učinke[10]. Opasnim materijama smatraju se i sirovine (repromaterijali) od kojih se proizvode opasne robe i otpadi uz uslov da imaju svojstva opasnih materija[11].

Zakonom o prevozu opasnih materija Republike Srpske, u odredbi člana 8 utvrđeno je koje materije ili predmeti se mogu smatrati opasnim materijama, i to su:

1) klasa 1 – eksplozivne materije i predmeti,
2) klasa 2 –gasovi,

[7] Ibid.
[8] Ibid
[9] Ibid
[10] F. Islamović, H. Kofrc, R. Šahinović, B. Bajrić, Sigurnosni propisi i osiguranje transporta opasnih materija, *Bosna i Hercegovina i Euroatlanske integracije, Bihać*, 2014. godine, str. 793-812.
[11] Ibid.

3) klasa 3 - zapaljive tečne materije,
4) klasa 4.1 - zapaljive čvrste materije, samoreagujuće materije i desenzitizovane eksplozivne čvrste materije,
5) klasa 4.2 - samozapaljive materije,
6) klasa 4.3 - materije koje u dodiru sa vodom razvijaju zapaljive gasove,
7) klasa 5.1 - oksidirajuće materije,
8) klasa 5.2 - organski peroksidi,
9) klasa 6.1 – toksične materije,
10) klasa 6.2 - zarazne materije,
11) klasa 7 - radioaktivne materije,
12) klasa 8 – nagrizajuće (korozivne) materije i
13) klasa 9 – razne opasne materije i predmeti[12].

MEĐUNARODNI DOKUMENTI I STANDARDI U OBLASTI PREVOZA OPASNIH MATERIJA

Određivanje uslova i radnji koje su u vezi sa prevozom opasnih materija vrši se primjenom sljedećih međunarodnih ugovora, i to:

a) na prevoz opasnih materija u drumskom saobraćaju - Evropski sporazum o međunarodnom drumskom prevozu opasnih materija (engl. *European Agreement Concercing the International Carriage of Dangerous Goods by Road* – u daljem tekstu: ADR) sa njegovim sastavnim dijelovima, prilozima A i B i aktom o notifikaciji. Ovaj sporazum je još 1972. godine ratifikovala tadašnja SFRJ. Do sada 41 država je ratifikovala ADR sporazum. Svi potpisnici ovog sporazuma dužni su da prilagode svoje nacionalne propise tako da oni ne smiju biti u suprotnosti sa ADR-om. Iako su pravila propisana ADR-om ista za sve, moguća su izuzeća ili posebna pravila koja će važiti na teritoriji pojedinih zemalja. Ova izuzeća su rijetka, ali ako se procijeni da su opravdana onda se ona unose u sporazum;

b) na prevoz opasnih materija u željezničkom saobraćaju - Prilog C Konvencije o međunarodnom željezničkom prevozu (engl. *Convention*

[12] Prema ADR-u: Klase 1a - Eksplozivne materije; Klase 1b - Predmeti punjeni eksplozivnim materijama; Klase 1c - Sredstva za paljenje, vatrometni predmeti i drugi predmeti; Klase 2 - Zbijeni gasovi, gasovi pretvoreni u tečnost i gasovi rastvoreni pod pritiskom; Klase 3 - Zapaljive tečnosti; Klase 4.1 - Zapaljive čvrste materije; Klase 4.2 - Materije sklone samopaljenju; Klase 4.3 - Materije koje u dodiru sa vodom razvijaju zapaljive gasove; Klase 5.1 - Oksidirajuće materije; Klase 5.2 - Organski peroksidi; Klase 6.1 - Otrovi; Klase 6.2 - Gadne i zarazne materije; Klase 7 - Radioaktivne materije; Klase 8 - Korozivne (nagrizajuće) materije; Klase 9 - Ostale opasne materije.

concerning International Carriage by Rail - COTIF), odnosno Pravilnik o međunarodnom željezničkom prevozu opasnih materija (engl. *Regulation concerning the International Carriage of Dangerous Goods by Rail* – u daljem tekstu: RID);

c) na prevoz opasnih materija na unutrašnjim plovnim putevima - Evropski sporazum o međunarodnom prevozu opasnih materija unutrašnjim plovnim putevima (engl. *European Agreement Concerning the International Carriage of Dangerous Goods by Inland Waterways* – u daljem tekstu: ADN), uključujući odgovarajuće anekse, te izmjene i dopune[13];

d) na prevoz opasnih materija u pomorskom saobraćaju - Međunarodna konvencija za zaštitu života na moru, sa pripadajućim izmjenama i dopunama i prema potrebi, i sljedeći međunarodni akti, i to: Međunarodni pomorski kodeks za opasne materije, sa pripadajućim izmjenama i dopunama (svi brodovi bez obzira na vrstu i veličinu); Međunarodni kodeks za bezbjednosne procedure za prevoz opasnih materija u rasutom stanju, sa pripadajućim izmjenama i dopunama; Međunarodni kodeks za gradnju i opremanje brodova za prevoz ukapljenih gasova sa pripadajućim izmjenama i dopunama; Međunarodni kodeks za gradnju i opremanje brodova za prevoz opasnih hemikalija u rasutom stanju, sa pripadajućim izmjenama i dopunama; Kodeks za gradnju i opremanje brodova za prevoz opasnih hemikalija u rasutom stanju, sa pripadajućim izmjenama i dopunama; Međunarodni kodeks za siguran prevoz brodovima pakiranog osiromašenog nuklearnog goriva, plutonija i visokoradioaktivnih otpada, sa pripadajućim izmjenama i dopunama; Međunarodna konvencija o sprečavanju zagađenja koja uzrokuju brodovi, izmijenjena Protokolom iz 1978. godine, sa pripadajućim izmjenama i dopunama;

e) na prevoz opasnih materija vazdušnim putem - Aneks 18 Konvencije o međunarodnom civilnom vazduhoplovstvu; Tehničke instrukcije Međunarodne organizacije za civilno vazduhoplovstvo za bezbjedan transport opasnih materija vazdušnim putem sa izmjenama i dopunama; Uputstvo za postupanje u slučaju opasnosti za avionske nezgode koje su povezane sa opasnim materijama, IATA *Dangerous Goods Regulations* (IATA Trening knjigama i regulativom) i dr.;

f) na prevoz opasnih materija u poštanskom saobraćaju – primjenjuju se propisi Svjetskog poštanskog saveza.

Cilj ovih propisa, ali i domaćih zakona i podzakonskih akata jeste da omoguće bezbjedan prevoz opasnih materija i da minimaliziraju rizik nesreće, koja je povezana sa narušavanjem zdravlja ljudi ili zagađenjem životne sredine, primjenom opštih tehnika i organizacionih pravila za pakovanje, prevoz i manipulaciju opasnim materijama.

[13] Član 4 Zakona o prevozu opasnih materija.

Pakovanje

Ambalaža u kojoj se prevoze opasne materije mora da obezbjeđuje potpunu zaštitu života i zdravlja ljudi, kao i zaštitu životne sredine prilikom prevoza opasnih materija i rukovanja opasnim materijama, tačnije ona mora da bude zatvorena, nepropusna, čvrsta, jaka sa adekvatnim zatvaračem tako da prilikom prevoza sprečava eventualno prosipanje ili uništenje opasne materije[14].

Prema zakonskom rješenju, za prevoz opasnih materija upotrebljava se ambalaža:

1) koja prema kvalitetu i izradi odgovara količini i specifičnosti opasnih materija koje se u njoj prevoze,
2) u kojoj je u skladu sa odredbama međunarodnih ugovora dopušten prevoz opasnih materija,
3) koja je provjerena i odobrena u skladu sa odredbama međunarodnih ugovora i
4) koja ima znakove upozorenja, natpise, oznake i listice za označavanje opasnosti, te druge podatke o opasnim materijama i ambalaži u skladu sa odredbama međunarodnih ugovora[15].

Označavanje ambalaže vrši njen proizvođač, u skladu sa međunarodnim ugovorima. Isto tako, proizvođač ambalaže ima obavezu pribavljanja odobrenja za ambalažu. Sličnu obavezu ima i učesnik u prevozu opasnih materija koji, u svakom slučaju koristi ambalažu koja je u skladu sa međunarodnim ugovorima i drugim propisima, s tim da se radi o ambalaži koja ima prethodno pomenuto odobrenje i oznaku.

Obaveze učesnika u prevozu

U posebnom poglavlju zakona propisane su obaveze učesnika u prevozu opasnih materija ponaosob (preventivne mjere bezbjednosti i postupak u slučaju nezgode), i to: pošiljalaca, organizatora prevoza, pakiralaca, punilaca, vlasnika ili korisnika teretnog prostora, utovarilaca, prevoznika i primalaca opasnih materija.

Generalna je obaveza svih učesnika u prevozu opasnih materija da preduzimaju sve potrebne mjere kako bi se spriječila nezgoda, odnosno kako bi se u najvećoj mogućoj mjeri umanjile eventualne posljedice nezgode. Takođe,

[14] Lj. Mitrović, M. Jokić, *Pravo unutrašnjih poslova,* Visoka škola unutrašnjih poslova Banja Luka, Banja Luka, 2015. godine, str. 187-200.
[15] Član 11 Zakona o prevozu opasnih materija Republike Srpske.

važna obaveza svih učesnika u prevozu opasnih materija jeste da u slučaju opasnosti, odnosno nezgode, odmah obavještavaju najbližu policijsku stanicu o tome, te prilažu potrebne podatke radi preduzimanja adekvatnih mjera. Uz to, za slučaj nezgode, a sve u skladu sa međunarodnim ugovorima, prevoznik, savjetnik za bezbjednost ili organizator prevoza dostavljaju izvještaj o nezgodi u što kraćem roku, a ne dužem od 30 dana, nadležnoj organizacionoj jedinici Ministarstva unutrašnjih poslova.

I na kraju, prevoznik, pošiljalac, primalac i organizator prevoza sarađuju međusobno, ali i sa ovlašćenim licama nadležnih državnih organa svakako s ciljem preduzimanja odgovarajućih bezbjednosnih i preventivnih mjera, te postupanja prilikom nastanka nezgode[16].

Odobrenje za prevoz eksplozivnih materija

Prevoz eksplozivnih materija[17] posebno je regulisan Zakonom o prevozu opasnih materija i za njega je neophodno posjedovati odobrenje. Zahtjev za izdavanje odobrenja za prevoz eksplozivnih materija podnose pošiljalac, uvoznik, organizator prevoza, primalac ili kupac eksplozivne materije. Ovaj zahtjev obavezno sadrži: podatke o proizvođaču, pošiljaocu, prevozniku i primaocu i kontakt telefone; UN brojeve opasnih materija i naziv u skladu sa međunarodnim ugovorima; podatke o vrsti, tehničkom nazivu, količini i načinu pakovanja eksplozivne materije; određivanje pravca kretanja (itinerara); podatke o mjestu utovara i istovara; datum i približan čas otpočinjanja prevoza; podatke o vozilu i vozaču za prevoz opasnih materija u drumskom saobraćaju (broj ADR certifikata za vozača i vozilo i rok važenja) i podatke o savjetniku za bezbjednost i kontakt telefon; odobrenje nadležnog organa susjedne države kojim se odobrava uvoz ili tranzit; odobrenje za uvoz/izvoz eksplozivnih materija izdato od Ministarstva spoljne trgovine i ekonomskih odnosa Bosne i Hercegovine (ukoliko se radi o prevozu preko granice); podatke da je eksplozivna materija stavljena u promet u skladu sa propisima o prometu eksplozivnih materija i zapaljivih tečnosti i gasova i odobrenje za nabavku eksplozivnih materija.

Odobrenje za prevoz eksplozivnih materija u unutrašnjem saobraćaju izdaje centar javne bezbjednosti, odnosno stanica javne bezbjednosti Ministarstva sa čijeg područja se upućuje eksplozivna materija, a u međunarodnom saobraćaju nadležna organizaciona jedinica Ministarstva u

[16] Član 18 Zakona o prevozu opasnih materija Republike Srpske.

[17] Eksplozivne materije u smislu Zakona o prometu eksplozivnih materija i zapaljivih tečnosti i gasova Republike Srpske su: a) privredni eksplozivi, b) sredstva za iniciranje eksplozivnih materija, c) pirotehnička sredstva, d) municija, e) baruti i f) proizvodi punjeni eksplozivnim materijama.

sjedištu. Izdato odobrenje za prevoz u unutrašnjem saobraćaju važi i za povrat preostalih količina eksplozivnih materija, uz najavu povrata policijskoj stanici na čijem području su eksplozivne materije upotrebljavane. Ukoliko je ugovoren uvoz ili izvoz veće količine eksplozivnih materija koje ne mogu da se prevezu preko granice Bosne i Hercegovine i teritorije Republike Srpske jednim prevoznim sredstvom, ni sa više prevoznih sredstava istovremeno, odobrenje za prevoz izdaje se za cijelu količinu eksplozivnih materija i u tom slučaju prevoz cijele količine eksplozivnih materija izvršava se preko istog graničnog prelaza i u roku ne dužem od dva mjeseca[18].

Nadležna organizaciona jedinica Ministarstva unutrašnjih poslova Republike Srpske koja izdaje odobrenje za prevoz eksplozivnih materija može, po potrebi, da naredi preduzimanje i posebnih mjera bezbjednosti prilikom prevoza određene eksplozivne materije (pravac kretanja, pratnja pošiljaoca ili prevoznika, pratnja pripadnika policije i dr.), s tim da troškove posebnih mjera bezbjednosti plaćaju pošiljalac ili primalac eksplozivne materije (pri uvozu, izvozu ili tranzitu troškove plaća prevoznik ili primalac). Slične, posebne mjere bezbjednosti mogu se narediti i prilikom prevoza ostalih opasnih materija, prije svega otrova i radioaktivnih materija.

Zakonom su propisane posebne mjere bezbjednosti za prevoz opasnih materija u drumskom saobraćaju (a i za prevoz ovih materija u željezničkom saobraćaju, prevoz na unutrašnjim plovnim putevima i prenos u poštanskom saobraćaju). Pored ovih mjera, na prevoz opasnih materija primjenjuju se i odredbe Evropskog sporazuma o međunarodnom drumskom prevozu opasnih materija (ADR). Radi se o sljedećim mjerama koje se odnose na vozilo i vozača, odnosno posadu vozila, i to: u motornom vozilu kojim se prevoze opasne materije smiju se nalaziti vozač, suvozač i pratioci; suvozač se mora nalaziti u vozilu u slučajevima predviđenim odredbama ADR; u vozilu se ne smiju držati materije koje mogu izazvati požar; pušenje cigareta u kabini vozila, u pravilu, nije dozvoljeno; ne smiju se vršiti popravke na vozilu koje mogu izazvati varničenje usljed kojeg može doći do požara ili eksplozije; vozač je dužan da vozilom upravlja sa posebnim oprezom; brzina kretanja vozila ne smije biti veća od 70 km na čas (za otrove do 60 km na čas); vozač se ne smije za vrijeme prevoza udaljavati od vozila; o svakom udesu, nezgodi ili kvaru koji ne može sam otkloniti, vozač je dužan odmah obavijestiti najbližu policijsku stanicu; prevoz opasnih materija motornim vozilom može se vršiti samo na putevima koji su određeni za takvu vrstu vozila; motorna vozila koja prevoze

[18] Član 28 Zakona o prevozu opasnih materija Republike Srpske.

opasne materije mogu se zaustavljati i parkirati samo na mjestima određenim i obilježenim za to i dr..[19]

POSEBNE OBAVEZE UČESNIKA U PREVOZU OPASNIH MATERIJA U DRUMSKOM SAOBRAĆAJU

Kao jedan od učesnika u prevozu opasnih materija, prevoznik ima dvije važne obaveze, i to: 1. da osigura vozilo za prevoz opasnih materija od odgovornosti za štetu prouzrokovanu trećim licima i 2. da prevoz opasnih materija povjeri vozaču koji je stručno osposobljen za prevoz opasnih materija[20]. S druge strane, pošiljalac koji predaje opasne materije na prevoz u drumskom saobraćaju ima sljedeće obaveze, i to: 1) upoznaje prevoznika sa propisanim označavanjem vozila, 2) upoznaje prevoznika sa opasnim materijama, 3) označava pakovanja znakovima upozorenja, natpisima, oznakama i listicama za označavanje opasnosti i 4) ispunjava i druge uslove za prevoz u skladu sa međunarodnim ugovorima[21].

Opasne materije mogu da prevoze samo ona lica koja su za rukovanje i prevoz opasnih materija stručno osposobljena, ali i koja su napunila 21 godinu života. Uz navedeno, vozač koji obavlja prevoz opasne materije mora da: 1) posjeduje ispravu o stručnoj osposobljenosti za prevoz opasnih materija u skladu sa međunarodnim ugovorima, 2) posjeduje dokaz o osiguranju od odgovornosti za štetu prouzrokovanu trećim licama[22], 3) posjeduje isprave i

---

[19] Lj. Mitrović, *Policijsko pravo – pravo unutrašnjih poslova*, Defendologija centar za bezbjednosna, sociološka i kriminološka istraživanja Banja Luka, Banja Luka, 2008. godine, str. 181-209.

[20] U skladu sa odredbama člana 43 Zakona o prevozu opasnih materija i Pravilnikom o stručnom osposobljavanju vozača motornih vozila za prevoz opasnih materija i drugih lica koja učestvuju u prevozu opasnih materija vozači vozila u kojima se prevoze opasne materije moraju imati ispravu koju je izdalo nadležno tijelo (ADR certifikat), kojom se potvrđuje da su pohađali obuku i položili ispit o posebnim uslovima koje je potrebno zadovoljiti u prevozu opasnih materija (više u: E. Festić, A. Imamović, Značaj edukacije i opšti uslovi za bezbjedan transport opasnih materija prema ADR-u, *Zaštita i sigurnost*, godina 1., broj 2).

[21] Član 39 Zakona o prevozu opasnih materija.

