САВРЕМЕНЕ СТУДИЈЕ БЕЗБЕДНОСТИ
2/2024

CONTEMPORARY SECURITY STUDIES
2/2024

САВРЕМЕНЕ СТУДИЈЕ БЕЗБЕДНОСТИ
2/2024

Београд, 2024.

Рецензенти

др Роберто СЕТОЛА, Биомедицински универзитетски кампус,
Рим, Италија

др Јонас ЈОХАНСОН, Универзитет у Лунду,
Одсек за управљање ризиком и друштвену безбедност, Лунд, Шведска

др Марина МИТРЕВСКА, Универзитет Св. Ћирил и Методије у Скопљу,
Филозофски факултет, Институт за безбедност, одбрану и мир, Скопље,
Северна Македонија

др Наталија ЛУКИЋ, Универзитет у Београду,
Правни факултет, Београд, Србија

др Јелена КОСТИЋ, Институт за упоредно право,
Београд, Србија

др Ђорђе ЂОРЂЕВИЋ, Криминалистичко-полицијски универзитет,
Београд, Србија

др Биљана СИМЕУНОВИЋ-ПАТИЋ, Криминалистичко-полицијски универзитет,
Београд, Србија

др Снежана СОКОВИЋ, Универзитет у Крагујевцу,
Правни факултет, Крагујевац, Србија

др Милован СУБОТИЋ, Универзитет одбране,
Институт за стратегијска истраживања, Београд, Србија

др Милош МИЛЕНКОВИЋ, Универзитет одбране,
Институт за стратегијска истраживања, Београд, Србија

др Вељко БЛАГОЈЕВИЋ, Институт за међународну политику и привреду,
Београд, Србија

др Лука ГЛУШАЦ, Универзитет у Београду,
Институт за филозофију и друштвену теорију, Београд, Србија

др Мирко ФИЛИПОВИЋ, Универзитет у Београду,
Факултет за специјалну едукацију и рехабилитацију, Београд, Србија

др Јована БАНОВИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Слађана ЈОВИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Александра ИЛИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Владимир АЈЗЕНХАМЕР, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Јасмина ГАЧИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Владимир ЈАКОВЉЕВИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Божидар БАНОВИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Зоран ДРАГИШИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Горан МАНДИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Дејана ЈОВАНОВИЋ ПОПОВИЋ, Универзитет у Београду,
Факултет безбедности, Београд, Србија

др Марко МИЛОШЕВИЋ, Географски институт Јован Цвијић САНУ,
Београд, Србија

др Марија ЂОРИЋ, Институт за политичке студије,
Београд, Србија

САДРЖАЈ

ПРЕГЛЕДНИ ЧЛАНЦИ

ОСВРТИ

ПРИКАЗИ КЊИГА

ПРЕГЛЕДНИ ЧЛАНЦИ

Примљено: 16. септембар 2024.
Прихваћено: 02. децембар 2024.

УДК 327.5:332.142.4(98)
COBISS.SR-ID 161879305
DOI: 10.5937/ssb2402009T

РЕМИЛИТАРИЗАЦИЈА И БОРБА ЗА ЕКОНОМСКУ ЕКСПЛОАТАЦИЈУ АРКТИКА У СЕНЦИ РАТА У УКРАЈИНИ

др Борис ТУЧИЋ*, ванредни професор

* Факултет безбједносних наука Универзитета у Бањој Луци, boris.tucic@fbn.unibl.org

РЕМИЛИТАРИЗАЦИЈА И БОРБА ЗА ЕКОНОМСКУ ЕКСПЛОАТАЦИЈУ АРКТИКА У СЕНЦИ РАТА У УКРАЈИНИ

Сажетак: *Циљ рада је да се анализирају најзначајније импликације савремених међународних односа по безбедност Арктика. Као рефлексија актуелних глобалних дешавања, са исходиштем у украјинском конфликту, подручје Арктика предмет је релативно интензивне (ре)милитаризације с обе стране, али и војно-безбедносне реконфигурације, у смислу да је НАТО, пријемом Финске и Шведске у чланство, значајно учврстио своју позицију на балтичком, нордијском и арктичком правцу, те ојачао своје непосредно присуство на руској граници. Анализа предмета истраживања реализована је у теоријском оквиру науке о међународним односима, уз коришћење одабраних научних метода, а као један од закључака спроведене анализе намеће се констатација да је, управо одражавајући стање у савременим међународним односима и њихову, између осталог, изражену милитантну димензију, војна безбедност Арктика предоминантна у односу на остале димензије његове безбедности. При томе, додатни отежавајући моменат представља и 'кинески фактор', односно тенденција НР Кине да се, преко руског Арктика, постепено наметне као незаобилазан чинилац у политичким, привредним, али и безбедносним процесима у региону, о чему изразито негативан став директно испољавају западне арктичке земље предвођене САД, док Руска Федерација дугорочно мора водити рачуна да кинеско присуство и утицај у региону не пређу 'прихватљиве оквире'.*
Кључне речи: *Арктик, (ре)милитаризација, НАТО, украјински конфликт, кинески фактор*

Увод

Са Северним полом, као његовим епицентром, и Северним леденим океаном, као воденом масом која га уоквирује, Арктик захвата подручје којем гравитира осам земаља, при чему највећи део арктичке обале, око 54%, припада Руској Федерацији у којој живи око 2,5 милиона од укупно 4 милиона арктичког становништва, укључујући и неколико десетина различитих аутохтоних етничких групација са овог простора. У периоду Хладног рата, примарно захваљујући чињеници

да се управо на простору Арктика, преко Великог и Малог диомедског острва, могла идентификовати најкраћа удаљеност између територија САД и тадашњег СССР у пречнику од само 2,5 километра, овај простор је послужио као погодан полигон за инсталирање ракетних система кратког и средњег домета и провођење политика међусобног одвраћања у односима између две стране. Окончањем Хладног рата и крахом биполаризма Арктик губи на свом дотадашњем геополитичком, односно војном значају и манифестује се као „зона изузетности" (енгл. *Zone of excellence*), у којој су дојучерашњи хадноратовски односи замењени све интензивнијом сарадњом арктичких земаља у бројним областима, укључујући и изградњу различитих, додуше не у потпуности институционализованих структура посредством којих би она била најефикасније реализована, посебно узимајући у обзир да је, у поређењу са Антарктиком, на пример, правна регулисаност бројних питања на овом подручју била неупоредиво сиромашнија. Климатске промене у последњих неколико деценија највидљивије су управо на арктичком подручју, осигуравајући му привредни, транспортни, па и безбедносни значај у политикама кључних регионалних и глобалних актера какав раније није уживао. Услед глобалног отопљавања и редукције глечера, на подручју Арктика идентификоване су нове и, што је посебно битно, економичније транспортне руте између Атлантског и Тихог океана, међу којима се посебно издвајају Севернозападна, која је под јурисдикцијом Канаде и којом се значајно скраћује удаљеност између источне Азије и западне Европе, те Северноисточна, која је под контролом Москве. Централноарктичка рута, којом би се значајно смањила удаљеност између Северне Америке и Азије, услед оштрих климатских услова најмање је у употреби, иако се очекује да ће наредних деценија и она добити на значају. Други битан разлог „пробуђеног" значаја Арктика садржан је у чињеници да ово подручје представља значајну сировинску базу, са око 30% светских резерви природног гаса, 13% резерви нафте, 9% резерви угља, као и незанемерљивим количинама минерала и метала, попут урана, бакра, титанијума, сребра и злата, односно дијаманата и графита (Boyd et al., 2016; Andersson and Kalvig, 2022; Broek, 2023). Све ово, поред тога што је представљало адекватну основу за интензивнији економски развој, довело је Арктик у специфичну позицију изложености хибридним безбедносним претњама на које су арктичке државе морале понудити адекватне одговоре.

Савремени међународни односи карактеришу се снажном ревитализацијом хладноратовских тензија и израженом поларизацијом између политичког Запада и, како се то често означава, „глобалног Југа" (El Aynaoui, Magri, Saran, 2023), а чија је преломна тачка украјински конфликт и бројне импликације које је овај догађај проузроковао. Тектонске промене глобалног међународног поретка снажно су се рефлектовале и на регион Арктика и његову безбедност. У оквирима теоријских поставки науке о међународним односима, уз примену одабраних научних метода, попут анализе садржаја, индуктивне, дедуктивне те компаративне методе, у раду се анализирају неке од најзначајнијих импликација савремених глобалних дешавања у међународним односима по различите аспекте арктичке безбедности, међу којима су свакако највидљивије његова интензивна ремилитаризација и предоминација војне у односу на остале димензије безбедности, чиме је Арктик, за кратко време, од „зоне сарадње" поново трансформисан у „зону конфронтације", односно полигона за непосредно одмеравање снага кључних регионалних и глобалних актера, с тим што се, за разлику од хладноратовског периода, као такмац у трци за контролом над Арктиком данас све више намеће и НР Кина. Уз спорадично војно присуство, Кина свој утицај превасходно остварује на економском плану, постепено ширећи своје инвестиционо деловање од руског Арктика ка његовим осталим деловима, чиме, с једне стране, обезбеђује неопходан импулс за његов привредни развој, док, с друге, поготово уколико се политика Пекинга у постојећим околностима посматра кроз призму блиске сарадње са Москвом, проузрокује негативне реакције западних арктичких земаља на челу са САД и тиме индукује негативне импликације по безбедност региона.

