Terorističko djelovanje Ruske Federacije nad kritičnom infrastrukturom Ukrajine

Fadljević, Fran

Sveučilište u Zagrebu

Fakultet političkih znanosti

Diplomski studij politologije

Teroristično djelovanje Ruske Federacije nad kritičnom infrastrukturom Ukrajine

DIPLOMSKI RAD

Mentor: izv. prof. dr. sc. Robert Mikac

Student: Fran Fadljević

Zagreb

rujan, 2024.

Izjavljujem da sam diplomski rad „Terorističko djelovanje Ruske Federacije nad kritičnom infrastrukturom Ukrajine“, koji sam predao na ocjenu mentoru izv. prof. dr. sc. Robertu Mikcu, napisao samostalno i da je u potpunosti riječ o mojem autorskom radu. Također, izjavljujem da dotični rad nije objavljen ni korišten u svrhe ispunjenja nastavnih obveza na ovom ili nekom drugom učilištu, te da na temelju njega nisam stekao ECTS-bodove.

Nadalje, izjavljujem da sam u radu poštivao etička pravila znanstvenog i akademskog rada, a posebno članke 16-19. Etičkog kodeksa Sveučilišta u Zagrebu.

____

Sadržaj

1. Uvod

Tema koja se nastoji istražiti u diplomskom radu odnosi se na ukrajinsku kritičnu infrastrukturu koja se našla pod udarom Ruske Federacije. U tom kontekstu potrebno je istaknuti kako već duže vrijeme traje oružani sukob Ruske Federacije i Ukrajine koji je započet 2014. godine uslijed povijesnih, političkih i teritorijalnih konflikata i neslaganja. Neki od primjera takvih konflikata i neslaganja koji su generirali sadašnje ratno stanje su neriješeno pitanje ruske manjine u istočnim dijelovima Ukrajine-Donjecku i Lugansku, teritorijalni spor oko poluotoka Krima te političko protivljenje Ruske Federacije eventualnom ukrajinskom ulasku u NATO savez. Pritom, međunarodna zajednica je u nekoliko navrata pokušavala ponuditi političko rješenje za napetosti i konflikte između Ruske Federacije i Ukrajine od kojih najviše vrijedi istaknuti Sporazum iz Minska koji je potpisan 2014. godine između Ukrajine, Rusije i separatističkih grupa istočnom djelu Ukrajine, uz posredovanje Organizacije za europsku sigurnost i suradnju (OESSS). Navedeni sporazum je imao za cilj ponuditi politički i zakonski kompromisna rješenja za obje strane u sporu te se sastojao od sigurnosnih, političkih, ekonomskih te humanitarnih mjera. Navedene mjere su parcijalno poštivane te se navodi kako je „postignut određeni napredak u pitanjima kao što je razmjena zatvorenika (članak 6.) i povlačenje teškog naoružanja s linije dodira (članak 2.), ali prekid vatre (članak 1.) kršio se gotovo svakodnevno" (Åtland 2020: 17). Nakon niza neuspješnih bilateralnih i multilateralnih pregovora obiju strana te diplomatskih sastanaka, u veljači 2022. godine predsjednik Ruske Federacije Vladimir Putin objavio je početak vojne operacije u Ukrajini. U prvim mjesecima rata glavni vojni cilj zapovjedništva Ruske Federacije sastojao se od raketnih napada na ukrajinsku infrastrukturu zračnog, kopnenog i pomorskog prometa, nuklearnu infrastrukturu, naftnih i plinskih postrojenja te od kibernetičkih napada. Slijedom toga, „tijekom više od 100 dana od početka invazije na Ukrajinu, agresorska država ciljano je napadala kritičnu infrastrukturu Ukrajine u različitim područjima s ciljem maksimiziranja svog resursa moći" (Peptan, 2022: 38), a umanjivanja sposobnosti Ukrajine. Napadi na kritičnu infrastrukturu Ukrajine koji u vrijeme pisanja ovoga rada i dalje traju ukazuju na važnost kvalitetnog upravljanja krizama te posebice na važnost zaštite kritične infrastrukture Ukrajine od strane ruskih terorističkih napada.

U radu će se analizirati sustav zaštite kritične infrastrukture Ukrajine gdje će se objasniti koncept izgradnje državnog sustava zaštite kritične infrastrukture u Ukrajini te će se opisati izazovi i problemi funkcioniranja sustava zaštite kritične infrastrukture Ukrajine. Nadalje, prikazati će se kako je sustav zaštite kritične infrastrukture Ukrajine reagirao i odgovorio na ruske terorističke napade od početka oružanog sukoba 2014. godine s posebnim naglaskom na razdoblje eskalacije rata od 2022. godine. Kako bismo objasnili način na koji je sustav zaštite kritične infrastrukture odgovorio na ruske terorističke napade najprije će se navesti primjeri terorističkih napada koji su izvršeni na kritičnu infrastrukturu Ukrajine od strane Ruske Federacije. Napadi na kritičnu infrastrukturu Ukrajine podijelit će se s obzirom na vrstu infrastrukture te će se analizirati napadi na kritičnu infrastrukturu zračnog prometa, pomorskog prometa, kopnenog prometa, napadi na nuklearne elektrane, napadi na kritičnu infrastrukturu nafte i plina, kibernetički napadi te napadi na obrazovnu i zdravstvenu kritičnu infrastrukturu. Temeljem uvida u vrste napada na objekte kritične infrastrukture Ukrajine u završnom dijelu rada pružit će se prijedlog reformi za unapređenje sustava zaštite kritične infrastrukture Ukrajine. Analizom odgovora sustava zaštite kritične infrastrukture Ukrajine te uvida u napade na objekte kritične infrastrukture Ukrajine odredit će se koji dijelovi sustava zaštite kritične infrastrukture nisu u stanju odgovoriti na prijetnje. Slijedom toga, pružiti će prijedlozi za reforme gdje će se pokušati uzeti u obzir kvalitetne prakse drugih europskih država koje bi se mogle primijeniti u kontekstu sustava zaštite kritične infrastrukture Ukrajine. Osim toga, predložiti će se reforma oružanih snaga s naglaskom na proces usvajanja NATO standarda, modernizaciju vojne opreme te razvoj i unapređenje kibernetičkog sustava.

1.1. Problem istraživanja

Problem istraživanja diplomskog rada jest rat odnosno oružani sukob između Ruske Federacije i Ukrajine koji je započeo 2014. godine ruskom invazijom na Krim te koji je kulminirao u veljači 2022. godine kada je Ruska Federacija započela cjelovitu invaziju nad Ukrajinom. U tom kontekstu vrijedi spomenuti kako je niz političkih događanja utjecalo na sve veći antagonizam između Ruske Federacije i Ukrajine te samim time na eskalaciju sukoba. Neki od takvih političkih događanja su Euromajdan odnosno golemi prosvjed ukrajinske javnosti protiv proruske vlade na čelu Ukrajine, ruska okupacije Krima i nezakonito otimanje teritorija Ukrajine te zahtjevi Ukrajine za članstvom u NATO savezu te Europskoj uniji. Sukladno tome, u okviru gore navedenog konteksta, problem koji je potrebno istražiti jest dugotrajni oružani sukob između Ukrajine i Rusije koji je eskalirao u veljači 2022. godine nakon što je vojska Ruske Federacije mjesecima prije invazije gomilala trupe na granici sa Ukrajinom pod krinkom kopnenih vojnih vježbi. Slijedom takvih događanja predsjednik Ruske Federacije Vladimir

Putin je u zoru 24. veljače 2022. godine objavio kako je pokrenuta tzv. specijalna vojna operacija gdje se kao formalni razlog navela tzv. „demilitarizacija“ i „denacifikacija“ Ukrajine u ruske sigurnosne svrhe. Vladimir Putin je u svome govoru izjavio kako je „svrha ove operacije zaštititi ljude koji se već osam godina suočavaju s poniženjem i genocidom kijevskog režima. U tu svrhu nastojat ćemo demilitarizirati i denacificirati Ukrajinu, kao i izvesti pred sud one koji su počinili brojne krvave zločine nad civilima, uključujući i građane Ruske Federacije“ (Atlanticcouncil.org, 2023).

Stoga, oružani sukob Ruske Federacije i Ukrajine predstavlja problem koji je potrebno istražiti te koji je sa sobom donio niz popratnih pojava od kojih su u svrhu ovoga rada nama najznačajniji teroristički napadi Ruske Federacije na ukrajinsku kritičnu infrastrukturu.

1.2. Predmet istraživanja

Predmet istraživanja diplomskog rada jest sustava zaštite kritične infrastrukture u širem smislu i kritična infrastruktura Ukrajine u užem smislu, koja je od početka oružanog sukoba 2014. godine pretrpjela mnogobrojne napade i uništenja što uključuje i stradavanje civilnog stanovništva. Kritična infrastruktura predstavlja izrazito važan dio sigurnosnog sektora svake države s obzirom da poremećaj u njezinom radu ima za posljedicu sigurnosnu ugrozu države i njezinih građana. Sukladno tome, „definicija kritične infrastrukture općenito obuhvaća takve objekte, sustave, mreže ili njihove dijelove čiji će prekid ili uništenje izazvati teške posljedice za društvene i gospodarske sektore države, utjecati na njezin obrambeni potencijal i nacionalnu sigurnost“ (Kondratov, 2017: 10). Kritična infrastruktura je širok pojma čija definicija varira od države do države te ovisi o političkom i sigurnosnom kontekstu u okviru kojega se država nalazi. Sukladno tome autori Mikac, Cesarec i Larkin navode kako „SAD, Australija, Francuska, Njemačka, Poljska i Hrvatska kritičnu infrastrukturu vide kao infrastrukturu u njenom stvarnom pojmu dok zemlje poput Švedske, Nizozemske, Španjolske i Velike Britanije definiciju više usmjeravaju prema (javnim) uslugama koje su osnovna podrška funkcionalnom gospodarskom i društvenom životu zajednice i države“ (Mikac, Cesarec, Larkin, 2018: 24). Koncept ukrajinske kritične infrastrukture zakonski je definiran te je nekoliko puta spominjan u kontekstu Strategije nacionalne sigurnosti Ukrajine iz 2015. godine gdje je „sigurnost kritične infrastrukture po prvi put spomenuta kao jedno od ključnih područja državne politike nacionalne sigurnosti te su identificirani njezini prioriteti“ (Kondratov, 2017: 13).

Autor Oleksandr Sukhodolia u knjizi „The External Dimension of the European Union’s Critical Infrastructure Protection Programme“ navodi niz dokumenta koji su utjecali na razvoj sustava zaštite kritične infrastrukture Ukrajine. Jedan od takvih dokumenata je „Sporazum o pridruživanju" između Ukrajine i Europske unije, u kojem je područje zaštite kritičnih infrastruktura određeno s dvije direktive a to su Direktiva Vijeća EU 2008/114/EZ i Direktiva (EU) 1148/2016 koje su postale „smjernice za unutarnje napore Ukrajine u razvoju zakonodavne osnove za politiku zaštite kritične infrastrukture" (Sukhodolia, 2022: 134). Nadalje, u dokumentu „O poboljšanju mjera za osiguranje zaštite kritičnih infrastrukturnih objekata" iz 2017. godine navodi se kako su „poduzete mjere za osiguranje sustava zaštite kritične infrastrukture kao i poboljšanje pravne osnove za uspostavu sveobuhvatnog državnog sustava o sustavu zaštite kritične infrastrukture Ukrajine" (ibid: 134). Također, Sukhodolia ističe napore Vlade Ukrajine u kontekstu razvoja sustava zaštite kritične infrastrukture gdje ističe tzv. „Koncept izgradnje državnog sustava zaštite kritične infrastrukture u Ukrajini" koji je odobren od strane ukrajinske Vlade te koji određuje „glavne smjernice, mehanizme i uvjete za sveobuhvatno zakonodavno uređenje" (ibid: 135). Ciljevi takvog koncepta nastoje se ostvariti kroz niz mjera od kojih najviše treba istaknuti „razvoj zakona o kritičnoj infrastrukturi, izrada propisa o kritičnoj infrastrukturi, uspostavljanje javno-privatnog partnerstva, razvoj postupaka razmjene informacija za procjenu rizika i dijeljenje najboljih praksi te daljnje usklađivanje ukrajinskog i EU zakonodavstva u području sustava zaštite kritične infrastrukture" (ibid: 135). Što se tiče zakonskog određenja sustava zaštite potrebno je spomenuti kako je 2019. godine potvrđen i usvojen zakonski prijedlog o zaštiti kritične infrastrukture gdje se utvrđuje kako se sustav zaštite kritične infrastrukture definira kao „skup organizacijskih, zakonodavnih, znanstvenih i drugih mjera s ciljem osiguravanja sigurnosti i otpornosti kritične infrastrukture" (ibid: 135). Osim toga, u okviru Zakona određuje se koncept kritične infrastrukture koji se definira kao „skup objekata koji su strateški važni za gospodarstvo i nacionalnu sigurnost, čije neispravno funkcioniranje može biti štetno vitalnim nacionalnim interesima" (ibid: 135).

S obzirom na to predmet istraživanja odnosi se na niz objekata ukrajinske kritične infrastrukture poput hidroelektrana, nuklearnih elektrana, telekomunikacijskih čvorišta, pomorskih i zračnih luka, vijadukata, mostova te bolnica. Kroz konkretne primjere nastojat će se opisati na koji način je koji tip kritične infrastrukture bio napadnut te kakve posljedice je napad prouzročio.

1.3. Cilj istraživanja

Što se tiče ciljeva istraživanja predstavit će se jedan glavni te dva dodatna cilja istraživanja. Prvi, glavni cilj istraživanja jest analizirati povijest ruskih terorističkih napada na ukrajinsku kritičnu infrastrukturu te identificirati oblike i metode ruskog terorističkog djelovanja. Nadalje, drugi cilj istraživanja odnosi se na procjenu učinkovitosti ukrajinskih sigurnosnih snaga u odgovoru na terorističko djelovanje nad kritičnom infrastrukturom te bi se na taj način pružila ocjena ukrajinskog upravljanja kriznim situacijama u kontekstu zaštite kritične infrastrukture. Zaključno, treći cilj istraživanja jest istražiti međunarodnu reakciju na terorističke napade nad ukrajinskom kritičnom infrastrukturom te samim time identificirati učinkovitost postojećih mehanizama suradnje i podrške.

1.4. Hipoteza i istraživačka pitanja

Hipoteza rada glasi: „Sustav zaštite ukrajinske kritične infrastrukture ne može se uspješno suprotstaviti ruskom terorističkom djelovanju stoga je potreba reforma i uspostava novog sustava zaštite kritične infrastrukture Ukrajine“. Sukladno tome, pretpostavlja se kako postojeći sustav zaštite ukrajinske kritične infrastrukture ne raspolažu adekvatnim protuterorističkim mjerama. Iz tog razloga potrebna je reforma te uspostava novog sustava zaštite kritične infrastrukture Ukrajine koji bi se fokusirao na protuterorističku zaštitu kritične infrastrukture. Sukladno postavljenoj hipotezi postavit će se tri istraživačka pitanja. Prvo istraživačko pitanje glasi: „Kako se definira sustav zaštitite kritične infrastrukture Ukrajine te na koji način funkcionira sustav zaštite kritične infrastrukture Ukrajine“? Drugo istraživačko pitanje glasi: „Kako je sustav zaštite kritične infrastrukture Ukrajine odgovorio na ruske terorističke napade u kontekstu oružnog sukoba?“ te će se u okviru tog istraživačkog pitanja istražiti u kojoj mjeri je sustav zaštite kritične infrastrukture Ukrajine spreman odnosno nespreman upravljati kriznim situacijama u kontekstu terorističkih napada. Zaključno, treće istraživačko pitanje odnosi se na mogućnosti reforme i uspostave sustava zaštite kritične infrastrukture koji bi adekvatno prevenirao i reagirao na terorističke prijetnje stoga treće istraživačko pitanje glasi: „Što je potrebno reformirati kako bi sustav zaštite kritične infrastrukture Ukrajine uspješno prevenirao i reagirao na terorističke prijetnje“?

1.5. Teorijsko-metodološki okvir istraživanja

U kontekstu teorije i metoda istraživanja rad će se bazirati na ključnim elementima teorije realizma. Teorija realizma nastoji analizirati međunarodne odnose kroz prizmu državne moći. U tom smislu, jedan od najpoznatijih teoretičara realizma, John Mearsheimer, izrekao je kako je „za realiste, međunarodna politika sinonim za politiku moći“ (Mearsheimer, 2007: 72). Među teoretičarima realizma postoje brojne razlike koje su najvidljivije u tumačenju koncepta moći gdje postoji ključna razlika između defanzivnih, ofenzivnih te strukturalnih realista. Defanzivni realisti poput Kennetha Waltza protive se državnom povećanju udjela moći s obzirom da će ih, kako tvrdi Waltz (1979), sustav kazniti ako pokušaju dobiti mnogo snage. Suprotno tome, ofenzivni realisti poput Johna Mearsheimera ističu kako je državama oportuno stjecanje pozicije hegemona jer je „posjedovanje nadmoćne moći najbolji način da se osigura vlastiti opstanak" (Mearsheimer, 2007: 72). S obzirom na aktualnu narav oružanog sukoba između Rusije i Ukrajine korištena teorija realizma biti će korištena na osnovama ofenzivnog realizma. Posljednja podvrsta teorije realizma jest strukturalni realizam koji moć analizira relacijski odnosno u kontekstu odnosa cilja i sredstva gdje je „ moć sredstvo za postizanje cilja, a krajnji cilj je preživljavanje" (ibid: 72).