[22] Ovo osiguranje je namijenjeno, prije svega, svim pravnim osobama koje imaju zakonsku obavezu da pribave policu osiguranja odgovornosti za štete koje mogu nastati u prijevozu opasnih materija. Osigurava se odgovornost vlasnika ili nosioca prava korištenja na robi koja ima svojstvo opasne materije za štete koje mogu da nastanu trećim osobama u toku prijevoza opasnih materija, a koje za posljedicu imaju smrt, povredu tijela ili zdravlja, oštećenja stvari i imovine ili zagađenje životne sredine, a u skladu sa odredbama Zakona o obligacionim odnosima Federacije BiH, zakonima koji regulišu ovu materiju i Uredbom o prijevozu štetnih i opasnih materija. Osiguravajuća zaštita se pruža od štetnih posljedica eksplozije, naglog širenja štetnih gasova, iscurenja opasne materije, oštećenja prouzrokovanih termičkim ili hemijskim

dodatnu opremu u skladu sa međunarodnim ugovorima, 4) je upoznat sa obavezama i specifičnostima prevoza, 5) obezbijedi da vozilo, opasne materije i teret odgovaraju propisima, 6) obezbijedi da su pakovanja i vozilo označeni odgovarajućim znakovima upozorenja, natpisima, oznakama i listicama za označavanje opasnosti, te drugim informacijama o opasnim materijama i vozilu u skladu sa međunarodnim ugovorima i 7) vodi računa su ispunjeni drugi uslovi za prevoz u skladu sa međunarodnim ugovorima.

Prevoz opasnih materija obavljaju vozila koja:

1) su proizvedena i opremljena u skladu sa međunarodnim ugovorima,
2) imaju certifikat o ispravnosti vozila za prevoz određenih opasnih materija, ako je to određeno međunarodnim ugovorima, i
3) označena su u skladu sa međunarodnim ugovorima[23].

Ministar saobraćaja i veza, uz saglasnost ministra, ministra za prostorno uređenje, građevinarstvo i ekologiju, ministra poljoprivrede, šumarstva i vodoprivrede, ministra industrije, energetike i rudarstva i ministra zdravlja i socijalne zaštite, donosi rješenje kojim određuje dozvoljena parking mjesta za vozila koja prevoze opasne materije i uslove koje ta mjesta ispunjavaju, kao i ograničenja za prevoz opasnih materija na javnim putevima. I na kraju, minister unutrašnjih poslova, uz saglasnost ministra saobraćaja i veza i ministra zdravlja i socijalne zaštite, donosi pravilnik o načinu prevoza opasnih materija u drumskom saobraćaju[24].

Izdavanju certifikata o ispravnosti vozila za prevoz određenih opasnih materija[25] prethodi pregled ispravnosti vozila i obrada dokumentacije na osnovu

---

dejstvom spolja na prijevoznom sredstvu i ostalih nekontrolisanih i neočekivanih događaja koji dovode do zagađenja životne okoline. Također, osiguranje pokriva rizik kod utovara, prijevoza, usputne manipulacije i istovara opasnih materija (*supra*). Nezaobilazno je spominjanje nuklearnih i hemijskih udesa u transportu do kojih može doći u željezničkom, cestovnom, vodenom (riječnom, pomorskom, prekookeanskom) i zračnom transportu, kao i cjevovodima (pneumatskom transportu kapsulama), više u: F. Islamović, H. Kofrc, R. Šahinović, B. Bajrić, Sigurnosni propisi i osiguranje transporta opasnih materija, *Bosna i Hercegovina i Euroatlanske integracije*, Bihać, 2014. godine, str. 793-812.

[23] Član 16 Zakona o prevozu opasnih materija.

[24] Pravilnik o načinu prevoza opasnih materija u drumskom saobraćaju, Službeni glasnik Republike Srpske, broj 7/2017.

[25] Prema ADR-u, sva vozila koja prevoze opasne materije moraju da budu posebno označena. Za to se koriste dvije vrste oznaka, i to listice opasnosti i table za obilježavanje vozila, čije su dimenzije i izgled određeni pravilima ADR-a. Listica ima oblik nagnutog kvadrata i na njoj je simbolima prikazana vrsta i stepen opasnosti. Tabla za obilježavanje je narandžasta, sa crnim okvirom i horizontalno je podijeljena na dva polja. U gornjem polju se sa dvije ili tri cifre obilježavaju vrste opasnosti, a u donjem polju je numerička oznaka materije prema nomenklaturi ADR-a. Na osnovu podataka sa table, stručne ekipe u slučaju, prije svega saobraćajne nesreće znaju kako treba da postupaju, zbog čega tabla mora biti napravljena od materijala sa koga se podaci mogu pročitati i ako je tabla bila 15 minuta u plamenu. Za

koje se certifikat izdaje, a ove radnje obavlja pravno lice koje ovlasti Ministarstvo saobraćaja i veza. Pravilnik o postupku i mjestu pregleda vozila za prevoz opasnih materija, izdavanje i izgled certifikata, u skladu sa međunarodnim ugovorima, kao i uslove koje ispunjava pravno lice koje ove poslove obavlja donosi ministar saobraćaja i veza. Inače, vozila za prevoz opasnih materija su motorna ili priključna vozila specijalno opremljena za prevoz određenih opasnih materija u drumskom saobraćaju[26]. Prema propisima za dobijanje certifikata o ispravnosti, vozila za prevoz opasnih materija moraju ispunjavati odgovarajuće zahtjeve ADR-a i Zakona o prevozu opasnih materija. Takođe treba dodati i veliki broj podzakonskih akata koji su neizbježni u Bosni i Hercegovini, a odnose se na zaštitu od statičkog elektriciteta, jednokratno ispitivanje motornih i priključnih vozila, standarde za izgradnju cisterni za nadogradnju vozila i sl..[27]

INSPEKCIJSKI NADZOR

Nadzor nad sprovođenjem Zakona o prevozu opasnih materija i podzakonskih akata donesenih na osnovu tog zakona u okviru svoje nadležnosti sprovode Ministarstvo saobraćaja i veza Republike Srpske i Ministarstvo unutrašnjih poslova Republike Srpske. S druge strane, inspekcijski nadzor nad sprovođenjem Zakona o prevozu opasnih materija neposredno vrši nadležna

---

obilježavanje opasnih materija postoje i oznake koje se stavljaju na ambalažu da bi se na taj način skrenula pažnju na opasnosti pri rukovanju. Ove oznake ne treba miješati sa oznakama za vozila, odnosno ne treba ih koristiti za obilježavanje vozila koja transportuju opasne materije. U gornjem dijelu table upisana je oznaka vrste opasnosti, i to korišćenjem brojeva klasa opasnih materija. Oznaka ima dvije ili tri cifre. Prva cifra označava osnovnu opasnost, a druga i treća dodatne opasnosti. Treća cifra nije obavezna, a ako nema nijedne dodatne opasnosti, na drugo mjesto se upisuje nula. Ako je opasnost jako izražena, upisane su dvije iste cifre. U donjem dijelu table je takozvani UN broj, tj. broj koji označava koja se opasna materija prevozi (više u: Lj. Mitrović, *Policijsko pravo – pravo unutrašnjih poslova*, Defendologija centar za bezbjednosna, sociološka i kriminološka istraživanja Banja Luka, Banja Luka, 2008. godine, str. 181-209).

[26] Opasne materije mogu se prevoziti isključivo prevoznim sredstvima koja su proizvedena i opremljena u skladu sa međunarodnim standardima. Ova vozila moraju posjedovati važeći certifikat za prevoz opasnih materija, te biti označena znakovima upozorenja, natpisima, oznakama, listicama za označavanje opasnosti i drugim podacima o opasnim materijama i vozilu, sve u skladu sa odredbama odgovarajućih međunarodnih standarda (više u: Lj. Mitrović, *Policijsko pravo – pravo unutrašnjih poslova*, Defendologija centar za bezbjednosna, sociološka i kriminološka istraživanja Banja Luka, Banja Luka, 2008. godine, str. 181-209).

[27] H. Prcanović, E. Festić, D. Agić, Organizacija inspekcije vozila za prevoz opasnih materija prema standardu BAS ISO/IEC 17020, 7. Naučno-stručni skup sa međunarodnim učešćem "KVALITET 2011", Neum, 1-4. juni 2011. godine.

organizaciona jedinica Ministarstva unutrašnjih poslova Republike Srpske i Republička uprava za inspekcijske poslove.

Nadzor nad prevozom opasnih materija sprovode inspektori za eksplozivne materije i poslove zaštite od požara u nadležnim organizacionim jedinicama Ministarstva unutrašnjih poslova Republike Srpske za klasu 1, a nadležni inspektori Republičke uprave za inspekcijske poslove za klase 2, 3, 4.1, 4.2, 4.3, 5.1, 5.2, 6.1, 6.2, 8 i 9.

Inspektori za eksplozivne materije i poslove zaštite od požara prilikom inspekcijskog nadzora mogu vršiti pregled prostorija, radilišta i uređaja preduzeća, drugih pravnih lica i preduzetnika ili pojedinaca, te prikupljati obavještenja i preduzimati druge radnje potrebne za utvrđivanje primjene propisanih bezbjednosnih mjera i tehničkih normativa[28]. Isto tako, inspektori za eksplozivne materije i poslove zaštite od požara mogu, a radi sprečavanja izbijanja i širenja požara, odnosno nastanka eksplozije narediti preduzimanje sljedećih mjera, i to:

1. narediti da se utvrđene nepravilnosti otklone i odrediti rok za njihovo otklanjanje,
2. zabraniti upotrebu ambalaže za prevoz, ako ambalaža nije u skladu sa međunarodnim ugovorima,
3. zabraniti dalji prevoz ili rukovanje opasnim materijama licima koja nisu stručno osposobljena za prevoz i rukovanje opasnim materijama,
4. zabraniti dalji prevoz vozilima koja ne posjeduju certifikat o ispravnosti vozila za prevoz određenih opasnih materija, izuzev ako vozila prema međunarodnim sporazumima ne treba da posjeduju certifikat,
5. privremeno zabraniti vršenje pojedinih radnji u vezi sa prevozom koje se odnose na pripreme za prevoz, utovar, pretovar i istovar opasnih materija, ako u pogledu mjesta ili vremena za obavljanje tih radnji nisu ispunjeni propisani uslovi,
6. zabraniti pravnom ili fizičkom licu prevoz opasne materije ako utvrde da su u toku pripreme za prevoz ili u toku prevoza učinjeni teži propusti u pogledu preduzimanja mjera bezbjednosti i
7. naložiti preduzimanje odgovarajućih mjera zbog kršenja međunarodnih ugovora, u zavisnosti od kategorije povrede odredaba o prevozu opasnih materija[29].

[28] Član 72 Zakona o prometu eksplozivnih materija i zapaljivih tečnosti i gasova.
[29] Član 60 Zakona o prevozu opasnih materija.

Ministarstvo za saobraćaj i veze Republike Srpske određuje puteve kojima se moraju kretati motorna vozila kojima se prevoze eksplozivne materije i zapaljive tečnosti i gasovi i mjesta za parkiranje tih motornih vozila.

SAVJETNIK ZA BEZBJEDNOST

Zakonom o prevozu opasnih materija propisana je jedna posebna, specifična obaveza svih pravnih, odnosno fizičkih lica sa sjedištem, odnosno prebivalištem u Republici Srpskoj čija registrovana djelatnost obuhvata prevoz opasnih materija drumskim saobraćajem, željeznicom ili unutrašnjim plovnim putevima. Naime, sva ova pravna, odnosno fizička lica čija djelatnost obuhvata prevoz opasnih materija u saobraćaju, te druge radnje u vezi sa navedenim prevozom, kao npr. pakovanje, utovar, istovar, punjenje, pražnjenje, moraju imati najmanje jednog savjetnika za bezbjednost prevoza opasnih materija, s tim da podatke o savjetnicima ova pravna lica dostavljaju Ministarstvu saobraćaja i veza Republike Srpske najkasnije 15 dana od dana imenovanja, kao i podatke o eventualnim izmjenama.

Savjetnik za bezbjednost je fizičko lice čiji je zadatak sprečavanje rizika prilikom prevoza opasnih materija, njegovih posljedica na lica, imovinu i životnu sredinu.

Poslove savjetnika za bezbjednost prevoza opasnih materija može obavljati lice koje je u stalnom radnom odnosu u pravnom licu ili kod fizičkog lica (preduzetnika) i koje obavlja i druge poslove, odnosno lice koje nije zaposleno u pravnom licu ili kod fizičkog lica, s tim da posjeduje certifikat o stručnoj osposobljenosti za obavljanje ovih poslova.

Pravilnik kojim propisuje uslove koje moraju da ispunjavaju javne ustanove koje se bave stručnim osposobljavanjem savjetnika, način i postupak stručnog osposobljavanja savjetnika, izgled i rok važenja certifikata o stručnoj osposobljenosti savjetnika za bezbjednost, kriterijume za izbor članova ispitne komisije, broj članova, način sprovođenja ispita i visinu naknade[30], svakako sve u skladu sa direktivama Evropske unije, donosi ministar saobraćaja i veza.[31] Inače, stručno osposobljavanje savjetnika obavljaju javne ustanove prema planu i programu stručnog osposobljavanja savjetnika koje je rješenjem ovlastio ministar saobraćaja i veza. Provjeru znanja savjetnika i izdavanje certifikata o stručnoj osposobljenosti za prevoz opasnih materija, u skladu sa međunarodnim ugovorima, obavlja Ministarstvo saobraćaja i veza. Za utvrđivanje stručne

[30] Pravilnik o stručnom osposobljavanju savjetnika za bezbjednost i uslovima koje moraju ispunjavati ustanove koje vrše stručno osposobljavanje savjetnika za bezbjednost, Službeni glasnik Republike Srpske, broj 82/2016.

[31] Član 36 stav 3 Zakona o prevozu opasnih materija Republike Srpske.

osposobljenosti savjetnika plaća se naknada, a članovi ispitne komisije imaju pravo na naknadu za svoj rad.

Savjetnik za bezbjednost obavlja sljedeće poslove, i to:

a) prati i primjenjuje propise iz oblasti prevoza opasnih materija,
b) vrši nadzor nad rukovanjem opasnim materijama u pravnom licu ili kod fizičkog lica u skladu sa propisima kojima se uređuje prevoz opasnih materija,
c) savjetuje odgovorns lica u pravnom licu ili kod fizičkog lica,
d) savjetuje lica koja učestvuju u prevozu opasnih materija u pravnom licu ili kod fizičkog lica,
e) nadgleda i prati stručno osposobljavanje lica u pravnom licu ili kod fizičkog lica koja učestvuju u prevozu opasnih materija, te vodi evidencije o njihovom osposobljavanju,
f) sprovodi odgovarajuće mjere radi sprečavanja nezgoda, odnosno težih kršenja propisa,
g) nalaže i preduzima odgovarajuće mjere u slučaju nezgode i
h) izrađuje godišnji izvještaj i obavlja druge poslove u vezi sa prevozom opasnih materija[32].

Važnu novinu u zakonodavstvu Republike Srpske iz 2016. godine predstavlja i odredba člana 37 Zakona o prevozu opasnih materija koja predviđa stručnu obuku lica koja učestvuju u prevozu opasnih materija, odnosno eksplozivnih materija, zapaljivih tečnosti i gasova (u skladu sa propisima o prometu eksplozivnih materija, zapaljivih tečnosti i gasova). Ova obuka se obavlja u skladu sa posebnim pravilnikom koji donosi ministar rada i boračko-invalidske zaštite i istim se propisuju način i postupak stručnog osposobljavanja lica koja učestvuju u prevozu opasnih materija, odnosno pri pakovanju, utovaru, istovaru, punjenju i pražnjenju koje je u vezi sa tim prevozom, uslovi koje ispunjavaju ustanove koje vrše stručno osposobljavanje, te sadržaj i rok važenja potvrde o stručnoj osposobljenosti[33].

Stručno osposobljen za prevoz opasnih materija mora da bude i vozač vozila za prevoz opasnih materija[34]. Stručno osposobljavanje vozača, u skladu sa međunarodnim ugovorima obavlja pravno lice koje pribavi ovlaštenje ministra unutrašnjih poslova. S druge strane, provjeru stručne osposobljenosti vozača obavlja Ministarstvo unutrašnjih poslova, a o položenom stručnom ispitu Ministarstvo izdaje posebnu potvrdu.

---

[32] Član 35 Zakona o prevozu opasnih materija Republike Srpske.

[33] Pravilnik o stručnom osposobljavanju vozača motornih vozila za prevoz opasnih materija i drugih lica koja učestvuju u prevozu opasnih materija, Službeni glasnik Republike Srpske, broj 115/2016.

[34] Član 43 Zakona o prevozu opasnih materija Republike Srpske.

POSEBNE MJERE BEZBJEDNOSTI PRILIKOM PREVOZA EKSPLOZIVNIH MATERIJA KOJE MOŽE ODREDITI MINISTARSTVO UNUTRAŠNJIH POSLOVA REPUBLIKE SRPSKE

Radi se o sljedećim mjerama:

a) određivanje obaveznog pravca kretanja;
b) tehnička pratnja pošiljaoca ili prevoznika;
c) pratnja stručnog lica za rukovanje opasnom materijom koja se prevozi;
d) neprekidno trajanje prevoza bez zaustavljanja;
e) kretanje u koloni (kada se kreće više vozila natovarenih opasnim materijama);
f) određivanje vremena polaska vozila sa polazišta;
g) određivanje vremenskog termina za kretanje vozila na određenim dijelovima puta;
h) određivanje pratnje radnika organa unutrašnjih poslova, i
i) ograničenje prevoza zbog vremenskih uslova[35].

Policijska uprava ili policijska stanica, odnosno nadležna organizaciona jedinica Ministarstva unutrašnjih poslova Republike Srpske u mjestu iz kojeg se upućuje eksplozivna materija, u odobrenju za prevoz eksplozivnih materija u unutrašnjem saobraćaju, koje daje uz neophodne konsultacije sa organizacionom jedinicom za eksplozivne materije i poslove zaštite od požara iz policijske uprave može pošiljaocu odrediti jednu ili više posebnih mjera u zavisnosti od:

1) procjene bezbjednosne situacije u opštini i šire;
2) vrste eksplozivnih materija;
3) osjetljivosti na spoljne uticaje (toplotne, mehaničke, eksplozivne i električne impulse) i razorne moći (brizantni i visoko brizantni eksplozivi) koja zavisi od hemijske strukture i fizičkih osobina eksploziva;
4) količine materije;
5) vrste prevoznog sredstva;
6) bezbjednosti smještenog tereta;
7) opasnosti koja može nastupiti usljed rasipanja tereta;
8) bezbjednosti određenog putnog pravca;
9) uticaja vremenskog faktora na bezbjednost (godišnje doba, doba dana, elementarne nepogode i dr.) i

[35] Lj. Mitrović, M. Jokić, *Pravo unutrašnjih poslova,* Visoka škola unutrašnjih poslova Banja Luka, Banja Luka, 2015. godine, str. 187-200.