Војно-безбедносна димензија

(Ре)милитаризација Арктика

Ремилитаризација арктичког подручја започела је пре избијања украјинског конфликта 2022. године, међутим, са овим догађајем она је значајно добила на свом интензитету. Губитком његовог војног значаја по окончању Хладног рата, САД су највећи део својих војних база на подручју Арктика или редуковале или у потпуности угасиле, као што је био случај са базом Тул на Гренланду, чији је састав за кратко

време смањен са 6.000 на само 100 војника, базама на Исланду, из којих је повучено 2.000 америчких војника, или са самом Аљаском, са које је највећи број радара премештен на друге, како се у том тренутку процењивало, важније локације. Но, са интензивирањем руских активности на арктичком подручју, јачањем активности Москве на изградњи Северноисточне транспортне руте, отварањем нових лука и њиховим опремањем за цивилну и војну употребу, те, како западни аутори често указују, са чувеним говором председника Путина на Минхенској конференцији о безбедности из фебруара 2007. године, који је протумачен као бацање „рукавице у лице" униполарном поретку на челу са САД, ситуација се постепено мења (Fried, Volker, 2022). Арктик све чешће постаје предмет различитих стратешких и оперативних докумената Вашингтона, како у домену спољне политике тако и одбране, почевши од нове Поморске стратегије из 2007. – *Cooperative Naval Strategy for 21st Century: Sea Power* (Office of the Chief of Naval Operations, 2007), којом је, између осталог, као један од циљева предвиђена интернационализација поморских рута које су биле под контролом Отаве и Москве, преко Мапе пута за развој америчке флоте 2014–2030. из 2014. године, која је представљала документациону основу за поновно успостављање Друге америчке флоте 2018. године након њеног гашења 2011, уз премештање зоне одговорности ове војне формације са ширег подручја Атлантика на појас који захвата његов северни део, Северни ледени океан и источне обале САД (US DoN, 2014), до, на пример, Националне одбрамбене стратегије из 2022. године (US DoD, 2022). Стратегија је на једном месту обухватила циљеве садржане и у другим, специфико ванијим поморским документима[1], Руска Федерација и НР Кина се јасно означавају као извор свих безбедносних претњи по САД, те указује на потребу модернизације и повећања америчких војних капацитета на арктичком подручју. Документом је предвиђено и интензивније патролирање америчке војске дуж границе руског Арктика и јачање контроле над Северноисточном рутом како би се спречило даље ширење руског утицаја. Са повећањем америчког војног присуства на арктичком подручју интензивиране су и војне вежбе САД са њиховим савезницима, како у оквиру НАТО-а тако и са тада још увек неутралним државама, Шведском и Финском. Према адмиралу Мајклу Гилдеју (*Michael Gilday*), бившем команданту

1 На пример, заједнички документ поморских и копнених снага под називом *A Blue Arctic: Regaining Arctic Dominance: Predominance of Integrated Naval Power* из 2021. године или поморски акциони планови из истог периода.

поморских операција, на пример, само током 2020. године САД су са савезницима реализовале 20 војних вежби и операција на Арктику (Naval News, 12.1.2021). Такође, у складу са прокламованим циљевима да се успостави чвршћа контрола над Северноисточном рутом, поготово на подручју Мурманска, САД и Норвешка су најавиле обнављање некада веома значајне базе Олафсверн, удаљене само 350 километара од руске границе, до чега постепено и долази од маја 2021. године, када је прва америчка нуклеарна подморница упловила у базу. Паралелно са погоршањем свеукупне ситуације у односима Руске Федерације и Запада услед дешавања у Украјини, САД додатно јачају и своје ваздухопловно присуство на овом подручју – четири стратешка бомбардера Б1 лансер распоређена су на норвешки војни аеродром Орланд, 150 ловаца Ф – 35 и Ф – 22 *Raptors* премештено је на Аљаску, а приступило се и обнављању војне базе Тул на Гренланду и распоређивању борбених авиона у оквиру ње.

Но, без обзира на јачање америчког, односно НАТО присуства последњих година, Руска Федерација и даље поседује већи број војних база на Арктику за око једну трећину, што јој омогућава очување стратешког преимућства на овом простору. Према неким оценама, САД и савезницима је потребно десет година интензивног улагања како би изједначили своје војно присуство на Арктику са Москвом (Gronholt – Pedersen, Fouche, 16.11. 2022). Руски Арктик стављен је под команду Заједничке команде руских оружаних снага, те спада у одговорност Северне флоте, која је креирана председничким указом бр. 803 од 21. децембра 2020. године (RF President, 2020), са основним задатком да штити подручје од Мурманска на западу до Анадира на истоку. Од њеног успостављања до марта 2024. године, као што ће се видети, Северна флота функционисала је као самостална организациона јединица, док је данас утопљена у обновљену Лењинградску војну област. Уз учешће Савезне агенције за посебно грађевинарство, јачање војног присуства Руске Федерације на Арктику манифестује се кроз изградњу и модернизацију аеродрома, инсталирање нових војних инфраструктурних објеката, постављање антиракетних система С – 400, те увећање присуства копнених снага. На острву Костелња, на пример, које је позиционирано у центру Северноисточне руте, постављени су суперсонични ракетни системи „Бастион", летови руских стратешких авиона у близини Аљаске последњих година вишеструко су увећани – од шест током 2015. до преко шездесет током 2020. године, док се о безбедности Северно-

источне руте старају суперсонични ловци МИГ 31 БМ. Посебан геостратешки значај за Москву има полуострво Кола, на којем су стациониране, између осталог, ваздухопловна база Северноморск 1, подморничке базе Гаџијево и Околнаја, те космодром Плесетск, на којем су инсталирани најмодернији термонуклеарни системи интерконтиненталних балистичких ракета RS – 24Yars, званично представљени у оквиру војне вежбе „Гром" из 2019. године. Поред тога, о чему сведочи и иновирана америчка Стратегија за Арктик из јула 2024. године (US DoD, 2024), посебну забринутост западних савезника изазива све интензивнија сарадња Русије и Кине на овом подручју на привредном, научно-истраживачком, инфраструктурном, енергетском, али и војно-безбедносном плану, укључујући, на пример, и заједнички прелет руских и кинеских бомбардера у близини Аљаске јула 2024. године, што је проузроковало реакцију америчких и канадских ваздухопловних снага. У сврху спровођења заједничких операција и јачања стратешког партнерства, руски и кинески авиони до сада су реализовали седам заједничких летова на различитим локацијама, међутим, ово је био први пут да су овакве активности спроведене на овом подручју, што је у западним престоницама протумачено као јасна амбиција Кине, као „самопроглашене државе у близини Арктика" (Descamps, 2019), да се наметне као незаобилазан фактор политичких и безбедносних процеса у региону (Williams, Bingen, MacKenzie, 2024). Иако је реч о два модела авиона још из времена Хладног рата – руском стратешком бомбардеру Тупољев ТУ 95 и кинеском бомбардеру Х6, обе врсте авиона су и данас изразито функционалне и капацитиране за транспорт и употребу нуклеарног наоружања, при чему симболика јачања руско-кинеског војног партнерства на Арктику није изражена само кроз чињеницу да се радило о њиховом првом заједничком лету на овом подручју, већ и кроз чињеницу да су руски и кинески авиони заједнички и полетели, али и слетели у Анадир, једну од девет руских ваздушних лука на арктичком подручју. У сваком случају, након руско-кинеске поморске вежбе у Беринговом мору 2022. године, због које је Норвешка подигла борбену готовост своје морнарице на највиши ниво, ово је свакако био догађај који је изазвао посебну забринутост САД и савезника.

Проширење НАТО-а и учвршћивање балтичког, нордијског и арктичког правца

Друга веома битна војно-безбедносна импликација погоршања односа између Руске Федерације и политичког Запада и, посебно, украјинског конфликта по арктички регион, односи се на ширење структуре НАТО на овом подручју. Под утицајем заоштравања односа са Руском Федерацијом, након вишедеценијске војне неутралности, априла 2023, односно марта 2024. године Финска и Шведска су постале чланице Северноатлантског савеза, чиме се „однос снага" у региону померио на 7:1 у корист Савеза. Један од разлога покретања специјалне војне операције од стране руске војске фебруара 2022. године било је, између осталог, заустављање даљег ширења НАТО-а на Исток и његовог ширег учвршћивања на руским границама, међутим, након уласка три балтичке државе у састав Савеза крајем марта 2004. године, Русија је пријемом Финске у чланство организације дошла у позицију да је присуство НАТО-а на њеним непосредним границама проширено чак за нових 1.370 километара. Уопште, највећи значај уласка Шведске и Финске у чланство Савеза геостратешког је карактера, јер је на тај начин НАТО додатно учврстио своје источно крило и позицију на Балтику. Посредством Шведске, НАТО је добио додатну дубину у контексту одбране балтичког подручја, док је уласком Финске у чланство Савеза, уз поменути појачани излазак на руске границе, Савез значајно ојачао своје присуство на арктичком подручју.

И не само то, НАТО је на овај начин појачао контролу над руским маневрима и капацитетима стационираним на, за руску страну, изузетно важном полуострву Кола и Мурманској области. Протежући се између Белог мора на југу и Баренцовог мора на северу, полуострво Кола својим највећим делом лежи у Руској Федерацији, док његови мањи делови припадају Финској и Норвешкој. Према оценама аутора (Alberque, Schreer, 2022; Forsberg, 2023), уласком Финске и Шведске у његово чланство НАТО је значајно ојачао свој нордијско-скандинавски блок, иако су ове земље и раније, у оквиру Нордијске безбедносне сарадње (*NORDEFCO*), покушавале да заједно са Норвешком, Исландом и Данском изнађу одговоре на нека од кључних питања њихове безбедности и одбране.

Након превазилажења препрека у процесу приступања индукованих из политичких односа са Турском и Мађарском, Шведска и Финска су се релативно брзо, континуираним издвајањем за потребе одбране и изнад Вашингтонским уговором прописаних 2% БДП на

годишњем нивоу[2], модернизацијом и јачањем властитих војних капацитета, те пружањем подршке Украјини у наоружању и војној опреми, верификовале као активне и лојалне чланице Савеза.[3] Као главни снабдевач новим оружјем, оруђем и опремом за потребе финске и шведске армије истичу се САД, поготово када је реч о, на пример у случају Финске, набавци нових борбених авиона, али и ХИМАРС ракетних система (Bisht, 4.8.2023). Такође, број заједничких војних вежби и маневара у којима су учествовале нове чланице Савеза се значајно увећао, да би 2024. године, заједно са Норвешком, оне биле и домаћини војне вежбе „Нордијски одговор 24" (енгл. *Nordic Response 24*), у оквиру једног од највећих војних маневара НАТО-а од његовог оснивања под називом „Непоколебљива одбрана" (енгл. *Steadfast Defence*).