Teorija realizma jedna je od najpoznatijih teorija međunarodnih odnosa za koju je karakterističan „pesimističan pogled na ljudsku prirodu, uvjerenje kako su međunarodni odnosi konfliktni, da se spomenuti konflikti u konačnici rješavaju ratom, naglasak na nacionalnu sigurnost i preživljavanje država" (Luša, 2011: 15, prema Jackson i Sorensen, 2010: 59). Osim toga za teoriju realizma jest karakterističan naglasak na pojmove kao što su sila, moć, interes, suverenost i slično. U tom smislu autor Jović ističe kako „država, njeno ponašanje, njeni interesi i njena uloga - za realiste ostaju središnje polje interesa svakog studija međunarodne politike" (Jović, 2013: 15). U kontekstu istraživanja, teorija realizma će biti primijenjena u svrhu razumijevanja početka oružanog sukoba Ruske Federacije i Ukrajine. Takav odabir je logičan s obzirom da je tematika rada vezana uz međunarodne odnose i pojmove poput moći, interesa, sile i suverenosti.

Nadalje, u radu će se koristiti kvalitativna metoda što se odnosi prvenstveno na metodu analize sadržaja odnosno analizu dokumenata kao što su knjige, znanstveni časopisi te službena izvješća međunarodnih organizacija i/ili nevladinih udruga. Samim time proces zaključivanja će biti induktivan što znači da će se zaključivati od svih prikupljenih detaljnih informacija prema jedinstvenom zaključku.

1.6. Pregled literature i ključni pojmovi

Ključni izvori literature odnose se na knjige i znanstvene radove koji analiziraju teme poput sustava zaštite kritične infrastrukture Ukrajine, ruskih napada na objekte kritične infrastrukture te mogućnosti reforme sustava zaštite kritične infrastrukture. U svrhu objašnjenja definicije i načina funkcioniranja sustava zaštite kritične infrastrukture najvažniji izvor predstavlja rad autora Sergiya Kondratova „*Developing the criticial infrastructure protection system in Ukraine*“ te rad autora Oleksandra Sukhodolie „*Implementation of critical infrastructure protection in Ukraine: achievements and challenges*“ u okviru kojih se objašnjava razvojni proces sustava zaštite kritične infrastrukture Ukrajine te glavni problemi i izazovi u radu. Nadalje, za određivanje razine spremnosti i funkcionalnost objekata kritične infrastrukture Ukrajine ključno je napraviti analizu ruskih napada na objekte kritične infrastrukture Ukrajine gdje je ključan izvor rad „*Considerations on some aggressions against critical infrastructure on the territory of Ukrajine during the „special military operation“ conducted by the Russian Federation*“ autora Catalina Peptana. Završno, za prijedlog reformi sustava zaštite kritične infrastrukture Ukrajine ključni su radovi „*Modern trends in the Armed Forces of Ukraine transformation toward NATO standards*“ autora Andriia Ordynovycha te „*Ukraine Cybersecurity Governance Assessment*“ autorice Natalie Spinu.

1.7. Očekivani rezultati istraživanja

Očekivani rezultati istraživanja su takvi da se najprije dobije jasan uvid u razumijevanje teme terorističkog djelovanja Ruske Federacije nad kritičnom infrastrukturom Ukrajine. Osim toga, očekivani rezultati su da se potvrdi odabrana hipoteza te da se uspješno i precizno odgovori na istraživačka pitanja koja nas fokusiraju na područje razmatranja.

2. Sustav zaštite kritične infrastrukture Ukrajine

Glavni cilj i svrha ovog poglavlja jest objasniti pojam i funkcioniranje sustava zaštite kritične infrastrukture Ukrajine. U ovom poglavlju istraživačko pitanje glasi: „Kako se definira sustav zaštitite kritične infrastrukture Ukrajine te na koji način funkcionira sustav zaštite kritične infrastrukture Ukrajine“? Kako bismo uspješno odgovorili na istraživačko pitanje o definiranju i funkcioniranju zaštite kritične infrastrukture Ukrajine nastojat ćemo objasniti koncept izgradnje državnog sustava zaštite kritične infrastrukture u Ukrajini te će se opisati izazovi i problemi sustava zaštite kritične infrastrukture Ukrajine.

Najprije, potrebno je istaknuti važnost tako zvane „Zelene knjige“ iz 2015. godine koja predstavlja glavnu okosnicu razvoja politike zaštite kritične infrastrukture Ukrajine. Dokument „Zelena knjiga“ je iznimno važan zbog definiranja svrhe sustava zaštite kritične infrastrukture gdje se navodi kako je svrha „osigurati stabilno funkcioniranje infrastrukture i time jamčiti opskrbu robom i uslugama vitalnim za stanovništvo, društvo, poslovanje i vladu“ (Sukhodolia, 2018: 108). Osim toga „Zelena knjiga“ jasno adresira prijetnje kritičnoj infrastrukturi Ukrajine te ih klasificira prema „pristupu svih opasnosti (prirodne katastrofe, hitni slučajevi i tehnički kvarovi, zlonamjerne aktivnosti) s naglaskom na elemente kritične infrastrukture koji bi mogli biti ugroženi (fizički elementi, sustavi upravljanja i komunikacije, osoblje)“ (ibid: 108). Nadalje, „Zelena knjiga“ je presudan dokument u okviru sustava zaštite kritične infrastrukture Ukrajine s obzirom da je temeljem tog dokumenta kako navodi autor Sukhodolia pojam „kritična infrastruktura“ implementiran u zakonodavstvo Ukrajine. Također, „Zelena knjiga“ je presudna za postojanje stručne rasprave o problemima i izazovima u sustavu zaštite kritične infrastrukture Ukrajine te o mogućnostima reforme sustava nacionalne sigurnosti prema NATO i EU standardima u svrhu zapadnoeuropskih političkih i vojnih integracija. Značaj „Zelene knjige“ analizira i autor Sergiy Kondratov koji navodi kako je „Zelena knjiga“ „razvijena kako bi podržala nacionalnu stručnu raspravu o ključnim problemima u uspostavi sustava zaštite kritične infrastrukture za Ukrajinu i načinima za njihovo rješavanje, što će biti vrijedan input u procesu sustavne reforme cjelokupnog sektora nacionalne sigurnosti čime se njegova struktura i funkcije približavaju onima koji postoje u zemljama članicama EU i NATO-a“ (Kondratov, 2017: 11). Slijedom navedenog, dokument „Zelena knjiga“ definira dva ključna pojma za naše istraživanje a to su pojam kritične infrastrukture te sustav zaštite kritične infrastrukture Ukrajine.

2.1. Izazovi i prijetnje

Kako bismo definirali i objasnili funkcioniranje sustava zaštite kritične infrastrukture Ukrajine najprije će se ukazati na izazove i prijetnje koje ugrožavaju kritičnu infrastrukturu Ukrajine te će se zatim definirati i objasniti sustav zaštite kritične infrastrukture Ukrajine. Sukladno tome, ubrzani razvoj tehnologije te fenomeni povezani sa procesom globalizacije doprinijeli su razvoju umreženog političkog i gospodarskog sustava. Posljedično, takvi sustavi postaju puno više ranjiviji i izloženi različitim vrstama sigurnosnih rizika. U tom kontekstu procesi globalizacije i sve većeg međusobnog umrežavanja političkih i gospodarskih sustava odvijaju se u „u kontekstu nagle eskalacije terorističkih prijetnji, posebice na međunarodnoj razini, sve većeg broja katastrofa izazvanih čovjekom, uključujući one uzrokovane ljudskim faktorom, sve većeg broja prirodnih katastrofa uzrokovanih, između ostalog, globalnom klimom" (ibid: 11).

S obzirom na snažno izraženu međuovisnost političkih i gospodarskih funkcija države logično je i postojanje snažne ovisnosti različitih funkcija države o ulozi kritične infrastrukture. Posljedično, disbalans na relaciji (ne)učinkovitog funkcioniranja kritične infrastrukture i političkih te gospodarskih funkcija države koje su ovisne o ulozi kritične infrastrukture može generirati probleme kod niza aktera. O takvom suodnosu kritične infrastrukture i državnih funkcija raspravljaju autori Mikac, Cesarec i Larkin te objašnjavaju „budući da je današnji svijet iznimno ovisan o pojedinim sektorima kritične infrastrukture, kao što su energetski sektor, prometni sektor, komunikacija (informacijska i komunikacijska tehnologija), te javne usluge i servisi, svaki značajniji poremećaj u funkcioniranju može uzrokovati ozbiljne teškoće kod pojedinaca i privrednih subjekata ili institucija koje obavljaju državne funkcije" (Mikac, Cesarec, Larkin, 2018: 32).

Što se tiče trenutnih prijetnji koje ugrožavaju kritičnu infrastrukturu Ukrajine potrebno je istaknuti kako Kondratov razlikuje tri vrste prijetnje kritičnoj infrastrukturi Ukrajine a to su nesreće i tehnički kvarovi, opasne prirodne pojave te zlonamjerne radnje. Slično tome autori Mikac, Cesarec i Larkin razlikuju prijetnje tehnološke prirode, prijetnje prirodnog podrijetla te „hotimične radnje sa štetnom namjerom-terorizam, zlouporaba u ekonomske ili političke svrhe, poticanje oružanih sukoba (npr. građanski rat), akcije društvenog podrijetla (npr. nemiri)" (ibid: 28). Upravo se zlonamjerne radnje odnosno hotimične radnje sa štetnom namjerom odnose na fenomen terorističkih napada na kritičnu infrastrukturu Ukrajine poput nuklearnih elektrana, hidroelektrana, brana, vijadukata, mostova i slično. Kondratov navodi kako je najozbiljnija opasnost koja prijeti sustavu zaštite kritične infrastrukture Ukrajine „korištenje nuklearnih energetskih objekata u terorističke svrhe" (Kondratov, 2017: 22). Takva tvrdnja je u potpunosti ispravna i logična s obzirom da nepravilno postupanje s nuklearnim energetskim postrojenjima od strane terorista može za posljedicu imati nuklearnu katastrofu poput one iz Černobila iz 1986. godine. U tom kontekstu vrijedi spomenuti kako je „ tijekom zauzimanja nuklearne elektrane Černobil od strane trupa Ruske Federacije primijećen čin međunarodnog terorizma, granatiranje teritorija nuklearne elektrane Zaporožje". Sukladno tome takvo postupanje oružanih snaga Ruske Federacije može se okarakterizirati kao korištenje nuklearnog terora u vojno političke svrhe. S obzirom na ogroman rizik koji proizlazi iz granatiranja teritorija nuklearne elektrane Zaporožje može se shvatiti kako je korištenje nuklearnih energetskih objekata (kao meta) u terorističke svrhe zaista jedna od najvećih opasnosti koje prijete opstojnosti i funkcionalnosti sustava zaštite kritične infrastrukture Ukrajine. Kako bi dobili bolji uvid u katastrofalne posljedice koje mogu proizaći iz korištenja nuklearnih energetskih postrojenja u terorističke svrhe vrijedi ukazati na izjavu ukrajinskog predsjednika Volodymra Zelenskog koji je u jednom od svojih intervjua izjavio kako je „napad mogao izazvati razaranje jednako šest Černobila" (ibid: 86).

Osim nuklearnog terora koji predstavlja najozbiljniju opasnost koja prijeti opstojnosti i funkcionalnosti sustavu zaštite kritične infrastrukture Ukrajine mnogi autori izdvajaju nove prijetnje koje mogu uzrokovati kolaps sustava zaštite kritične infrastrukture Ukrajine. Takve nove prijetnje su kibernetički napadi koji postaju sve intenzivniji te od kojih se sve teže moderni demokratski sustavi mogu braniti. Od početka rata u Ukrajini zabilježen je porast kibernetičkih napada na kritičnu infrastrukturu Ukrajine gdje je pritom potrebno istaknuti kako „mete kibernetičkih napada putem interneta uključuju poslužitelje vladinih agencija, velikih tvrtki, financijskih institucija, političkih stranaka, masovnih medija i, u novije vrijeme, informacijsku i telekomunikacijsku infrastrukturu vojnih objekata" (Kondratov, 2017: 22). Posljedice koje proizlaze iz kibernetičkih napada na kritičnu infrastrukturu mogu biti destruktivne za niz aktera i područja nacionalne sigurnosti. Sukladno tome, navodi se kako „kibernetički napadi mogu rezultirati gubitkom osjetljivih informacija i štetom za ekonomsku i nacionalnu sigurnost, gubitkom privatnosti, krađom identiteta ili ugrožavanjem vlasničkih informacija ili intelektualnog vlasništva" (Clark i Hakim, 2016: 5). U svrhu boljeg razumijevanja kako kibernetički napadi mogu ugroziti nacionalnu sigurnost spomenuti će se slučaj koji se dogodio u istočnoj Ukrajini 2015. godine kada je uslijed kibernetičkog napada na mrežu električne energije „struja prekinuta u više od 600 000 domova, a Rusija je identificirana kao vjerojatni izvor napada" (ibid: 7).

Sukladno navedenim prijetnjama i izazovima koji ugrožavaju opstojnost i funkcionalnost kritične infrastrukture u sljedećem pododjeljku definirati će se sustav zaštitite kritične infrastrukture Ukrajine te način na koji sustav zaštite kritične infrastrukture Ukrajine funkcionira.

2.2. Definicija sustava zaštite kritične infrastrukture Ukrajine

Kako bismo ispravno definirali sustav zaštite kritične infrastrukture Ukrajine najprije će se definirati kritična infrastruktura Ukrajine te će se adresirati ključni objekti koji spadaju pod termin kritična infrastruktura Ukrajine.

Kritična infrastruktura, kao što je već rečeno u pododjeljku 1.2 jest širok i kontekstualno ovisan pojam što znači da će različite države u različito vrijeme različito definirati koncept vlastite kritične infrastrukture. Takvu karakteristiku definicije pojma kritične infrastrukture najbolje sažima Kondratov koji navodi kako „ s obzirom na velik broj čimbenika koji na ovaj ili onaj način utječu na život suvremenih ljudi, društava ili država, nužno je jasno definirati opseg onih sustava, mreža i objekata čiji rad podržava usluge i funkcije kritično važne za postojanje javnosti, društva i države“ (Kondratov, 2017: 12). Sukladno tome, svaka država će definirati koncept kritične infrastrukture s obzirom na posebne potrebe njezinih stanovnika stoga za jednu državu određena infrastruktura može ali ne mora spadati pod termin kritična infrastruktura. Autor Peptan navodi kako se infrastruktura može definirati kao „skup fizičkih ili virtualnih cjelina koje osiguravaju normalno funkcioniranje sastavnica države ili zajednice“ (Peptan, 2022: 37). U onoj mjeri u kojoj su takve cjeline važne za normalno funkcioniranje države i društva u cjelini mogu se definirati kao više ili manje kritične. Nadalje, autori poput Mikca, Cesarec i Larkina navode kako „razliku u definiranju čine i odrednice poput teritorijalnog određivanja kritične infrastrukture, odnosno odluke zemalja da razmatraju kritičnu infrastrukturu „samo“ na nacionalnom nivou ili na nacionalnom, regionalnom i lokalnom nivou“ (Mikac, Cesarec, Larkin, 2018: 23).

Što se tiče Ukrajine i njezinog shvaćanja koncepta kritične infrastrukture potrebno je spomenuti kako se politička svijest o važnosti definiranja kritične infrastrukture Ukrajine razvijala periodički. Pojam kritične infrastrukture Ukrajine prvi put se pojavljuje 2006. godine u „tekstu Preporuka parlamentarnih rasprava o razvoju informacijskog društva“ (Kondratov, 2017: 13). Nadalje, pojam kritične infrastrukture Ukrajine razmatrao se u kontekstu razvoja nacionalne sigurnosne strategije 2012. godine kada se kritična infrastruktura „spominje u kontekstu definiranja načina za poboljšanje energetske sigurnosti i načina za osiguranje informacijske sigurnosti" (ibid: 13). Važnost pojma kritične infrastrukture prepoznata je 2015. godine kada se formirala nova Strategija nacionalne sigurnosti Ukrajine u okviru koje se spominje važnost kritične infrastrukture odnosno „sigurnost kritične infrastrukture po prvi je put spomenuta kao jedno od ključnih područja državne politike nacionalne sigurnosti te su identificirani njezini prioriteti" (ibid:13). Slijedom navedenog može se uočiti kako je važnost pojma kritične infrastrukture kontinuirano rasla što ukazuje na to kako su glavni akteri nacionalne sigurnosti Ukrajine prepoznali glavne funkcije kritične infrastrukture.

Definicija kritične infrastrukture Ukrajine glasi: „kritična infrastruktura Ukrajine znači i uključuje sustave i resurse, fizičke ili virtualne, koji podržavaju funkcije i usluge čiji će prekid uzrokovati najteže negativne učinke na aktivnost društva, socioekonomski razvoj zemlje i nacionalnu sigurnost" (Kondratov, 2017: 14). Takva definicija kritične infrastrukture Ukrajine obuhvaća niz objekata koji pripadaju različitim državnim sigurnosnim sektorima. Od svih sektora koje navodi Kondratov posebno je važno istaknuti nuklearni sektor, energetski sektor, sektor transportnog sustava te sektor hrane i poljoprivrede s obzirom da su ti sektori kritične infrastrukture Ukrajine najviše ugroženi trenutnom agresijom Rusije. Sukladno riziku kojemu su izloženi gore navedeni sektori te kritična infrastruktura Ukrajine općenito potrebno je uspostaviti kvalitetan sustav zaštite kritične infrastrukture.