10) drugih momenata od značaja za bezbjednost u drumskom saobraćaju[36].

Isto tako, policijska uprava ili policijska stanica, odnosno nadležna organizaciona jedinica Ministarstva unutrašnjih poslova Republike Srpske, može narediti da se više posebnih mjera preduzme istovremeno.

LITERATURA

1. Festić, E., Imamović, A., Značaj edukacije i opšti uslovi za bezbjedan transport opasnih materija prema ADR-u, *Zaštita i sigurnost*, godina 1., broj 2.
2. Islamović, F., Kofrc, H., Šahinović, R., Bajrić, B., Sigurnosni propisi i osiguranje transporta opasnih materija, *Bosna i Hercegovina i Euroatlanske integracije*, Pravni fakultet Univerziteta u Bihaću i Centar za društvena istraživanja Internacionalnog Burč univerziteta, Bihać, 2014. godine.
3. Mitrović, Lj., *Policijsko pravo – pravo unutrašnjih poslova*, Defendologija centar za bezbjednosna, sociološka i kriminološka istraživanja Banja Luka, Banja Luka, 2008. godine.
4. Mitrović, Lj., Jokić, M., *Pravo unutrašnjih poslova,* Visoka škola unutrašnjih poslova Banja Luka, Banja Luka, 2015. godine.
5. Prcanović, H., Festić, E., Agić, D., Organizacija inspekcije vozila za prevoz opasnih materija prema standardu BAS ISO/IEC 17020, 7. Naučno-stručni skup sa međunarodnim učešćem *"KVALITET 2011"*, Neum, 1-4. juni 2011. godine.
6. Zakon o prometu eksplozivnih materija i zapaljivih tečnosti i gasova, Službeni glasnik Republike Srpske, br. 78/2011 i 58/2016.
7. Zakon o prevozu opasnih materija Republike Srpske, Službeni glasnik Republike Srpske, broj 15/2016.
8. Pravilnik o načinu prevoza opasnih materija u drumskom saobraćaju, Službeni glasnik Republike Srpske, broj 7/2017.
9. Pravilnik o povredama odredaba o prevozu opasnih materija, Službeni glasnik Republike Srpske, broj 7/2017.
10. Pravilnik o stručnom osposobljavanju savjetnika za bezbjednost i uslovima koje moraju ispunjavati ustanove koje vrše stručno osposobljavanje savjetnika za bezbjednost, Službeni glasnik Republike Srpske, broj 82/2016.

[36] Lj. Mitrović, M. Jokić, *Pravo unutrašnjih poslova,* Visoka škola unutrašnjih poslova Banja Luka, Banja Luka, 2015. godine, str. 187-200.

11. Pravilnik o stručnom osposobljavanju vozača motornih vozila za prevoz opasnih materija i drugih lica koja učestvuju u prevozu opasnih materija, Službeni glasnik Republike Srpske, broj 115/2016.

TRANSPORT OF HAZARDOUS MATERIALS AS AN ELEMENT OF CRITICAL INFRASTRUCTURE

Full prof. Ljubinko Mitrović, PhD
Vanja Mitrović

Abstract: The modern society simply cannot be perceived without the transport of goods with particular importance being placed on the safe transport of a special type of goods - hazardous materials. Hazardous substances, whose danger is indicated by their name, are substances dangerous to the life of citizens, their health and environment, traffic safety, the people's property, that is, material goods of individuals, companies and other legal entities. According to the largest number of experts in this field, hazardous substances are considered to be: explosive substances and objects; compressed gases, liquefied gases and gases dissolved under pressure; flammable liquids; flammable solids; substances prone to spontaneous combustion; substances that develop flammable gases in contact with water; oxidizing substances; organic peroxides; poisons; polluting and infectious substances; radioactive substances; corrosive, i.e. caustic substances and other dangerous substances. Hazardous substances, due to their dangerous nature, need to be treated in a strictly controlled, standardized and legally regulated process.

This paper is about hazardous substances, especially explosive substances and flammable liquids and gases and their transport in road traffic in the Republic of Srpska.

Keywords: road transport, dangerous substances, explosive substances and objects, ADR.

Pregledni rad

PRIVATNA BEZBJEDNOST U ZAŠTITI KRITIČNE INFRASTRUKTURE REPUBLIKE SRPSKE

Mr Dragana Kosić[1]
Dr Željko Zorić[2]

Apstrakt: Kritična infrastruktura je danas najznačajniji dio nacionalne bezbjednosti svake države. Ovo je decidno naznačeno u nacionalnim strategijama koje kritičnu infrastrukturu i resurse definišu kao neophodne (krucijalne) elemente (sektore) za svakodnevno funkcionisanje političkih, ekonomskih, društvenih i kulturnih sistema jedne države. Pod pojmom kritična infrastruktura smatraju se (uglavnom) sva prirodna i materijalna dobra, imovina, tehnički sistemi, komunikacije, poslovne djelatnosti i službe koje su od posebnog (bitnog) značaja za državu. odnosno: energija, transport, poljoprivreda i hrana, voda, javno zdravlje i bezbjednost, hitne službe, odbrambena industrija, informacije i telekomunikacije, bankarstvo i finansije, zaštita životne sredine, industrija, proizvodnja i nauku. Na koji način će se definisati kritična infrastruktura zavisi od spremnosti države da istu definiše u skladu sa svojim stvarnim potrebama. Kada se posmatra Republika Srpska, konstatuje se da postoje početne ideje da se definiše kritična infrastruktura (Zakon), ali je još uvijek nejasno koji subjekt će da se stara o preventivnoj i represivnoj zaštiti dritične infrastrukture. Pošto razvijene zemlje scijeta svoju kritičnu infrastrukturu povjeravaju na preventivnu zaštitu sektoru privatne bezbjednosti, nema nikakvih prepreka da tako bude i u Republici Srpskoj. Da bi se to i ostvarilo, država, može i mora u privatnoj bezbjednosti prepoznati ključnog aktera u zaštiti kritične infrastrukture. Dobar reper mogu da nam budu rješenja u Srbiji i Hrvatskoj koja su u privatnoj bezbjednosti prepoznale ovaj sektor kao ključni u prevenciji kritične infrastrukture. Sveobuhvatni pristup mora da uključi sve državne i nadnacionalne aktere, kao i privatne, poslovne, sigurnosne i naučno-akademske organizacije u zaštiti kritične infrastrukture. Na žalost, u Republici Srpskoj, još uvijek ključni akteri (vlast) nije upoznata ni sa postojanjem zakonskih rješenja, njihovom implementacijom, kao ni sa mogućnostima privatnog sektora bezbjednosti. U radu će pomenuto biti

[1] Kompanija Sector Security, B. Popovića 9, Banja Luka, Republika Srpska dragana.kosic@sectorsecurity.org
[2] Kompanija Sector Security, B. Popovića 9, Banja Luka, Republika Srpska zeljko.zoric@sectorsecurity.org

detaljnije analizirano, a zaključak će obuhvatiti prijedlog mjera koje mogu prevazići novonastalu nepoznanicu zaštite kritične infrastrukture u Republici Srpskoj.

Ključne riječi: privatna bezbjednost, kritična infrastruktura, zaštita, Republika Srpska

UVOD

Zakonom o bezbjednosti kritičnih infrastruktura u Republici Srpskoj (Sl.glasnik Republike Srpske br. 58/19) po prvi put se sistemski pristupa prepoznavanju objekata kritične infrastrukture i razvoju mjera koje će doprinijeti njihovoj preventivnoj zaštiti. Zastoj u primjeni Zakona u praksi, ne treba biti ograničavajući faktor razvoju primjene Zakona kroz debate na naučnim skupovima. Na taj način će se animirati ključni akteri razvoja podzakonskih akata (organi Vlade Republike Srpske) koji će otkloniti novonastale nedoumice, prije nego se Zakon počne primjenjivati. Olakšavajuća okolnost je učenje iz iskustava okruženja (Hrvatske i Srbije) koje su daleko odmakle u praktičnoj primjeni zakona i podzakonskih akata koji se odnose na kritičnu infrastrukturu. Ono što može biti nedoumica, jeste izostanak preciznog definisanja subjekata koji će biti direktni izvršioci zaštite kritične infrastrukture. Ukoliko analiziramo iskustvo zemalja okruženja zaključiće se da je glavni i najbrojniji akter u zaštiti objekata kritične infrastrukture privatni sektor bezbjednosti. Valja napomenuti da je i prije usvajanja i primjene Zakona u zemljama okruženja ovaj sektor uveliko obezbjeđivao objekte kritične infrastrukture iako kao takvi još uvijek nisu bili označeni. Sličnu situaciju imamo danas u Republici Srpskoj. Iskustvo koje privatni sektor ima u fizičko-tehničkoj zaštiti ovih objekata, je u svakom slučaju kapital, koji daje za puno pravo ovom sektoru da bude bitan subjekt u kreiranju zaštite objekata kritične infrastrukture. Zakonskim rješenjima pristupilo bi se privatno - javnom partnerstvu kao najpouzdanijem načinu u primjeni mjera zaštite kritične infrastrukture.

U Republici Srpskoj, na žalost, privatni sektor bezbjednosti još uvijek nije prepoznat kao važan subjekt u primjeni mjera zaštite kritične infrastrukture. Ovo je i najznačajniji argument koji naučna zajednica u Republici Srpskoj treba iskoristiti u iniciranju subjekata vlasti da se rješavanju ovoga pitanja posveti mnogo veći značaj.

ZAKON O BEZBJEDNOSTI KRITIČNIH INFRASTRUKTURA U REPUBLICI SRPSKOJ

Navedenim zakonom uređuje se kritična infrastruktura Republike Srpske, sektori kritične infrastrukture u Republici Srpskoj, upravljanje kritičnim infrastrukturama, obaveza izrade analize rizika, bezbjednosnog plana objekata iz sektora kritične infrastrukture, bezbjednosni koordinator i lice odgovorno za upravljanje i zaštitu objekata kritične infrastrukture, saradnja u oblasti kritične infrastrukture, postupanje sa zaštićenim podacima, nadzor nad sprovođenjem ovog zakona, kao i prekršajne odredbe. Kao što se da zaključiti, zakonom se jasno definiše cilj, svrha usvajanja zakona, koji za konačno ima prepoznavanje Republike Srpske kao subjekta spremnog da prihvati preporuke EU, a koje se odnose na zaštitu kritčne infrastrukture. Dugogodišnje iskustvo privatnog sektora bezbjednosti u zaštiti objekata kritične infrastrukture[3], jasno ukazuje na činjenicu da su otvorena brojna pitanja, na koja treba dati odgovor, kako bi se u zaštitu ovih objekata ušlo bez bilo kakvih nedorečenosti. Može se reći da su otvorena pitanja posljedica, dijelom, neshvatanja privatnog sektora bezbjednosti i njegove uloge u zaštiti upravo ovih objekata. Ovaj stav se temelji na činjenici da predlagač zakona nije pozvao predstavnike privatnog sektora bezbjednosti na stručnu raspravu koja bi se odnosila upravo na razjašnjavanje svih onih pitanja, koja danas, tri godine poslije usvajanja zakona predstavljaju jednu veliku enigmu.

Nejasnih pitanja, koja zahtijevaju hitan odgovor je mnogo, a za potrebe ovoga rada navešće se samo neka. Prvo, ko vrši procjenu ugroženosti objekata kritične infrastrukture. Bilo koje ministarstvo RS ne mora nužno imati lice osposobljeno za vršenje ovih poslova. Ova nejasnoća automatski navodi na mogućnost, koju zakon daje, da se pomoć može tražiti od strukovnih udruženja.[4]Pri tome potpuna je nepoznanica ko čini strukovno udruženje, i kakve uopšte ono treba imati kompetencije da se uključi u pružanje pomoći ministarstvu? Da li je to udruženje iznad ministarstva? Da li njegov stav ministarstvo mora da prihvati? Sljedeće pitanje, koje i najviše, iz razumljivih razloga, interesuje privatni sektor, jesu mjere fizičko-tehničke zaštite koje trebaju biti primijenjene kod zaštite objekata kritične infrastrukture. Potpuna je nejasnoća u pogledu vrste i obima mjera koje će se koristiti kod zaštite ovih objekata. Imajući u vidu, spomenuto dugogodišnje iskustvo privatnog sektora bezbjednosti u zaštiti objekata kritične infrastruktire, potpuno je jasno nastojanje ovoga sektora da s enametne zakonodavcu kao važan subjekt, ne samo kod sprovođenja jmera zaštite, već i kod njihovog definisanja.

[3] Član 3 pomenutog Zakona. Prim.autora.
[4] Član 8.stav 4.pomenutog Zakona.

Kada je u pitanju, analiza pomenutog zakona, i njegov značaj na mogući angažman privatnog sektora bezbjednosti u zaštiti objekat kritične infratrukture dodatnu nejasnoću u primjenu zakona ostavljaju odredbe ćlanoava od 22 do 25 Zakona. Naime članom 22. je definisano da Vlada Republike Srpske u roku od šest mjeseci od dana stupanja na snagu ovog zakona donese podzakonski propis o postupku provjere subjekata i objekata kritične infrastrukture, a što nije urađeno. Dalje, članom 23.zakona, obavezuju se rukovodioci republičkog organa uprave da donesu sektorske mjere iz člana 8. stav 3. ovog zakona u roku od 18 mjeseci od dana stupanja na snagu zakona, a što nije urađeno. Član 24. zakona upućuje na rok od devet mjeseci ministra da donese Metodologiju iz člana 8. stav 1. ovog zakona, a što takođe, nije urađeno. Republički organi uprave dužni su da u roku od šest mjeseci od dana donošenja Metodologije predlože kritične infrastrukture iz sektora njihove nadležnosti i nivo njihove kritičnosti. Ova obaveza, propisana članom 25. zakona nije realizovana. Navedeno upućuje na zaključak da postoji potreba preispitivanja valjanosti samoga zakona, odnosno pokretanja stručne rasprave koja će u konačno rješenje implementirati pomenuto iskustvo privatnog sektora bezbjednosti.

PRIVATNI SEKTOR BEZBJEDNOSTI U REPUBLICI SRPSKOJ

U periodu 1996-2002. došlo je do napuštanja koncepta organizovanog i pravnog učešća svih bezbjednosnih subjekata u zaštiti državne i društvene svojine prelaskom na tržišnu ekonomiju i legitimnu pojavu više vrsta svojine: državne, društvene, privatne i dr (Daničić, Stajić, 2008:90). Transformacija kapitala, koja je dovela do ekspanzije razvoja privatnog kapitala, za bezbjednosni sistem predstavljala je novi izazov ranije nepoznat na ovim prostorima.

Pojavom privatnog kapitala koji nije bio u neposrednoj nadležnosti zaštite MUP-a RS novonastali nezaštićen prostor popunjava - privatna bezbjednost. Vođena poslovnom etikom i profitom privatna bezbjednost uspješno ispunjava prazninu koja se pojavila između policije i novonastalog privatnog kapitala. Nastanak ovih agencija nisu pratila zakonska i podzakonska rješenja kojima bi se odredili uslovi za osnivanje i rad preduzeća za obezbjeđenje lica i imovine, uredila detektivska djelatnost, odredili uslovi koje moraju zadovoljiti lica koja će obavljati poslove fizičke i tehničke zaštite lica i imovine, kao i neposredan nadzor nadležnih državnih organa. Divlje tržište rada, samovolja u radu, neprincipijelnost i niz drugih propusta u radu novonastalih agencija primorali su predstavnike vlasti da zakonski urede oblast privatne bezbjednosti. Valja napomenuti da su i neke agencije u Republici Srpskoj prepoznale potrebu zakonskog uređenja kako bi se izbjegla nelojalna i

neprofesionalna konkurencija koja je „lovila u mutnom“. Privatna agencija koja je inicirala potrebu zakonskog uređenja sektora privatne bezbjednosti je bila prva privatna agencija u RS Sector security koja je i danas vodeća agencija u Republici Srpskoj, a druga u Bosni i Hercegovini. (Zorić:2019).

Zakon o agencijama za obezbjeđenje lica i imovine i privatnoj detektivskoj djelatnosti usvojen je 2012.godine, a objavljen u Sl.glasniku Republike Srpske, br.4/12). Danas, na teritoriji Republike Srpske egzistira oko 45 privatnih bezbjednosnih kompanija. Najveća koncentracija privatnih sigurnosnih kompanija je i dalje na području PU Banja Luka. U vrijeme usvajanja Zakon je u mnogome doprinio da se uredi privatni sektor bezbjednosti i spriječe zloupotrebe ovog sektora u novonastalim društvenim promjenama.

Kako je vrijeme prolazilo, pojavljivali su se novi zahtjevi privatnog sektora u zaštiti imovine i poslovanja, a na koje privatni sektor bezbjednosti nije u mogućnosti odgovoriti zbog zakonskih ograničenja. Danas su primjetni sve češći zahtjevi javnog sektora, posebno lokalnih zajednica, za angažovanjem privatnog sektora bezbjednosti u zaštiti određenih aktivnosti, a koji su opet u koliziji sa zakonskim rješenjima koja jasno naglašavaju uslove u kojima se može angažovati privatna bezbjednosna agencija. Imajući ovo u vidu postoji potreba da se razmotri opcija razvoja i usvajanja novog zakona koji bi omogućio privatnom sektoru da se aktivnije uključi u bezbjednosni sistem, a posebno u onaj koji treba da se bavi zaštitom kritične infrastrukture.