Посматрајући индивидуалне капацитете нових чланица Савеза, аналитирачи су углавном сагласни да је кључни допринос Финске њен, у поређењу са њеном укупном популацијом, незанемарљив војни контигент копнене војске, те артиљеријске снаге, укључујући и постројења на непосредном арктичком подручју. Такође, значајан је допринос који нове чланице остварују и у домену ваздухопловних снага, јер се процењује да ће Норвешка, Шведска, Данска и Финска заједнички располагати са око 200 борбених авиона, због чега су већ означене као „НАТО арктичке ваздушне снаге у Европи" (Kuusela, 2024). На тај начин се, бар делимично, умањује предоминација руских ваздушних снага у региону.

Са својим вишедеценијским војно-неутралним *background*-ом, Шведска и Финска не само да не спадају у групу земаља које располажу нуклеарним војним капацитетима, већ је и њихова снажна антинуклеарна кампања, поготово у Шведској, прерасла у битну компоненту државног и друштвеног идентитета. Уједно, у прошлости су бројни милитантни елементи спољне политике САД били снажно критиковани од стране политичких представника, али и цивилног сектора у овим земљама. Од маја 2022. године, када је поднесен заједнички захтев за пријем у чланство Савеза, представници Финске и Шведске су

2 Финска, на пример, попела се на седмо место међу НАТО чланицама по издвајањима за војне потребе, са 2,41% БДП у 2024. години, док се Шведска налази на четрнаестом месту са 2,2% БДП за исто раздобље. Војни буџет Финске за 2024. годину износи 6.2 милијарде евра и за око 5% је већи у односу на онај за 2023. годину, док у Шведској он износи 4,2 милијарде евра и у односу на 2020. годину он је удвостручен.

3 При томе, почетком септембра 2024. године и Шведска и Финска дале су сагласност на употребу њиховог наоружања испорученог Украјини за нападе у дубину руске територије.

настојали промовисати минималистички приступ овом питању, сводећи неспорно радикалан заокрет у својој спољној и одбрамбеној политици на потребу за осигурањем гаранција у оквиру система колективне одбране из члана 5. Вашингтонског уговора (NATO, 1949), али и одбијајући било какву идеју о распоређивању на својој територији система погодних за инсталирање нуклеарних пуњења, а који би били искоришћени у евентуалном сукобу са Руском Федерацијом (Forsberg, 2023). Иако су промишљања на наведену тему још увек на теоријском нивоу, чини се да је данас ситуација донекле измењена. Док је фински председник и даље става да не постоји могућност да амерички ракетни системи са нуклеарним бојевим главама буду распоређени на финској територији, шведски премијер је нешто флексибилнији, истичући да би то било веома могуће, али само у околностима постојања отвореног оружаног сукоба између НАТО-а и Руске Федерације (Nezirovic, 13.5.2024).

У сваком случају, пријем Финске и Шведске отворио је потпуно нову геополитичку димензију за НАТО, доприносећи јачању његовог утицаја и позиције на балтичком, нордијском, односно арктичком подручју. Међутим, без обзира на неспоран нови квалитет који је НАТО добио пријемом две нове чланице, а поготово Финске, не сме се пренебрегнути чињеница да ће, у случају избијања директног оружаног сукоба, међу првима на удару бити управо новопридошле чланице Савеза.

Наравно, Руска Федерација је са негодовањем реаговала на улазак Шведске и Финске у чланство Савеза и слабљење њеног геополитичког положаја које је овај догађај директно индуковао, при чему је вероватно најколоритнији приказ руског става манифестован кроз изјаву председника Русије још из 2016. године: „Данас када гледамо преко границе ми видимо Финце. Но, уласком Финске у НАТО, ми ћемо преко границе видети непријатеље" (Euronews, 1.7.2016). Уз појачана упозорења Хелсинкију и Стокхолму на могуће последице њиховог уласка у чланство Савеза, један од кључних потеза Москве у контексту адаптације новонасталој ситуацији био је указ председника Русије од 26. фебруара 2024. године, на дан када је Мађарска извршила ратификацију шведског приступног споразума у НАТО, којим је, између осталог, обновљена некадашња совјетска Лењинградска војна област, сачињена од десет организационих јединица и Санкт-Петерсбургом као централним градским језгром. Уједно, тиме је Северна флота престала да постоји као самостална област, утопивши се у

новонасталу војну формацију (RF President, 2024). Додатни одговор на увећане безбедносне опасности на северозападној граници Руске Федерације представљало је и инсталирање додатних ракетних система, међу којима доминирају Искандери и Кинжали, на полуострво Кола, што је, с друге стране, довело до усвајања новог одбрамбеног плана од стране норвешког парламента, којим је као један од циљева предвиђено и дуплирање ракетних одбрамбених капацитета земља – ваздух, као одговор на руске ракете кратког и средњег домета (Nilsen, 11.6.2024).

Импликације по економску безбедност Арктика

Уколико под економском безбедношћу подразумевамо свеукупност интерних и екстерних фактора, услова и потенцијала који одређеном ентитету омогућавају ефикасно функционисање, остваривање самоодрживог привредног развоја, високог животног стандарда, те ефективну заштиту, као два кључна фактора економске безбедности Арктика манифестују се импликације глобалних климатских промена на свеукупне привредне активности на овом подручју, те значајна природна богатства којима се Арктик карактерише. Истовремено, могуће је идентификовати и неколико веома значајних препрека остварењу економске безбедности Арктика, од којих неки нису у потпуности нови, али су последњих година, а посебно од избијања украјинског конфликта, добили на значају. Један од њих тиче се обуставе било каквог заједничког деловања арктичких земаља кроз наменски успостављене структуре, међу којима се посебно истичу Арктички савет и Баренцов Евро-атлантски савет. Њихов значај огледа се у томе што су управо посредством њих настојало заједнички решавати бројна питања од интереса за све земље региона, од негативних еколошких импликација по биодиверзитет Арктика, које су последица његовог пребрзог „отварања", преко успостављања различитих облика научно-истраживачке сарадње, до утврђивања заједничких правила провођења економских, истраживачких и других активности, а на основу којих би се бар делимично ублажила несигурност која је резултат недовољне правне регулисаности овог подручја. Како је Руска Федерација преузела председавање Арктичким саветом у периоду 2022–2023. године, избијањем украјинског конфликта преосталих

седам земаља региона суспендовало је своје деловање у овој организацији, чиме је ефективан рад Савета обустављен. Слична ситуација била је и са Баренцовим Евро-атлантским саветом, с том разликом што је у овом случају Руска Федерација, након што је Финска одбила да пренесе председавање Саветом на Москву, иступила из његовог чланства. Евро-атлантски савет је наставио са радом без највеће и најзначајније арктичке државе, а функцију председавајућег по истеку финског мандата преузео је нордијски трио – Финска, Шведска и Норвешка, на обнављајући мандат од годину дана.

Други значајан моменат везан за економску безбедност Арктика, иако је и он, у суштини, геополитичког карактера, односи се на „кинески фактор" и све интензивније укључивање Пекинга у регионалне привредне процесе. Иако не спада у групу арктичких земаља, Кина се од 2018, доношењем документа „Политика према Арктику" (енгл. *Arctic Policy Paper*) (PRC State Council, 2018), прогласила за „земљу близу Арктика" (енгл. *near – Arctic state*) те, позивајући се на решења Конвенције о праву мора (UNCLS, 1982) и Уговор из Свалбарда из 1920. године, којим је регулисан специфичан међународноправни статус Свалбардског архипелага у оквиру Норвешке, истакла право на пловидбу и прелетање над арктичким подручјем, рибарење, инсталацију телекомуникационе инфраструктуре на морском дну, те инвестициона улагања. Један од идентификованих кинеских праваца деловања на Арктику јесте развој „Поларног пута свиле", као сегмента шире иницијативе „Појас и пут", којом би требало бити омогућено снажније привредно и транспортно повезивање Азије и Европе посредством нових транспортних рута, а посебно Северноисточне руте, која је под контролом Москве. Захваљујући свом активизму, али и подршци неких арктичких земаља, попут Исланда и Данске, Кина је 2018. године успела обезбедити и статус посматрача у оквиру Арктичког савета.

Поред ранијих кинеских улагања у Гренланду, Исланду, Норвешкој и Финској у домену научног истраживања, рударења и транспортне инфраструктуре (US Congress FAC, 2022), данас се као кључни партнер остваривању кинеских интереса на Арктику манифестује Руска Федерација. С једне стране, у околностима изолације и санкционисања од стране Запада, Москва је у Кини пронашла заменско тржиште за своје енергенте, као и инвестиоциону подршку у руском делу Арктика, док је Кина, с друге, у Русији препознала незаобилазну платформу преко које би даље ширила свој утицај, са коначним циљем позиционирања као „велике поларне силе" до 2030. године (Lamazhapov

et al., 14.11.2023; Ngila, 11.5.2023). Но, колико год се радило о тренутно обострано корисном партнерству, чији се квалитет неретко осликава кроз успешност енергетског пројекта „Јамал ЛНГ" (енгл. *Yamal LNG*), у којем, додуше, нису партиципирали само Пекинг и Москва већ и неке западноевропске земље, попут Француске и СР Немачке, не сме се изгубити из вида да Русија и Кина имају и бројне различите интересе у региону и да Русија не гледа са превише одобравања на кинеске амбиције јачања свог присуства неруском делу Арктика и контакте са другим, условно, западним арктичким земљама. Према доступним подацима, Кина је до сада инвестирала преко 90 милијарди долара у региону, примарно у руском делу Арктика, али и у различите пројекте у нордијским земљама, при чему се као кључне области кинеских улагања издвајају транспортна инфраструктура, енергетика, те научно-истраживачке активности (US Congress FAC, 2022). Но, све израженије присуство Кине на Арктику, по правилу у сарадњи са Москвом, у Вашингтону се доживљава као „дестабилизујућа сила" која својим економским и војним капацитетом може значајно угрозити америчке националне интересе на овом подручју (Tallis, Rosen, Overfield, 2022), те је, у складу са наведеним, и незанемарљив део најновије америчке Националне стратегије за Арктик из 2024. године управо посвећен модалитетима деловања САД и савезника како би се нарастајући утицај „руско-кинеске осовине" сузбио (US DoD, 2024: 4).