Sustav zaštite kritične infrastrukture Ukrajine definiran je u već spomenutom dokumentu a to je tako zvana „Zelena knjiga" u okviru koje se navodi kako ona „oblikuje sustav zaštite kritične infrastrukture Ukrajine s fokusom na preusmjeravanje pozornosti vlade i javnosti s 'reaktivne' politike koja se bavi posljedicama krize na prevenciju krize i planiranje za izvanredne situacije, jačanje koordinacije različitih uključenih aktera i uspostavljanje učinkovitih javno-privatnih partnerskih odnosa na terenu" (Sukhodolia, 2018: 108). Dakle, „Zelena knjiga" nastoji pospješiti sustav upravljanja krizama na način da se fokus stavi na prve dvije faze upravljanja krizama a to su prevencija i pripravnost. Osim toga, dokument „Zelena knjiga" fokus stavlja i na jačanje koordinacije i umreženosti različitih aktera što je izrazito bitno iz nekoliko razloga. Najprije, koordinacija i umreženost ključna je kako bi različiti akteri mogli surađivati i dijeliti informacije kako bi zajedničkim snagama mogli poduzeti pravovaljane sigurnosne procedure. Osim toga, koordinacija i umreženost ključna je za kvalitetnu prevenciju i pripravnost s obzirom da jasna podjela rada implicira brzu identifikaciju problema te samim time bržu reakciju na opasnosti.

O važnosti koordinacije i umreženosti različitih aktera u okviru sustava zaštite kritične infrastrukture autori Mikac, Cesarec i Larkin navode kako „glavni izazovi koji utječu i na kompleksnost sustava zaštite kritične infrastrukture mogu se svesti na nivo umreženosti komponenti sustava, kojom se na taj način slabi otpornost, i problematiku kako ojačati kritičnu infrastrukturu da bude stabilnija u svojoj neizbježnoj međuovisnosti" (Mikac, Cesarec, Larkin, 2018: 32). Nadalje, za razumijevanje sustava zaštite kritične infrastrukture od presudne važnosti je činjenica kako ne postoji način putem kojeg se kritična infrastruktura može u potpunosti zaštititi. Drugim riječima, „kritičnu infrastrukturu nije moguće u potpunosti zaštititi, niti otkloniti sve njezine ranjivosti, ali je moguće osigurati da sustav ne bude pod aktivnom prijetnjom" (ibid: 31). Slijedom navedenih karakteristika sustava zaštite kritične infrastrukture u sljedećem odlomku definirat će se sustav zaštite kritične infrastrukture Ukrajine.

Sustav zaštite kritične infrastrukture Ukrajine definira se kao „skup mjera implementiranih u regulatorne, institucionalne i tehnološke alate usmjerene prema osiguravanju sigurnosti, zaštite i otpornosti kritične infrastrukture" (Kondratov, 2017: 14). Takva definicija sustava zaštite kritične infrastrukture Ukrajine upućuje na postojanje instrumenata koji omogućavaju opstojnost i funkcionalnost objekata kritične infrastrukture. Takvi instrumenti odnosno alati kao što su regulatorni, institucionalni i tehnološki alati najčešće su u vlasništvu privatnog sektora. U tom smislu Kondratov ističe kako su najčešći akteri koji kontroliraju većinu sredstava važnih za sigurnost kritične infrastrukture tako zvani privatni operateri koji imaju zadaću da „osiguravaju pouzdanost, otpornost i održivost svojih sredstava/sustava" (ibid: 24). S druge strane zadaća država jest omogućiti pristup svim potrebitim informacijama te omogućiti postojanje kvalitetnog institucionalnog okvira u okviru kojega će djelovati privatni operateri. Zadaću države u sustavu zaštite kritične infrastrukture Ukrajine Kondratov objašnjava u smislu da bi država trebala „osigurati odgovarajuće informacije vlasnicima/operatorima, stvoriti adekvatan regulatorni okvir i poticaje za ulaganje u sigurnost kritične infrastrukture te uvjete za nastavak konkurentnosti poslovanja koje zahtijeva ulaganja u sigurnost kritične infrastrukture" (ibid: 24).

Glavni cilj sustava zaštite kritične infrastrukture Ukrajine koji ovisi o samoj funkciji kritične infrastrukture Ukrajine jest da se omogući snabdijevanje cijeloga društva potrebnim resursima odnosno cilj je osigurati „opskrbu stanovništva, društva, poduzeća i države vitalnim dobrima i uslugama" (ibid: 23). U sljedećem pododjeljku objasnit će se način funkcioniranja sustava zaštite kritične infrastrukture Ukrajine odnosno režim rada sustava zaštite kritične infrastrukture Ukrajine za vrijeme trajanja određene opasnosti.

2.3. Način funkcioniranja sustava zaštite kritične infrastrukture Ukrajine

Način funkcioniranja sustava zaštite kritične infrastrukture Ukrajine objasnit će se na način da će se prvo opisati koje su to glavne zadaće sustava zaštite kritične infrastrukture Ukrajine. Zatim će se objasniti način rada sustava zaštite kritične infrastrukture za vrijeme trajanja određene opasnosti. Naposlijetku će se definirati objekti i subjekti sustava zaštite kritične infrastrukture Ukrajine te će se definirati podjela sustava zaštite kritične infrastrukture Ukrajine s obzirom na objekt i vrstu prijetnje.

Glavne zadaće sustava zaštite kritične infrastrukture Ukrajine odnose se na 1) opću koordinaciju sustava zaštite kritične infrastrukture u Ukrajini, 2) prevenciju kriznih situacija, 3) podrška u odlučivanju 4) primjena nadzornih i kontrolnih mehanizama te 5) međunarodna suradnja. U okviru svake glavne zadaće postoji niz manjih zadaća.

Slijedom toga, opća koordinacija sustava zaštite kritične infrastrukture Ukrajine obuhvaća niz zadaća od kojih najviše treba istaknuti suradnju i međupovezanost niza aktera odnosno „koordinaciju i razmjenu informacija s mrežom sigurnosnih i obrambenih kriznih (informacijskih) centara“ (Kondratov, 2017: 30). Osim toga, u okviru opće koordinacije sustava kritične infrastrukture Ukrajine od presudnog značaja jest sustavan pristup zaštite kritične infrastrukture što podrazumijeva suradnju svih aktera zaštite kritične infrastrukture odnosno „koordinaciju napora svih dionika (državnih agencija, lokalnih upravnih tijela, poslovnog sektora i društva) u pogledu zaštite kritične infrastrukture, uključujući horizontalno sučelje između operatera međuovisnih i homogenih kritičnih sredstava“ (ibid: 30). Također, u okviru zadaće opće koordinacije sustava zaštite kritične infrastrukture Ukrajine spada i temeljita analiza procjene rizika određenih prijetnji gdje se rizik prijetnje određuje putem „procjena prijetnji za kritičnu infrastrukturu na nacionalnoj razini s obzirom na međuodnose između pojedinih infrastrukturnih dobara i sektora, utjecaj svih vrsta prijetnji te procjena rizika na regionalnoj i nacionalnoj razini“ (ibid: 30).

Nadalje, zadaća prevencije kriznih situacija uključuje niz sigurnosnih radnji od kojih se najviše ističe proces zaštite kritične infrastrukture. Proces zaštite se dijeli na fizičku zaštitu objekata kritične infrastrukture, tehničku zaštitu te kibernetičku zaštitu kibernetskog sustava Ukrajine. Kibernetička zaštita se odnosi na „zaštitu imovine kritične infrastrukture od kibernetičkih napada, zaštitu podataka i tehničkih informacija u sustavima upravljanja procesima na objektima kritične infrastrukture od neovlaštenog zaključavanja ili modifikacije“ (ibid: 31). S druge strane fizička i tehnička zaštita objekata kritične infrastrukture odnosi se na „osiguranje stabilnog rada kritične infrastrukture u izvanrednim situacijama i posebnim razdobljima“ (ibid: 31). Također, s obzirom na ratne okolnosti u kojima se nalazi Ukrajina vrijedi napomenuti kako je ključno postojanje prevencije u kontekstu „skladištenja rezervi materijala te procjene i praćenje inventara resursa“ (ibid: 31).

Zadaća podrška u odlučivanju se odnosi na ulogu sustava zaštite kritične infrastrukture gdje se naglasak stavlja na rano prepoznavanje nepravilnosti u radu kritične infrastrukture odnosno to se odnosi na „praćenje i identifikaciju potencijalnih kriza povezanih s radom kritične infrastrukture“ (ibid: 32). Također, podrška u odlučivanju ima ključnu ulogu u sistematizaciji podataka koji su potrebni za pravilno funkcioniranje kritične infrastrukture. Takva uloga zahtjeva postojanje procedura kao što su „prikupljanje, uspoređivanje i analiza podataka koji se tiču objekata kritične infrastrukture i njihovog rada“ (ibid: 32). Osim takvih zadaća, podrška u odlučivanju je važna kako bi osigurala pravovremeno opskrbljivanje objekata kritične infrastrukture svim potrebnim resursima a tako nešto je moguće zahvaljujući procesu „identifikacije i predviđanja količina resursa potrebnih za zaštitu kritične infrastrukture“ (ibid: 32).

U okviru zadaće primjene nadzornih i kontrolnih mehanizama ključno je postojanje kriterija i regulativa koji će određivati funkcioniranje sustava zaštite kritične infrastrukture. Primjena nadzornih i kontrolnih mehanizama uglavnom se odnosi na proces „razvoja i implementacije standarda, normi i propisa za sustav zaštite kritične infrastrukture“ (ibid: 32). Također, zadaća primjene nadzornih i kontrolnih mehanizama ključna je za provjeru i procjenu sigurnosti objekata kritične infrastrukture te za „provjere i procjene informacijske sigurnosti imovine kritične infrastrukture“ (ibid: 32). Primjena nadzornih i kontrolnih mehanizama ključna je zadaća u prvoj fazi upravljanja krizama odnosno fazi prevencije s obzirom da nastoji pružiti koordinacijska i interaktivna pomoć u prevenciji opasnosti koje prijete objektima kritične infrastrukture. Kondratov takvu ulogu zadaće primjene nadzornih i kontrolnih mehanizama definira kao „informativnu, savjetodavnu, stručnu i tehnološku podršku operaterima kritične infrastrukture i potrošačima usluga (javnosti) za prevenciju, odgovor i ublažavanje potencijalnog utjecaja takvih prijetnji“ (ibid: 32).

Posljednja ključna zadaća koja se ističe jest međunarodna suradnja. Iako zadaća međunarodne suradnje izravno ne utječe na funkcionalnost i opstojnost kritične infrastrukture ona je iznimno važna u svrhu poboljšanja rada te prilagodbe na suvremene standarde zaštite kritične infrastrukture. U tom smislu važna je procjena standarda zapadnih zemalja odnosno „analiza regulatornih zahtjeva EU-a (kao i SAD-a i drugih zemalja) i njihova potencijalna implementacija u Ukrajini“ (ibid: 33). Međunarodna suradnje je važna posebice za države kao što je Ukrajina s obzirom na ograničene uvjete samostalnog razvoja kvalitetnog sustava zaštite kritične infrastrukture. Osim zajedničkih međunarodnih projekata od velike važnosti je izravan utjecaj stranih stručnjaka u proces izgradnje zakonodavnog okvira sustava zaštite kritične infrastrukture. Kvalitetan primjer takve prakse međunarodne suradnje jest razvoj energetskog sektora Ukrajine kada je „elemente planiranja u slučaju nepredviđenih situacija“ razvio tim stručnjaka iz SAD-a, Kanade i zemalja EU i implementirao ih u nacrt „Plana za funkcioniranje energetskog sektora Ukrajine u zimskom razdoblju 2015/2016” i “Plan za postizanje energetske održivosti Ukrajine“ (Sukhodolia, 2018: 115).

Nakon objašnjenih ključnih zadaća sustava zaštite kritične infrastrukture Ukrajine u narednim dijelovima će se objasniti kako sustav zaštite funkcionira za vrijeme trajanja neposredne opasnosti. Slijedom toga, objasnit će se pet načina rada odnosno pet režima rada sustava zaštite kritične infrastrukture Ukrajine ovisno o razini opasnosti koja prijeti.

Autor Sukhodolia razlikuje pet režima rada te ih dijeli na 1) zeleni, 2) žuti, 3) narančasti, 4) plavi i 5) crveni režim rada. Svaki od režima rada ima zasebne odgovore koji se razlikuju s obzirom na razinu opasnosti kojoj su objekti kritične infrastrukture izloženi. Zeleni režim rada se odnosi na najčešći način rada sustava zaštite kritične infrastrukture Ukrajine gdje objekti kritične infrastrukture Ukrajine funkcioniraju u normalnim uvjetima s obzirom da sustav zaštite kritične infrastrukture „radi na predviđanju i prevenciji prijetnji te koristi alate za rano upozoravanje“ (ibid: 109). Žuti režim predstavlja aktivniji način rada sustava zaštite kritične infrastrukture Ukrajine za razliku od zelenog režima rada s obzirom da je glavna aktivnost žutog režima rada „odvraćanje od prijetnji i zaštita kritične infrastrukture“ (ibid: 109). Također, žuti režim rada nastoji spriječiti napade na određene objekte kritične infrastrukture odnosno „radi za zaštitu odabranih objekata unutar projektiranog sustava zaštite objekta (unutarnji resursi) i provjerava spremnost vanjskih resursa u cilju sprječavanja realizacije prijetnji“ (ibid: 109). Ono što je zajedničko zelenom i žutom režimu rada sustava zaštite kritične infrastrukture Ukrajine jest normalan način rada objekata kritične infrastrukture što znači normalnu i redovnu opskrbu stanovništva svim potrebnim resursima poput električne energije, toplinske energije, vode, interneta i slično.

Narančasti režim rada predstavlja odgovor sustava zaštite kritične infrastrukture kada objekti kritične infrastrukture imaju poseban način rada te tada postoje „neka ograničenja u pravnim i gospodarskim režimima“ (ibid: 109). Takva ograničenja se odnose na poteškoće u radu objekata kritične infrastrukture Ukrajine poput prekida opskrbe električnom energijom stanovništvom poput slučaja kada su „slični režimi na tržištu električne energije uvedeni u Ukrajini nekoliko puta u razdoblju 2014. – 2017.“ (ibid: 109). U narančastom režimu sustav zaštite kritične infrastrukture Ukrajine koristi sve potrebne „vanjske snage i resurse za uklanjanje prijetnji i negativnih posljedica“ (ibid: 109) koje su potrebne kako bi se objekti kritične infrastrukture vratili u funkcionalno stanje. Plavi režim predstavlja odgovor na opasnosti koje uzrokuju „ozbiljna ograničenja u pravnim i ekonomskim režimima“ što znači da objekti kritične infrastrukture izgube sposobnost opskrbe stanovništva svim potrebnim resursima. Iz tog razloga sustav zaštite kritične infrastrukture Ukrajine u plavom režimu „radi na vraćanju sposobnosti kritičnih infrastruktura da obavljaju svoje funkcije za društvo i državu“ (ibid: 109).

Zadnji režim koji predstavlja izvanredno stanje u funkcioniranju sustava zaštite kritične infrastrukture jest crveni režim. U okviru tog režima ističe se aktivna uloga državnog aparata koji nadzire upravljanje cjelokupnom kritičnom infrastrukturom odnosno „država preuzima punu kontrolu nad režimom funkcioniranja kritične infrastrukture“ (ibid: 109). Crveni režim zaštite kritične infrastrukture Ukrajine se aktivira za vrijeme izvanrednih stanja kao što su primjerice prirodne katastrofe i rat. Za to vrijeme sustav zaštite kritične infrastrukture koristi „sve raspoložive snage i resurse unutar posebnog razdoblja“ (ibid: 109).

Gore navedeni režimi sustava zaštite kritične infrastrukture Ukrajine sa sobom nose brojne izazove. Jedan od trenutno najvećih izazova jest brzina reakcija i način reakcije. Takav izazov posljedica je ratnog stanja u kojem se nalazi Ukrajina s obzirom da je nerijetko potrebno donositi odluke na temelju nepotpunih informacija i sa premalo potrebnih resursa za reakciju. O takvom izazovu raspravlja Sukhodolia koji ističe probleme sa kojima se suočavaju akteri koji provode sigurnosne politike odnosno tehničkog osoblja koje mora da „izvrši postavljene zadatke u ograničenom vremenskom roku, hitnim slučajevima, nedostatku resursa i znanja na terenu“ (ibid: 109).