Danas je još uvijek nepoznanica koliko u Republici Srpskoj ima objekata kritične infrastrukture, niti se zna ko i kako će da vrši zaštitu tih objekata. Evidentno je, već sada, bez svake sumnje, da raspoloživi resursi javnog sektora (policija) nisu u mogućnosti pružiti adekvatnu zaštitu ovim objektima. Pozivajući se na iskustvo okruženja, da se zaključiti da je ogroman broj objekata kritične infrastrukture povjeren subjektima privatnog sektora bezbjednosti. Ova saznanja ostavljaju dovoljno prostora da se paralelno uz definisanje objekata kritične infrastrukture realizuje i process izrade i usvakanja novog zakona koji će regulisati radne aktivnosti privatnog sektora bezbjednosti. Iskustva država Evropske unije su nedvosmisleno pokazala da je privatni sektor bezbjednosti, posebno u vrijeme pandemije korona virusa, pokazao da je bio, i da jeste, jedan od ključnih faktora u primjeni mjera kojima se sprječava širenje ovoga virusa. Tako je privatni sektor ključni subjekt u zaštiti objekata kritične infrastrukture, kao što su aerodromi, luke, željezničke stanice, pošte, finansijske ustanove… Znači, mjesta na kojima je najveći prolaz ljudi. Republika Srpska treba i mora iskoristiti ova saznanja i što prije ući u realizaciju projekta privatno – javnog partnerstva zaštite objekata kritične infrastrukture. Osim podizanja nivoa bezbjednosti, otvoriće se i nova radna mjesta, a čime će se indirektno

smanjiti pritisak na zavode za zapošljavanje, a vjerovatno smanjiti i trend iseljavanja produktivne radne snage iz Republike Srpske.

Da bi privatni sektor bio kvalitetan subject u zaštiti kritične infrastrukture, kao što je već navedeno, potrebno je što prije pristupiti izmjeni postojećeg zakona kojim ser eguliše rad ovoga sektora, kako bi se sektoru dala mogućnost, prilika, da se bavi zaštitom objekata kritične infrastructure, bez obzira na vlasničku strukturu nad tim objektima. Na primjer, treba dati mogućnost privatnom sektoru da se bavi zaštitom objekata koji su sada u isključivoj nadležnosti MUP-a Republike Srpske. Bojazan da će na taj način privatni sektor "ojačati" i postati, možda, oružana formacija koja se može zloupotrijebiti je u najmanju ruku neozbiljna i predstavlja produkt pogrešne percepcije o mjestu i ulozi privatnog sektora u ostvarivanju sistema bezbjednosti.

Zloupotreba ovoga sektora se može spriječiti zakonskim rješenjima, kroz jasno definisanje zadataka kontrolnom aparatu. Dugogodišnje iskustvo rada privatnih agencija u Republici Srpskoj je dobra pretpostavka za uvođenje ovoga sektora u sistem zaštite kritične infrastructure. Kao što je navedeno, ovaj sektor, već sada učestvuje u zaštiti objekata koji će, bez svake sumnje, biti kritična infrastruktura. Dosadašnje iskustvo predstavlja značajnu iskustvenu referencu za ovaj sektor u zaštiti objekata koji će sasvim izvjesno biti kritična infrastruktura (finansijske ustanove, objekti za proizvodnju hrane, terminali fosilnih goriva i sl.). Suština uvođenja privatnog sektora u zaštitu kritične infrastrukture se nalazi u spremnosti javnog sektora da prihvati privatni sektor kao ravnopravnog partnera u ostvarivanju zajedničkog cilja.

Izmjenama ili usvajanjem novoga zakona cjelovito bi se uredili poslovi obaveznog obezbjeđenja i zaštite određenih objekata kritične infrastrukture, kao i poslovi i način rada pravnih i fizičkih lica u oblasti privatnog obezbjeđenja i kontrolnog aparata. Zakonodavac bi jasno odredio koji su to obavezni objekti koje sleduje privatno obezbjeđenje. Zakonom bi se jasnije uredili uslovi za licenciranje pravnih i fizičkih lica za obavljanje poslova privatnog obezbjeđenja. Ovlašćenja radnika privatnog obezbjeđenja bila bi usklađena sa onima koja su zastupljena u okruženju, odnosno sa savremenim trendovima. Naravno, zakonom bi se uredili i svi drugi odnosi privatno-javnog partnerstva koji nisu u direktnoj vezi sa zaštitom objekata kritične infrastrukture.

MODELI ODNOSA PRIVATNE BEZBJEDNOSTI I JAVNE BEZBJEDNOSTI

Ono što nama u Republici Srpskoj danas nedostaje jeste sistemski pristup problemu zaštite objekata kritične infrastrukture. Takav pristup će jasno

izdvojiti sve radnje, mjere, postupke... koji mogu dovesti so željenog odnosa u privatno – javnom partnerstvu zaštite kritične infrastrukture. Ukoliko usvojimo sistemski pristup imaćemo situaciju da potreba definiše zakon, a ne da zakon definiše potrebu. Suština sistemskog pristupa je definisanje potrebe koja će sama po sebi definisati zakonski okvir. Od usvojenog modela privatno – javnog partnerstva zavisiće i uspjeh zaštite objekata kritične infrastrukture.

U principu, saradnja policije i subjekata privatnog sektora bezbjednosti treba da se odvija u granicama njihovih nadležnosti i ovlašćenja koja subjekti državnog i nedržavnog sektora bezbjednosti mogu primjeniti u određenim situacijama. Do te saradnje može doći na inicijativu bilo koje od strana, ali u praksi do toga često dolazi po zahtjevu policije, u situacijama kada su policijski službenici ovlašćeni da intervenišu i da primjene odgovarajuće mjere, a naročito ako je došlo do ugrožavanja bezbjednosti lica i imovine. Pojedini domaći autori zastupaju stav da priroda odnosa privatne bezbjednosti i policije u Republici Srpskoj ne odlikuju ni saradnja ni rivalitet. U takvom miljeu, privatna bezbjednost ne može biti ravnopravno tretirana, pa je i ostvarena saradnja najčešće samo u domenu pomoći policijskim organima. Drugi teoretičari ukazuju da odnos javne i privatne sfere bezbjednosti karakteriše neravnopravno partnerstvo, pri čemu njihova saradnja nije institucionalizovana, već se ostvaruje od slučaja do slučaja, a njen oblik zavisi od potreba za nivoom zaštite vitalnih vrijednosti koje se obezbjeđuju (Bošković, Keković, 2003:90). Takođe, ima mišljenja da odnose između privatne bezbjednosti i policije karakterišu sledeći modeli: nezavisnost, komplementarnost, kooperativnost i partnerstvo.

a. Nezavisnost

Nezavisnost predstavlja model koji podrazumijeva da privatni i javni akteri bezbjednosti imaju svoje posebno definisane zadatke, pri čemu ovi akteri skoro i da ne ostvaruju kontakte.

b. Konkurentnost

Pod konkurencijom se podrazumijeva model odnosa privatne bezbjednosti i policije u kome nedostaje međusobno povjerenje. Prema ovom modelu, relacije ovih aktera bezbjednosti karakteriše konkurentsko nadmetanje za dobijanje poslova, što najčešće otežava, pa i onemogućava njihovu saradnju.

c. Komplementarnost

Komplementarnost je model odnosa privatne bezbjednosti i policije u kome privatna bezbjednost i policija egzistiraju na tržištu bezbjednosnih usluga rame uz rame, sa jasnim preciznim granicama i razgraničenjima u podjeli zadataka, uporedo sa međusobnim dopunjavanjem u sprovođenju svojih djelatnosti.

d. Kooperativnost

Kooperativnost podrazumijeva model odnosa privatne bezbjednosti i policije zasnovan na međusobnoj saradnji, izražen kroz davanje obostrane podrške, sa ciljem osnaživanja svakog od učesnika.

e. Partnerstvo

Partnerstvo predstavlja model odnosa između privatne bezbjednosti i policije gdje oba aktera bezbjednosti ostvaruju najveći nivo kooperativnosti u postupanju i potpunu jednakost između učesnika čija je djelatnost usmjerena ka postizanju zajedničkog cilja (Daničić, Filipović, 2015:39).

ZAKLJUČAK

Iz napisanog jasno proizilaze sljedeći zaključci:

Opšti:

1. Republika Srpska ima potrebu da hitno definiše objekte kritične infrastrukture i da definiše minimalne mjere njihove zaštite.

Posebni:

2. Uvažavajući novonastale društvene potrebe, aktuelna bezbjednosna događanja, kako u Republici Srpskoj, tako i u okruženju, evidentno je da se privatni sektor može i mora prihvatiti kao ravnopravan partner na polju zaštite objekata kritične infrastukture.
3. Preduslov za uvođenje privatnog sektora bezbjednosti u zaštitu objekata kritične infrastrukture je izmjena postojećeg zakona kojim se reguliše rad privatnih agencija i jasno uvođenje privatnog sektora, kroz podzakonske akte koji proizilaze iz zakona o zaštiti kritične infrastrukture, u ovaj proces.
4. Naučna zajednica mora biti pokretač svih izmjena koje su u radu navođene. Na ovaj način omogućiće se zasnivanje privatno - javnog partnerstva na naučnim osnovama, a što u konačnom garantuje uspjeh jednog projekta, kakav je zaštita najznačajnijih objekata jednog društva-objekata kritične infrastrukture.

LITERATURA

1. Barković, I., i Širić, M. (2010). Uloga i značaj javno-privatnog partnerstva u Republici Hrvatskoj: izabrani primjeri. *Ekonomski vjesnik: Review of Contemporary Entrepreneurship, Business, and Economic Issues*, *23*(1), 184-201.

2. Vidović, D.I., *Korporativna sigurnost*, udruga hrvatskih menadžera sigurnosti-UHMS, Zagreb, 2011
3. Davidović, D., Alternativni činioci bezbjednosti (hrestomatija), *Fakultet bezbednosti*, Beograd, 2006.
4. Daničić, M., Filipović, V., *Privatna bezbjednost*, Fakultet za pravne i poslovne studije dr Lazar Vrketić, Novi Sad, 2015.
5. Daničić, M., Stajić, Lj., *Privatna bezbjednost*, Visoka škola unutrašnjih poslova, Banja Luka 2008.
6. Cvetković, P. (2015). Javno-privatno partnerstvo kao metod restrukturiranja javnog sektora: Pravni aspekti. Restrukturiranje javnih preduzeća u uslovima institucionalnih ograničenja, *Ekonomski fakultet u Beogradu*, 175-195.
7. Kržalić, A., *Trend privatne sigurnosti u Bosni i Hercegovini*. Sarajevo: Centar za sigurnosne studije. 2016
8. Mitrović,Lj., Pavlović, G., *Sistem bezbjednosti Bosne i Hercegovine – pravni aspekti i aktuelno stanje,* Međunarodno udruženje naučnih radnika – AIS, Banja Luka, 2012.
9. Nađ, I., *Zbirka propisa iz djelokruga privatne zaštite,* hrvatska udruga menadžera sigurnosti, Zagreb, 2012.
10. Stanojević, P., & Jeftić, Z. Kontinuitet funkcionisanja kritične infrastrukture u okviru projekta „Pojas i put".
11. Todorović, B. Inicijativa „Pojas i put" i zaštita odgovarajuće kritične infrastrukture na balkanskom raskršću.
12. Zorić, Ž. Cooperation between the private and public security in order to realise security system. International scientific and profefessional Conference Security and crises management-theory and practice, "safety for future 2019", 2019, Beograd.

Ostali izvori:

1. *Private Security: Report of the Task Force on Private Sevurity,* US Government Printing Office, Washington, DC, 1976.
2. *Zakonom o bezbjednosti kritičnih infrastruktura u Republici Srpskoj* (Sl.glasnik Republike Srpske br. 58/19)

PRIVATE SECURITY IN PROTECTION OF THE CRITICAL INFRASTRUCTURE OF THE REPUBLIC OF SRPSKA

Dragana Kosić, MA
Željko Zorić, PhD

Abstract: Nowadays, the critical infrastructure is being considered the most important part of the national security of every country. This is clearly indicated in national strategies that place critical infrastructure and resources as necessary (crucial) elements (sectors) for the daily functioning of the political, economic, social and cultural systems of a country. The term critical infrastructure includes (mainly) all natural and material goods, property, technical systems, communications, business activities and services of special (essential) importance to the state, namely: energy, transport, agriculture and food, water, public health and safety, emergency services, defense industry, information and telecommunications, banking and finance, environment, industry, manufacturing and science. How the critical infrastructure will be defined depends on the readiness of the state to define it in accordance with its real needs. In terms of the Republic of Srpska, it is noted that there are initial ideas to define critical infrastructure (Law), but it is still unclear which entity will take care of the preventive and repressive protection of critical infrastructure. Since developed countries often entrust the preventive protection of their critical infrastructure to the private security sector, there are no obstacles to do the same in the Republic of Srpska. In order to achieve this, the state can and must recognize private security as a key entity in the protection of critical infrastructure. The good example could be solutions from Serbia and Croatia, which have identified the private security sector as the key one in the prevention of critical infrastructure. A comprehensive approach should encompass all state and supranational actors, as well as private, business, security and scientific-academic organizations in the protection of critical infrastructure. In the Republic of Srpska, unfortunately, the key actors (the government) is still not familiar with relevant legislation, its implementation, as well as with the possibilities of the private security sector. This paper will analyze the aforementioned in more detail, and the conclusion will include a proposal for measures that can overcome the newly emerging unknown of critical infrastructure protection in the Republic of Srpska.

Keywords: private security, critical infrastructure, protection, the Republic of Srpska

Pregledni rad

KOMPARATIVNI PRIKAZ ULOGE POLICIJE U ZAŠTITI KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ I SRBIJI

Dr Gojko Šetka[1]
Aleksandar Đekić, MA[2]

Apstrakt: U okviru skoro svih savremenih sistema zaštite i spasavanja kritična infrastruktura, odnosno njena zaštita ima značajnu ulogu. Zbog svog značaja za društvo i državu, kritična infrastruktura je uređena u normativnom, funkcionalnom i institucionalnom pogledu. Ugrožavanje kritične infrastrukture se može manifestovati na različite načine. Zbog velikog broja oblika i vidova ugrožavanja kritične infrastrukture javila se potreba za preduzimanjem velikog broja potrebnih mjera od strane svih činilaca u društvu, s ciljem smanjenja rizika i spremnosti za adekvatno reagovanje na otklanjanje potencijalnih načina ugrožavanja i posljedica njenog ugrožavanja. Dakle, većina zemalja je uredila sistem zaštite kritične infrastrukture sa normativnog aspekta, propisujući i donoseći razne zakonske i podzakonske akte. Normativni sistem zaštite krtične infrastrukture razvijen je i u Republici Srpskoj i Republici Srbiji. U ovome radu biće riječi o ulozi policije u zaštiti kritične infrastrukture, poslovima koje policija vrši u pogledu njene zaštite, a biće dat i komparativni prikaz uloge Ministarstva unutrašnjih poslova u zaštiti kritične infrastrukture u Republici Srpskoj i Srbiji.

Ključne riječi: policija, poslovi policije, kritična infrastruktura, zaštita, ugrožavanje.

UVODNA RAZMATRANJA

Bezbjednost se može posmatrati sa različitih aspekta na više načina. Rijetki su pojmovi koji se mogu shvatiti na tako različite načine kao što je pojam bezbjednosti. Najšire posmatrano, pod izrazom bezbjednost podrazumjeva se stanje u kome državi ili građanima kao pojedincima ne prijeti nikakva opasnost. Znači, to je stanje u kome je neko (država, građani, njihova

[1] Fakultet bezbjednosnih nauka, Univerzitet u Banjoj Luci, imejl: gojko.setka@fbn.unibl.org
[2] Uprava za policijsku obuku, Ministarstvo unutrašnjih poslova Republike Srpske, imejl: aleksandar.djekic@mup.vladars.net

imovina i sl.) obezbjeđen od bilo kakve opasnosti.[3] Upravo posmatrajući šta je to bezbjednost, može se konstatovati da svaka država teži ka ostvarivanju što većeg nivoa bezbjednosti. Bezbjednost kao pojava sa svim svojim elementima predstavlja osnovnu potrebu svakoga čovjeka pojedinca, svih ljudi i cjelokupnog društva. Funkcija bezbjednosti predstavlja skup određenih aktivnosti putem kojih država ostvaruje svoju djelatnost ili zadatake. Uz ovo se može povezati omogućavanje nesmetanog funkcionisanja životnog ciklusa i ostvarivanje osnovnih prava i sloboda svakoga čovjeka. S druge strane, za sam pojam bezbjednosti vežu se razne bezbjednosne pojave koje se mogu posmatrati kao izvori i oblici ugrožavanja bezbjednosti. Da bi se sistem bezbjednosti mogao ostvariti u određenom društvu i ispuniti cilj i zadatak države u pogledu ove tematike, potrebno je poznavati i dio koji se odnosi na ugrožavanje bezbjednosti. Ugrožavanje bezbjednosti posmatra se na više načina. Za ovu oblast zaštite definisanje pojma ugrožavanje bezbjednosti potrebno je posmatrati sa prirodnog, ljudskog i tehničko – tehnološkog aspekta. Generalno, ugrožavanje bezbjednosti je pojava prirodnog, ljudskog ili tehničko – tehnološkog porijekla koja proizvodi ili može da proizvede štetne posljedice po referentne vrijednosti i interese.[4] Pojava ugrožavanja bezbjednosti može se posmatrati sa više aspekata i to sa aspekta izvora ugrožavanja bezbjednosti, nosioca ugrožavanja bezbjednosti, oblika i vidova ugrožavanja bezbjednosti, objekta ugrožavanja bezbjednosti i posljedice koja može nastati usljed ugrožavanja bezbjednosti.

Imajući u vidu prethodno opisano o samom pojmu bezbjednosti i mogućnosti ugrožavanja bezbjednosti, može se konstatovati da kritična infrastruktura predstavlja jedan od osnova funkcionisanja društvene zajednice u svakodnevnom životu. Nesmetano funkcionisanje sistema kritične infrastrukture i jeste prioritet svake države. Tema kritične infrastrukture i njene zaštite sve više dobija na značenju i zauzima posebno mjesto u savrmenom društvu. Kiritčna infrastruktura sa svojim sadržajem i karakteristikama predstavlja bitan dio bezbjednosnog sistema države. Kao takva njena zaštita je jedan od prioriteta svake države. Postoje razni oblici i načini ugrožavanja kritične infrastrukture, zato je i potrebno sprovođenje aktivnosti u pogledu njene zaštite.