Напослетку, иако нису *stricto sensu* везани за постојеће стање у међународним односима и, конкретно, односе између великих сила, бројни економисти као значајне факторе који негативно утичу на економску безбедност Арктика истичу пре свега његову неконкурентност у глобалним оквирима, одсуство високо софистицираних производних технологија и, посебно, доминантно ослањање на необновљиве изворе енергије чија интензивна експлоатација представља значајан удео привредних активности у региону (Golubev et. al., 2019). Са рапидним погоршањем односа између кључних регионалних и глобалних актера, простор за отклањање наведених негативних фактора по економску безбедност Арктика додатно је редукован (Erzikov, 26.3.2024).

Закључак

Уз интензивне глобалне климатске промене које су значајно утицале на његово „отварање" и повећање приступачности у привредном и транспортном смислу, геополитички статус и безбедност Арктика фундаментално су детерминисани стањем у савременим међународним односима и интеракцијама између кључних регионалних и глобалних актера. Рапидно погоршање односа између Руске Федерације, с једне, те политичког Запада, с друге стране, које је започело 2014, а кулминацију достигло покретањем специјалне војне операције руске војске на простору Украјине 2022. године, изразито негативно се одразило по безбедност Арктика, трансформишући га за кратко време од „простора сарадње", како је означаван у периоду непосредно након окончања Хладног рата, у простор директног одмеравања снага између две стране.

Рефлексија негативног стања у савременим међународним односима по безбедност Арктика огледа се пре свега у његовој (ре)милитаризацији, односно концентрацији и модернизацији војних капацитета на овом подручју од стране готово свих арктичких земаља, при чему је предност у овој својеврсној трци у наоружању још увек на страни Руске Федерације, која је и највећа и најзаступљенија држава овог подручја и која је процес јачања свог војног присуства на Арктику започела раније него западне земље, делимично се ослањајући на наслеђене совјетске војне капацитете који су, распадом савезне државе, били угашени.

Истовремено, под утицајем украјинског конфликта, дошло је и до војно-безбедносне реконфигурације у региону, у смислу да су, након вишедеценијског статуса војне неутралности, Финска и Шведска постале чланице НАТО-а, чиме је Савез не само значајно ојачао своју позицију на балтичком, нордијском и арктичком правцу, већ је и преко Финске проширио своје присуство на руској граници у дужини од 1370 километара, на тај начин значајно негативно утичући на положај Русије и провоцирајући дубоке војно-организационе промене како би се додатно заштитила северозападна граница Русије, и то у околностима треће године њеног војног ангажовања на простору Украјине.

Актуелно милитантно стање у међународним односима, односно (ре)милитаризација Арктика и улазак Финске и Шведске у чланство НАТО-а као његови непосредни регионални изрази, директно су утицали на предоминацију војне у односу на остале димензије безбед-

ности у региону, слабећи при томе ионако крхке наменске структуре посредством којих су требала бити решавана кључна питања од заједничког интереса арктичких земаља, попут Арктичког или Баренцовог Евро-атлантског савета.

Додатни усложњавајући моменат за односе у региону представља и све присутнији „кинески фактор", односно тенденција НР Кине да се такође наметне као један од кључних актера политичких, привредних, али и безбедносних процеса у региону. Иако своје присуство доминантно остварује економским инструментима, и то пре свега у руском делу Арктика, амбиције Пекинга и, посебно, руско-кинеско партнерство у бројним пројектима различитог карактера, од стране западних арктичких земаља, на челу са САД, доживљавају се као директна претња по њихове интересе и националну безбедност. С друге стране, ни сама Руска Федерација, без обзира на значај Кине, њеног тржишта, али и инвестиција у околностима изолованости од стране политичког Запада, мора водити рачуна о властитој позицији и не сме дозволити да кинеско присуство и утицај на Арктику изађу изван „прихватљивих оквира".

Уопште, ситуација на Арктику и стање његове безбедности представљају „школски пример" рефлексије глобалних безбедносних процеса и односа на регионалну раван. Или, како су кључни актери савремене глобалне безбедности, са њиховим међусобним односима, интересима и интеракцијама, истовремено и кључни актери регионалне безбедности Арктика, безбедносни статус арктичког подручја непосредно је условљен стањем у глобалним међународним односима, односно природом односа између кључних глобалних и регионалних актера.

Литература

Alberque, W., Schreer, B. (2022). Finland, Sweden and NATO Membership. *Global Politics and Strategy*, 64(3): 67–72.

Andersson, P. S., Kelvig, P. (2022). *Does China Control Arctic Raw Mineral Materials. How Much, What, How and Why*. Copenhagen: Danish Institute for International Studies.

Bisht, I. S., (4.8.2023). US Approves Finland M270 Multiple Launch Rocket System Upgrades. *The Defense Post*. Retrieved 3.9.2024. from https://thedefensepost.com/2023/08/04/us-finland-m270-upgrades/.

Boyd, R. et. al. (Ed.) (2016). *Mineral Resources in the Arctic: an introduction*. Oslo: Geological Survey of Norway.

Broek, E. (2023). *The Arctic is Hot: Addressing the Social and Environmental Implications*. Stockholm: International Peace Research Institute. Retrieved 26.8.2024. from https://www.sipri.org/publications/2023/sipri-policy-briefs/arctic-hot-addressing-social-and-environmental-implications.

Descamps, M. (2019). *The Ice – Silk Road: Is China 'Near – Arctic State'*? Focus Asia: Perspective and Analysis. Nacka: Institute for Security and Development Policy.

El Aynaoui, K., Magri, P., Saran, S. (Eds.). (2023). *The Rise of Global South: New Consensus Wanted*. Annual Trends Report. Milano: ISPI, ORF, Policy Center for the New South.

Erzikov, S. (26.3.2024). The Arctic as a Resource Base. *Bellona*. Retrieved 5.9.2024. from https://bellona.org/news/arctic/2024-03-the-arctic-as-a-resource-base.

Euronews, (1.7.2016). Putin Warns Finland: Russia Will Respond If Helsinki Joins NATO. *Euronews*. Retrieved 2.9.2024. from https://www.euronews.com/2016/07/01/putin-warns-finland-russia-will-respond-if-helsinki-joins-nato.

Forsberg, T. (2023). Finland and Sweden's Road to NATO. *Current History*, 122(842): 89–94.

Fried, D., Volker, K. (18.2.2022). The Speech in which Putin Told Us Who He Was. *Politico*. https://www.politico.com/news/magazine/2022/02/18/putin-speech-wake-up-call-post-cold-war-order-liberal-2007-00009918.

Golubev, S. S. et al. (2019). Problems of Economic Security of the Arctic Region. *Journal of Environmental Management and Tourism*, 10(7): 1495–1508.

Gronholt-Pedersen, J., Fouche, G. (16.11.2022). Dark Arctic: NATO Allies Wakeup to Russian Supremacy in the Region. *Financial Post*. Retrieved 2.9.2024. from https://financialpost.com/pmn/business-pmn/nato-allies-wake-up-to-russian-supremacy-in-the-arctic.

Kuusela, J. (2024). *As a New Arctic Ally, Finland Contribute to Arctic Security and Defence*. Polar Points, Wilson Center. Retrieved 3.9.2024. from https://www.wilsoncenter.org/blog-post/no-25-new-arctic-ally-finland-contributes-arctic-security-and-defence.

Lamazhapov, E., Stendstal, I., Heggelund, G. (14.11.2023). China's Polar Silk Road: Long Game or Failed Strategy? The Arctic Institute, Center for Circumpolar Security Studies. Retrieved 3.9.2024. from https://www.thearcticinstitute.org/china-polar-silk-road-long-game-failed-strategy/.

Naval News. (12.1.2021). *Ice – Strengthened Ships for the US Navy?* Retrieved 29.8.2024. from https://www.navalnews.com/naval-news/2021/01/ice-strengthened-ships-for-the-u-s-navy/.

NATO. (1949). *The North Atlantic Treaty*. Brussels: NATO Headquarters.

Nezirovic, L. (13.5.2024). Sweden Open to Hosting Nuclear Weapons in Wartime: Prime Minister. *Anadolu Ajansi*. Retrieved 3.9.2024. from https://www.aa.com.tr/en/europe/sweden-open-to-hosting-nuclear-weapons-in-wartime-prime-minister/3218245.

Ngila, F. (11.5.2023). China is cementing its position as an Arctic superpower through Russia. *BRICS Portal*. Retrieved 4.9.2024. from https://infobrics.org/post/38360.

Nilsen, T. (11.6.2024). Norway Doubles Up on Missile Defence as Russia Flexes its Semi – Ballistic Arsenal. *The Barents Observer*. Retrieved 3.9.2024. from https://

thebarentsobserver.com/en/security/2024/06/russia-flexing-semi-ballistic-nuke-carriers-norway-doubles-missile-defence.

Office of the Chief of Naval Operations. (2007). *A Cooperative Strategy for 21st Century: Seapower*. Washington, DC: Office of the Chief of Naval Operations, Marine Corps, US Coastguard.