Osim opisanih režima sustava zaštite kritične infrastrukture Ukrajine za potpuno razumijevanju nužno je definirati objekte koji se nalaze pod zaštitom te subjekte koji upravljaju procesom zaštite takvih objekata. Definiranje objekata je ključno kako bi se jasno utvrdila „razina zahtjeva za zaštitu kritične infrastrukture, raspodjela ovlasti i odgovornosti među svim uključenim dionicima“ (ibid: 110) odnosno kako bi se adresiralo za koju vrstu kritične infrastrukture je potrebno više resursa kako bi se održala njezina funkcionalnost. Slijedom toga, objekti kritične infrastrukture mogu se podijeliti u četiri kategorije. Kategorija 1. se odnosi na objekte kritične infrastrukture koji su od najveće važnosti za stanovnike Ukrajine odnosno objekti u kategoriji

1. su „od ključne važnosti za državu i imaju nacionalnu važnosti, višestruke i složene veze s drugim infrastrukturnim objektima“ (ibid: 110) i kao takvi zahtijevaju najviše resursa i napora da ih se zaštiti. Nadalje, objekti kritične infrastrukture koji su važni za sigurnost na regionalnoj razini spadaju u kategoriju 2. te njihov prekid u radu dovodi do kolapsa na regionalnoj razini. S obzirom da objekti kritične infrastrukture u kategoriji 2. nemaju važnost koja je nacionalnog karaktera zaštićeni su „u okviru javno-privatnog partnerstva prema zakonom utvrđenim uvjetima“ (ibid: 110). Objekti kategorije 3. su u uskoj vezi s objektima kategorije 2. s obzirom da su također zaštićeni u okviru javno-privatnog partnerstva no jedina razlika jest ta da objekti kategorije 3. nisu regionalnog karaktera već su važni infrastrukturni objekti koji moraju biti zaštićeni u okviru privatno-javnog partnerstva s obzirom na cjelokupni državni značaj. Posljednji objekti su objekti kategorije 4. se definiraju kao potrebni infrastrukturni objekti gdje glavnu odgovornost u njihovom radu nema nacionalna niti regionalna vlast već operater koji ima odgovornost „osigurati stabilno funkcioniranje objekata“ (ibid: 110).

Funkcionalnost i opstojnost sustava zaštite objekata kritične infrastrukture Ukrajine ovisi o subjektima koji upravljaju zaštitom objekata kritične infrastrukture. Najvažniji subjekti koji upravljaju zaštitom kritične infrastrukture Ukrajine su državna tijela. Njihova uloga je prepoznata od strane Kondratova koji navodi kako bi „ključnu ulogu u aktivnostima usmjerenim na održivu sigurnost kritične infrastrukture trebala imati država preko svojih ovlaštenih tijela“ (Kondratov, 2017: 37). Državna tijela imaju najvažniju ulogu u upravljanju sustavom zaštite kritične infrastrukture a njihova uloga je prepoznatljiva kada su „elementi kritične infrastrukture u potpunom ili djelomičnom vlasništvu države“ (ibid: 37). Državna tijela koja su glavna za upravljanje sustavom zaštite kritične infrastrukture Ukrajine su Integrirani sustav za prevenciju, odgovor i suzbijanje terorističkih akata i minimiziranje njihovih posljedica (USSPRM-T), Jedinstveni državni sustav Civilne zaštite (USSCP) i Državni sustav fizičke zaštite (SPPS). Osim tih tijela potrebno je spomenuti tzv. Državno izvanredno povjerenstvo koje predstavlja „stalno tijelo za koordinaciju aktivnosti središnjih i lokalnih izvršnih vlasti usmjerenih na osiguranje antropogene i ekološke sigurnosti, zaštite stanovništva i teritorija protiv posljedica izvanrednih situacija“ (ibid: 38). Državno izvanredno povjerenstvo osnovano je 2015. godine te jedna od njegovih ključnih zadaća jest omogućiti stalnu opskrbu energetskih resursa odnosno „osiguranje stabilnog rada sektora goriva i energije u izvanrednim situacijama“ (ibid: 39). Osim toga, Državno izvanredno povjerenstvo ima za cilj osigurati optimalnu razinu funkcioniranja „rada prometne infrastrukture, poštanskih i elektroničkih komunikacijskih usluga“ (ibid: 39). Također, Državno izvanredno povjerenstvo je ključno tijelo koje potiče suradnju i koordiniranost svih razina vlasti u svrhu oporavka nacionalnog gospodarskog sustava nakon što su se utrošila financijska sredstva i resursi na rješavanje krize. Kondratov tako nešto definira kao zadaću „koordinacije napora središnjih i lokalnih izvršnih vlasti za osiguranje otpornosti nacionalnog gospodarstva i sredstava javne uprave tijekom odgovora na hitne situacije“ (ibid: 39).

Sukladno navedenim objektima i vrstama prijetnji potrebno je napraviti razlikovanje različitih sustava zaštite kritične infrastrukture Ukrajine. Sukladno tome, Sukhodolia navodi kako je za uspješan sustav zaštite kritične infrastrukture Ukrajine potrebno „kombinirati napore najrelevantnijih sustava koji su ranije uspostavljeni u Ukrajini: sustav civilne zaštite – I SSCP; sustav fizičke zaštite – S PPS; protuteroristički sustav – USSPRM-T i sustav kibernetičke sigurnosti – NCSS“ (Sukhodolia, 2017: 82). Dakle, sukladno vrsti prijetnje i objektu ugroženosti aktivirati će se neki od gore navedenih sustava zaštite kritične infrastrukture.

Zaključno, u ovom poglavlju definiran je sustav zaštite kritične infrastrukture Ukrajine te se posebna pažnja usmjerila na izazove i probleme u funkcioniranju sustava zaštite kritične infrastrukture Ukrajine. Također, u svrhu boljeg razumijevanja sustava zaštite kritične infrastrukture definiran je pojam kritične infrastrukture. Osim toga, objašnjen je način funkcioniranja te su se definirali režimi rada koji odgovaraju na različite razine opasnosti. Naposlijetku, definirani su objekti kritične infrastrukture Ukrajine te subjekti koji upravljaju zaštitom iste.

3. Odgovor sustava zaštite kritične infrastrukture Ukrajine na ruske teroristički napade

Glavni cilj i svrha ovog poglavlja jest prikazati kako je sustav zaštite kritične infrastrukture Ukrajine reagirao i odgovorio na ruske terorističke napade od početka oružanog sukoba 2014. godine s posebnim naglaskom na razdoblje eskalacije rata od 2022. godine. U okviru ovog poglavlja temeljem istraživačkog pitanja koje glasi: „Kako je sustav zaštite kritične infrastrukture Ukrajine odgovorio na ruske terorističke napade u kontekstu oružnog sukoba?“ nastojat će se istražiti proces upravljanja kriznim situacijama sustava zaštite kritične infrastrukture Ukrajine s posebnim naglaskom na treću fazu upravljanja krizama a to je faza reakcije. Upravo na taj način istražiti će se u kojoj mjeri je sustav zaštite kritične infrastrukture Ukrajine spreman odnosno nespreman upravljati kriznim situacijama u kontekstu ruskih terorističkih napada.

Kako bismo objasnili način na koji je sustav zaštite kritične infrastrukture odgovorio na ruske terorističke napade najprije će se navesti primjeri terorističkih napada koji su izvršeni na kritičnu infrastrukturu Ukrajine od strane Ruske Federacije. Teroristički napadi usmjereni na kritičnu infrastrukturu Ukrajine mogu se podijeliti s obzirom na vrstu kritične infrastrukture. Slijedom toga, razlikuju se napadi na kritičnu infrastrukturu zračnog prometa, pomorskog prometa, kopnenog prometa, napadi na nuklearne elektrane, napadi na kritičnu infrastrukturu nafte i plina, kibernetički napadi te napadi na obrazovnu i zdravstvenu kritičnu infrastrukturu.

3.1. Teroristički napadi na kritičnu infrastrukture zračnog, pomorskog i kopnenog prometa Ukrajine

Teroristički napadi na kritičnu infrastrukturu zračnog, pomorskog i kopnenog prometa su najčešći oblik terorističkog djelovanja s obzirom da uzrokuju paniku i strah među stanovništvom te prekid mobilnosti i obrambene sposobnosti. Autor Peptan ističe kako su međunarodni i civilni aerodromi bili objekti kritične infrastrukture koji su bili među prvim metama ruskih napada na početku invazije na Ukrajinu. Peptan navodi kako su mete bile „kijevska međunarodna zračna luka Boryspil, zračna luka Hostomel, civilna zračna luka Zhuliany, civilna zračna luka Vinnytsia, međunarodna zračna luka Mykolaiv, zračna luka Ivano-Frankivsk“ (Peptan, 2022: 39). Takvi napadi su za cilj imali i da se prekine svaki oblik pružanja vojne pomoći od strane zemalja EU i SAD-a putem zračnog prometa. Dakle, napadi na kritičnu infrastrukturu zračnog prometa bili su „usmjereni na ometanje napora nekih zemalja koje su pokazale solidarnost s Ukrajinom da joj mogu pružiti vojnu pomoć zračnim putem kako bi se suprotstavile agresiji invazijskih snaga" (ibid: 39).

Nadalje, što se tiče pomorskog prometa Ukrajine, Ruska Federacija je prije invazije blokirala područja Crnog mora, Azovskog mora i Kerčkog tjesnaca s dvostrukim ciljem „ometanja ukrajinskog poljoprivrednog i industrijskog izvoza na međunarodna tržišta preko luka Odesa, Herson, Mariupol, Berdjansk i Mikolaiv, s velikim posljedicama za ukrajinsko gospodarstvo, kao i osiguranje potpore za moguću agresiju na Ukrajinu s njenog južnog krila" (ibid: 39). Takva djelovanja Ruske Federacije okarakterizirana su kao kršenje međunarodnog poretka točnije kao kršenje pravila i načela Konvencije Ujedinjenih naroda o pravu mora. Također, Peptan ističe kako je zauzimanje pomorskih luka prouzročilo prehrambenu krizu u pojedinim zemljama s obzirom da je Ukrajina u takvim okolnostima bila u nemogućnosti da izvozi žito. Peptan sažima kako se „kritična infrastruktura u kategoriji pomorskih luka, od vitalne važnosti za ukrajinsko gospodarstvo i s velikim utjecajem na izvoz žita ili drugih sirovina, nije mogla koristiti iz strateških i vojnih razloga" (ibid: 40). Takvo postupanje je snažno negativno utjecalo na gospodarstvo Ukrajine, sposobnost obrane te općenito na ekonomsko i socijalno blagostanje stanovnika Ukrajine.

Osim zračnog i pomorskog prometa slični postupci Ruske Federacije bili su usmjereni i na kopneni promet. U tom smislu, cilj ruskog djelovanja nad kritičnom kopnenom infrastrukturom bio je „uništavanje cestovnih i željezničkih mostova, vijadukata, strateški važnih prometnica koja povezuju geografske regije zemlje, glavnih željeznica i željezničkih čvorova koji su pomogli osigurati izvoz određenih proizvoda - željezne rude, ugljena, poljoprivrednih proizvoda - koji su osiguravali važna financijska sredstva za državni proračun, te na kraju, ali ne manje važno, strateški važnih prometnica" (ibid: 40). Takvo djelovanje Ruske Federacije iako nije usmjereno na vojne ciljeve s obzirom da mete napade nisu vojni objekti ono je za krajnji cilj imalo postizanje vojne prednosti nad neprijateljem. Dobar primjer takvog djelovanje jest napad na strateški važan most Zatoka u regiji Odesa koji povezuje tu regiju sa ostatkom Ukrajine. Most Zatoke bio je „predmet višestrukih napada vojske Ruske Federacije, čiji je cilj s jedne strane ometati izvoz žitarica lukama kroz Rumunjsku i Bugarsku, a s druge strane izoliranje regije od ostatka Ukrajine" (ibid: 40).

Ono što je posebno važno za naglasiti u kontekstu ruskih napada na kritičnu infrastrukturu kopnenog, zračnog i pomorskog prometa jest utjecaj na šire stanovništvo Ukrajine. Utjecaj je negativan u nizu konteksta od kojih najviše vrijedi istaknuti prekid opskrbe stanovništva potrebnim resursima kao što su struja, voda i hrana. Takvi ishodi su bili česti diljem Ukrajine a jedan od najpoznatijih primjera su gradovi Mariupolj i Nicolaev gdje je kritična cestovna i željeznička infrastruktura „pretrpjela ozbiljnu štetu, uz prekid opskrbe električnom energijom, grijanjem, svježom vodom, hranom ili medicinskom opremom i potrepštinama“ (ibid: 41). Osim prekida u opskrbi stanovništva potrebnim resursima, posljedice ruskih napada na kritične infrastrukture kopnenog, zračnog i pomorskog prometa bile su i u dometu stradavanja civilnog stanovništva Ukrajine. Statistički podaci pokazuju kako je od početka invazije Ruske Federacije na Ukrajinu poginulo skoro preko 10.000 civilnog stanovništva. U tom smislu navodi se kako je „od 24. veljače 2022., koji je označio početak velikog oružanog napada Ruske Federacije, do 10. rujna 2023. OHCHR zabilježio 27.149 civilnih žrtava u zemlji: 9.614 poginulih i 17.535 ranjenih“ (Ohchr.org, 2023).

3.2. Teroristički napadi na kritičnu infrastrukturu u kategoriji nuklearnih elektrana

Nuklearne elektrane predstavljaju objekte kritične infrastrukture koji su iznimno važni za osiguravanje stanovništva stalnom opskrbom električnom energijom te za osiguravanje energetske sigurnosti države. U kontekstu Ukrajine potrebno je ukazati kako se pitanje nuklearnih elektrana veže i uz pitanje zaštite okoliša i zdravlja stanovništva s obzirom na poznate katastrofalne učinke na okoliš i zdravlje stanovništva nakon katastrofe iz Černobila 1986. godine. Na teritoriju Ukrajine postoji četiri aktivne nuklearne elektrane „s 15 nuklearnih reaktora u pogonu, koji osiguravaju oko 50% energetskih potreba zemlje“ (Peptan, 2022: 41). Tijekom invazije Ruske Federacije na Ukrajinu dogodilo se niz incidenata vezanih uz sigurnost nuklearnih elektrana Ukrajine. Važno je istaknuti kako je uzrok takvih incidenata izravno rusko oružano djelovanje nad nuklearnim elektranama a ne puko slučajno ili nenamjerno djelovanje s kolateralnom štetom. O takvim postupcima oružanih snaga Ruske Federacije govori Peptan koji navodi kako su „od početka „specijalne vojne operacije” koju je pokrenula Ruska Federacija u Ukrajini, nuklearne elektrane bile meta usklađenog djelovanja ruske vojske, pri čemu je černobilska elektrana zauzeta 24. veljače 2022. i bombardirana 4. ožujka 2022. nakon čega je uslijedilo zauzimanje elektrane Zaporožje koja osigurava oko 25% ukrajinske proizvodnje energije“ (ibid: 41). S obzirom da nuklearne elektrane ne predstavljaju vojnu prijetnju te ne spadaju u skupinu vojnih objekata već u skupinu objekata civilne kritične infrastrukture postavlja se pitanje svrhe granatiranja i zauzimanja takvih objekata. O tome su se vodile brojne polemike i rasprave te se može izvući nekoliko zaključaka. Najprije, Ukrajina uvelike ovisi o nuklearnoj energiji kako bi zadovoljila potrebe stanovništva za električnom energijom stoga je logično za očekivati kako će „preuzimanjem kontrole nad objektom i ostalima, Rusija imati mogućnost paliti i gasiti svjetla u Ukrajini" (En.as.com, 2022). Dakle, zauzimanjem ključnih ukrajinskih nuklearnih elektrana Ruska Federacija ima na raspolaganju kontrolu proizvodnje i distribucije električne energije diljem Ukrajine te na taj način utječe na društvene i ekonomske aspekte rata. Osim toga, navodi se kako je zauzimanje ukrajinskih nuklearnih elektrana od strane Ruske Federacije imalo za cilj stvoriti atmosferu straha odnosno tvrdi se kako „postoji i psihološki učinak korištenja straha kao oružja" (En.as.com). Slično tome, Peptan navodi kako je okupiranje ukrajinskih nuklearnih elektrana od strane Ruske Federacije značilo upotrebu tzv. nuklearnog terora u vojne svrhe odnosno da „vlasti Ruske Federacije imaju za cilj osigurati postrojenja u slučaju dugotrajnog rata u Ukrajini, čime imaju kontrolu nad njima i mogućnost izazivanja dodatnog straha među svjetskom zajednicom" (Peptan, 2022: 41).

O rizicima i opasnostima koji proizlaze iz ruskog zauzimanja i granatiranja ukrajinskih nuklearnih elektrana izvještavala je i Međunarodna agencija za atomsku energiju. U jednom od svojih mjesečnih izvještaja o stanju ukrajinske nuklearne sigurnosti, glavni direktor Međunarodne agencije za atomsku energiju, Rafael Mariano Grossi kazao je kako nuklearna elektrana Zaporizhzhya mora biti zaštićena te kako je „nastavak granatiranja, pogađajući jedini izvor vanjskog napajanja elektrane, krajnje neodgovoran" (Iaea.org, 2022). Osim Međunarodne agencije za atomsku energiju koja je izrazila snažnu zabrinutost za nuklearnu sigurnost važno je spomenuti kako je i glavni tajnik UN-a također izrazio zabrinutost i poslao snažnu poruku u kojoj navodi kako poziva „na povlačenje bilo kakvog vojnog osoblja i opreme iz nuklearne elektrane i izbjegavanje bilo kakvog daljnjeg raspoređivanja snaga ili opreme unutar elektrane" (News.un.org, 2022). S obzirom na opasnosti koje proizlaze iz granatiranja i oružane opsade nuklearnih elektrana nužno je napomenuti kako su napadi na kritičnu infrastrukturu u kategoriji nuklearnih elektrana jedni od najrizičnijih napada na objekte kritične infrastrukture s obzirom na katastrofalne posljedice koje mogu izazvati.