Posmatrano sa teorijskog aspekta u pogledu ove teme postoje razne definicije kritične infrastrukture, koje su dosta slične i sa kojima su obuhvaćeni isti ili slični elementi, a o čemu će biti izloženo u narednom tekstu ovoga rada. Značaj kritične infrastrukture ogleda se i u njenom normiranju u važećim

[3] Jovičić D., 2008, *Organizacija i nadležnost policije*, Fakultet za bezbjednost i zaštitu Banja Luka, str. 12.

[4] Mijalković S., Keserović D., 2010, *Osnovi bezbjednosti*, Fakultet za bezbjednost i zaštitu Banja Luka, str. 102.

pravnim aktima. Većina zemalja ovu problematiku predstavila je i kroz propisivanje i donošenje zakonskih i podzakonskih propisa u pogledu zaštite kritične infrastrukture, odnosno mjera i inicijativa za zaštitu kritične infrastrukture. Takođe, pored mjera neophodnih za zaštitu propisani su institucionalni okviri u pogledu subjekata zaštite kritične infrastrukture i izrade dokumenata neophodnih za sprovođenje mjera zaštite.

U daljem radu pored pojma, karakteristika i zaštite kritične infrastrukture, biće predstavljen normativni osnov zaštite kritične infrastrukture u Republici Srpskoj i Republici Srbiji, sa posebnim osvrtom na ulogu i rad policije u pogledu zaštite kritične infrastrukture.

POJAM, KARAKTERISTIKE I ZAŠTITA KRITIČNE INFRASTRUKTURE

O samom pojmu kritične infrastrukture postoji više različitih stavova u pogledu teorijskog definisanja. Malen je broj domaće literature kojom se proučava materija kritične infrastrukture i svi njeni elementi, a i trenutno postojeći u većoj mjeri preuzeti su iz strane literature. Definicija infrastrukture odnosi se na sredstva i imovinu koji su ključni za funkcionisanje kompletnog društva. Sama polazna osnova definisanja kritične infrastrukture kod nas započinje u normativnim izvorima koji su preuzeti iz dokumenata Evropske unije. U Republici Srpskoj osnovna definicija kritične infrastrukture polazi iz člana 2. zakona[5], a u istom je propisano da su kritične infrastrukture sistemi, mreže i objekti od posebne važnosti, čije uništenje ili ugrožavanje može izazvati ozbiljan poremećaj u slobodnom kretanju ljudi, prevozu robe i pružanju usluga, negativno uticati na unutrašnju bezbjednost, zdravlje i život ljudi, imovinu, životnu sredinu, spoljnu bezbjednost, ekonomsku stabilnost, te neprekidno funkcionisanje republičkih organa. Na nešto sličan način kritična infrastruktura definisana je i u Republici Srbiji, u članu 4. Zakona o kritičnoj infrastrukturi. Pomenutim zakonom pod kritičnom infrastrukturom podrazumjevaju se sistemi, mreže, objekti ili njihovi dijelovi, čiji prekid funkcionisanja ili prekid isporuke roba odnosno usluga može izazvati ozbiljne posljedice po nacionalnu bezbjednost, zdravlje i živote ljudi, imovinu, životnu sredinu, bezbjednost građana, ekonomsku stabilnost, odnosno ugroziti funkcionisanje Republike Srbije. Analizirajući obe definicije, odnosno kako je to propisano u oba zakona, može se zaključiti da su iste dosta slične, da obuhvataju skoro iste elemente i da se pod istim podrazumjeva sve ono što je neophodno za nesmetano funkcionisanje cjelokupnog društvenog sistema.

5 Član 2. - Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj (Službeni glasnik RS broj: 58/19).

Takođe, na nešto sličan način kritična infrastruktura definisana je i u Republici Hrvatskoj, donesenim zakonom[6] koji je na snazi, a kojim je uređena ova oblast. Pomenutim zakonom u članu 3. propisano je da su nacionalne kritične infrastrukture sustavi, mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice po nacionalnu sigurnost, zdravlje i život ljudi, imovinu i okoliš, sigurnost i ekonomsku stabilnost i neprekidno funkcionisanje vlasti. Kao što je u Republici Srpskoj i Srbiji na dosta sličan način kritična infrastruktura definisana je i u zakonskom osnovu Republike Hrvatske. Pored navedenih definicija kritične infrastrukture, a koje su sadržane u zakonskim propisima, postoji i niz drugih definicija koje su sadržane u drugim dokumentima. Vlada Kanade 2001. godine predložila je jednu definicija koja se koristi u dokumentima UN. Kritična infrastruktura se sastoji od fizičkih i informacionih tehnoloških objekata, mreža, službi i materijalnih dobara koji, ukoliko budu urušeni ili uništeni, mogu imati ozbiljan uticaj na zdravlje, bezbednost, sigurnost i ekonomsko blagostanje ili efikasno funkcionisanje vlasti. Ovu definiciju najčešće koriste institucije UN u obrazloženju sadržaja pojma kritične infrastrukture.[7]

Kritična infrastruktura kao važan segment svakoga savremenog bezbjednosnog sistema ima veći broj posebnih karakteristika. Jedna od takvih karakteristika jesu sistemi kritične infrastrukture. Pod sistemima kritične infrastrukture podrazumjevaju se sva ona dobra i svi oni sistemi iz kojih se određuje kritična infrastruktura i koji prate samu definiciju i pojam kritične infrastrukture. Sistemi kritične infrastrukture uglavnom su predviđeni direktivama EU, a kasnije preuzeti i predviđeni normativima drugih zemalja. Posmatrajući normative Republike Srpske i Srbije propisani su sektori kritične infrastrukture na dosta sličan način, s tim da je u Republici Srpskoj taj sistem dosta šire predstavljen. Članom 3. zakona[8] propisano je da su sektori kritične infrastrukture industrija, energetika i rudarstvo (proizvodnja uključujući ulazne resurse, objekte, sisteme za prenos, skladištenje, transport proizvoda, energenata i energije, sisteme za distribuciju), informaciono – komunikaciona infrastruktura (elektronske komunikacije, prenos podataka, informacioni sistemi, pružanje audio i audio i video medijskih usluga), saobraćaj (drumski, željeznički i vazdušni saobraćaj i saobraćaj unutrašnjim plovnim putevima), zdravstvo (zdravstvena zaštita, proizvodnja, transport i nadzor nad lijekovima), komunalne djelatnosti (objekti komunalne infrastrukture, a naročito u oblasti proizvodnje i isporuke vode, prečišćavanja i odvođenja otpadnih voda,

[6] Zakon o kritičnim infrastrukturama Republike Hrvatske (Narodne novine broj: NN: 56/13).

[7] Jakovljević V., 2010, *Resursi kritične infrastrukture i njihov značaj za upravljanje vanrednim situacijama*, Godišnjak FB 2010, Beograd.

8 Član 3. - Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj (Službeni glasnik RS broj: 58/19).

proizvodnja i isporuke toplotne energije, zbrinjavanja otpada iz stambenih i poslovnih prostora i slično), vodoprivreda (regulacioni i zaštitni vodeni objekti), hrana i piće (proizvodnja i snadbjevanje hranom i pićem, sistem sigurnosti hrane i pića, robne zalihe), finansije (bankarstvo, berze, investicije, sistemi osiguranja i plaćanja), prozvodnja, skladištenje i prevoz opasnih materija (hemijski, biološki, radiološki i nuklearni materijali), javne službe, vaspitanje i obrazovanje, kulturna i prirodna dobra (vjerski objekti, spomenici kulture, prostore kulturno – istorijske cjeline, arheološka nalazišta, znamenita mjesta, umjetnička djela i istorijski predmeti, arhivska građa, stara i rijetka knjiga, kao i zaštićena dobra propisana Zakonom o zaštiti prirode). Posmatrajući prethodni tekst može se zaključiti da je široka lepeza sektora kritične infrastrukture, a koja nije jedinstvena. Pored navedenih postoje i druga dobra koja se mogu ubrajati pod sektore kritične infrastrukture, a i zakonskim propisom je predviđeno da Vlada Republike Srpske može odrediti druge sektore kritične infrastrukture na prijedlog Ministarstva unutrašnjih poslova. Govoreći o kritičnoj infrasturkturi može se istaći činjenica da postoje dva niova, i to jedan su resursi koji predstavljaju kritičnu infrastrukturu i drugi nivo su mjere zaštite kritične infrastrukture.

Ono što je i osnova kritične infrastrukture jeste njena zaštita. Kada se govori o zaštiti bilo kojega segmenta društva prvenstveno se misli na preduzimanje određenih mjera i radnji u pogledu otklanjanja pojavnih oblika ugrožavanja i posljedica koje mogu nastati po određeno dobro. U poledu toga i sama zaštita kritične infrastrukture podrazumjeva određene aktivnosti kojima se obezbjeđuje funkcionalno i nesmetano djelovanje određenog dobra, kao i sprečavanje nastanka određenih posljedica po takva dobra. Zakonom o bezbjednosti kritične infrastrukture propisano je da se pod zaštitom kritične infrastrukture podrazumjevaju sve aktivnosti kojima je cilj da obezbjede funkcionalnost, neprekidno djelovanje i isporuku robe i usluga kritične infrastrukture, te da se spriječi ugrožvanje kritične infrastrukture.[9] Osnovni cilj zaštite kritične infrastrukture jeste da se održi njena funkcionalnost u slučajevima pojava vanrednih situacija. Zaštita kritične infrastrukture se definiše kao strategija, politika i spremnost koja je neophodna da se odvrati ili spriječi napad, odnosno pruži odgovor u slučaju da dođe do napada na kritične infrastrukture.[10] Osnova zaštite je izrada i postojanje procjene ugroženosti kritične infrastrukture i plan mjera njene zaštite. Ovo je posebno važno i bitno za postojanje i korištenje u vanrednim situacijama, te predstavlja osnov za dalje reagovanje u takvim pojavnim oblicima. Upravo takva važnost ogleda se u

[9] Član 4. tačka 4. Zakona o bezbjednosti kritičnih infrastruktura u Republici Srpskoj (Službeni glasnik RS broj: 58/19).

[10] Mićićović M., 2014, *Specifičnost zaštite kritične infrastrukture*, Bezbednost 3/2014, Beograd.

zakonskim propisima u kojima je propisana potreba sprovođenja mjera u pogledu analize rizika mogućeg prekida rada kritične infrastrukture i izrade planova obezbjeđenja. Bezbjednosni plan prema važećim normativima sačinjava se po određenim stavkama koje je su neophodne, a takođe propisan je i rok za njegovu izradu. Bezbjednosni plan donose subjekti koji su odgovorni za kritičnu infrastrukturu uz prethodno pribavljenu saglanost nadležnog organa.

NORMATIVNI OSNOV ZAŠTITE KRITIČNE INFRASTRUKTURE U REPUBLICI SRPSKOJ I SRBIJI

Kao što je prethodno navedeno značaj i važnost kritične infrastrukture za određenu državu ogleda se i kroz njeno normiranje u važećim zakonskim i podzakonskim propisima. Takva oblast kroz zakonske i podzakosnke propise regulisana je i u Republici Srpskoj i Republici Srbiji. Početkom 2018. godine vlasti Republike Srpske započele su proces pripreme, a kasnije i donošenja zakonskog propisa kojima se reguliše oblast bezbjednosti kritične infrastrukture. Takvim zakonom uređena je obaveza izrade bezbjednosnog plana objekta iz sektora kritične infrastrukture, kao i bezbjednosni koordinator i bezbjednosni menadžer za kritičnu infrastrukturu. Takođe, regulisana je i oblast saradnje sa drugim subjektima u oblasti kritične infrastrukture, postupanje sa tajnim podacima koji su u vezi sa kritičnom infrastrukturom i njenom bezbjednošću, nadzor nad sprovođenjem zakona i drugih propisa, kao i kaznene odredbe. Takav zakonski propis u Republici Srpskoj usvojen je 2019. godine.[11] Razlog donošenja takvoga zakona jeste i preuzimanje pravnih izvora EU i usklađivanje zakonodavstva RS sa propisima EU. U članu 1. Zakona o bezbjednosti kritičnih infrastruktura u Republici Srpskoj, propisano je da zakon uređuje kritične infrastrukture Republike Srpske, sektore kritične infrastrukture, upravljanje kritičnim infrastrukturama, obaveza izrade analize rizika, izradu bezbjednosnog plana objekata iz sektora kritične infrastrukture, bezbjednosni koordinator i lice odgovorno za upravljanje i zaštitu objekata kritične infrastrukture, postupanje sa zaštićenim podacima, nadzor na sprovođenjem zakona i prekršajne odredbe.

Takođe, zaštita kritične infrasturkture normativno je regulisana i u Republici Srbiji kroz donošenje Zakona o kritičnoj infrastrukturi.[12] Pomenutim zakonom propisana su osnovna pitanja u pogledu ove tematike, kao što su sektori kritične infrastrukture, način određivanja kritične infrastrukture, način

[11] Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj (Službeni glasnik RS broj: 58/19).

[12] U Republici Srbiji takav propis donesen je 2018. godine kada je i stupio na snagu.

njene zaštite, stepen tajnosti određenih podataka, način korištenja takvih podataka, kao i određen dio koji se odnosni na kaznene odredbe. Razlika zakonskih propisa u pogledu ove materije jeste da je Republika Srbija propisala i postupak određivanja, zaštite i izvještavanja u pogledu evropske kritične infrastrukture.

Pored zakona koji se direktno odnosi na zaštitu kritične infrastrukture u Republici Srpskoj donesen je i u direktnoj primjeni i Zakon o zaštiti i spasavanju u vanrednim situacijama.[13] Pomenutim zakonom propisana je oblast sistema zaštite i spasavanja, subjekti koji su nadležni za oblast zaštite i spasavanja u vanrednim situacijama, prava i dužnost republičkih organa i organa jedinica lokalne samouprave, prava i dužnost građana, način otklanjanja elementarnih nepogoda, planiranje sistema zaštite i spasavanja, nadzor nad sprovođenjem takvih mjera, kao i druga pitanja koja su od važnosti za oblast zaštite i spasavanje u vanrednim situacijama. Kao i u Republici Srpskoj takav zakonski propis donesen je i u Republici Srbiji i to Zakon o vanrednim situacijama.[14] Zakonom su propisana skoro ista pitanja kao i u Republici Srpskoj u pogledu djelovanja i sprovođenja potrebnih mjera u slučajevima vanrednih situacija.

Svaku oblast zaštite potrebno je normirati određenim propisima, tako i zaštitu kritične infrastrukture. Međutim, nije dovoljna samo izrada i donošenje takvih propisa, potrebno je imati u vidu da se takav propis može primjeniti na pravilan i adekvatan način. Normativna djelatnost može se ispitati sa dva aspekta koji se međusobno povezuju. S jedne strane to je posebna aktivnost koja registruje i izražava određene šire ili uže potrebe društva propisivajući adekvatne načine ponašanja. To je djelatnost koja mora uočiti potrebe društva, istovremeno mu dajući obavezan karakter. Ona nalazi svoju osnovu u životu, da bi zatim na određen način djelovala na životne, finansijske, tehničke, sigurnosne i druge procese. S druge strane normativna se djelatnost javlja kao nomotehnika u najširem smislu. Postavlja se pitanje, ne samo što, nego i kako normirati. Kako izraziti ono što se uređuje propisima da bude logično, razumljivo i operativno provedivo.[15]

[13] Trenutno važeći zakon je iz 2012. godine, a isti je pretrpio dvije izmjene i dopune i to 2017. godine i 2021. godine (Sužbeni glasnik RS broj: 121/12, 46/17 i 111/21).

14 Zakon o vanrednim situacijama (Službeni glasnik RS broj 111 od 29.12.2009., broj 92 od 07.12.2011. godine i broj 93 od 28.09.2012. godine).

[15] Trut D., 2020, *Utjecaj normativnog okvira na upravljanje kritičnom infrastrukturom,* Zbornik radova VII. Međunarodne znanstveno – stručne konferencije, Zagreb.

ULOGA I POSLOVI POLICIJE REPUBLIKE SRPSKE I SRBIJE U ZAŠTITI KRITIČNE INFRASTRUKTURE

Kada se govori o zaštiti cjelokupnog društva ili samo nekoga od segmenata društva, prva pomisao je na policiju kao državni organ. U našem pravnom sistemu policija bi se mogla definisati kao organ državne uprave čiji je prevashodni zadatak da štiti javni poredak, tj. da izvršava poslove koji se odnose na bezbjednost države i njenih građana, održavanjem javnog reda i mira, prevencijom i represijom kriminaliteta, te izvršavanjem drugih poslova iz njene nadležnosti.[16] Međutim, i pored ovakvoga definisanja i značaja policije za jedno društvo, može se reći da policija nije jedini organ koji ima obavezu djelovanja u oblasti bezbjednosti države i njenih građana. Postoje i mnogi drugi subjekti koji svojim djelokrugom rada mogu doprinijeti bezbjednosti društva i društvenih vrijednosti.

Posmatrajući kritične infrastrukture i njihovu zaštitu, kao važan segment društva, može se reći da policija u toj oblasti ima veliku i značajnu ulogu, kako u Republici Srpskoj, tako i u Republici Srbiji. U oba društva koja se posmatraju u ovome radu, postojeći zakonski propisi u oblasti zaštite i bezbjednosti kritične infrasturkutre u nadležnosti su Ministarstva unutrašnjih poslova. Takođe, zakonskim propisima predviđene su uloge i poslovi policije u oblasti vanrednih situacija i situacija zaštite i spasavanja, a koje se direktno vežu na kritične infrastrukture. Kada se govori o poslovima policije kao jednoga državnog aparata, prvenstveno se misli na poslove održavanja javnog reda i mira i poslove iz oblasti prevencije i represije kriminaliteta i drugih prekršaja. U tom smislu policija kao državni organ sa širokim opisom poslova može se posmatrati i sa aspekta rada u vanrednim situacijama. Šta to zapravo predstavljaju vanredne situacije propisano je definisanjem takvoga stanja važećim zakonskim propisom. Vanredna situacija je situacija u kojoj su rizici i prijetnje ili posljedice katastrofa, vanrednih događaja i drugih opasnosti za stanovništvo, životnu sredinu i materijalna dobra takvoga obima i inteziteta da njihov nastanak ili posljedice nije moguće spriječiti ili otkloniti redovnim djelovanjem nadležnih organa i službi, zbog čega je za njihovo ublažavanje i otklanjanje neophodno upotrijebiti posebne mjere, snage i sredstva uz pojačan režim aktivnosti.[17] Posmatrajući ovakvu definiciju vanredne situacije može se zaključiti da se takva situacija direktno veže za kritične infrastrukture koje predstavljaju dobra za društvo kao posebne vrijednosti i čiji je cilj zaštita i sprečavanje mogućnosti ugrožavanja ili prestanka normalnog funkcionisanja.