PRC State Council. (2018). *China's Arctic Policy*. Beijing: The State Council Information Office.

RF President. (21.12.2020). *Presidential Decree of the Russian Federation No. 803 about the Northern Fleet*. Moscow: CIS Legislation. Retrieved 2.9.2024. from https://cis-legislation.com/document.fwx?rgn=158338.

RF President. (26.2.2024). *Presidential Decree of the Russian Federation No.141 about military administrative division of the Russian Federation*. Moscow: CIS Legislation. Retrieved 4.9.2024. from https://cis-legislation.com/document.fwx?rgn=158337.

Tallis, J., Rosen, M., Overfield. C. (2022). *Arctic Economic Security: Recommendations for Safeguarding Arctic Nations against China's Economic Statecraft*. Arlington: CNA.

United Nations. (1982). *United Nations Convention on the Law of the Sea*. New York: United Nations.

US Congress. (2022). *China Regional Snapshot: Arctic*. Washington, DC: US Congress, Foreign Affairs Committee. Retrieved 6.9.2024. from https://foreignaffairs.house.gov/china-regional-snapshot-arctic/.

US Department of Defense. (2022). *National Defense Strategy 2022*. Washington, DC: Pentagon, Secretary of Defense.

US Department of Defense. (2024). *2024 Arctic Strategy*. Washington, DC: Pentagon, Secretary of Defense.

US Department of Navy. (2014). *Arctic Roadmap 2014–2030*. Washington, DC: Chief of Naval Operations.

Williams, H., Bingen, K.A., MacKenzie, L. (2024). *Why Did Russia and China Stage a Joint Bomber Exercise Near Alaska?* Washington, DC: Center for Strategic and International Studies.

REMILITARIZATION AND THE STRUGGLE FOR AN ECONOMIC EXPLOATATION OF ARCTIC AS A REFLECTION OF WAR IN UKRAINE

Dr. Boris TUČIĆ, Associate Professor

Summary

Main goal of the paper is to analyze some of the most important implications of the contemporary international relations to the security of Arctic region. As a reflexion of the current state of the international relations and the revitalization of the "Cold war" interactions among key global players, Arctic region has been subject of relatively intensive (re)militarization from both – Russian and "Western" – sides, as well as of military reconfiguration, in a sense that NATO, through the admission of Finland and Sweden in its membership in April 2023 and March 2024, significantly strenghtened its Baltic, Nordic and Arctic flanks, as well as its presence at the Russian border. The analysis of the subject has been done within the theoretical framework of the science of international relations and by using the selected scientific methods, such as content analysis, inductive and deductive methods, as well as the comparative analysis. One of the conclusions of the analysis is that, as an implicitaion of its (re)militarization, military reconfiguration and of the state of contemporary international relations in general, military security of the Arctic region is by far predominant dimension of its security at the moment. Additional complicating moment regarding the complex situation in the Arctic comes with the "Chinese factor" and the strong intention of Beijing, primarily over Moscow, to gradually impose itself as a inevitable political, economic, as well as security "force" in the Arctic region. Western countries, led by the US, the intention of China see as a direct threat to their national interests, while the Russian Federation's long term best interests, no matter how important its partnership with Beijing is right now, is to keep its presence and influence in the region within the acceptable framework.

Keywords: *Arctic, (re)militarization, NATO, Ukrainian conflict, 'Chinese factor'.*

Примљено: 21. октобар 2024.
Прихваћено: 03. децембар 2024.

УДК 327.36(73)(234.9)
COBISS.SR-ID 161891593
DOI: 10.5937/ssb2402029E

THE U.S. ROLE AND POLICIES IN INTERNATIONAL PEACEKEEPING OPERATIONS AND PEACE BUILDING: POTENTIAL ENGAGEMENT WITH THE SOUTH CAUCASUS*

Dr. Ruben ELAMIRYAN**, Associate Professor

* Disclaimer. This paper was funded through a US Department of State Public Diplomacy Section grant, and the opinions, findings and conclusions or recommendations expressed herein are those of the Author and do not necessarily reflect those of the Department of State.

** Department of World Politics and International Relations, Russian-Armenian University, ruben.elamiryan@rau.am

THE U.S. ROLE AND POLICIES IN INTERNATIONAL PEACEKEEPING OPERATIONS AND PEACE BUILDING: POTENTIAL ENGAGEMENT WITH THE SOUTH CAUCASUS[1]

Summary: *The paper is discussing the potential US peace-keeping engagement with the South Caucasus after the Third Nagorno-Karabakh war. Based on the case-study of the Third Nagorno-Karabakh war, followed by ethnic cleaning of the Armenians of Nagorno-Karabakh and continuous Azerbaijani aggression towards the sovereign territory of the Republic of Armenia, the paper analyzes the US interests and draws potential scenarios for US peacekeeping engagement in Armenia-Azerbaijani conflict. It draws five potential scenarios, which are: direct military engagement, support to a UN (or other international organization, for instance, OSCE) mission, support to the EU mission in Armenia, NATO engagement, distancing, and argues that the most realistic model is the US direct diplomatic engagement with major support to the EU/EU countries' efforts, including military, in Armenia.*
Keywords: *Armenia, United States, Azerbaijan, Peacekeeping, South Caucasus, Peacebuilding*

Introduction

The beginning of the 21st century was marked by global transformations in international relations. They include, in part, the recent change in the world order, which influence the global security system and the strategic environment in many areas of the world by virtue of a knock-on effect. Different notions, sometimes mutually exclusive, are used to describe it: a new world order, chaos, polycentric and multipolar world, and a world without poles, to name a few. In this context, one of the key issues in current

[1] Disclaimer. This paper was funded through a US Department of State Public Diplomacy Section grant, and the opinions, findings and conclusions or recommendations expressed herein are those of the Author and do not necessarily reflect those of the Department of State.

international relations is the future face of the new world order in five, ten and twenty years.

Without getting too deep into an academic debate on formulas, it is still possible to say that the changes in the world order boil down to the consolidation and restoration of Russia's positions, which were lost after the Soviet Union's collapse, strategic uncertainty and the EU's search for a geopolitical future, a shift of the US strategic focus to the Asia-Pacific Region and the growth and expansion of China's interests and influence. The rise of middle powers is another variable of the developing new international order. As a consequence, global turbulence and uncertainties heavily impact regional security architectures in various parts of the world, making some actors to leave and bringing in new ones (Elamiryan, 2019). Turbulence, uncertainty and transformation of the world order, in fact, change the Yalta-Potsdam system of international relations, established after the Second World War, establishing and developing a new world order. These changes cover not only the sphere of relations between the world's leading centers of power, but also the security environment in various regions of the world is being transformed.

The Caucasus is no exception. The third Artsakh war of 2020 clearly demonstrated the changed strategic environment in the South Caucasus. From this point of view, this study is devoted to the study of the transformations that are taking place in international relations, as well as a systemic analysis and identification of their impact on Russia's foreign and security policy in the South Caucasus. In the meantime, the Ukrainian conflict of 2022 became simultaneously a result and accelerator of those transformations, bringing unprecedented turbulence and uncertainty to international relations.

The changing global geopolitical landscape comprehensively impacts major power politics in various parts of the world. This leads to rising confrontation on global, regional, and local levels, driving rise of multiple conflicts in the periphery. The Armenian-Azerbaijani conflict is one of those conflicts, which heated up and erupted into the 44-day war in Autumn of 2020, when the whole world was dealing with the Covid pandemic, on the one hand, and world order transformations, on the other. Though the war was stopped by the Trilateral Statement of the Presidents of Russia and Azerbaijan, and Prime Minister of Armenia, followed by the placement of Russian peacekeepers in Nagorno Karabakh, in fact, the war has never stopped since then, ending up in ethnic cleansing of Armenian population of Nagorno Karabakh. In the meantime, starting from at least the end of

the Third World War the US has taken major responsibility for the fate of humanity by, inter alia, engaging in numerous peacekeeping operations and peace building activities.

From this perspective the main objective of this research is to study the US experience and approaches in peacekeeping operations and peace building processes, and reflect that experience towards the South Caucasus, discussing the potential US engagement on the example of Armenian-Azerbaijani conflict.

The main hypothesis is that given the shifting major power politics in the South Caucasus, when the US demonstrates comprehensive and multifaceted interest towards the South Caucasus, the US might directly or indirectly (through the third parties, such as NATO, UN, and so on) get involved in the peacekeeping operations and peace building processes in the South Caucasus, in particular, in the framework of the Armenian-Azerbaijani conflict.

Methodology and Scope of the Research

The research starts with comprehensive research of definitions to reveal the working approach for peacekeeping and peace building. It will be continued by the study of the US engagement in peacekeeping operations and peace building activities, revealing both historical path and contemporary state. This will be followed by the analysis of the Armenian-Azerbaijani conflict as a case-study for peacekeeping and peace building. Finally, the received results will be discussed through the US interests and priorities to reveal potential US engagement with the conflict management and resolution. The research is primarily based on such methods as: discourse analysis, historical and comparative study, case-study, scenario-building method.

Changing World Order, U.S. and the South Caucasus

The US presence in Eurasia, and particularly, in the South Caucasus goes back at least for a century when after the World War One it appeared as a global political, economic, and geopolitical actor. Since then, the US foreign policy toward Eurasia has faced steady rise providing zigzags of cooperation with countries, which now occupy the region of the South

Caucasus. The cooperation has increased drastically since 1991 when the three South Caucasus countries received independence after the disintegration of the Soviet Union.

In this context this subsection reveals the current basic US interests in Eurasia and determines the role, which the South Caucasus can play in that strategic environment. To understand the above, it is worth analyzing the US National Security Strategy of 2017 (Strategy, 2017), which still remains in force and gives the basic understanding on the US interests abroad.