3.3. Teroristički napadi na kritičnu infrastrukturu nafte i plina

Objekti kritične infrastrukture nafte i plina važni su za učinkovito funkcioniranje države i društva kako u vrijeme mira tako i u vrijeme rata. Objekti kritične infrastrukture nafte i plina mogu se podijeliti s obzirom na funkcije koje obavljaju pa se tako razlikuju objekti „za vađenje, rafiniranje i transport naftnih i plinskih proizvoda" (Peptan, 2022: 41). Kao i ostali objekti kritične infrastrukture Ukrajine koji su bili izloženi snažnim ruskim napadima tako su podjednako bili izloženi i objekti kritične infrastrukture nafte i plina. Područja koja su bila najčešće izložena takvim vrstama napada odnosila su se na rubna područja grada Kijeva i Harkova. Sukladno takvom postupanju, došlo je do obustave proizvodnje nafte i plina gdje „energetska tvrtka Naftogaz obustavlja rad u obližnjoj rafineriji nafte Shebelinsky, a proizvođač plina Ukrgasvydobuvannya obustavlja rad u nekoliko proizvodnih pogona" (ibid: 42). Ruski napadi na objekte kritične infrastrukture nafte i plina osim što su imali za cilj nanijeti snažne društvene i ekonomske gubitke imali su u pozadini i vojne ciljeve poput uništenja važnih tvornica nafte koje opskrbljuju ukrajinsku vojsku. Shodno tome, Peptan tvrdi kako je „vrijedno spomenuti da je rafinerija nafte u Kremenčuku, od vitalne važnosti u kontekstu pružanja većeg dijela potpore gorivom za obrambene snage, bila podvrgnuta vojnoj agresiji 2. travnja 2022., pri čemu je potpuno uništena, uključujući i skladišta nafte" (ibid: 42). Slično kao i napadi na objekte nuklearne kritične infrastrukture koji generiraju strašne posljedice za stanovništvo i okoliš tako i napadi na objekte kritične infrastrukture nafte i plina mogu dovesti do snažnog zagađenja okoliša i zdravlja ljudi te do ogromnih ekonomskih i društvenih poteškoća. O takvoj problematici raspravlja Peptan koji ističe kako je Ukrajina prije rata jedan dio svojih potreba za naftom i plinom uspjela zadovoljiti zahvaljujući domaćem tržištu, no nakon invazije Ruske Federacije postala je potpuno ovisna o uvozu nafte i plina te takvo „stanje stvari ima nepovoljne posljedice za cjelokupni ukrajinski društveni život, uključujući mogućnost logističke potpore za oružane snage uključene u obrambeni rat zemlje" (ibid: 42).

3.4. Kibernetički teroristički napadi i teroristički napadi na obrazovnu i zdravstvenu kritičnu infrastrukturu

Kibernetički napadi Ruske Federacije na objekte kritične infrastrukture Ukrajine započeti su netom prije ruske invazije na Ukrajinu te su imali za cilj destabiliziranje ključnih političkih institucija Ukrajine te stjecanje vojno-taktičkih prednosti nad protivnikom. Slično tome, Peptan navodi kako su ruski kibernetički napadi imali dva cilja a to su „s jedne strane, poremetiti ispravno funkcioniranje ukrajinskih državnih tijela i gospodarskih, financijskih i vojnih sposobnosti, a s druge strane mijenjati ili prikupljati informacije iz okruženja od interesa koje bi mogle pružiti taktičke ili strateške prednosti ruskim oružanim snagama" (ibid: 42). Ruski kibernetički napadi bili su usmjereni na važne objekte poput sjedišta nacionalne televizije i nacionalnog pružatelja internetskih usluga. Nadalje, osim takvih objekata koji su bili primarna meta napada na početku rata potrebno je napomenuti kako je Ukrajina bila izložena kibernetičkim napadima i prije eskalacije rata gdje su mete bile tvrtke za distribuciju električne energije. Tako se navodi kako je „dana 23. prosinca 2015. ukrajinski Kyivoblenergo, regionalna tvrtka za distribuciju električne energije, izvijestila o prekidu pružanja usluga korisnicima“ (E-ISAC, 2016: 6). Nakon provedene analize od strane nadležnih tijela ustanovljeno je kako je takvo stanje uzrokovano kibernetičkim napadom odnosno „do prekida je došlo zbog nezakonitog ulaska treće strane u računalne i SCADA sustave tvrtke“ (ibid: 6). Kibernetički napadi predstavljaju veliki izazov sustavu zaštite kritične infrastrukture Ukrajine s obzirom na snažnu međupovezanost informacijskog sustava Ukrajine. Posljedično, kibernetički napadi mogu izazvati kolaps u funkcioniranju ključnih političkih i gospodarskih institucija te tako uzrokovati prekid opskrbe stanovništva životno važnim resursima. O takvim posljedicama i djelovanju kibernetičkih napada argumentira i Peptan koji navodi kako je očito da „zbog visokog stupnja međuovisnosti između sektora kritične infrastrukture na teritoriju Ukrajine, kao rezultat njihove povezanosti kroz složene informacijske sustave, kibernetički napadi mogu generirati neke 'kaskadne' učinke, što proizvodi neželjene posljedice za cjelokupni ukrajinski društveni život“ (Peptan, 2022: 43).

Posljednji objekti kritične infrastrukture koji su se našli pod ruskim terorističkim udarima su objekti zdravstvene i obrazovne infrastrukture. Navedeni objekti ključni su za normalno funkcioniranje države i društva kako u mirnodopsko vrijeme tako i u ratnim okolnostima. Što se tiče obrazovnih institucija Ukrajine podaci ukazuju na poražavajuću brojku ruskih napada gdje se navodi kako je „1978 obrazovnih ustanova svih razina bilo meta oružanih akcija, od kojih su 194 potpuno uništene“ (ibid: 43). U svrhu boljeg razumijevanja ruskih terorističkih napada i okupacije obrazovnih institucija potrebno je spomenuti istraživanje organizacije za ljudska prava Human Rights Watch koja je u studenom 2022. godine provela terensko istraživanje o stanju obrazovnih institucija u Ukrajini za vrijeme okupacije Ruske Federacije. Istraživanje je pokazalo kako su oružane snage Ruske Federacije koristile obrazovne institucije Ukrajine u razne vojne svrhe što je protivno svim odredbama međunarodnog prava. Tako se navodi kako su u regijama koje su dokumentirane u izvješću „ruske snage često koristile škole i vrtiće da utabore svoje vojnike i parkiraju vojna vozila i drugu opremu u školskim dvorištima“ (Hrw.org, 2023). Osim u svrhu vojnog skladištenja, oružane snage Ruske Federacije koristile su obrazovne institucije i u vojno-taktičke svrhe. Naime, iz terenskog istraživanja se saznalo kako su škole često korištene kao vojne baze za oružano djelovanje protiv neprijatelja. Dobar primjer takvog djelovanje jest „kada su ruski vojnici u ožujku 2022. zauzeli školu u Borodianki, u regiji Kijevska, na otprilike mjesec dana, koristili su zgradu škole kao bazu i za paljbu na ukrajinske snage“ (ibid). U kontekstu ruskog terorističkog djelovanja nad obrazovnim institucijama Ukrajine potrebno je razmišljati u okviru vojne i političke logike. Naime, s obzirom da se objekti poput škola, vrtića, institucija visokih učilišta i slično smatraju civilnim objektima te kao takvi svaki oblik vojnog djelovanja nad njima je strogo zabranjen prema odredbama međunarodnog prava logično je očekivati kako su oružane snage Ruske Federacije odlučile zauzeti upravo takve objekte te na taj način osigurati sigurno vojno utočište smatrajući da oružane snage Ukrajine neće provoditi oružane akcije nad takvim objektima.

Nadalje, osim objekata kritične obrazovne infrastrukture ono što je izazvalo veliku pažnju javnosti bili su ruski teroristički napadi nad kritičnom zdravstvenom infrastrukturom. Tako se navodi kako su „oružani napadi Ruske Federacije gađali bolnice i medicinske klinike, rodilišta, banke krvi, centre za liječenje raka, psihijatrijske rehabilitacijske ustanove, hitne centre, itd., izazivajući ogorčenje cijele međunarodne zajednice" (Peptan, 2022: 43). Prema izvještajima Svjetske zdravstvene organizacije navodi se kako su „1004 napada, koje je potvrdila Svjetska zdravstvena organizacija tijekom proteklih 15 mjeseci rata punih razmjera, odnijela najmanje 101 život, uključujući zdravstvene radnike i pacijente, a mnogo više ih je ozlijeđeno" (Who.int, 2023).

Osim izvještaja Svjetske zdravstvene organizacije postoje brojna ostala istraživanja koja su nastojala utvrditi točan broj zdravstvenih objekata koji je bio gađan te broj poginulih i ozlijeđenih zdravstvenih radnika i pacijenata. Jedno od takvih istraživanja je ustanovilo kako su bila „334 dokumentirana napada na 267 ukrajinskih zdravstvenih ustanova između 24. veljače 2022. i 25. veljače 2023." (Barten, 2023: 5). Posljedica takvih napada prema istraživačima bilo je to da je „u napadima ubijeno 9 zdravstvenih radnika i 105 civila, a još je 26 ozlijeđenih zdravstvenih radnika i 88 civila" (ibid: 7). Usprkos tome što je svaki ruski teroristički napad na zdravstvene objekte bio iznimno medijski popraćen vrijedi izdvojiti napad na rodilište u gradu Mariupolju kada je napad rezultirao „sa 6 mrtvih i 33 ozlijeđene osobe" (ibid: 8). Razlog zašto je taj napad izdvojen jest što je izazvao veliku emocionalnu reakciju javnosti s obzirom da je gađano rodilište koje niti na jedan način, jednako kao niti bilo koja druga zdravstvena ustanova, nije predstavljalo vojnu niti bilo kakvu drugu vrstu prijetnje.

Ono što je posebno zabrinjavajuće vezano uz terorističke napade na obrazovne i zdravstvene objekte kritične infrastrukture jest rizik koji proizlazi iz napada na takve objekte koji se prvenstveno odnosi na sigurnost zdravlja i života pojedinaca a pogotovo djece. S tim u vezi, međunarodna organizacija Save the Children upozorila je kako je „oko šest milijuna ukrajinske djece u opasnosti, a više od 1,5 milijuna djece već je napustilo zemlju zbog toga što su škole i bolnice glavne mete ruske vojske" (Peptan, 2022: 43).

3.5. Odgovor sustava zaštite kritične infrastrukture Ukrajine na ruske terorističke napade

Kako bismo mogli analizirati način na koji je reagirao sustav zaštite kritične infrastrukture Ukrajine na ruske terorističke napade moramo razlučiti već spomenute režime rada sustava zaštite kritične infrastrukture Ukrajine te se usmjeriti na crveni režim rada koji se aktivira za vrijeme trajanja izvanrednih stanja poput prirodnih katastrofa i rata. Nadalje, u svrhu boljeg objašnjenja odgovora sustava zaštite kritične infrastrukture Ukrajine na ruske prijetnje i napade potrebno je napraviti razlikovanje između različitih sustava zaštite kritične infrastrukture Ukrajine gdje se razlikuju već spomenuti sustav civilne zaštite, sustav fizičke zaštite, protuteroristički sustav te sustav kibernetičke sigurnosti. Takvi sustavi odgovaraju na različite vrste prijetnja odnosno „različite vrste kriza pokreću različite sustave prevencije i odgovora na krize i, sukladno tome, zahtijevaju uključenost različitih subjekata" (Ivaniuta, 2017: 89). Slijedom toga, u ovom poglavlju će se analizirati na koji je način sustava zaštite kritične infrastrukture Ukrajine odgovorio na ruske terorističke napade od početka rata 2014. godine.

Sukladno ukrajinskom Zakonu o kritičnoj infrastrukturi definirane su mjere za osiguranje stabilnosti i zaštite objekata kritične infrastrukture te su definirani subjekti koji su zaduženi za planiranje i provedbu mjera zaštite. Članak 22. Zakona o kritičnoj infrastrukturi jasno navodi kako „Nacionalna policija Ukrajine, Nacionalna garda Ukrajine, Služba sigurnosti Ukrajine, Oružane snage Ukrajine, Državna služba Ukrajine za izvanredne situacije i druge komponente sigurnosnog i obrambenog sektora u okviru svojih nadležnosti planiraju odgovarajuće mjere za zaštitu kritične infrastrukture" (Verhovna Rada, 2021). Navedena tijela imaju ključnu zadaću u obavljanju zadataka zaštite objekata kritične infrastrukture a njihova uloga se posebno intenzivirala početkom 2022. godine kada je započeta invazija Ruske Federacije na Ukrajinu.

Kao što je prikazano u prethodnim pododjeljcima, najčešći oblici napada kojima su bili izloženi objekti kritične infrastrukture su zračni napadi poput raketnih udara te zračnog granatiranja. Sukladno tome, glavnu aktivnost u fazi reakcije imao je sustav fizičke zaštite kritične infrastrukture Ukrajine. U izvješću ukrajinske Agencije za obnovu navodi se kako „nakon kritičnih napada na ukrajinsku energetsku infrastrukturu korištenjem bespilotnih letjelica i projektila od sredine studenog 2022., Vlada i Glavni stožer Oružanih snaga Ukrajine poduzeli su mjere za zaštitu ove vitalne imovine" (Facebook.com, 2023). Agencija navodi kako su provedene mjere zaštite električne energije ponajprije od prijetnje dronova i projektila. Primarni način zaštite sastoji se od gradnje betonske konstrukcije oko mreže električne energije poznatije kao UkrEnerga. Betonska konstrukcija, kako se navodi, rezultirala je „ zaštitom 22 trafostanice i 63 autotransformatora u 14 regija“ (ibid). Osim mjera zaštite i prevencije, Agencija za obnovu ističe kako se provodi tzv. aktivna obrana „22 trafostanice od izravnih pogodaka najjačih projektila u 14 regija“ (ibid). Prema riječima ukrajinskog ministra energetike, Hermana Halushchenka, aktivnu zaštitu energetskog sustava pruža „protuzračna obrana koja je sada puno snažnija nego lani, te pasivna zaštita“ (War.ukraine.ua, 2023). Tijekom razdoblja od početka rata 2014. godine protuzračna obrana Ukrajine se postepeno unaprjeđivala sukladno obrambenim potrebama pa je tako primjerice u rujnu 2023. godine objavljeno kako će Ukrajina „od svojih partnera dobiti više samohodnih protuavionskih topova 'Gepard', posebno za zaštitu ukrajinske energetske mreže od mogućih ruskih napada tijekom nadolazećeg jesensko-zimskog razdoblja“ (ibid).

Protuzračna obrana Ukrajine predstavlja ključni način zaštite objekata kritične infrastrukture. Zbog konstantnih ruskih napada na objekte kritične infrastrukture postoji snažna potreba za dodatnim resursima protuzračne obrane što je ujedno u više navrata naglašavao predsjednik Zelenski koji je u dijalogu sa Jensom Stoltenbergom, glavnim tajnikom NATO saveza kazao kako su razgovarali „o situaciji oko očekivanih ruskih napada na kritičnu infrastrukturu Ukrajine i mogućnosti opskrbe dodatnih sustava protuzračne obrane od strane država članica NATO-a“ (Rubryka.com, 2023). U kontekstu protuzračne obrane potrebno je spomenuti kako se u jeku rata razvio inovativni senzorski sustav za prepoznavanje zračnih opasnosti poznatiji kao „Safe Skies“. Navedeni sustav „može otkriti ciljeve na vrlo malim visinama i predvidjeti njihov kurs za daljnju neutralizaciju“ (U24.gov.ua, 2023). Sustav „Safe Skies“ je relativno novi protuzračni obrambeni sustav gdje se pretpostavlja kako je za „učinkovitu zaštitu teritorija Ukrajine potrebno 12.500 uređaja“ (ibid) te samim time potrebno je prikupiti znatna financijska sredstva kako bi se novi sustav mogao koristiti na cijelom teritoriju Ukrajine.

Nadalje, nakon izbijanja oružanog sukoba 2014. godine uspostavljeno je niz mjera sustava zaštite kritične infrastrukture za odgovor na ruske napade. Jedna od takvih mjera odnosi se na postupak ponovne uspostave Nacionalne garde Ukrajine kao postrojbe koja je s teškim naoružanjem „bila u stanju odbiti napade na zaštićene objekte te je imala zadatak zaštititi kritičnu infrastrukturu“ (NATO, 2020: 53). Također, s ciljem zaštite objekata kritične infrastrukture kopnenog, zračnog i pomorskog prometa odlučeno je kako će se pojačati zaštita prometne infrastrukture kroz suradnju sa tzv. posebnim agencijama kao što je primjerice „Posebna služba za željeznice“ (ibid: 53). U cilju jačanja zaštite i oporavka objekata kritične infrastrukture poboljšana je suradnja lokalnih vlasti s raznim državnim resorima poput „državne

Službe Ukrajine za izvanredne situacije, Oružane snage, Nacionalna garda, Sigurnosne službe" (ibid: 53) i slično.