[16] Jovičić D., Šetka G., 2015, *Organizacija i nadležnost policije*, Fakultet za bezbjednost i zaštitu Banja Luka, str. 31-23.

[17] Član 5. tačka 1. Zakona o zaštiti i spasavanju u vanrednim situacimaja (Službeni glasnik RS broj: 121/12).

Postojećim zakonskim propisima precizno su definisane nadležnosti i poslovi policije u ovakvim situacijama, međutim u praksi je prisutan niz situacija gdje se zahtjeva djelovanje policije, a koje prevazivali normativne osnove.

Sama uloga policije Republike Srpske, kao i njena nadležnost u oblast zaštite kritične infrasturkutre i djelovanja u vanrednim situacijama, nije propisana lex specialis Zakonom o policiji i unutrašnjim poslovima, nego je to propisano Zakonom o bezbjednosti kritične infrastrukture Republike Srpske i Zakonom o zaštiti i spasavanju u vanrednim situacijama. Kao što je u prethodnom dijelu teksta istaknuto, Ministarstvo unutrašnjih poslova Republike Srpske nadležno je za sprovođenje Zakona o bezbjednosti kritične infrasturkutra u Republici Srpskoj.[18] Ovo ministarstvo je kontakt tačka ispred Vlade Republike Srpske, a koje sarađuje i održava odnose sa drugim organima u Republici Srpskoj, Bosni i Hercegovini, organima Evropske unije i organima drugih država u oblasti zaštite kritične infrastrukture, razmjeni informacija i sprovođenju drugih aktivnosti. Takođe, ovo ministarstvo nadležno je za određivanje i identifikovanje kritične infrastrukture i to donošenjem rješenja zajedno sa drugim subjektima. Jedna od posebnih nadležnosti jeste učestvovanje zajedno sa drugim subjektima u izradi analize rizika i bezbjednosnog plana zaštite kritične infrastrukture. Ono što posebno proizilazi iz postojećeg propisa jeste zaštita tajnih podataka i sprovođenje inspekcijskog nadzora u ovoj oblasti, a za što je nadležno isto ministarstvo. S druge strane veliku i značajnu ulogu policija ima i u sistemu zaštite i spasavanja u vanrednim situacijama. Sama uloga policije i njeni poslovi u ovoj oblasti propisani su važećim normativima. Prije svega takva uloga ogeda se u činjenici da je policija, odnosno Ministarstvo unutrašnjih poslova sa svojim organizacionim jedinicama jedan od snaga zaštite i spasavanja.[19] Od 2012. godine do 2017. godine policija je imala dosta veću i značajniju ulogu u pogledu zaštite i spasavanja u vanrednim situacijama, međutim izmjenama i dopunama zakona[20] došlo je smanjenja nadležnosti policije i prebacivanjem istih u nadležnost Republičke uprave civilne zaštite.[21]

Policija Republike Srbije ima dosta širi opis poslova u oblasti zaštite kritične infrastrukture i postupanja policije u vanrednim situacijama. Činjenica koja

[18] Službeni glasnik RS broj: 58/19.

[19] Organizacione jedinice ministarstva dijele se na unutrašnje i spoljašnje i to u sjedištu i van sjedišta ministarstva (uprave u sjedištu, PU van sjedišta, jedinice, odjeljenja, sektori, odjesci, policijske stanice, stanična odjeljenja policije).

[20] Zakon o izmjenama i dopunama zakona o zaštiti i spasavanju u vanrednim situacijama (Službeni glasnik RS broj: 46/17).

[21] Republička uprava civilne zaštite od 2016. godine djeluje samostalno kao upravna organizacija u okviru Vlade Republike Srspke, a koja je prethodno bila u organizacionom sastavu Ministarstva unutrašnjih poslova Republike Srpske.

dosta govori o tome jeste i sama organizacija Ministarstva unutrašnjih poslova Republike Srbije u okviru kojeg je formirana posebna organizaciona jedinica koja u svome djelokrugu rada ima nadležnost zaštite kritične infrastrukture i zaštite i spasavanja u vanrednim situacijama, a to je Sektor za vanredne situacije.[22] Sprovođenje Zakona o kritičnoj infrasturkturi u Republici Srbiji je takođe u nadležnosti policije, odnosno Ministarstva unutrašnjih poslova. Sami zakonski propisi u pgoledu zaštite kritične infrasturkture dosta su slični, tako da je i sama uloga policije dosta slična u Republici Srpskoj i Srbiji. Ono po čemu policija Republike Srbije, odnosno nadležno ministarstvo ima značajniju ulogu jeste imenovanje oficira za vezu na prijedlog operatora kritične infrastrukture.[23] Dosta značajniju ulogu policija Republike Srbije ima i u primjeni Zakona o vanrednim situacijama.[24] Ovim zakonom propisan je širok djelokrug ministarstva u pogledu zaštite i spasavanja, kao i samo angažovanje policije za poslove zaštite i spasavanja kao jednog od nekoliko predviđenih snaga zaštite i spasavanja. Takođe, uloga policije ogleda se i u procesu rukovođenja od strane nadležnog organa ministarstva u slučajevima kada učestvuje policija.

Na osnovu prethodno opisanog vidljivo je da policija ima veliku ulogu kako u zaštiti kritične infrasturkture, tako i u postupanju u vanrednim sitacijama

[22] Sektor za vanredne situacije kao organizaciona jedinica Ministarstva unutrašnjih poslova Republike Srbije formiran je 2019. godine, spajanjem do tada postojećih organizacionih jedinica i to Sektora za zaštitu i spasavanje i Uprave za vanredne situacije Ministarstva unutrašnjih poslova. **Sektor za vanredne situacije** obavlja poslove normativne, upravne, organizaciono-tehničke, preventivne, preventivno-tehničke, obrazovne, informativno-vaspitne i druge prirode za organizovnje, planiranje, sprovođenje, kontrolu mera zaštite životne sredine, zdravlja i materijalnih dobara građana, očuvanje uslova neophodnih za život i pripremanje za prevladavanje situacije u uslovima požara, elementarnih nepogoda tehničkih i tehnoloških nesreća, dejstva opasnih materija i drugih stanja, opasnosti većih razmera koje mogu da ugroze zdravlje i živote ljudi i životnu sredinu ili da prouzrokuju štetu većeg obima i pružanje pomoći kod otklanjanja posledica (smanjivanje i sanaciju) prouzrokovanih u vanrednim situacijama, a posebno: izrade i predlaganje zakona, normativa i preporuka koji ispunjavaju zahteve Evropske unije u oblasti zaštite i spasavanja u vanrednim situacijama u cilju potpunog pravnog uređivanja za obavljanje poslova; uspostavljanje institucionalnih, organizacionih i personalnih uslova za sprovođenje zaštite i spasavanja u vanrednim situacijama; preuzimanje preventivnih mera radi sprečavanja izbijanja požara i ublažavanja posledica elementarnih nepogoda, tehničko-tehnoloških nesreća i sl. kao i prevencija u cilju sprečavanja ugrožavanja zdravlja građana usled dejstva opasnih materija i drugih stanja opasnosti; vrši stručno osposobljavanje pripadnika organizacionih jedinica na poslovima delokruga Sektora (Uprave i Odeljenja), i dr.

[23] Zakonom o kritičnoj infrasturkturi Republike Srbije propisano je da operatori kritične infrastrukture moraju imati oficira za vezu. Oficir za vezu je lice koje služi kao kontakt između operatora i nadležnog ministarstva, a u vezi pitanja iz oblasti kritične infrastrukture i njene zaštite. Oficira za vezu predlaže operator, a imenuje se od strane nadležnog ministarstva i istome se izdaje licenca. Imenovanje oficira za vezu vrši se uz prethodno sagledavanja da li isto ispuanjava zakonom propisane uslove.

[24] Zakon o vanrednim situacijama (Službeni glasnik RS broj: 111/2009, 92/2011 i 93/2012).

koje u najvećoj mjeri mogu doprinijeti ugrožavanju kritične infrastrukture. Teško je predvidjeti sve situacije u kojima se zahtjeva potreba angažovanja policije i propisati nešto tako kroz djelokrug rada policije. Kao što je u prethodnom tekstu navedeno u praksi postoji niz situacije gdje u zaštiti kritične infrastrukture i postupanju policije u zaštiti i spasavanju dolazi do djelovanja i van zakonskih propisa jer iste nisu predviđene i za iste nije propisan precizan način djelovanja. Upravo iz toga razloga zahtjeva se sprovođenje postupka procjene ugroženosti kritične infrastrukture, odnosno njenih segmenata od svih oblika i vidova ugrožavanja. U Republici Srbiji nešto tako se i radi, te je nadležno ministarstvo izradilo procjenu rizika od katastrofa u Republici Srbiji. Međutim, i pored izrade procjena i drugih dokumenata u praksi postoje razne mogućnosti za potrebe reagovanja policije u slučajevima ugrožavanja ili pojave vanrednih situacija. Prije svega ovo je potrebno posmatrati kroz činjenicu da li je nekakvo ugrožvanje ili vanredna situacija izazvana od strane ljudskog faktora ili prirodnih pojava.

Određeno ponašanje čovjeka koje je najčešće sa obilježjem krivičnog djela može dovesti do pojave raznih događaja koje se manifestuju kao vanredne situacije. Najčešći oblici takvoga ponašanja mogu biti u vidu terorizma ili terorističkih akata, otmice, iznude, prijetnje oružjem, kao i mnoge druge aktivnosti koje mogu dovesti do ugrožavanja određenih vrijednosti društva. Svakako da je terorizam prijetnja današnjice koja dominantno ugrožava pojedinačne države i vrijednosti koje su zaštićene (život i zdravlje ljudi, imovina itd.). Posebno je izražena teroristička prijetnja po kritičnu infrastrukturu.[25] Cjelokupnan sistem kritične infrastrukture direktna je meta terorističkog djelovanja. Upravo iz ovoga može se zaključiti kakvu ulogu policija ima u zaštiti kritične infrasturkutre u pogledu postojanja mogućeg ugrožavanja kao ljudskog faktora. Jedan od osnovnih poslova policije koji proizilazi iz djelokruga rada jeste sprečavanje vršenja krivičnih djela, otkrivanje krivičnih djela i njihovih izvršilaca, pronalazak izvršilaca krivičnih djela i predaja nadležnim organima. Ovo zahtjeva stalno postupanje policije i hitno djelovanje po ukazanoj potrebi u pogledu utvrđivanja identiteta izvršilaca krivičnih djela usmjerenih ka ugrožavanju kritične infrasturkutre ili prouzrokovanju pojava vanrednih situacija, otkrivanje meta napada, kao i svih drugih neophodnih informacija u cilju pravovremenog reagovanja i preduzimanja potrebnih mjera zaštite. Takođe, jedna od mjera policije koja je može se reći prva i najbitnija u ovakvim ili sličnim situacijama je evakuacije i

[25] Šikman M., Amidžić G., 2014, *Nadležnost i uloga policije u vanrednim situacijama u Republici Srpskoj*, Bezbednost 3/2014.

zbrinjavanje stanovništva iz dijelova koji su ugroženi i njihovo smještanje na bezbjedno mjesto.[26]

S druge strane prirodne pojave u posljednih nekoliko godina dosta su česte u pogledu ugrožavanja kritične infrastrukture i izazivanja pojava vanrednih situacija. Najčešći oblik koji je u prethodnom periodu bio prisutan na prostoru kako Republike Srpske, tako i na prostoru Republike Srbije, jesu poplave kao elementarne nepogode izazvane velikim padavinama. Takve pojave najviše bile su pristune tokom 2010. i 2014. godine. U ovim godinama za vrijeme ovakvih pojava dolazilo je i do težih posljedica po ljudski život, nastupanja smrti, kao i izazivanja velikih materijalnih šteta. Naravno, pri ovakvim pojavama u ulozi zaštite i spasavanja i zaštite kritične infrastrukture veliku i značajnu ulogu imala je policija. Preduzimalo se niz potrebnih mjera, angažujući maksimlne ljudske resurse uz stalne službe rada, organizovanje pojedinih oblika dežurstava, izrada određenih procjena, planova i na kraju samih izvještaja o postupanju. Angažovanje policije bilo je prisutno tokom samih dešavanja, ali i nakon prestanka istih, odnosno u sprovođenju mjera sanacije objekata i prostora u kojima su izazvane posljedice.[27] U ovim pojavama najviše su pogođeni sektori poljoprivrede, privrede i transporta. Policija je imala veliki zadatak za vrijeme trajanja ovakve situacije. Pored očuvanja povoljnog stanja bezbjednosti po svim segmenitima, aktivno je učestvovala u evakuaciji stanovništa u mjestima gdje je to bilo potrebno, kao i dostavu potrebnih životnih namjernica stanovništvu koje je bilo blokirano u poplavljenim područjima. Naravno, pored policije učestvovali su i drugi subjekti zaštite, kao i druge organizacije. Pored navedenoga jedna od može se reći „svježih“ prirodnih pojava koja je dovela do ugrožavanja i obustave normalnog funkcionisanja kritične infrastrukture jeste pogoršanje epidemiloške situacije izazvane pojavaom virusa „COVID 19“. Sa ovom pojavom bile su

[26] Tokom 2022. godine u više navrata u Republici Srpskoj i Srbiji dolazilo je do zaprimanja prijetnji da se u pojedinim objektima nalaze eksplozivne naprave. Jedno od takvih slučajeva koje je dovelo do uznemiravanja cjelokupne javnosti jeste upućivanje prijetećih poruka putem elektronske mreže sa sadržajem da se u objektima škola nalaze eksplozivne naprave i da može doći do posljedica. Ovakvom pojavom bile su obuhvaćene sve škole u Republici Srpskoj. Pored školskih ustanove iste ili slične poruke bile su upućene i prema bolnicama i drugim ustanovama koje po svojim karakteristima pripadaju grupi sektora kritične infrastrukture. Naravno, u svim situacijama veliku i znajačnu ulogu imala je policija i to od momenta zaprimanja prijava o takvi, porukama, do same potrebe djelovanja i preduzimanja svih mjera i cilju provjere tačnosti takvih prijetnji i eventualnog sprečavanja nastanka posljedica. Sektori kritične infrastrukutre koji su bili obuhvaćeni ovakvim prijetnjama na jedan period bili su onesposobljeni i u istim je došlo do prekida normalnog procesa rada.

[27] Učešće policijskih službenika za vrijeme trajanja takvih pojava, kao i nakon prestanka pojava u pogledu čišćenja prostora gradova i optšina, kao i objekata u gradovima i optšinama, a koje su pogođeni poplavama.

pogođene sve zemlje regiona. Ova pojava u Republici Srpskoj i Srbiji bila je pristuna od mjeseca martu 2020. godine.[28] Od pojave prvih slučajeva nadležni organi su započeli sa analizom cjelokupne situacije i sprovođenje određenih aktivnosti. Aktivnosti su se realizovale kroz preporuke i naredbe, kao i donošenje određenih odluka. Neke od tih odluka bile su obustave nastavnih procesa u svim obrazovnim ustanovama, ograničenja, a zatim i potpuna obustava rada trgovinskih i ugostiteljskih objekata, donošenje odluka ograničenja kretanja tzv. „policijski čas“, donošenje odluka u pogledu korištenja zaštitne opreme (maske i rukavica), kao i druge mjere koje su nadležni organi smatrali kao adekvatne. Upravo policija je bila jedini organ koji je u najvećem broju imao obavezu kontrole poštovanja naredbi i odluka nadležnih organa i njihovo dalje sprovođenje. Policija je imala ulogu i obavezu kontrole i primjene propisa u pogledu daljeg sankcionisanja za nekorištenje zaštitnih maski i rukavica kako je to bilo propisano, zatim imala je obavezu sprovođenja poslova u pogledu poštovanja odluke o ograničenom kretanju i sankcionisanju onih koji taku odluku nisu poštovali. Takođe, policijski organ bio je jedini koji je izdavao određene potvrde o mogućem nesmetanom kretanju uz prethodno ispunjene uslove, a koji su bili precizno propisani. Policija je vršila i sprovođenje mjera u pogledu poštovanja radnog vremena ugostiteljskih objekata. Pored niza mjera koje su bile sprovedene za vrijeme trajanja takve situacije, policija je imala obavezu i sprovođenja mjera nakon prestanka vanredne situacije, a jedna od tih je bezbjedna distribucija i prevoz doza vakcina koje su bile transportovane u i kroz Republiku Srpsku i Srbiju. Takođe, jedno od čestih prirodnih pojava usljed kojih dolazi do ugrožavanja kritične infrastrutkure i pojave vanrednih situacija jesu požari. Uloga policije u ovakvim situacijama nije izostavljena, postoji potreba za preduzimanjem raznih aktivnosti, a neke od tih jesu i zajedničko učešće sa drugim subjektima u lokalizovanju požara.