The Strategy does not provide a clear US perception and vision towards the South Caucasus. It only touches upon Georgia in the section titled "Europe". This allows us to expand that section on the other South Caucasus countries, too.

Describing the US interests toward Europe the Strategy states that "The United States is safer when Europe is prosperous and stable, and can help defend our shared interests and ideals. The United States remains firmly committed to our European allies and partners. The NATO alliance of free and sovereign states is one of our great advantages over our competitors, and the United States remains committed to Article V of the Washington Treaty. European allies and partners increase our strategic reach and provide access to forward basing and overflight rights for global operations. Together we confront shared threats. European nations are contributing thousands of troops to help fight jihadist terrorists in Afghanistan, stabilize Iraq, and fight terrorist organizations across Africa and the greater Middle East. The NATO alliance will become stronger when all members assume greater responsibility for and pay their fair share to protect our mutual interests, sovereignty, and values".

At the same time the Strategy outlines the following priority actions:

Political: "The United States will deepen collaboration with our European allies and partners to confront forces threatening to undermine our common values, security interests, and shared vision. The United States and Europe will work together to counter Russian subversion and aggression, and the threats posed by North Korea and Iran. We will continue to advance our shared principles and interests in international forums".

Economic: "The United States will work with the European Union, and bilaterally with the United Kingdom and other states, to ensure fair and reciprocal trade practices and eliminate barriers to growth. We will encourage European foreign direct investment in the United States to create jobs. We will work with our allies and partners to diversi European energy sources to ensure the energy security of European countries. We will work

with our partners to contest China's unfair trade and economic practices and restrict its acquisition of sensitive technologies".

Military and Security: "The United States fulfills our defense responsibilities and expects others to do the same. We expect our European allies to increase defense spending to 2 percent of gross domestic product by 2024, with 20 percent of this spending devoted to increasing military capabilities. On NATO's eastern flank we will continue to strengthen deterrence and defense, and catalyze frontline allies and partners' efforts to better defend themselves. We will work with NATO to improve its integrated air and missile defense capabilities to counter existing and projected ballistic and cruise missile threats, particularly from Iran. We will increase counterterrorism and cybersecurity cooperation" (Strategy, 2017).

Based on the above we can conclude that the Strategy:

- Provides no specific focus on the South Caucasus countries.
- Emphasizes prosperity and stability in Europe
- Outlines a special role of the NATO for the US: as an actor in the region, as well as a place of deepening cooperation.
- Stresses the energy security of Europe,
- Prioritizes strengthening deterrence and defense on NATO's eastern flank,
- Accentuates the necessity to deter Russia (as a political and military threat) and China (as an economic threat) in the region, as well as Iran.

Interestingly Central Asia is separated into a special chapter in the NSS, which could be estimated as a stress of special importance of the region for the US interests in comparison to the South Caucasus. On the other hand, the special focus on Central Asia indirectly increases the importance of the South Caucasus. The latter geographically connects the region with the NATO European allies.

It is worth mentioning that the Strategy also emphasizes the return to the theory of Political Realism. Particularly, it states that "this strategy is guided by principled realism" (Strategy, 2017). Interestingly enough the strategy corresponds with the ideas of well-known apologist of political realism John Mearsheimer, who in his recent book states that "... there is good reason to think that with the rise of China and the resurrection of Russian power having put great power politics back on the table, Trump eventually will have no choice but to move toward a grand strategy based on realism, even if doing so meets with considerable resistance at home" (Mearsheimer, 2019).

More light to the understanding of the US interests in the South Caucasus brings the recent visit of the US 27th National Security Advisor John Bolton to the South Caucasus in October 2018. In exclusive interview with Voice of America/Turan Bolton emphasized that the South Caucasus is a critically important region for the United States. Bolton outlined the following main directions of interest:

- Clear desire to make tighter presser on Iran.
- High interest to see the resolution of Nagorno-Karabakh conflict on acceptable for both Armenia and Azerbaijan terms (Bolton, Baku, 2018).

From Baku Bolton traveled to Yerevan, where in the interview to Radio Azatutyun he again prioritized the necessity of resolution of Nagorno-Karabakh conflict. At the same time the following idea deserves special attention: "I think that the perspectives for more stable democracy are outstanding here. And I think that the issue of full sovereignty is essential for Armenia not to depend on extreme foreign influence. I think that for people it is better to have here more opportunities on international level than to be restricted by historical clashes" (Bolton, Yerevan, 2018).

Obviously, these issues are tied together and the basic idea, inter alia, is to decrease the foreign impact in Armenia and the region, in general. Based on the Strategy, most probably under the "foreign impact" Bolton means Russia, as especially in case of Armenia, it is Russia who enjoys very strong dominant positions.

Moreover, Bolton went further and suggested the Armenian government to buy weaponry from the US instead of Russia. This could be interpreted rather as another step to decrease the Russia's influence, than to gain economic advantage for the US companies provided low military spending of Yerevan. In Yerevan Bolton also touched upon the necessity of harder line and pressure on Iran. However, interestingly he separated the issues above from the economic ones, encouraging the Armenian government to attract investments from the Armenian Diaspora in the US, instead of relying on financial support from the US government (Bolton, Yerevan, 2018)).

Thus, we see that strategic environment in the South Caucasus is formed around the containment of Russia and Iran – an idea, which is clearly resembled in the Strategy. At the same time the Strategy makes it clear that the issue is not only about Russia and Iran, but also China. Particularly, it states that "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity..." (Strategy, 2017).

In January 2021 Joe Biden became the 46th President of the United States of America, replacing Donald Trump in the White House. In March 2021 the White House has published an Interim National Security Strategic Guidance (Guidance). In the introduction section President Biden writes that he is "issuing this interim guidance to convey my vision for how America will engage with the world" (US Interim National Security Strategic Guidance, 2021).

The Guidance directs departments and agencies until the new National Security Strategy is published. Hence, it can be referred to a preliminary official document, which set the US foreign policy priorities. However, the Guidance does not have any reflection on the South Caucasus. It does not even refer to Georgia separately as the US National Security Strategy of 2017 did. At the same time, the Guidance speaks about the development and strengthening of relations with the US allies and partners, particularly, in the framework of NATO. The Guidance speaks also about the necessity to contain China, Russia, and Iran. A very similar approach was present in the Strategy. At the same time, the Guidance in opposite to the Strategy sets the US decisive support towards democracy and democratic development in the world (US Interim, 2021).

Very similar approach is presented in the article written by Biden for the Foreign Affairs in March-April 2020 and entitled "Why America must lead again", before he formally announced to run for the US Presidency. The article contained neither any specific reflection on the South Caucasus, as a region, nor any single country of the region (Bolton, 2018).

Finally, it is important to mention that on April 24, 2021 Joe Biden used the term "Genocide" in speech devoted to the massive killings of Armenians in Turkey early 20th century. On the one hand, this might be seen as a US claim to return to the South Caucasus (Bolton, 2018). On the other hand, given the ongoing deterioration of the US – Turkey relations, Biden's speech on Armenian Genocide might be a signal to Turkey.

When it comes to the new US national Security Strategy of 2022, it states that "as we support Ukraine, we will also work to enhance the stability and resilience of other democracies. We will support the European aspirations of Georgia and Moldova and their commitment to important institutional reforms", as well as mentions that the US will back diplomatic efforts to resolve conflict in the South Caucasus (US National Security Strategy 2022), though it is not very clear which conflict is meant (US National Security Strategy, 2022).

Thus, we see that on strategic level the US does not have special strategic interests in the South Caucasus. It is interested in long-term strategic stability in the region, which is located in the NATO and EU neighborhood. At the same time, the US is interested to provide energy sovereignty for the EU, where the Caspian gas can play a vital role. Finally, the US is interested to contain Russia (as a political and military threat), China (as economic threat), and Iran (military, political) in the region.

On the other hand, there is significantly growing collaboration between Armenia and the US. The number of high level mutual visits is a clear indicator (Bilateral Relations). In the meantime, at the start of the Capstone meeting of the Armenia-US Strategic Dialogue, the Minister of Foreign Affairs of the Republic of Armenia gave opening remarks, where he mentioned that: "the bilateral agenda continues to expand and include dimensions critical for the resilience and sustainable development of Armenia. In this context, I want to recall the high-level Armenia-US-EU meeting held on the 5th of April, 2024 in Brussels and the arrangements indicated in the joint press statement... Coming to the agenda of today's meeting, we have a wide array of concrete steps and plans to discuss ranging from economic and energy diversification to defense and justice reforms. We have been efficient in utilizing three working groups under the auspices of Armenia-US Strategic Dialogue and holding relevant meetings in 2023. Considering the growing nature and dynamics of bilateral relations, we are hopeful to upgrade our Strategic Dialogue to a Strategic Partnership Commission that could further enhance the structured approach to our multifaceted cooperation" (Opening remarks).

Third Nagorno-Karabakh War and Geopolitics of the South Caucasus

On September 27, 2020 Azerbaijan with support of Turkey started a new war against the non-recognized Nagorno-Karabakh. The conflict was frozen after the First Karabakh war of 1992-1994 with Three-party Ceasefire Agreement of May 1994. The OSCE Minsk Group with the co-chairmanship of Russia, US, and France was leading the peace talks. Though the ceasefire regime was constantly being violated during these years and very often Azerbaijan was claiming to shift the peace talks to the UN umbrella, however, there was a general recognition of the Minsk Group with the co-chairmanship format and the fact that Russia, US, and France

have the exclusive right to deal with the conflict resolution. With Nagorno-Karabakh conflict being the number one foreign policy issue for Armenia, the talks format has been under no question by the Armenia's authorities since the format was established in mid-90th. The situation has not changed also after the Velvet Revolution in Armenia of 2018.