Osim sustava fizičke zaštite kritične infrastrukture ključna je uloga sustava kibernetičke sigurnosti. Kibernetički napadi na Ukrajinu od strane Ruske Federacije stalna su pojava koja je svoj vrhunac doživjela 2022. godine. Prema autoru Kohutu glavne protumjere koje se koriste za upravljanje kibernetičkom sigurnošću objekata kritične infrastrukture odnose se na otkrivanje zlonamjernih aktivnosti, ublažavanje mogućih kibernetičkih napada te uspostavu sigurnosne politike. Otkrivanje zlonamjernih aktivnosti obično se odnosi na „proces praćenja log datoteka od strane iskusnih administratora i korištenje sustava za otkrivanje upada" (Kohut, 2020: 62). Osim toga, u kontekstu uspostave sigurnosne politike navodi se kako je potrebno „razviti sigurnosnu politiku za upravljačku mrežu i njezine pojedinačne komponente" (ibid: 62). Ključno tijelo zaduženo za koordinaciju i kontrolu rada subjekata kibernetičke sigurnosti jest Vijeće za nacionalnu sigurnost i obranu Ukrajine. Navedeno tijelo nadgleda rad ostalih agencija među kojima je i Državna služba za posebne komunikacije i zaštitu informacija Ukrajine koja ima zadatak „provoditi organizacijske i tehničke mjere za sprječavanje, otkrivanje i odgovaranje kibernetičkih incidenata i kibernetičkih napada te eliminaciju njihovih posljedica" (Tkachuk, 2019: 8). Nadalje, važna ustrojstvena jedinica Državne službe za posebne komunikacije i zaštitu informacija Ukrajine jest Državni centar za kibernetičku zaštitu i suzbijanje kibernetičkih prijetnji čija je glavna zadaća „osigurati funkcioniranje Ukrajinskog tima za hitne slučajeve" (ibid: 9). Dakle, Ukrajinski tim za hitne slučajeve jest operativno tijelo kibernetičke sigurnosti koje „izravno odgovara na kibernetički napad, pomaže u obnavljanju funkcioniranje mreže i eliminira negativne učinke kibernetičkih incidenata" (ibid: 10).

Zaključno, u ovom poglavlju nastojao se objasniti način na koji je sustav zaštite kritične infrastrukture Ukrajine odgovorio na ruske terorističke napade. Pritom se u prvom djelu poglavlja pozornost usmjerila na analizu ruskih terorističkih napada na objekte kritične infrastrukture kako bi se ukazalo na logiku ruskog djelovanja te ranjivost ukrajinskog sustava zaštite. U drugom dijelu poglavlja objašnjen je način na koji sustav zaštite kritične infrastrukture Ukrajine reagira na ruske terorističke napade gdje se najveća pažnja usmjerila na protuzračnu obranu Ukrajine te na sustav kibernetičke zaštite.

4. Reforma sustava zaštite kritične infrastrukture Ukrajine

Glavni cilj i svrha ovog poglavlja jest ukazati koji dijelovi u okviru zaštite kritične infrastrukture Ukrajine nisu dovoljno učinkoviti da odgovore na napad, eliminiraju prijetnju te vrate sustav kritične infrastrukture u funkcionalno stanje. U ovom poglavlju istraživačko pitanje glasi: „Što je potrebno reformirati kako bi sustav zaštite kritične infrastrukture Ukrajine uspješno prevenirao i reagirao na terorističke prijetnje“? Kako bi se uspješno pružio odgovor istražiti će se koji sastavni dijelovi zaštite kritične infrastrukture nisu pravovaljano reagirali na ruske terorističke napade. Slijedom toga, analizirati će se ruski teroristički napadi na ukrajinsku kritičnu infrastrukturu od početka oružanog sukoba 2014. godine. Nadalje, nakon pomnog uvida u nedostatke u okviru zaštite kritične infrastrukture Ukrajine nastojat će se objasniti koji reformski proces jest potreban za unapređenje sustava zaštite kritične infrastrukture Ukrajine. Temeljem analize odgovora sustava zaštite kritične infrastrukture Ukrajine te uvida u napade na objekte kritične infrastrukture Ukrajine odredit će se koji dijelovi sustava zaštite kritične infrastrukture nisu u stanju odgovoriti na prijetnje. Slijedom toga, pružiti će prijedlozi za reforme gdje će se pokušati uzeti u obzir kvalitetne prakse drugih europskih država koje bi se mogle primijeniti u kontekstu sustava zaštite kritične infrastrukture Ukrajine.

4.1. Ugroženost objekata kritične infrastrukture Ukrajine

Dijelovi sustava zaštite kritične infrastrukture čija funkcionalnost i djelovanje je najviše ugroženo odnosi se na one sustave koji ne mogu kvalitetno zaštiti objekte kritične infrastrukture. Takve sustave je relativno lako prepoznati temeljem niza čimbenika poput ljudskih žrtava, materijalne štete te financijskih iznosa potrebnih za reparaciju štete nastale napadom. U kontekstu financijskih iznosa potrebnih za reparaciju štete nad objektima kritične infrastrukture Ukrajine važno je ukazati na istraživanje provedeno od strane Kyiv School of Economics gdje je glavni fokus „usmjeren na procjenu štete nanesene fizičkoj infrastrukturi Ukrajine tijekom rata (uništenje stambenih zgrada, komunalnih usluga, cesta, željeznica, obrazovnih i medicinskih ustanova itd.); te procjena financijske vrijednosti tih šteta“ (Kse.ua, 2024). Rezultati istraživanja ukazuju kako je najviše financijskih iznosa potrebnih za reparaciju štete uloženo u objekte kritične infrastrukture kopnenog prometa prvenstveno na ceste gdje je bilo potrebno uložiti preko 27 milijardi dolara. Osim navedenog istraživanja koje je potvrdilo kako sustav zaštite kritične infrastrukture kopnenog prometa nije u stanju spriječiti ruske napade važno je spomenuti i izjavu ukrajinskog ministra prometa Oleksandra Kubrakova koji je izjavio kako je „oštećeno ili srušeno oko 300 mostova na glavnim autocestama, oštećeno je oko 8000 kilometara cesta, a znatne su štete i na željezničkim prugama“ (Railtarget.eu, 2022). Slijedom toga, prvi dio sustava zaštite kritične infrastrukture koji nužno reformirati odnosi se na sustav zaštite kritične infrastrukture kopnenog prometa s obzirom na ogromne materijalne i financijske štete koje su prouzročene neadekvatnim odgovorima na napade.

Osim na primjeru objekata kritične infrastrukture kopnenog prometa, slaba učinkovitost sustava zaštite kritične infrastrukture da pravovaljano odgovori na ruske napade može se uočiti i na primjeru objekata kritične infrastrukture u kategoriji nuklearnih elektrana. Prema istraživanju Kyiv School of Economics u izvještajima se navodi kako su „štete ukrajinskom energetskom sektoru iznosile najmanje 11 milijardi dolara, uključujući 8,3 milijarde dolara u energetskom sektoru i 2,7 milijardi dolara u komunalnoj infrastrukturi (uključujući centralno grijanje, vodoopskrbu i odvodnja te objekti za gospodarenje otpadom iz kućanstva)“ (Energycharter.org, 2023). Materijalna šteta nastala napadima na objekte kritične infrastrukture u kategoriji nuklearnih objekata još je veća ako se uzme u obzir činjenica kako su oružane snage Ruske Federacije zauzeli niz nalazišta prirodnih resursa. Tako se navodi kako je „Ruska Federacija preuzela kontrolu nad ukrajinskim nalazištima minerala u vrijednosti najmanje 12,4 bilijuna dolara dok je Ukrajina izgubila 63% nalazišta ugljena, 11% nalazišta nafte, 20% nalazišta prirodnog plina, 42% naslaga metala i 33% naslaga elemenata rijetkih zemalja i drugih kritičnih minerala, uključujući litij“ (ibid: 6). Osim materijalne štete prouzročene ruskim napadima na nuklearne elektrane bitno je spomenuti i rizik koji je proizlazi iz vojnih aktivnosti unutar prostora nuklearne elektrane. Tako se navodi kako je u području nuklearne elektrane Zaporižja „u svibnju 2023. Rusija nastavila povećavati svoju vojnu prisutnost i stvorila je obrambene položaje izgrađene od vreća s pijeskom na zgradama reaktora dok su prema IAEA-u ruske vojne snage skladištile vojnu opremu, oružje i eksplozivne materijale u turbinskoj sali reaktora“ (ibid: 8). Navedene vojne aktivnosti koje su provedene unutar same nuklearne elektrane ukazuju kako je sustav zaštite kritične infrastrukture u kategoriji nuklearnih elektrana zakazao te kako je potrebna hitna provedba potrebnih reformi kako bi se rizici koji proizlaze iz takvih aktivnosti sveli na najmanju moguću razinu.

Osim materijalne štete te ogromnih financijskih iznosa potrebnih za reparaciju nastale štete važan pokazatelj slabe učinkovitosti sustava zaštite objekata kritične infrastrukture odnosi se na posljedice za sigurnost zdravlja i života građana. U tom smislu najviše se ističe niska razina učinkovitosti sustava zaštite objekata zdravstvene i obrazovne kritične infrastrukture. U pododjeljku 3.4. objašnjena je dinamika ruskih raketnih napada na objekte zdravstvene infrastrukture poput bolnica, rodilišta, banaka krvi i slično. Potrebno je nadodati kako takvi napadi imaju negativan utjecaj na širok spektar aktera i ključnih sastavnica poput pacijenata, medicinskog osoblja te medicinskih potrepština i opreme. O takvom utjecaju raspravljaju autori Gostin i Rubenstein koji ističu kako je „većina napada uključivala korištenje teškog oružja protiv objekata zdravstvene zaštite, osoblja, pacijenta i medicinske potrepštine“ (Gostin i Rubenstein, 2022: 1). Osim izravnih posljedica na zdravlje i sigurnost građana poput razaranja bolnica, smrti i ozljeda postoje i neizravne posljedice koje imaju dugoročno negativan učinak na javne politike. Primjeri takvih učinaka odnose se na probleme u prevenciji zaraznih bolesti ili pak u pružanju osnovnih zdravstvenih usluga poput pedijatrijske skrbi, usluge dijalize te skrbi za oboljele od leukemije i slično. Takve učinke su izdvojili i Gostin i Rubenstein koji tvrde kako postoje širi poremećaji „rutinske njege, zdravlja majke i djeteta, složene skrbi za oboljele od raka ili one kojima je potrebna dijaliza bubrega te nekontrolirano širenje zaraznih bolesti, uključujući COVID-19, tuberkulozu i HIV/AIDS“ (ibid: 1). Takve neizravne i dugoročne učinke na javne politike vidljivi su i u području objekata obrazovne kritične infrastrukture. Naime, zbog korištenja obrazovnih institucija Ukrajine u vojne svrhe od strane oružanih snaga Ruske Federacije, o čemu se raspravljalo u pododjeljku 3.4., došlo je do snažnog egzodusa djece i adolescenata u inozemstvo što će definitivno negativno utjecati na buduće tržište rada Ukrajine te će tako nešto polučiti negativne demografske trendove. Takvi negativni trendovi potkrijepljeni su statističkim podacima u poglavlju 3.4. no u svrhu boljeg razumijevanja potrebno je prikazati statističke podatke UNICEF-a gdje se navodi iznimno važan podatak kako je „gotovo polovica djece izbjeglica iz Ukrajine, njih 173.000, trenutno upisano u poljski školski sustav, uključujući osnovne i srednje škole“ (Unicef.org, 2023). Osim negativnog učinka na edukaciju i obrazovanje, napadi na obrazovne objekte te posljedično egzodus obrazovnih ljudi negativno utječe i na sektor istraživanja i razvoja koji predstavlja ključan sektor za dugoročni rast i razvoj. Slijedom toga, brojni ukrajinski znanstvenici i istraživači ne mogu sudjelovati na međunarodnim konferencijama i seminarima što za posljedicu imalo „ograničenje razmjene ideja i znanja te je to otežalo ukrajinskim istraživačima da budu u toku s najnovijim dostignućima u svom području“ (Al Gharaibeh, Ahmad, Malkawi, 2023: 10).

Temeljem ključnih faktora poput ljudskih žrtava, materijalne štete i financijskih iznosa potrebnih za reparaciju nastale štete izdvojeni su objekti kritične infrastrukture koji su najugroženiji odnosno objekti koje sustav zaštite kritične infrastrukture Ukrajine nije u stanju obraniti od konstantnih ruskih napada. Slijedom toga, u sljedećem pododjeljku predložiti će se načini za reformiranje sustava zaštite kritične infrastrukture u svrhu održavanja sigurnosti i funkcionalnosti društva. U tom smislu, naglasak će biti na poboljšanju responzivnosti, jačanju energetske održivosti te na modernizaciji sustava zaštite kritične infrastrukture Ukrajine. Također, u okviru modernizacije fokus će biti na integraciju naprednih tehnologija poput umjetne inteligencije te naprednih vojnih tehnologija. Osim toga, kroz primjere dobre prakse drugih europskih država u održavanju sustava zaštite kritične infrastrukture pokušat će se objasniti kako se putem međunarodne koordinacije u dijeljenju informacija mogu unaprijediti dijelovi sustava zaštite kritične infrastrukture Ukrajine koji ne mogu zaštiti ključne objekte kritične infrastrukture od ruskih napada.

4.2. Reforma sustava zaštite kritične infrastrukture Ukrajine

Reforma sustava zaštite kritične infrastrukture Ukrajine česta je tema brojnih međunarodnih pregovora između predstavnika Ukrajine i država Zapada. Ključna stavka takvih pregovora odnosi se na modernizaciju vojske Ukrajine posebice na unapređenje sustava protuzračne obrane te zračnih snaga. Takvi zahtjevi su od iznimne važnosti s obzirom da sustav protuzračne obrane predstavlja ključan faktor za sigurnost objekata kritične infrastrukture poput kopnenih prometnica, nuklearnih elektrana te objekata zdravstvene i obrazovne infrastrukture koje su izdvojene u prethodnom pododjeljku kao najugroženije vrste objekata kritične infrastrukture. Navedeni razlozi upućuju na nužnost reforme protuzračnog sustava Ukrajine te na unapređenje zračnih snaga Ukrajine. Osim reforme oružanih snaga Ukrajine, u ostatku poglavlja analizirati će se mogućnosti za unapređenje međunarodne suradnje i implementacije dobrih praksi iz drugih europskih država. Posljednja reforma o kojoj će u poglavlju biti riječ odnosi se na mogućnosti unapređenja kibernetičke sigurnost u svrhu zaštite objekata kritične infrastrukture.

4.2.1. Reforma oružanih snaga Ukrajine

Najučinkovitiji način za unapređenje protuzračnog sustava jest zamjena trenutnog ukrajinskog protuzračnog sustava iz sovjetske ere sa modernim zapadnim protuzračnim sustavom koji može uspješno parirati ruskim raketnim sustavima kao što su S-400 i Kinžal. Takvi zahtjevi za reformom protuzračnog obrambenog sustava aktualizirali su se nakon ruske invazije u veljači 2022. godine kada su glavni zahtjevi bili usmjereni na dobivanje tehnološki naprednog američkog sustava protuzračne obrane „MIM-104 Patriot“. Nakon niza pregovora i sastanaka navedeni sustav protuzračne obrane izručen je Ukrajini od strane SAD-a te je tom prilikom ukrajinski predsjednik Volodimir Zelenski izrekao kako je to „vrlo važan korak za stvaranje sigurnog zračnog prostora za Ukrajinu i to je jedini način na koji bismo mogli spriječiti terorističku zemlju i njihove terorističke napade da pogađaju naš energetski sektor, naše ljude i našu infrastrukturu“ (Aa.com.tr, 2022). Trenutno najvažnija stavka u osiguranju djelotvornog sustava zaštite kritične infrastrukture Ukrajine je stalna opskrba navedenim sustavom protuzračne obrane kako bi se omogućila stalna vojna nadmoć nad protivnikom u zračnom prostoru te na taj način zaštitili najugroženiji objekti kritične infrastrukture. Takav zaključak nudi i autor John Venable koji tvrdi kako bi se „američka strategija trebala usredotočiti na davanje više sustava protuzračne obrane Ukrajincima, kao što je sustav Patriot, kako bi se uskratilo rusko zrakoplovstvo, a nastavila opskrba topništvom, raketama i tenkovima potrebnim za borbu protiv neprijatelja“ (Venable, 2023: 5).