Sagledavanjem kako sa normativnog, tako i sa pratičnkog aspekta može se zaključiti da nema dileme da je postupanje policije u pogledu zaštite kritične infrasturkture i u pojavama vanrednih situacija veoma važno. Uloga policije u ovakvim situacijama može se posmatrati kroz dva vida djelovanja. Prvi vid djelovanja je preduzimanje osnovnih redovnih poslova i zadataka koji se odnose na očuvanje stanja bezbjednosti u svim segmentima. Ovdje se misli na svakodnevne uobičajne poslove koje su u nadležnosti policije. Drugi vid djelovanja policije odnosi se na sprovođenje konkretnih aktivnosti vezanih za određenu pojavu. U zavisnosti o kakvoj prirodnoj pojavi se radi, obliku i izvoru ugrožavanja, kao i samom objektu koji je ugrožen, zahtjeva se djelovanje

[28] U Republici Srpskoj prvi slučaj evidentiran je 05.03.2020. godine, a u Republici Srbiji 06.03.2020. godine.

policijskih organa. Takvo djelovanje podrazumjeva razne mjere i radnje uz maksimalne ljudske i materijalno – tehničke resurse sa kojima se raspolaže. Ono što je važno u ovakvim situacijama jeste stalni proces rukovođenja i konstano usmjeravanja sprovođenja potrebnih aktivnosti. Takođe, treba imati u vidu da se u ovakvim situacijama angažuju mnogobrojni subjekti, te je neophodna stalna koordinacija i komunikacija između policijskog organa i subjekata uključenih u preduzimanje potrebnih mjera i aktivnosti. Postoje određene aktivnosti, odnosno mjere i radnje koje u ovakvim slučajevima isključivo može preduzeti samo policija, jer se radi o takvim poslovima koji su u nadležnosti samo policijskog organa.

Kada se govori o zaštiti kritične infrastrukture jedna od prvih, može se reći najblažih i osnovnih mjera, jeste preventivno djelovanje. Preventivno djelovanje u ovoj oblasti ne podrazumjeva samo djelovanje policije, nego svih subjekata iz ove oblasti zaštite. Međutim, kao i u najevećem dijelu policijski organi su osnovni i najvažniji u pogledu regoavanja na ove pojave. Uloga policije u preventivnom djelovanju ogelda se u vidu pružanja savjeta, načina reagovanja i ponašnja koje je usmjereno prema građanima. Takođe, važno je istaći i potrebu povećanja svjesti i znanja o kritičnim infrasturkturama i njenoj zaštiti u svim oblastima rada. Činjenica je da u obrazovnom sistemu nema dovoljno nastavnog procesa koji se bavi ovom problematikom. Imajući u vidu značaj kritičine ifrastrukture, njene sve sektore, kao i mogućnosti ugrožavanja, postoji potreba stalnog stručnog usavršavanja određenih subjekata, prvenstveno policijskih službenika koji u najvećoj mjeri imaju obavezu primjene postojećih pravnih propisa iz ove oblasti.

ZAKLJUČAK

Kritične infrastrukture i njena zaštita danas predstavljaju jednu od ključnih i najaktuelnih tema u većini zemalja. Međutim, može se istaći i činjenica da u pojedinim zemljama svijest o ovoj važnoj temi još uvijek nije dostigla dovoljan nivo. Samo shvatanje značaja kritične infrastrukture za cjelokupno društvo je uslov za pronalaženje adekvatnih mjera njihove zaštite. Takođe, ovo je i jedan od preduslova za izradu i donošenje pravnih propisa u pogledu zaštite sektora kritične infrastrukture. Zadatak cjelokupnog društva jeste predviđanje i stavaranje dovoljno dobrih i adekvatnih mjera za sprečavanje nastanka pojava kojima se ugrožavaju sektori kritičine infrasturkutre i djelovanje na takve pojave sa ciljem smanjenja posljedica. Iz prethodnog je vidljivo da u pojavama vanrednih situacija dolazi i do ugrožavanja kritičnih infrastruktura. Društvo bi trebalo da važećim normativima uredi sistem djelovanja svih adekvatnih subjekata u takvim pojavama u cilju zaštite kritične

ifrastrukture. Naravno, nije dovoljno samo postojanje takvih propisa, nego i njihova adekvatna primjena. U Republici Srpskoj i Sribiji takvi propisi postoje i donijeti su u cilju uvođenja i usaglašavanja sa određenim direktivama. Cjelokupnim sistemom upravljanja kritičnim infrasturkura i njihovom zaštitom u pojavama vanrednih situacija utvrđena je organizaciona strutkrua, djelokrug i nadležnosti rada svih subjekata i snaga, kao i razrada pojedinih procedura. Iz prethodnog teksta, a i važećih normativa jasno se vidi da policija predstavlja jedan od osnovnih i veoma važnih subjekata u pogledu ove problematike. Potvrda toga je i činjenica da je u Republici Srbiji organizaciono formirana posebna jedinica, odnosno sektor koji ima djelokrug rada u oblasti vanrednih situacija. Treba istaći i činjenicu da su neke od nadležnosti policije u ovoj oblasti propisane zakonskim propisima, dok u nekim slučajevima dolazi do potrebe reagovanja i van zakonskih propisa. Ovdje je potrebno sagledati stanje policijske organizacije i njene adekvatne obučenosti i opremljenosti za djelovanje i preduzimanje potrebnih mjera i radnji u cilju zaštite kritične infrastrukture. Pored toga bilo bi potrebno i često sprovođenje edukacija na temu zaštite kritične infrastrukture za sve resusre koji djeluju u ovoj oblasti, kao i za sve druge građane, a koje bi bile edukativno preventivnog karaktera. Jedna takođe od bitnih stavki u ovoj oblasti jeste i uspostavljanje zajedniče saradnje svih organa u ovoj oblasti, kao i povećanja nivo njihove međusobne komunikacije i koordinacije.

LITERATURA

1. Jovičić D., 2008, *Organizacija i nadležnost policije*, Fakultet za bezbjednost i zaštitu Banja Luka.
2. Jovičić D., Šetka G., 2015, *Organizacija i nadležnost policije*, Fakultet za bezbjednost i zaštitu Banja Luka.
3. Jakovljević V., 2010, *Resursi kritične infrastrukture i njihov značaj za upravljanje vanrednim situacijama*, Godišnjak FB 2010, Beograd.
4. Mijalković S., Keserović D., 2010, *Osnovi bezbjednosti*, Fakultet za bezbjednost i zaštitu Banja Luka.
5. Mićićović M., 2014, *Specifičnost zaštite kritične infrastrukture*, Bezbednost 3/2014, Beograd.
6. Trut D., 2020, *Utjecaj normativnog okvira na upravljanje kritičnom infrastrukturom,* Zbornik radova VII. Međunarodne znanstveno – stručne konferencije, Zagreb.
7. Šikman M., Amidžić G., 2014., *Nadležnost i uloga policije u vanrednim situacijama u Republici Srpskoj*, Bezbednost 3/2014.

8. Zakon o bezbjednosti kritičnih infrastruktura u Republici Srpskoj (Službeni glasnik RS broj: 58/19).
9. Zakon o kritičnoj infrastrukturi Republike Srbije od 09.11.2018. godine.
10. Zakon o kritičnim infrastrukturama Republike Hrvatske (Narodne novine broj: NN: 56/13).
11. Zakon o zaštiti i spasavanju u vanrednim situacijama (Sužbeni glasnik RS broj: 121/12, 46/17 i 111/21).
12. Zakon o vanrednim situacijama (Službeni glasnik RS broj 111 od 29.12.2009., broj 92 od 07.12.2011. godine i broj 93 od 28.09.2012. godine).

COMPARATIVE OVERVIEW OF THE ROLE OF THE POLICE IN THE PROTECTION OF CRITICAL INFRASTRUCTURE IN THE REPUBLIC OF SRPSKA AND REPUBLIC OF SERBIA

Gojko Šetka, PhD
Aleksandar Đekić, MA

Abstract: Almost all modern protection and rescue systems recognize the critical infrastructure, i.e. its protection, as a significant element. Due to its importance to the society and the state, critical infrastructure is regulated in normative, functional and institutional terms. Threats to critical infrastructure can be manifested in different ways. Due to large number of modalities to endanger the critical infrastructure, there was a need for all actors in a society to undertake a large number of necessary measures with the aim to reduce risks and be ready to respond adequately to the elimination of potential dangers or consequences of those dangers. Therefore, most countries have regulated the system of protection of critical infrastructure in normative terms, defining and passing various laws and by-laws. The normative system for the protection of the critical infrastructure has been developed both in the Republic of Srpska and the Republic of Serbia. This paper will discuss the role of the police in the protection of critical infrastructure, the activities the police perform in protecting critical infrastructure, and will provide a comparative overview of the role of the Ministry of the Internal Affairs in the protection of critical infrastructure in the Republic of Srpska and the Republic of Serbia.

Keywords: police, police work, critical infrastructure, protection, endangerment.

Pregledni rad

PROMJENE U MAĐARSKOJ STRUKTURI KIBERNETIČKE ODBRANE TOKOM PROVEDBE PROPISA EVROPSKE UNIJE

dr. Márton András[1]

Abstrakt: Narodna Skupština Mađarske je usvojila prvi zakon o informacijskoj sigurnosti državnih i lokalnih tjela pod brojem zakon 50/2013. Uloga ovog zakona je bila implementacija propisa EU-a o kibernetičkoj sigurnosti u mađarski pravni sistem. Glavni cilj uredbe je zaštita takozvane nacionalne elektroničke imovine, informatičkih sistema državnih institucija, općina i kritične infrastrukture. Zakon je stvorio modernu strukturu mađarske kibernetičke obrane. Ovim zakonom je osnovano Nacionalno Vijeće za Kibernetičku Koordinaciju kao glavno tijelo organizacija, koje koordinira rad državnih aktera u području kibernetičke obrane i prati aktivnosti državnih institucija u korist električne narodne imovine. U 2015. godini temeljito su izmijenjeni dotadašnji propisi radi osnivanja jedinstvene kibernetičke zaštite na nacionalnoj razini. U ovom zakonu za obavljanje operativnih poslova kibernetičke zaštite je uspostavljena Stručna Služba Nacionalne Sigurnosti. Dana 1. oktobra 2015. u okviru Stručne Službe Nacionalne Sigurnosti je osnovan Nacionalni Institut za Kibernetičku Obranu. Ovaj institut obavlja poslove upravljanja događajima u slučaju kibernetičkih napada na pojedine elemente kritičnih infrastruktura. Drugi važan zadatak instituta je službeni nadzor internetskih tržišta i pružatelja internetskih usluga. Cilj ovoga rada je predstaviti mađarsku nacionalnu strukturu kibernetičke obrane uz detaljan prikaz odgovornosti svakog aktera. Rad ukratko pokriva sudjelovanje Nacionalnog instituta za kibernetičku obranu u međunarodnoj saradnji. Navedene su organizacije koje podržavaju međunarodnu saradnju i koje omogućuju razmjenu informacija između država članica EU-a tokom upravljanja incidentima povezanima s kibernetičkim napadima.

Ključne reči: IT bezbjednost, sajber zaštita, upravljanje IT incidentima

[1] dr. Márton András PhD student, Pázmány Péter Katolikus Egyetem

RAZLOZI ZA KREIRANJE NIS 2 DIREKTIVE

Evrposka Unija nastoji da ojača sajber bezbjednost obnavljanjem direktive NIS 1, koja reguliše zaštitu bezbjednosti IT sistema.[2] Evropska Komisija želi da nadoknadi novim odredbama sajber zaštite nedostatke prethodne direktive NIS 1. Nova uredba je opravdana i činjenicom da je digitalizacija ubrzana u zemljama članicama zbog epidemije COVID-19. Zbog toga je bilo neophodno povećati nivo sajber zaštite. Prethodna direktiva NIS 1 nije na zadovoljavajući način regulisala pojedina pitanja. Najvažniji problem je bio što NIS 1 nije stvorila mogućnost saradnje država članica u oblasti upravljanja IT incidentima.

Direktiva NIS 1 je bila zadovoljna uspostavljanjem obaveze izvještavanja o sajber napadima na pružaoce osnovnih usluga i provajdere digitalnih usluga. U ovoj novoj direktivi je veoma široko definisan opseg pružalaca osnovnih usluga. U ovaj krug je, između ostalog, uključio i dobavljače vode za piće, one koji obavljaju poslove komercijalnog bankarstva i operatere električne mreže.

Najvažnija odredba direktive NIS 1 bila je što je obavezala države članice Evropske Unije da uspostave nacionalni organ zadužen za bezbjednost IT sistema. U Mađarskoj je ovaj zadatak 2018. godine dobila Služba nacionalne bezbjednosti.[3] Pored toga, morali su da naprave grupu za reagovanje na IT bezbjednosne incidente (u daljem tekstu: CERT). CERT znači stručna grupa koja je sastavljena prvenstveno od bezbjednosnih analitičara, organizovanih da otkrivaju, analiziraju, reaguju, izvještavaju i sprečavaju incidente sajber bezbjednosti.[4]

Evropska Komisija je obrazložila u pripremnom materijalu dostavljenom Evropskom Parlamentu za donošenje direktive NIS 2 da se sajber napadi razviju najbrže u svijetu i da su ovi napadi sve sofisticiraniji.[5]

U izvještaju Agencije za sajber bezbjednost EU (ENISA) za 2021. godinu je skrenuta pažnja lidera Evropske Unije da su preduzeća koja posluju u EU pretrpela tri puta više sajber napada u 2020. nego u 2015. Prema ENISA-i,

---

[2]Directive 2016/1148. of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union

[3] Stručna Služba Nacionalne Bezbednosti (Nemzetbiztonsági Szakszolgálat, NBSZ) u zakonu 1995/125. o službama nacionalne bezbednosti (1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról) 8. §

[4]CERT (Computer Emergency Responce Team) definition in:
https://www.lawinsider.com/dictionary/computer-emergency-response-team-cert

[5] The NIS2 Directive, A high cimmon level of cybersecurity in the EU, European Parliament Briefing,
in:https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

ovaj broj će nastaviti da raste u narednim godinama. Uprkos tome, pravna lica registrovana u EU troše 40% manje na IT zaštitu od pravnih lica registrovanih u SAD. Direktiva NIS 2 bi trebala da ostvari osnove mjera za upravljanje rizicima u sajber bezbjednosti i obavezu izvještavanja u svim sektorima obuhvaćenim direktivom, kao što su energetski sektor, saobraćaj, zdravstvo i digitalna infrastruktura.[6]

Cilj NIS 2 je da uskladi zahtijeve sajber bezbjednosti različitih država članica i njihove mjere za ostvaranje sajber bezbjednosti. U tom cilju uspostavlja minimalna pravila za države članice i definiše mehanizme za efikasnu saradnju između nadležnih organa svake države članice. Ona aktualizira listu sektora i aktivnosti koji podležu obavezama sajber bezbjednosti i definiše pravne sankcije kako bi se obezbijedilo sprovođenje.[7]

Direktiva uspostavlja Mrežu evropskih organizacija u vezi sa kibernetičkom krizom (EU-CiCLONE), koja će podržati koordinisano upravljanje incidentima i krizama u oblasti sajber bezbjednosti.[8]

Nova direktiva se neće odnositi obavezno na organizacije koje rade u oblastima odbrane, nacionalne bezbjednosti, javne bezbjednosti, sprovođenje zakona. Pravosuđe, parlamenti i centralne banke takođe nisu obuhvaćeni direktivom.[9]

Direktiva NIS 2 će se primjenjivati i na državnom i regionalnom nivou u administraciji države članice. Pored toga, države članice Evropske Unije mogu da odluče da primjenjuje direktivu i lokalna administrativna tijela. Nova direktiva je takođe usklađena sa sektorskim zakonodavstvom, posebno sa Uredbom o digitalnoj operativnoj otpornosti finansijskog sektora (DORA) i Direktivom o otpornosti kritičnih subjekata (CER). Države članice će imati 21 mjesec od stupanja na snagu NIS 2 da počnu sa njenom punom primjenom.[10]

UPRAVLJANJE IT DOGAĐAJIMA U MAĐARSKOJ

Zbog usklađivanja zakona Evropske unije, mađarski parlament je stvorio mađarski sistem upravljanja IT incidentima sa Zakonom L iz 2013. godine. Prilikom izrade zakona zakonodavac je imao u vidu ono što je usvojeno u Strategiji nacionalne bezbednosti Mađarske i Nacionalnoj strategiji sajber

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[7] https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0021.02/DOC_1&format=PDF
[8] Predlog Evropske Komisije za Evropski Parlament broj 2020/0359. str. 11.
[9] Predlog Evropske Komisije za Evropski Parlament broj 2020/0359. str. 1-2.
[10] https://hirlevel.egov.hu/2022/12/05/az-eu-megerositi-a-kiberbiztonsagot-es-reziliencat-az-unio-egesz-teruleten-a-tanacs-uj-iranyelvet-fogadott-el/

bezbednosti Mađarske. U Strategiji nacionalne bezbednosti Mađarske navodi se da je sajber bezbednost Mađarske i mađarskih građana osnovna vrednost. Stvaranje i održavanje naše sajber bezbednosti je preduslov za postizanje svih daljih vladinih ciljeva. Zbog novih bezbednosnih izazova, neophodno je stalno unapređivati sistem odbrane od informacionog i sajber ratovanja.[11]

Vlada Mađarske deluje u cilju definisanog u mađarskoj strategiji sajber odbrane. Kako se broj i sofisticiranost napada na vladu i druge ključne informaciono-komunikacione sisteme povećava, potreban je kontinuiran napor da se ojača zaštita informaciono-komunikacionih sistema. Opšti fenomen je nizak nivo svesti korisnika o bezbednosti informacija, iako je adekvatna svest korisnika o bezbednosti informacija jedan od ključnih elemenata u prevenciji sajber incidenata.[12]

Mađarska strategija sajber odbrane skreće pažnju na to da se, usled brzog razvoja informacionih tehnologija, funkcionisanje države i društva sve više zasniva na digitalizaciji. Slabosti elektronskih informacionih sistema stoga nose bezbednosni rizik. Globalni je trend da su zlonamerne aktivnosti u sajber prostoru sve češće, sofisticiranije i štetnije. Sve je veći broj država i nedržavnih aktera koji koriste sajber prostor za nezakonito pribavljanje kritičnih podataka i vršenje – čak i fizičke – štete u elektronskim informacionim sistemima ili putem njih. Stoga se sajber prostor sada smatra zasebnim operativnim prostorom pored kopna, mora, vazduha i svemira. Budući sukobi će se najverovatnije proširiti još više u sajber prostor.[13]

Strategija sajber bezbednosti uključuje u kategoriji ključne bezbednosne krize sajber napade na vladine IT sisteme, e-javnu upravu, komunalne provajdere, strateške kompanije, elemente vitalne infrastrukture i računarske mreže organizacija važnih za funkcionisanje društva.[14]