However, the Third Artsakh war has changed the security landscape not only for Armenia, Nagorno-Karabakh, and Azerbaijan, but the regional security architecture in general, or, to be more precise, it demonstrated the already transformed reality and made it explicit. For the first time after the disintegration of the Soviet Union, Turkey openly supported Azerbaijan and demanded full participation in the peace talks with Russia (without the US and France) (In Threat To Israel).

Being one of the most important security issues not only in the South Caucasus, but also in post–Soviet space, in general, if succeeded, the new format will mean complete change of the security architecture in the wider region. Russia and Armenia then opposed the Turkey's participation – each of them for own reason. Russia's Minister of Foreign Affairs made this clear in June 2021, stating that if Turkey enters the peace-building process in Nagorno-Karabakh, Iran, as a regional power, should have the same privileges, as Turkey (Foreign Minister Sergey Lavrov's remarks). On the other hand, Turkey is continuing strengthening its positions in Azerbaijan, most probably, with the aspiration of further expansion both in the South Caucasus and further to the Central Asia.

Thus, the dualism of the period is that Russia recognizes the region as a sphere of major or even exclusive interests, seeing it as a part of the post-Soviet space, while Turkey is returning to the South Caucasus through its alliance with Azerbaijan. However, what has already happened is the gradual shift of the South Caucasus from being an exclusive part of the post-Soviet space towards the Middle Eastern agenda.

Thus, looking back to the end of 2020, one could claim that the Third Nagorno-Karabakh war has significantly changed the power balance in the South Caucasus and beyond, particularly, strengthening Russia's and Turkiye's positions, weaking the positions of the West (or fully removing from the peace process by that time), but also creating a very fragile power balance on the ground, which, as the later history showed, collapsed very shortly with slight refocusing of Russia's attention towards Ukraine. The new status quo significantly contributed to the transformation and implementation of an updated Azerbaijani strategy towards Nagorno-Karabakh and the Republic of Armenia, inter alia, in the form of hybrid warfare. The new reality has

triggered a new wave of hybrid war against Nagorno-Karabakh and the Republic of Armenia, ended with ethnic cleansing of the non-recognized state and ongoing conflict with the Republic of Armenia.

Discussion and Conclusions

The end of Third Nagorno-Karabakh war has triggered the offensive and open territorial claims of Azerbaijan towards the Republic of Armenia. It continued and followed not only by diplomatic and information efforts of Azerbaijan, but also hybrid operations and direct military interventions.

This led to multiple and radical consequences, including Armenia freezing its Russia-led Collective Security Treaty Organization membership and deployment of the European Union Mission in Armenia on the border with Azerbaijan. Both steps are unprecedented, as Armenia joined then-Collective Security Treaty (became an Organization in 2002) in 1992 and has never left it or suspended the membership (Collective Security Treaty Organization). Moreover, until the 2020 Third Nagorno-Karabakh war it was among the most active members. Additionally, despite the fact that the European Union Mission in Armenia "is tasked with observing and reporting on the situation on the ground, contributing to human security in conflict-affected areas and supporting the confidence building between Armenia and Azerbaijan, where possible," (About European Union Mission in Armenia) it is the first ever this type of EU presence in Armenia, which implements peace-keeping efforts, though in indirect way. 23 EU Member States and the Third Contributing State Canada have joined the mission.

In this regard, provided the recent intensification of Armenia and US relations, a question could be raised about US more active peace-keeping engagement within Armenia-Azerbaijan normalization process to provide more stable strategic environment and contain potential new Azerbaijani aggression towards the Republic of Armenia.

Given the above, the followed potential scenarios of the US engagement might be specified:

- Direct military engagement
- Support to a UN (or other international organization, for instance, OSCE) mission
- Support to the EU mission in Armenia
- NATO engagement
- Distancing

Given the current political reality in the US, its strategic interests and priorities, the direct peace-keeping engagement in Armenia-Azerbaijan conflict currently seems unrealistic. On the other hand, the 'distancing scenario' also seems not very realistic, given the recent developments in Armenia – US relations especially over the last three years. The second scenario might have been workable if there is that kind of agenda is on the table. The same might be true with regard to potential NATO engagement.

Thus, given the current political, geopolitical, and security landscape in the world and South Caucasus, the most realistic scenario might be the US direct diplomatic engagement with major support to the EU mission in Armenia.

References

'About European Union Mission in Armenia', 11.04.2024, https://www.eeas.europa.eu/euma/about-european-union-mission-armenia_en?s=410283

Biden J. (2020). "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump", March/April, https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again

Bilateral Relations: United States of America, https://www.mfa.am/en/bilateral-relations/us

Bolton, C. "Məqsədimiz İrana qarşı sanksiyaların təsirini maksimal artırmaqdır", Voice of America, 25 October 2018, https://www.amerikaninsesi.org/a/siyasi/4628490.html?fbclid=IwAR3O3zyHnIL7pR RE28mMZm5S-XeASqLoFUqN1VUiggugMWNBX87CYJEOtU

'Collective Security Treaty Organization: 2002–2021', https://en.odkb-csto.org/25years/

Elamiryan R., Eastern Partnership countries on the cross-roads of the Eurasian Geopolitics: USA, EU, Russia, and China, Kozmetsky Center Briefing Series, 2019, https://kozmetskycenter.org/briefing-november-2019/

Foreign Minister Sergey Lavrov's remarks and answers to media questions at the Primakov Readings International Forum, via videoconference, Moscow, June 9, 2021, https://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/4779515

Interim National Security Strategic Guidance, 2021, March, https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf

In Threat To Israel, Erdogan Cites Turkish 'Entry' Into Karabakh, July 29, 2024, Azatutyun Radio, https://www.azatutyun.am/a/33055076.html

John Bolton: Soyedinennie Shtati, Administratsiya Trampa schitayut otnosheniya SSHA s Armeniey ochen prioritetnimi", Azatutyun Radio Station, 25 October 2018, https://rus.azatutyun.am/a/29563512.html?fbclid=IwAR3Jc2ooyTADMXMaF4y9arzNPGMyb4y7KOVUgV8AAI3G3rFeP6QrLcu8Aug (in Russian)

Mearsheimer J. (2018). Great Delusion: Liberal Dreams and International Realities.. New Haven and London: Yale University Press.

National Security Strategy of the United States of America. 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017- 0905.pdf

National Security Strategy of the United States of America. 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Opening remarks by Foreign Minister of Armenia at the U.S. Strategic Dialogue Capstone Meeting, 11 June, 2024, https://www.mfa.am/en/speeches/2024/06/11/arm_us/12689

УЛОГА И ПОЛИТИКА САД У МЕЂУНАРОДНИМ ОПЕРАЦИЈАМА ОДРЖАВАЊА И ИЗГРАДЊЕ МИРА: ПОТЕНЦИЈАЛНИ АНГАЖМАН СА ЈУЖНИМ КАВКАЗОМ

др Рубен ЕЛАМИРИАН, ванредни професор

Сажетак

Рад говори о потенцијалном мировном ангажману САД на Јужном Кавказу након Трећег рата у Нагорно-Карабаху. На основу студије случаја Трећег рата у Нагорно-Карабаху, праћеног етничким чишћењем Јермена Нагорно-Карабаха и континуираном агресијом Азербејџана на суверену територију Републике Јерменије, у раду се анализирају интереси САД и извлаче потенцијални сценарији за Мировни ангажман САД у јерменско-азербејџанском сукобу. Разматра се пет потенцијалних сценарија, а то су: директно војно ангажовање, подршка мисији УН (или друге међународне организације, на пример, ОЕБС), подршка мисији ЕУ у Јерменији, ангажовање НАТО-а, дистанцирање, и тврди да је најреалнији модел директно дипломатско ангажовање САД уз велику подршку напорима земаља ЕУ/ЕУ, укључујући војне, у Јерменији.

Кључне речи: *Јерменија, Сједињене Америчке Државе, Азербејџан, одржавање мира, Јужни Кавказ, изградња мира*.

Примљено: 31. октобар 2024.
Прихваћено: 30. новембар 2024.

УДК 343.9:004.738.5]:[351.824.11:336
COBISS.SR-ID 161904137
DOI: 10.5937/ssb2402045B

САЈБЕР НАПАДИ НА ФИНАНСИЈСКИ СЕКТОР КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Јована БРАЈОВИЋ*
Дејана ЈОВАНОВИЋ ПОПОВИЋ**, редовни професор

* Generali Osiguranje Srbija, jovanabrajovic296@gmail.com
** Факултет безбедности, Универзитет у Београду, dejana@fb.bg.ac.rs

САЈБЕР НАПАДИ НА ФИНАНСИЈСКИ СЕКТОР КРИТИЧНЕ ИНФРАСТРУКТУРЕ

Сажетак: *Финансијски сектор критичне инфраструктуре представља један од најугроженијих сектора када је реч о сајбер нападима, с обзиром на његову критичну улогу у глобалној економији и природу пословања у данашњици. Дигитализација финансија отвара врата сајбер нападима кроз широку и распрострањену доступност финансијских услуга на модерним технологијама и мрежама. Овај рад бави се истраживањем мера заштите од сајбер напада у финансијском сектору кроз анализу три значајна инцидента: напада на Централну банку Бангладеша, компромитацију података компаније 'Capital One' и напад рамосвером на 'Travelex' компанију за трансфер новца. Примарни циљ истраживања је анализа утицаја сајбер напада на финансијски сектор критичне инфраструктуре и идентификација ефикасних мера заштите које могу смањити ризик од сличних напада у будућности. Користећи преглед међународне литературе и студију случаја, рад наглашава важност интеграције технолошких и организационих мера, као и значај изградње сајбер отпорности кроз континуирано унапређење безбедносних протокола и културе свести о сајбер безбедности. Резултати истраживања показују да, иако сајбер напади носе значајан ризик, они такође могу подстаћи финансијске институције на иновације и унапређење мера заштите.*

Кључне речи: сајбер напад, критична инфраструктура, финансијски сектор критичне инфраструктуре, мере заштите од сајбер напада, сајбер криминал