Osim sustava protuzračne obrane za kvalitetnu reformu sustava zaštite kritične infrastrukture nužno je ojačati zračne snage Ukrajine što se odnosi na reformu stanja borbenih aviona Ukrajine. Kako bi se postigla zračna nadmoć nad ruskim borbenim avionima poput Mig-35 te Su-35 nužno je modernizirati ratno zrakoplovstvo. Ključan problem ukrajinskog ratnog zrakoplovstva odnosi se na zastarjele radarske sustave borbenih lovaca Ukrajine gdje se navodi kako „ruski zrakoplovi koriste rakete s aktivnim radarom za navođenje, kao što su R-77 i R-37M ultra dugog dometa, koje daleko nadmašuju poluaktivne R-27 koje nose ukrajinski lovci“ (Atlanticcouncil.org, 2023). Jedan od načina modernizacije odnosi se na zahtjeve za dobivanjem tehnološki naprednog američkog borbenog lovca F-16. Navedeni borbeni zrakoplov ima niz pozitivnih aspekata koji bi znatno unaprijedili sigurnost ključnih objekata kritične infrastrukture. Prva prednost F-16 borbenih zrakoplova odnosi se na poboljšanje radarske sustave gdje će F-16 lovci „biti opremljeni AIM-120 AMRAAM-ovima, projektilima zrak-zrak koji imaju slične, a vjerojatno i bolje performanse u usporedbi s ruskim R-77“ (ibid). Osim toga, F-16 borbeni zrakoplovi imat će bolje manevarske mogućnosti od aktualnih ukrajinskih borbenih zrakoplova na način da će putem snažnijeg radarskog sustava te većom otpornošću na ometanje „moći otkriti ruske zrakoplove na većim udaljenostima i omogućiti ukrajinskim pilotima da ostanu dalje izvan dometa prve crte ruske protuzračne obrane“ (ibid). Nadalje, modernizacija ratnog zrakoplovstva s američkim borbenim lovcima F-16 značilo bi uspostavljanje kvalitetnijeg sustava zaštite objekata kritične infrastrukture posebice u kontekstu borbe protiv ruskih bespilotnih letjelica koje teroriziraju ključne objekte kritične infrastrukture poput nuklearnih elektrana. Takvu pretpostavku iznosi i Yurii Ihnat, glasnogovornik zračnih snaga Ukrajine, koji je u jednom od intervjua izrekao kako su borbeni lovci F-16 potrebni u svrhu „zaštite objekata kritične infrastrukture Ukrajine među kojima je sedam nuklearnih elektrana“ (Weareukraine.info, 2023). Nabavkom borbenih lovaca F-16 Ukrajina bi dobila stratešku prednost nad ruskim bespilotnim letjelicama s obzirom da aktualno ukrajinsko ratno zrakoplovstvo ne može sa stopostotnom učinkovitošću obarati ruske dronove. Sukladno tome, Yurii Ihnat tvrdi kako su potrebni F-16 borbeni avioni „koji to mogu učiniti sa stopostotnom učinkovitošću, obaranjem projektila Kalibr i Kh-101 i bespilotnih letjelica Shahed“ (ibid).

4.2.2. Međunarodna suradnja i implementacija kvalitetnih praksi

U kontekstu reforme oružanih snaga Ukrajine nužno je spomenuti kako je od presudne važnosti suradnja sa državama članicama NATO-a posebice u smislu transformacije vojno-sigurnosnih standarda iz sovjetske ere prema modernim NATO standardima. Suradnja Ukrajine i država članica ne predstavlja samo vojnu transformaciju već i političku i ekonomsku transformaciju. Takve sveobuhvatne značajke transformacije objašnjava autor Andrii Ordynovych koji ističe kako „jedan od najpouzdanijih partnera Ukrajine u sektoru sigurnosti i obrane je Sjevernoatlantski pakt i njegove pojedinačne članice, koje tradicionalno podupiru Ukrajinu u provođenju ključnih unutarnjih reformi usmjerenih na postizanje ne samo stabilnog gospodarskog i političkog razvoja, već i stjecanje odgovarajuće sposobnosti za unutarnju i vanjsku obranu“ (Ordynovych, 2020: 69). Važnost vojno-sigurnosne transformacije ogleda se u poboljšanju kvalitete sustava zaštite kritične infrastrukture s obzirom na korištenje moderne tehnologije u zaštiti objekata kritične infrastrukture. Također, ističe se kako postoje tri kategorije standarda koje mogu unaprijediti obrambene snage Ukrajine a to su tehnički standardi, operativni standardi te administrativni standardi. Pritom, operativna standardizacija se odnosi na „sposobnost zajedničkog rada i podrške zajedničkim akcijama saveznika i partnera i njihovih cjelokupnih obrambenih snaga“ (ibid: 72) što je iznimno važno za sustav zaštite kritične infrastrukture Ukrajine u kontekstu implementacije dobrih praksi drugih europskih država.

Jedan od iznimno kvalitetnih primjera dobre prakse zaštite kritične infrastrukture koje bi Ukrajina mogla iskoristiti u ratnim okolnostima jest sustav zaštite kritične infrastrukture Poljske. Osim što Ukrajina i Poljska imaju slično povijesno iskustvo potrebno je spomenuti kako Poljska u brojnim dokumentima prepoznaje Rusku Federaciju kao ključnog remetilačkog faktora sigurnosti što je od iznimne važnosti s obzirom da će se obrana kreirati sukladno istom neprijatelju Poljske i Ukrajine. Tako primjerice autori Piekarski i Wojtasik tvrde kako „u jednom hibridnom scenariju, Rusija se smatra neprijateljskim akterom, a namjera joj je prisiliti Poljsku da izvrši svoje zahtjeve“ (Piekarski i Wojtasik, 2022: 7). Osim toga, autor Sliwa navodi kako je „Strategija nacionalne sigurnosti Republike Poljske objavljena u svibnju 2020. potvrdila rusku neoimperijalističku politiku i ambicije kao najveću prijetnju Poljskom i europskom sigurnosnom sustavu“ (Sliwa, 2022: 66). Poljska ima kvalitetno razrađen plan djelovanja sustava zaštite kritične infrastrukture kako u mirnodopsko vrijeme tako i za vrijeme kriznih stanja. Analizom poljskog sustava zaštite kritične infrastrukture potrebno je izdvojiti dva primjera kvalitetnih praksi zaštite kritične infrastrukture koje bi uvelike unaprijedile i reformirale ukrajinski sustav zaštite kritične infrastrukture. Prvi primjer odnosi se na povećanje situacijske osviještenosti u svrhu povećanja sigurnosti objekata kritične infrastrukture. U Poljskoj, situacijska osviještenost „može se povećati patroliranjem zračnog prostora oko kritične infrastrukture, način sličan onom koji se već koristi u Poljskoj tijekom događaja visokog profila poput sportskih igara i političkih samita“ (Piekarski i Wojtasik, 2022: 10). Slijedom toga, primjena situacijske osviještenosti u Ukrajini putem patroliranja iznad objekata kritične infrastrukture poput nuklearnih elektrana ili pak bolnica značilo bi važan korak ka povećanju sigurnosti takvih objekata. Drugi kvalitetan primjer zaštite kritične infrastrukture Poljske odnosi se na primjenu moderne tehnologije u borbi protiv bespilotnih letjelica odnosno dronova. U tom smislu, 2021. godine „agencija DARPA provela je testiranje sustava za bespilotne letjelice koje su koristile elektromagnetske valove u ovom slučaju mikrovalove kako bi onesposobile prijetnju oštećivanje ugrađenih računala“ (ibid: 9, prema: Tingley, 2021). Osim toga, s obzirom da su objekti kritične infrastrukture Ukrajine česta meta ruskih dronova, potrebno je uspostaviti moderne i učinkovite sustave zaštite kritične infrastrukture a jedan od takvih sustava odnosi se na „primjer kinetičkog sustava koji se sastoji od dnevne i noćne kamere, laser daljinomjera i višecijevnog mitraljez kalibra 12/7 mm s radarskim detektorom“ (ibid: 9, prema: Świat Dronów, 2022).

4.2.3. Reforma sustava kibernetičke sigurnosti

Kibernetički sektor Ukrajine bio je u nekoliko navrata izravna meta ruskih kibernetičkih napada. Najčešće mete hakerskih napada bile su ključne vladine organizacije te sektori kritične infrastrukture. Autor Peptan navodi kako „ prema izvješću Microsofta, destruktivni kibernetički napadi koje je tvrtka uočila od početka invazije na Ukrajinu izravno su ciljali ukrajinske vladine organizacije na nacionalnoj, regionalnoj i lokalnoj razini ili kritične infrastrukturne sektore koji bi mogli imati sekundarne negativne učinke na ukrajinsku Vladu, vojsku, gospodarstvo i civile” korištenjem različitih tehnika (Peptan, 2022: 42). U poglavlju 3.4. detaljno su opisani ciljevi i načini kibernetičkih napada na kritičnu infrastrukturu Ukrajine s fokusom na informacijsku povezanost kibernetičkog sustava Ukrajine. O potrebama reforme kibernetičkog sustava Ukrajine raspravljaju autori Zhyvko, Rudyi, Senyk i Kucharska koji navode kako „potrebu za promjenom potvrđuju napadi na kritičnu infrastrukturu i mnogi drugi incidenti koji su posljednjih godina stvorili glavne cyber-domete“ (Zhyvko, Rudyi, Senyk i Kucharska, 2020: 82). Kao polazišnu osnovu za reformu kibernetičke sigurnosti navodi se potreba izmjene i nadopune zakona i regulativa s obzirom na nejasnu postojeću zakonsku proceduru gdje „terminologija koja se koristi u području informacijske tehnologije pokazuje nedostatak jedinstva i dvosmislenog tumačenja mnogih pojmova“ (ibid: 85). Sukladno tome, potrebno je jasno definirati ključne pojmove i procedure kibernetičke sigurnosti. Osim toga, nužna je redovita modifikacija procedura s obzirom na stalne promjene geopolitičkog konteksta te samim time i sigurnosnih prijetnji kibernetičkoj sigurnosti. Dakle, „barem svake dvije godine, postojeća zakonska regulativa u ovom području zahtijeva prilagodbe novim izazovima i prijetnjama, kao i promjenama u geopolitičkom sigurnosnom okruženju“ (ibid: 86). Temeljem navedenih problema u okviru zakonskog uređenja kibernetičke sigurnosti potrebno je istaknuti kako bi ključan korak u osiguranju kvalitetnog funkcioniranja sustava zaštite kibernetičke infrastrukture bio izgradnja jedinstvene strategije kibernetičke sigurnosti koja bi pružila jasne smjernice u načinu reakcije na stalne ruske hakerske napade.

Osim zakonskog uređenja, kao djela reforme, nužno je predložiti i ostale prijedloge za uspješniju kibernetičku zaštitu. S obzirom na negativne pokazatelje o financiranju sustava kibernetičke sigurnosti te o kvalificiranosti osoblja o čemu raspravlja autor Spinu koji tvrdi kako “Ukrajini nedostaju financijski poticaji za privlačenje najboljih stručnjaka za rad u Vladi, a postoji i značajan problem suradnje između javnog i privatnog sektora, što je ključno za uspjeh u kibernetičkoj sigurnosti“ (Spinu, 2020: 11), potrebno je ulagati u stručnost i znanje osoblja te je nužna međunarodna suradnja kroz brojne zajedničke projekte. Sličan prijedlog ističe autor Khlaponin koji predlaže jačanje kapaciteta kibernetičke sigurnosti što se odnosi na „donošenje zakonodavnih inicijativa usmjerenih na promicanje obrazovanja o kibernetičkoj sigurnosti, istraživanja i inovacija, kao i dodjeljivanje dodatnih sredstava za programe kibernetičke sigurnosti“ (Khlaponin, Dolhopolov, 2023: 10). Nadalje, osim financijskih ulaganja, s obzirom na aktualno ratno stanje u Ukrajini, potrebno je reformirati dijelove aktivne i pasivne kibernetičke zaštite koji se suprotstavljaju ruskim hakerskim napadima. Slijedom toga, potrebno je implementirati moderne kibernetičke tehnologije poput „antivirusne tehnologije ili sigurnosne tehnologije krajnjih točaka kako bi se omogućilo odbijanje poznatog zlonamjernog softvera“ (E-ISAC, 2016: 18). Također, s obzirom na česte ruske hakerske upade potrebno je napraviti tzv. „konfiguraciju sustava za otkrivanje upada tako da se pravila mogu brzo primijeniti za traženje uljeza“ (ibid: 18). Osim toga, potrebno je uspostaviti zajedničku bazu podataka gdje bi se prikupljali svi potrebni dokazi koji bi se kasnije upotrijebili za pravovaljane kibernetičke operacije. Zaključno, u kontekstu tehničkih reformi kibernetičkog sustava postoji potreba za „razvoj operativnih centara, potreba za stručnjacima, hardverskom i softverskom podrškom, redovitom obukom o kibernetičkoj sigurnosti i vježbama za provedbu najboljih strategija i planova“ (Spinu, 2020: 12).

Zaključno, u ovom poglavlju su prikazane potencijalne reformske aktivnosti koje bi mogle značajno unaprijediti sustav zaštite kritične infrastrukture Ukrajine. Glavnina reformi odnosi se na transformaciju i modernizaciju oružanih snaga Ukrajine s glavnim fokusom na sustav protuzračne obrane te zračne snage Ukrajine. Također, prepoznata je potreba za većom međunarodnom suradnjom i koordinacijom u svrhu implementacije modernih vojnih standarda te dobrih praksi gdje se naveo primjer Poljske koja prednjači u razvijanju modernih sustava za obaranje bespilotnih letjelica. Posljednji prijedlog reformi odnosi se na kibernetički sustav Ukrajine koji predstavlja važan aspekt sustava zaštite objekata kritične infrastrukture. Ključni elementi reforme kibernetičkog sustava Ukrajine odnose se na uspostavljanje jedinstvene strategije kibernetičkog djelovanja, povećanje ulaganja u stručnost i kvalificirano osoblje te preuzimanje modernih metoda djelovanja.

5. Zaključak

Oružani sukob između Ruske Federacije i Ukrajine predstavlja izrazito kompleksan sigurnosni izazov s kojim se trenutno suočavaju Europa i svijet. Početak rata 2014. godine te njegova eskalacija 2022. godine izazvali su niz problema poput regionalne nestabilnosti, humanitarne krize te gospodarskog pada. Među najugroženijim područjima nacionalne sigurnosti i ekonomije našli su se sustavi i resursi koji su esencijalni za funkcioniranje društva i ekonomije a to su objekti kritične infrastrukture. Sigurnost i stabilnost objekata kritične infrastrukture od vitalnog su značaja za zaštitu nacionalne sigurnosti, održavanje gospodarske aktivnosti te osiguravanje dobrobiti građana. Slijedom toga, u radu se analizirao sustav zaštite kritične infrastrukture Ukrajine u kontekstu stalnih ruskih terorističkih napada. Istraživanje je najprije adresiralo ključne izazove i opasnosti koji prijete objektima kritične infrastrukture gdje su se najviše izdvojile terorističke prijetnje poput korištenja nuklearnih postrojenja u terorističke svrhe. Također, objasnio se koncept izgradnje državnog sustava zaštite kritične infrastrukture gdje je glavni fokus stavljen na tzv. „Zelenu knjigu“ odnosno dokument koji predstavlja glavnu okosnicu razvoja politike zaštite kritične infrastrukture.

Nadalje, u radu se pružila definicija kritične infrastrukture Ukrajine na način da se ukazalo na niz strateških dokumenta koji su postepeno prepoznali važnost zaštite objekata kritične infrastrukture te su se sukladno tome definirali objekti koji pripadaju različitim državnim sigurnosnim sektorima. Nakon definiranja predmeta našeg istraživanja objasnio se način funkcioniranja sustava zaštite kritične infrastrukture Ukrajine gdje su se izdvojili režimi rada sustava zaštite kritične infrastrukture s obzirom na razinu opasnosti te su se objasnile zadaće sustava zaštite poput opće koordinacije sustava zaštite kritične infrastrukture u Ukrajini, prevencije kriznih situacija, podrška u odlučivanju, primjena nadzornih i kontrolnih mehanizama te međunarodna suradnja. Izrazito značajan dio rada predstavlja analiza odgovora sustava zaštite kritične infrastrukture gdje su se naveli primjeri terorističkih napada koji su izvršeni na kritičnu infrastrukturu Ukrajine od strane Ruske Federacije te se na taj način utvrdila nemogućnost potpune zaštite sustava zaštite kritične infrastrukture Ukrajine. Kroz navedenu analizu terorističkih napada Ruske Federacije na objekte kritične infrastrukture Ukrajine poput nuklearnih postrojenja, objekata zračnog, pomorskog, kopnenog prometa te naftnih i plinskih postrojenja potvrdili smo postavljenu hipotezu da se sustav zaštite ukrajinske kritične infrastrukture ne može uspješno suprotstaviti ruskom terorističkom djelovanju stoga je potreba reforma i uspostava učinkovitijeg sustava zaštite kritične infrastrukture Ukrajine.

Dodatno, u radu su prikazani dijelovi sustava zaštite kritične infrastrukture čija funkcionalnost i djelovanje su najviše ugroženi ruskim terorističkim napadima. Takve sustave smo adresirali temeljem čimbenika poput ljudskih žrtava, materijalne štete te financijskih iznosa potrebnih za reparaciju štete nastale napadom. Slijedom toga, predložena je reforma sustava zaštite kritične infrastrukture. Ključna predložena reforma odnosi se na reformu oružanih snaga Ukrajine gdje je predložena zamjena trenutnog ukrajinskog protuzračnog sustava iz sovjetske ere sa modernim zapadnim protuzračnim sustavom koji može uspješno parirati ruskim raketnim sustavima kao što su S-400 i Kinžal. Osim sustava protuzračne obrane, predloženo je jačanje zračnih snaga Ukrajine kroz nabavu naprednih američkih borbenih lovaca F-16 te je stavljen naglasak na međunarodnu suradnju i implementacija kvalitetnih praksi te na reformu sustava kibernetičke sigurnosti.