Efikasno upravljanje izazove sajber prostora nezamislivo je bez međunarodne saradnje. Vlada Mađarske je definisao kao cilj da će biti aktivno uključena u međunarodne napore i razvije i implementira standarde koji regulišu odgovorno ponašanje u globalnom sajber prostoru i mere za izgradnju poverenja za unapređenje globalne sajber bezbednosti.[15]

---

[11] Odluka Vlade Mađarske broj 1163/2020. o Narodnoj Bezbednosnoj Štrategiji Mađarske (1163/2020. Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról), 31-32. tačke

[12] Odluka Vlade Mađarske broj 1163/2020. o Narodnoj Bezbednosnoj Štrategiji Mađarske (1163/2020. Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról), 21. tačka

[13] Odluka Vlade Mađarske broj 1139/2013. o Narodnij Sajber-bezbednosnoj Startegiji Mađarske (1139/2013. Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról), 70-71. tačke

[14] Odluka Vlade Mađarske broj 1163/2020. o Narodnoj Bezbednosnoj Štrategiji Mađarske (1163/2020. Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról), 124. d) tačka

[15] Odluka Vlade Mađarske broj 1163/2020. o Narodnoj Bezbednosnoj Štrategiji Mađarske (1163/2020. Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról), 162. tačka

Nacionalna strategija sajber bezbednosti Mađarske precizira odredbe Strategije nacionalne bezbednosti. Strategija sajber bezbednosti definiše nacionalne ciljeve, strateške zadatke i vladine instrumente kojih Mađarska može da sprovodi svoje nacionalne interese u mađarskom sajber prostoru. Mađarsi sajber prostor je deo globalnog sajber prostora. Prema definiciji u strategiji, sajber prostor Mađarske je deo elektronskih informacionih sistema globalnog sajber prostora koji se nalaze u Mađarskoj, kao i društvenih i ekonomskih procesa u vidu podataka koji se odvija u Mađarskoj ili je usmeren na Mađarsku, ili u koji je Mađarska uključena.[16]

U Strategiji sajber odbrane, takozvani naridna imovina podataka je navedena kao poseban deo nacionalne imovine uključenog u članak 38. Osnovnog zakona Mađarske. Ovaj deo nacionalne imovine ima pravo na istu zaštitu kao i drugi elementi nacionalne imovine. Strategija sajber odbrane takođe predviđa da mađarski sajber prostor pruža bezbednost i pouzdano okruženje a) za društveni razvoj i integraciju kroz slobodnu, neustrašivu komunikaciju za pojedince i zajednice, b) za ekonomske operatere, c) za učenje i zdrav duhovni razvoj za buduće generacije, g) za elektronsku javnu upravu.[17] Pored očekivanja koja je postavila Evropska Unija, mađarska strategija sajber bezbednosti usklađena je sa strateškim konceptom NATO-a usvojenim u novembru 2010. godine i politikom sajber odbrane iz 2011. i saveznim principima i ciljevima sajber odbrane formulisanim na sastanku NATO-a u Čikagu 2012.

NACIONALNI INSTITUT ZA SAJBER ODBRANU

Zakonom 50. iz 2013. o elektronskoj informacionoj bezbednosti državnih organa i organa lokalne samouprave (u daljem tekstu: Ibtv.) osnovan je Institut za sajber odbranu u Mađarskoj. Dok Ibtv. nije stupio na snagu, Strategija sajber odbrane je već zahtevala uspostavljanje vladinog centra za upravljanje događajima koji bi delovao kao članica organizacije akreditovane

[16] Odluka Vlade Mađarske broj 1139/2013. o Narodnij Sajber-bezbednosnoj Startegiji Mađarske (1139/2013. Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról), 3. tačka

[17] Odluka Vlade Mađarske broj 1139/2013. o Narodnij Sajber-bezbednosnoj Startegiji Mađarske (1139/2013. Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról), 8. tačka

od strane Evropske vladine CERT grupe, kao i sektorske centre za upravljanje događajima koji rade u oblasti pojedinačnih ogranaka.[18]

Mađarski institut za sajber odbranu osnovan je u okviru Stručne Službe Nacionalne Bezbednosti (u daljem tekstu: SSNB) 1. oktobra 2015. godine. Zakon 125. iz 1995. o službama nacionalne bezbednosti propiše da SSNB

a) pruža zaštitu od pretnji i napada koji dolaze iz sajber prostora u skladu sa pravilima nadležnosti utvrđenim u zakonu o elektronskoj informacionoj bezbednosti državnih organa i organa lokalne samouprave,

b) sa izuzetkom sektora nacionalne odbrane, rukovodi pripremom za pretnje iz sajber prostora i srodnim bezbednosnim zadacima,

c) proverava saobraćaj elektronskih komunikacionih mreža, otkriva pretnje i napade koji dolaze iz sajber prostora,

d) sprovodi ili pokreće neophodne mere za prekid napada iz sajber prostora.[19]

Kao rezultat zakonskih izmena koje su stupile na snagu 1. januara 2019. godine, Nacionalini Institut za sajber odbranu obavlja poslove upravljanja događajima za vitalne informacione sisteme, kao i upravljanje događajima i službeni nadzor u slučaju elektronskih komercijalnih usluga. i usluge vezane za informaciono društvo.

U pravne dužnosti Nacionalnog instituta za sajber odbranu spadaju i tzv rad „nacionalne kontakt tačke“, čiji je zadatak domaća koordinacija sajber incidenata sa visokim uticajem unutar Evropske Unije, primanje i slanje izveštaja o incidentima međunarodnim partnerskim organizacijama.

Svrha Nacionalnog instituta za sajber odbranu je podrška IT bezbednosti IT sistema širom zemlje. S jedne strane, ovaj rad ima preventivan karakter, sprovodi se otkrivanjem softverskih ranjivosti i pretnji po bezbednost informacija. S druge strane, on ima reaktivnu prirodu, jer je usmeren na istraživanje bezbednosnih incidenata koji se dešavaju u zaštićenim organima i koordinaciju njihovog upravljanja.

Tokom upravljanja ranjivostima, Nacionalni institut za sajber odbranu prikuplja informacije o ranjivostima softvera i štetnom softveru. Stručnjaci ispituju njihovu relevantnost za bazu korisnika i informišu operatere ovih sistema na opšti ili ciljani način kako bi sprečili bezbednosni incident izazvan pretnjom. U toku aktivnosti upravljanja incidentima, institut kontinuirano prima izveštaje o incidentima koji utiču na IT sisteme i preduzima osnovne mere. Prilikom likvidacije prijavljenog incidenta, sledeći korak je da se obavesti

[18] Odluka Vlade Mađarske broj 1139/2013. o Narodnij Sajber-bezbednosnoj Startegiji Mađarske (1139/2013. Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról), 10. c) tačka

[19] Zakon 125. iz 1995. o službama nacionalne bezbednosti (1995. čvi CXXV. törvény a nemzetbiztonsági szolgálatokról) 8. § (7)

organ ili lice koje ima ovlašćenja ili sposobnost o tome šta treba da se uradi. Institut će po potrebi održavati kontakt sa informatorom. Nakon toga sledi praćenje posledica relevantnog incidenta.[20]

Navedeni su zadaci Nacionalnog instituta za sajber odbranu:

- upravljanje bezbednosnim događajima;
- upravljanje pretnjama;
- dežurstvo;
- analiza/evaluacija;
- učešće u vežbama sajber odbrane, organizovanje vežbi;
- obuka, svest;
- podrška imenovanju službenika za zaštitu informacija;
- saradnja sa centralnim pružaocem usluga i korisnicima u vezi sa upravljanjem bezbednosnim incidentima;
- redovno informisanje rukovodstva, priprema tromesečnih izveštaja.[21]

Pored navedenog, Institut za sajber odbranu predstavlja Mađarsku u EU timu za saradnju u oblasti sajber odbrane. Grupa za saradnju je osnovana 2016. godine direktivom NIS 1 radi sprovođenja njenih odredbi. Grupa za saradnju omogućava razmenu informacija između vlasti država članica i konsultacije stručnjaka na dnevnoj bazi. Grupa se redovno sastaje. Ima unapred utvrđen plan rada za dve godine. Na osnovu iskustva iz prethodnih godina, najvažnija uloga Grupe za saradnju je razmena najboljih praksi između država članica, i razvoj najboljih praksi zasnovanih na iskustvima država članica.[22]

Regionalni nivo međunarodne saradnje obezbeđuje Centralnoevropska platforma za sajber bezbednost (CECSP). Od 2013. godine manastir obezbeđuje regionalnu stratešku i operativnu saradnju između zemalja V4 i Austrije. Osnovna svrha platforme je da pomogne u prikupljanju dobrih praksi, razmeni iskustava i razmeni znanja, kako bi se zahvaljujući regionalnoj saradnji stekle efikasnije odbrambene i otporne sposobnosti tokom odbrane od sajber napada. U cilju postizanja ovih ciljeva, članovi platforme redovno održavaju vežbe sajber bezbednosti, kao i sastanke na strateškom i tehničkom nivou. Nacionalni institut za sajber odbranu aktivno učestvuje u radu platforme.[23]

Mađarski nacionalni institut za sajber odbranu takođe aktivno učestvuje u radu zajedničke organizacije EU za sajber odbranu. Agencija Evropske unije za bezbednost mreža i informacija (ENISA) značajno doprinosi uspostavljanju i održavanju visokog nivoa mrežne i informacione bezbednosti unutar Unije.

[20] https://nki.gov.hu/intezet/tartalom/magunkrol/

[21] https://nki.gov.hu/szolgaltatasok/tartalom/incidenskezeles/

[22] The NIS Cooperation Group, in: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

[23] CECSP, in: https://www.enisa.europa.eu/news/enisa-news/central-european-cyber-security-platform-2014

ENISA obezbeđuje stvaranje i razvoj nacionalnih institucija za upravljanje događajima, razvijati kulturu mrežne i informacione bezbednosti u društvu i podizati njegovu svest, doprinoseći na taj način pravilnom funkcionisanju unutrašnjeg tržišta. Nacionalni institut za sajber odbranu je takođe predstavljen u odboru direktora ENISA-e. Pored toga, ekspertske grupe ENISA-e podržavaju mađarski stručnjaci.[24]

NACIONALNI SAVJET ZA KOORDINACIJU SAJBER BEZBJEDNOSTI

Ibtv i Nacionalna Strategija za sajber bezbednost Mađarske predviđaju osnivanje Nacionalnog Saveta za koordinaciju sajber bezbednosti (u daljem tekstu: Savet).[25] Njen zadatak je da koordinira aktivnosti državnih aktera koji obavljaju poslove sajber odbrane. Predsednik Saveta je šef Stručne Službe nacionalne bezbednosti. Članovi Saveta po Strategiji sajber bezbednosti:

a) 1 lice koje delegira ministar unutrašnjih poslova, b) 1 lice koje delegira ministar građevinarstva i investicija, c) 1 lice koje delegira ministar narodne odbrane, d) 1 lice koje delegira ministar pravde, e) 1 lice koje delegira ministar spoljnih poslova i trgovine, đ) 1 lice koje delegira ministar nadležan za kulturu i inovacije, g) 1 lice delegirano od strane ministra finansija, h) 1 lice koje delegira ministar poljoprivrede, i) 1 lice koje delegira ministar nadležan za administraciju, j) 1 lice delegirano od strane ministra tehnologije i industrije, k) 1 lice delegirano od strane ministra za ekonomski razvoj, l) 1 lice delegirano od strane ministra regionalnog razvoja, m) 2 lica koje delegira ministar nadležan za Kabinet premijera.[26]

Predsednik Saveta o svom radu izveštava ministra nadležnog za Kabinet premijera najmanje svakih šest meseci. Rad Saveta pomaže Forum za sajber bezbednost, koji je telo univerzitetskih, istraživačkih, stručnih, privrednih i drugih nevladinih aktera koje Savet poziva.

Koordinacione aktivnosti Saveta i sprovođenje njegovih odluka podržavaju Nacionalna radna grupa za sajber prostor i Radna grupa za sajber prostor međunarodne i Evropske unije. Na preporuku Nacionalne radne grupe za sajber prostor, Savet može izdati preporuke koje nemaju pravno obavezujuću snagu o najboljim praksama koje treba primeniti u oblasti upravljanja sajber napadima i bezbednosti elektronskih informacija. Zadatak Nacionalne radne

[24] ENISA: https://www.enisa.europa.eu/topics/cybersecurity-policy

[25] Vladin dekret broj 484/2013. o Nacionalni savet za Koordinaciju sajber bezbednosti (484/2013. Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról)

[26] Vladin dekret broj 484/2013. o Nacionalni savet za Koordinaciju sajber bezbednosti (484/2013. Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról) 1-2. §§

grupe za sajber prostor je jačanje nacionalne sajber bezbednosti u svim sektorima.[27]

Zadatak Radne grupe za sajber prostor Međunarodne i Evropske unije je da omogući redovnu razmenu informacija između državnih organa, u međunarodnim organizacijama, u Evropskoj uniji, kao i u bilateralnoj i multilateralnoj saradnji, kao i da omogući redovnu razmenu informacija u vezi sa razvoj relevantne pozicije koju će predstavljati Mađarska.[28]

Savet direktno podržava donošenje odluka vlade u oblasti sajber bezbednosti. Na taj način olakšava koordinaciju vladinih aktivnosti i prati sprovođenje vladinih odluka koje se odnose na sajber bezbednost. Uzimajući u obzir preporuke Foruma za sajber bezbednost, Savet priprema akcioni plan koji sadrži mere vlade. Naziv ovog dokumenta je Nacionalni akcioni plan za sajber bezbednost. Radu Saveta u tome pomažu dve radne grupe za sajber bezbednost. Konačnu verziju dokumenta Vlada prihvata. Nacionalni akcioni plan za sajber bezbednost mora da se pregleda svake godine od strane Saveta.[29]

ZAKLJUČAK

Mađarski sistem sajber odbrane karakteriše dvojnost. S jedne strane, sistem je veoma centralizovan. Radom Nacionalnog instituta za sajber odbranu upravlja vlada. S druge strane, struktura sajber odbrane je otvorena iz dva pravca. Jedan od razloga otvorenosti je što je sistem nastao kroz multilateralnu saradnju. Tako se uklapa u zahteve EU. Još jedan odraz otvorenosti sistema je to što je, u vezi sa aktivnostima Mađarskog nacionalnog instituta za sajber odbranu i Nacionalnog saveta za koordinaciju sajber bezbednosti, zakonodavac dozvolio učešće profesionalaca iz mađarskog IT sektora. Ovim je zakonodavac stvorio mogućnost da se rezultati istraživanja i razvoja sprovedenih u privatnom sektoru pojave u radu institucija nadležnih za državnu sajber zaštitu. Dobijena poluotvorena i poluzatvorena struktura ispunjava zahteve sajber zaštite modernog doba, jer se inovacije koje generiše privatni sektor i najbolje prakse

[27] Vladin dekret broj 484/2013. o Nacionalni savet za Koordinaciju sajber bezbednosti (484/2013. Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról) 3. § (1)

[28] Vladin dekret broj 484/2013. o Nacionalni savet za Koordinaciju sajber bezbednosti (484/2013. Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról) 3. § (3) - (6)

[29] Vladin dekret broj 484/2013. o Nacionalni savet za Koordinaciju sajber bezbednosti (484/2013. Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról) 5. § (1) - (2)

drugih članova multilateralnog sistema pojavljuju tokom centralizovanog, efikasnog rada.

LITERATURA

1. Directive 2016/1148. of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union,
2. European Committee 2020/0359. számú javaslat, Predlog Evropske Komisije za Evropsi Parlament broj 2020/0359.
3. Magyarország Alaptörvénye, Osvoni Zakon Mađarske
4. 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, Zakon 125 iz 1995. o službama nacionalne bezbednosti,
5. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, Zakonom 50. iz 2013. o elektronskoj informacionoj bezbednosti državnih organa i organa lokalne samouprave
6. 484/2013. Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács létrehozásáról, Vladin dekret broj 484/2013. o Nacionalni savet za Koordinaciju sajber bezbednosti
7. 1163/2020. Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, Odluka Vlade Mađarske broj 1163/2020. o Narodnoj Bezbednosnoj Štrategiji Mađarske
8. 1139/2013. Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, Odluka Vlade Mađarske broj 1139/2013. o Narodnij Sajber-bezbednosnoj Startegiji Mađarske
9. https://nki.gov.hu
10. https://www.lawinsider.com/dictionary/computer-emergency-response-team-cert
11. www.enisa.europa.eu
12. https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0021.02/DOC_1&format=PDF
13. https://hirlevel.egov.hu/2022/12/05/az-eu-megerositi-a-kiberbiztonsagot-es-reziliencat-az-unio-egesz-teruleten-a-tanacs-uj-iranyelvet-fogadott-el/
14. https://nki.gov.hu/intezet/tartalom/magunkrol/

CHANGES IN THE HUNGARIAN CYBER DEFENSE STRUCTURE DURING THE IMPLEMENTATION OF EUROPEAN UNION REGULATIONS

Márton András

Abstract: The National Assembly of Hungary adopted the first law on electronic information security of state and local bodies under the number 50/2013. The role of this law was to implement EU regulations on cyber security into the Hungarian legal system. The main goal of this regulation is the protection of so-called national electronic property, IT systems of state institutions, municipalities and critical infrastructure. The law created the modern structure of Hungarian cyber defense. The National Council for Cyber Coordination was established by this Law as the main body of the organization that coordinates the work of state actors in the field of cyber defense and monitors the activities of state institutions in favor of the electronic national property. In 2015, the existing regulations for the establishment of uniform cyber protection at the national level were thoroughly changed. In this law, the Expert Service of National Security was appointed to carry out the operational tasks of cyber protection. On October 1, 2015, the National Institute for Cyber Defense was established within the Expert Service of National Security. This institute performs event management tasks in case of cyber attacks on certain elements of critical infrastructures. Another important task of the institute is the official supervision of the Internet markets and Internet service providers. The aim of the study is to present the Hungarian national structure of cyber defense with a detailed description of the responsibilities of each actor. The study briefly covers the participation of the National Institute for Cyber Defense in international cooperation. Organizations that support international cooperation that enable the exchange of information between EU member states during the management of incidents related to cyberattacks are listed, too.

Keywords: IT security, cyber protection, IT incident management