Istraživanje se baziralo na ključnim elementima teorije realizma koja je primijenjena u svrhu razumijevanja početka oružanog sukoba Ruske Federacije i Ukrajine te daljnje eskalacije rata. Što se tiče metode prikupljanja podataka, u istraživanju se koristila isključivo kvalitativna metoda prikupljanja podataka gdje se kroz analizu sadržaja putem induktivne metode zaključivanja došlo do jedinstvenog zaključka o stanju sustava zaštite kritične infrastrukture Ukrajine. Korištena literatura pružila je jasan i razumljiv pregled ključnih pojmova te je potkrijepila argumentaciju o nesposobnosti sustava zaštite kritične infrastrukture te o potrebi reforme postojećeg sustava. Ključne poteškoće u istraživanju odnosile su se na nemogućnost pronalaska kvalitetnih izvora o mjerama i postupcima sustava zaštite kritične infrastrukture koji su izvršeni tijekom aktualnog oružanog sukoba. Usprkos tome, istraživanje je pružilo jasne dokaze o nemogućnosti sustava zaštite da se obrani od vanjskih prijetnji te se kroz analizu načina funkcioniranja sustava zaštite predložilo uspostavljanje već spomenutih reformi.

Zaključno, istražujući temu kritične infrastrukture Ukrajine koja se trenutno nalazi pod stalnim ruskim terorističkim napadima spoznao sam kako je učinkovita i kvalitetna zaštita objekata kritične infrastrukture nužna za pravilno funkcioniranje života građana i građanki Ukrajine kako u doba mira tako i u doba oružanog sukoba. Osim toga, objekti kritične infrastrukture, osim što su presudni za opće blagostanje građana, imaju odlučujući faktor i u vojnom djelovanju s obzirom na važnost prometne infrastrukture te crpilišta nafte u svrhu normalnog djelovanje oružanih snaga Ukrajine. Smatram kako je za cjelokupni uspjeh u osiguravanju visokokvalitetnog sustava zaštite kritične infrastrukture Ukrajine potrebna snažna međunarodna financijska potpora i politička volja. U tom smislu potrebno je jačanje administrativnih kapaciteta te poticanje obučavanja stručnog osoblja za rad u kriznim situacijama. Također, analizirajući brojne službene dokumente Ukrajine i stručnu literaturu nisam uočio nikakve inovativne prijedloge za budući razvoj sustava zaštite kritične infrastrukture Ukrajine što ukazuje na stagnaciju u razvojnom procesu te samim time na potrebu reformi u kontekstu međunarodne suradnje i implementacije kvalitetnih praksi. Potrebno je istaknuti kako je Ruska Federacija tijekom dvogodišnje agresije koristila niz terorističkih taktika stoga je za Ukrajinu nužno uz navedene reforme uspostava agilne obrane koja je prilagodljiva na sve vrste terorističkih napada. Oružani sukob između Ruske Federacije i Ukrajine ističe važnost zaštite kritične infrastrukture u suvremenim vojnim sukobima, gdje se kibernetički i hibridni ratovi sve više koriste kao sredstvo za postizanje političkih ciljeva. Međunarodna zajednica, kroz financijsku i vojnu pomoć, prepoznaje važnost zaštite kritične infrastrukture Ukrajine kao ključnog faktora u očuvanju njezine suverenosti i pravnog poretka. Ukupno gledano, kako bi se osigurala zaštita objekata kritične infrastrukture, regionalna sigurnost te sprječavanje daljnje eskalacije sukoba potrebna je međunarodna suradnja Ukrajine i međunarodne zajednice na političkom i financijskom području. Posljednje, s obzirom na ogroman broj ljudskih žrtava koji je prouzročen ruskim terorističkim napadima na objekte kritične infrastrukture Ukrajine smatram kako postoji pravna i moralna obaveza za osnivanje međunarodnog kaznenog suda za ruske zločine u Ukrajini čime bi se otvorila mogućnost za zadovoljavanje pravde i odgovornosti za počinjenje zločine. Na taj način mogli bi se istražiti i procesuirati ratne zločini, zločini protiv čovječnosti te ostali oblici povrede međunarodnog prava koje su počinili politički i vojni dužnosnici Ruske Federacije. Osnivanje takvog suda poslalo bi snažnu međunarodnu poruku o osudi svakog oblika sustavnog nasilja te bi se pružila moralna i pravna podrška žrtvama sukoba.

6. Popis literature

Aa.com.tr (2022) Patriot System. https://www.aa.com.tr/en/russia-ukraine-war/patriot-system-to-significantly-improve-ukraines-air-defense-zelenskyy/2769772 Pristupljeno 5. veljače 2024 → (Aa.com.tr, 2022)

Al Gharaibeh, Fakir; Ahmad, Ifzal; Malkawi, Rima (2023.) *Impact of the Russia-Ukraine War on Education and International Students*. Journal of International Women's Studies.

Åtland, Kristian (2020.) *Destined for deadlock? Russia, Ukraine, and the unfulfilled Minsk agreements.* Post-sovietAffairs. (http://18.195.19.6/bitstream/handle/20.500.12242/2700/1784644.pdf?sequence=1&isAllowed=y=)

Atlanticcouncil.org (2023) F-16s. https://www.atlanticcouncil.org/blogs/new-atlanticist/heres-what-f-16s-will-and-will-not-mean-for-ukraines-fight-against-russia/ Pristupljeno 5. veljače 2024 → (Atlanticcouncil.org, 2023)

Atlanticcouncil.org (2023) Putin Speech Ukraine. https://www.atlanticcouncil.org/blogs/new-atlanticist/markup/putin-speech-ukraine-war/ Pristupljeno 22. listopada 2023.→ (Atlanticcouncil.org, 2023)

Barten, Denis G. (2023.) *Attacks on Ukrainian healthcare facilities during the first year of the full-scale Russian invasion of Ukraine*. Department of Emergency Medicine, VieCuri Medical Center.

Butrimas, Vytautas, Hajek, Jaroslav, Oleksandr, Sukhodolia, Dmytro, Borbo, Karasov, Sergii (2020.) *Hybrid warfare against Critical Energy Infrastructure: The Case of Ukraine*. NATO Energy Security Centre of Excellence.

E-ISAC (2016.) Analysis of the Cyber Attack on the Ukrainian Power Grid.

En.as.com (2022) Latest News. https://en.as.com/en/2022/03/07/latest_news/1646686014_463478.html Pristupljeno 29. studenog 2023. → (En.as.com, 2022)

Energycharter.org (2023) UA Sectoral evaluation and Damage assessment. https://www.energycharter.org/fileadmin/DocumentsMedia/Occasional/2023_05_24_UA_sectoral_evaluation_and_damage_assessment_Version_X_final.pdf Pristupljeno 3. veljače 2024 → (Energycharter.org, 2023)

Facebook.com (2023) Agency For Restoration. https://www.facebook.com/agency.for.restoration/posts/pfbid02hCg48jzTENdDTUMmE2zWwcVbEnPUmu9cuCayiF1KpjK6gULr5eyMrtF5iJi52nN2l Pristupljeno 10. prosinca 2023 → (Facebook.com, 2023)

Gostin LO, Rubenstein LS (2022.) *Attacks on Health Care in the War in Ukraine: International Law and the Need for Accountability*. JAMA. 327(16):1541–1542.

Hrw.org (2023) Tanks Playground. https://www.hrw.org/report/2023/11/09/tanks-playground/attacks-schools-and-military-use-schools-ukraine Pristupljeno 30. studenog 2023. → (Hrw.org, 2023)

Iaea.org (2022) Ukraines ZNPP Must Be Urgently Protected. https://www.iaea.org/newscenter/pressreleases/ukraines-znpp-must-be-urgently-protected-iaeas-grossi-says-after-plant-loses-all-external-power-due-to-shelling Pristupljeno 29. studenog 2023. → (Iaea.org, 2022)

Ivanuita, Serhii (2017.) .) *Developing the criticial infrastructure protection system in Ukraine*. National institute for strategic studies.

Jović, Dejan (2013.) *Teorije međunarodnih odnosa. Realizam.* Politička kultura.

Khaloponin, Yurii, Dolhopolov, Serhii (2023.) *Legislative support for the protection of critical infrastructure from cyberattacks of Ukraine.* Kyiv National University of Civil Engineering and Architecture, Faculty of Automation and Information Technology, Department of Cybersecurity and Computer Engineering.

Kohut, Yurii (2020.) *Measures for protection of the information systems of Ukraine's critical infrastructures against cyberattacks.* Kultura Bezpieczeństwa, (38) 57-65.

Kondratov, Sergiy (2017.) *Developing the criticial infrastructure protection system in Ukraine*. National institute for strategic studies.

Kse.ua (2024) About The School. https://kse.ua/about-the-school/news/zbitki-naneseni-infrastrukturi-ukrayini-v-hodi-viyni-skladayut-mayzhe-63-mlrd/ Pristupljeno 31.siječnja 2024 → (Kse.ua, 2024)

Luša, Đana (2011.) *Suvremeni izazovi realističke teorije međunarodnih odnosa*. Međunarodne studije, 11 (3): 9-35.

Mearsheimer, J. J. (2007). *Structural realism*. International relations theories: Discipline and diversity, 83, 77-94.

Mikac Robert, Cesarec Ivana, Larkin Rick (2018.) *Kritična infrastruktura. Platforma uspješnog razvoja sigurnosti nacija.* Jesenski i Turk.

News.un.org (2022) Story. https://news.un.org/en/story/2022/08/1124452 Pristupljeno 29. studenog 2023. → (News.un.org, 2022)

Ohchr.org (2023) Ukraine Civilian Casualty Update. https://www.ohchr.org/en/news/2023/09/ukraine-civilian-casualty-update-11-september-2023 Pristupljeno 29. listopada 2023. → (Ohchr.org, 2023)

Ordynovych, Andrii (2020.) *Modern trends in the Armed Forces of Ukraine transformation toward NATO standards*. Political Science and Security Studies Journal.

Peptan, Catalin (2022.) *Considerations on some aggressions against critical infrastructure on the territory of Ukrajine during the „special military operation" conducted by the Russian Federation.* University „Constantin Brâncuși" of Târgu Jiu. (https://www.utgjiu.ro/rev_ing/pdf/2022-1/07_Peptan%20Catalin_CONSIDERATIONS%20ON%20SOME%20AGGRESSIONS%20AGAINST%20CRITICAL%20INFRASTRUCTURE%20ON%20THE%20TERRITORY%20OF%20UKRAINE.pdf)

Piekarski Michał, Wojtasik Karolina (2022). *Protection of Polish critical infrastructure (CI) against air threats.* Security and Defence Quarterly.

Railtarget.eu (2022) Technologies and Infrastructure. https://www.railtarget.eu/technologies-and-infrastructure/about-30-of-transport-infrastructure-in-ukraine-destroyed-due-to-the-war-2339.html Pristupljeno 31. siječnja 2024 → (Railtarget.eu, 2022)

Rubryka.com (2023) Zelenskyj Zvernuvsya Do Nato. https://rubryka.com/en/2023/09/28/zelenskyj-zvernuvsya-do-nato-z-prohannyam-nadaty-dodatkovi-ppo-dlya-zahystu-krytychnoyi-infrastruktury/ Pristupljeno 11. prosinca 2023 → (Rubryka.com, 2023)

Sliwa, Zdzislaw (2022.) *The synergy between technology and soldiers in warfare- The Russian armed forces image during the war in Ukraine*. Baltic Defence Collage.

Spinu, Natalia (2020.) *Ukraine Cybersecurity Governance Assessment.* Geneva Centre for Security Sector Governance.

Sukhodolia, Oleksandar (2018.*) Implementation of critical infrastructure protection in Ukraine: achievements and challenges.* Information & Security: An International Journal.

Sukhodolia, Oleksandar (2022.*) The External Dimension of the European Union's Critical Infrastructure Protection Programme*. Taylor&Francis.

Tkachuk, Nataliya (2019.) *National cyber security system of Ukraine: perspectives of policy development and capacity building.* Research Institute of Informatics and Law of the National Academy of Legal Sciences of Ukraine.

U24.gov.ua (2023) Safe Skies. https://u24.gov.ua/news/safe_skies Pristupljeno 11. prosinca 2023 → (U24.gov.ua, 2023)

Unicef.org (2023) Ukrainian refugee children. https://www.unicef.org/eca/press-releases/more-half-ukrainian-refugee-children-not-enrolled-schools-poland-unicef-unhcr Pristupljeno 4. veljače 2024 → (Unicef.org, 2023)

Venable, John (2023.) *The U.S. Should Focus Military Support for Ukraine on Weapons Systems That Will Aid the Fight— the F-16 Will Not Do That.* The Heritage Foundation.

Verhovna Rada (2021) Zakon Ukrajine o kritičnoj infrastrukturi. https://zakon.rada.gov.ua/laws/show/1882-20#Text Pristupljeno 10. prosinca 2023 → (Verhovna rada, 2021)

War.ukraine.ua (2023) Preparations Heating Season. https://war.ukraine.ua/war-news/preparations-heating-season-enter-final-stage-prime-minister-ukraine/ Pristupljeno 11. prosinca 2023 → (War.Ukraine.ua, 2023)

War.ukraine.ua (2023) Ukraine Protection Energy. https://war.ukraine.ua/war-news/ukraine-protection-energy-russian-attacks-winter/ Pristupljeno 11. prosinca 2023 → (War.Ukraine.ua, 2023)

Weareukraine.info (2023) We need F16 Aircraft. https://www.weareukraine.info/we-need-f-16-aircraft-not-only-to-shield-the-front-line-but-to-protect-the-objects-of-critical-infrastructure-of-ukraine/ Pristupljeno 6. veljače 2024 → (Weareukraine.info, 2023)

Who.int (2023) Attack On Health Care In Ukraine. https://www.who.int/europe/news/item/30-05-2023-who-records-1-000th-attack-on-health-care-in-ukraine-over-the-past-15-months-of-full-scale-war Pristupljeno 30. studenog 2023. → (Who. int, 2023)

Zhyvko, Z., Rudyi, T., Senyk, V., Kucharska, L. (2020). *Legal basis of ensuring cyber security of ukraine: problems and ways of eliminating*. Economics, Finance and Management Review, (2) 82–90.

Sažetak

Kritična infrastruktura Ukrajine obuhvaća različite sektore poput energetike, transporta, telekomunikacija, vodovoda, zdravstvenih objekata i sličnih sustava koji su ključni za stabilnost zemlje i ekonomski prosperitet. Uslijed oružane invazije Ruske Federacije objekti kritične infrastrukture Ukrajine postali su meta učestalih terorističkih napada i sabotaža što predstavlja ozbiljan izazov za nacionalnu sigurnost i stabilnost. Istraživanje je najprije analiziralo izazove i prijetnje koje ugrožavaju opstojnost i funkcionalnost kritične infrastrukture Ukrajine te način funkcioniranja sustava zaštite kritične infrastrukture gdje su opisane glavne zadaće sustava zaštite kritične infrastrukture Ukrajine te način rada sustava zaštite kritične infrastrukture za vrijeme trajanja određene opasnosti. Sljedeći važan korak u istraživanju odnosio se na analizu odgovora sustava zaštite kritične infrastrukture Ukrajine na ruske terorističke napade gdje je napravljen svojevrstan popis terorističkih napada Ruske Federacije na različite objekte kritične infrastrukture Ukrajine. Nakon uočenih problema i manjkavosti sustava zaštite kritične infrastrukture Ukrajine u završnom dijelu istraživanja predložene su reforme sustava zaštite kritične infrastrukture Ukrajine s fokusom na reformu oružanih snaga Ukrajine te reformu sustava kibernetičke sigurnosti. Također, kako bi se osigurala otpornost i funkcionalnost objekata kritične infrastrukture predložene su reforme sustava zaštite kritične infrastrukture Ukrajine koje se sastoje od niza mjera i politika usmjerenih na očuvanje sigurnosti i funkcionalnosti ključnih sektora.

Ključne riječi: Ukrajina, kritična infrastruktura Ukrajine, sustav zaštite kritične infrastrukture Ukrajine, objekti kritične infrastrukture Ukrajine, Ruska Federacija, teroristički napadi, oružani sukob

Abstract

Ukraine's critical infrastructure includes various sectors such as energy, transportation, telecommunications, water supply, health facilities and similar systems that are crucial for the country's stability and economic prosperity. Following the armed invasion of the Russian Federation, critical infrastructure facilities of Ukraine have become the target of frequent terrorist attacks and sabotage, which poses a serious challenge to national security and stability. The research first analyzed the challenges and threats that threaten the viability and functionality of the critical infrastructure of Ukraine and the functioning of the critical infrastructure protection system, where the main tasks of the critical infrastructure protection system of Ukraine and the mode of operation of the critical infrastructure protection system during the duration of a certain danger were described. The next important step in the research was related to the analysis of the response of the critical infrastructure protection system of Ukraine to Russian terrorist attacks, where a kind of list of terrorist attacks by the Russian Federation on various objects of critical infrastructure of Ukraine was made. After the observed problems and shortcomings of the critical infrastructure protection system of Ukraine, in the final part of the research, reforms of the critical infrastructure protection system of Ukraine were proposed with a focus on the reform of the armed forces of Ukraine and the reform of the cyber security system. Also, in order to ensure the resilience and functionality of critical infrastructure facilities, reforms to the critical infrastructure protection system of Ukraine were proposed, consisting of a series of measures and policies aimed at preserving the safety and functionality of key sectors.

Keywords: Ukraine, critical infrastructure of Ukraine, system of protection of critical infrastructure of Ukraine, objects of critical infrastructure of Ukraine, Russian Federation, terrorist attacks, armed conflict