Увод

Критична инфраструктура представља круцијални сегмент функционисања државе и друштва и као таква ставља се на врх листе приоритета када се говори о заштити. Критична инфраструктура се састоји од више различитих сектора, у зависности од државе до државе, али већина држава би међу секторима критичне инфраструктуре навела и сектор финансија. Сектор финансија обухвата низ финансијских институција попут банака и осигуравајућих кућа, а међу-

зависност сектора финансија са другим секторима наглашава неопходност неометаног функционисања овог сектора. Сајбер напади постали су свакодневница у данашњем свету где су готово сви процеси рада и функционисања дигитализовани. Напредак технологије омогућио је управљање новчаним токовима и подацима на само неколико кликова, а управо ту се отвара простор за сајбер нападе који погађају и финансијске институције. Предмет овог рада представљају сајбер напади на финансијске институције и анализа њиховог утицаја на финансијски сектор критичне инфраструктуре. Финансијски сектор критичне инфраструктуре представља један од најрањивијих сектора када су у питању сајбер напади сходно природи пословања, али и чињеници да је највећи број сајбер напада мотивисан финансијском добити. Рањивост овог сектора критичне инфраструктуре поспешена је све већом дигитализацијом финансија и готово потпуном зависношћу сектора од телекомуникационих и информационих технологија и инфраструктуре. Студија случаја рада заснива се на анализи примера сајбер напада на Централну банку Бангладеша, "Capital one" и „Travelex" финансијске институције. Кроз студију случаја ова три сајбер напада рад даје анализу утицаја сајбер напада на финансијски сектор критичне инфраструктуре проучавајући добре, али и лоше праксе примењене у овим случајевима. Кроз студију наведена три случаја рад тежи приказивању последица које су сајбер напади произвели на финансијски сектор, како на појединачне институције тако и на финансијски систем уопште. Такође, рад кроз студију случаја анализира узроке настанка сајбер напада извлачећи потенцијална решења за заштиту финансијског сектора. Упоређујући појединачне случајеве из студије рад тежи проналажењу најоптималнијих начина унапређења мера заштите од сајбер напада, као и предвиђању могућих праваца у развоју сајбер напада.

Финансије као део критичне инфраструктуре и дигитализација финансија

Као један од осам сектора критичне инфраструктуре у Републици Србији, сектор финансија је такође ближе одређен Уредбом за одређивање критеријума критичне инфраструктуре и начину извештавања о критичној инфраструктури у Републици Србији. На основу ове уредбе, под финансијским сектором критичне инфраструктуре

у Републици Србији сматрају се системи, мреже, објекти или њихови делови, а чије уништење или оштећење може изазвати озбиљније последице у виду угрожавања или отежања економске стабилности државе. Овде се убрајају привредна друштва попут банака или осигуравајућих кућа, али и свих оних привредних друштава који у делатности финансија заузимају значајан удео у свом делокругу пословања. Такође, не треба изоставити ни органе државне управе под којима се подразумевају Пореска управа, Управа за трезор, Управа царине, Управа за јавни дуг, Агенција за осигурање депозита и др. (Службени гласник Републике Србије, 69/2022).

Финансијски сектор такође нуди широк спектар услуга и производа како појединцима тако и корпорацијама. Сваки значајан поремећај у испоруци услуга носи са собом значајне економске, социјалне и потенцијално политичке ефекте на стабилност заједнице. Важно је напоменути да је економска стабилност основ за политичку и војну безбедност (Dumitru & Ferarau, 2018). Узимајући у обзир увезаност великих приватних и државних предузећа на регионалном и међународном нивоу, укључујући велике светске банке, последице које оштећење или уништење финансијског сектора критичне инфраструктуре лако прелази границе и утиче на друге земље. Финансијске услуге играју суштинску улогу у расту привреде и економије, те су од виталног значаја за опстанак државе. На основу овога следи да су услуге банкарске индустрије и финансијског сектора уопште од велике важности за сваку државу (Somogyi, Nagy, 2021).

Увођењем нових финансијских технологија, старомодни начин пословања финансијских институција замењен је употребом нових технолошких решења. Ово се односи на дигиталне технологије које имају потенцијал, односно могућност да трансформишу пружање финансијских услуга, подстицање развоја нових, или модификовања већ постојећих пословних модела, апликација, процеса и производа (Pazarbasioglu et al., 2020). Овим решењима постиже се лака доступност клијентима, али и постизање економије обима, све то праћено ниским трошковима и великом ефикасношћу.

Дигитализација финансија настала је природно као продукт модерног друштва праћеног дигитализацијом и свих осталих процеса свакодневног функционисања. Дигитални финансијски сервиси су финансијски сервиси који се ослањају на дигиталне технологије за испоруку и употребу од стране потрошача. Дигитални финансијски сервиси доживели су своју експанзију услед иновација у технологији и

пословним моделима. Дигитализација финансијских сервиса значајно умањује потешкоће у сваком кораку током финансијског циклуса, од отварања рачуна до потврђивања трансакција, али и аутоматизације других специфичних процеса, попут, на пример, процена кредитне способности (Pazarbasioglu et al., 2020).

Како је дошло до уске повезаности између модерних технологија и финансијских институција и услуга тако се и формирао Финтек (енгл. Fintech). Финтек представља израз који обједињује финансије (енгл. Finance) и технологију (енгл. Technology) и користи се за технолошка решења која су у служби финансија. Финтек обухвата све активности од мобилног плаћања, трансфера, кредитних одобрења путем мобилних апликација, па све до крипто-валута и инвестиција у роботе. Развојем финтека су се у почетку бавили искључиво екстерни сарадници финансијских институција, да би се касније исти определили за интерни развој у циљу смањења трошкова и повећања иновативности (Goldstein, Jiang & Karolyi, 2019).

Банке, али и друге финансијске институције почеле су да своје услуге нуде путем мобилних апликација, као и веб-сајтова. Значај заштите финансијског сектора повећава се заједно са опсегом и модернизацијом његових модела рада с обзиром на све већу потхрањеност овог система корисничким подацима. Како би се испратио брз напредак недолазећих претњи потребно је држати корак са развојем технологија и бити спреман на благовремену реакцију. Заштита финансијских институција од сајбер напада се постиже само континуираним праћењем и вишеструким мерама заштите финансијских система.

Сајбер напади и мере заштите од сајбер напада

Сајбер напади представљају врсту напада који за циљ имају злонамерно ометање или саботирање рада рачунара или рачунарских мрежа, крађу или уништавање података или се напад на рачунар користи у сврхе неког другог вида напада. Постоји мноштво врста сајбер напада, а њихов број се константно увећава, међутим, постоји неколико основних типова међу којима су најчешћи фишинг, рансомвер, дистрибуирано ускраћивање услуга (DDOS) и друге врсте малвера, односно злонамерних софтвера. Сајбер напади се такође у великој мери разликују по својој софистицираности, при чему сајбер криминалци

покрећу како насумичне тако и циљане нападе на предузећа, односно компаније.

Са неког ширег аспекта, сајбер нападе можемо, на основу мете, класификовати у нециљане и циљане. Нециљани напади функционишу по принципу обима, односно нападач циља што више уређаја. Неретко се ови напади изводе уз помоћ природе, односно отворености интернета. Као примери оваквих напада углавном се јављају фишинг, рамсовер и скенирање. Циљани напади јесу такви да нападач на уму има неку конкретну организацију или особу, или је плаћен за циљање исте. Овакви напади изискују време за припрему како би се пронашао најадекватнији начин за постизање успешног напада. Такође, они представљају и већу претњу с обзиром на ниво припреме. Најчешћи облици циљаних напада јесу фишинг, подметање ботнетова, али и подметање у ланцу снабдевања (Biju, Gopal & Prakash, 2019).

Многи аутори се слажу да се сајбер напади могу класификовати на следећи начин:

1. фишинг;
2. напад ускраћивањем услуга;
3. употреба ботова;
4. спам;
5. „човек у средини" метода;
6. спуфинг;
7. логичке бомбе;
8. малвери;
9. SQL injection;
10. напад на лозинку.

Мере заштите од сајбер напада могу се поделити у неколико врста, као и сами напади, међутим, важно је напоменути да када говоримо о финансијским институцијама и финансијском сектору уопште ове мере имају већу тежину и озбиљност тиме што су праћене многобројним стратегијама и плановима заштите којима се ове мере ефикасно координирају и планирају. Превасходно је неопходно објаснити основне видове заштите од сајбер напада.

Мере заштите могу се поделити на:

1. антивирусни програми;
2. заштитни зид;
3. аутентикација;
4. контрола приступа;

5. енкрипција података;
6. сегментација мреже;
7. редовно ажурирање софтвера.

Поред горенаведених мера које можемо сврстати у тактичке, односно практичне мере, важно је истаћи и значај стратегијских мера. Стратегијске мере се односе на (NIST, 2018):

1. развој и изградњу безбедносних политика;
2. развој и имплементацију безбедносних политика;
3. обучавање и едукацију запослених;
4. изградњу "Zero trust" културе;
5. усклађеност са међународним и државним регулативама и стандардима.

Сајбер напад на Централну банку Бангладеша

Сајбер напад на Централну банку Бангладеша 2016. године потресао је глобални финансијски систем до његових темеља. У фебруару 2016. године Централна банка Бангладеша доживела је сајбер напад, током којег су нападачи покушали да украду 951 милион долара са њеног рачуна резерви у Њујоршкој банци федералних резерви (ФЕД). Нападачи су успели да се неприметно увуку у мреже банке и дођу до система мреже за Светске међубанкарске финансијске телекомуникације (СВИФТ) (Bukth & Huda, 2017). Може се закључити да је већ прва линија одбране била лоше постављена, односно да заштитни није адекватно одиграо своју улогу и дошло је до неовлашћеног упада у систем. Касније је откривено да је "Dridex" малвер коришћен за напад. У основи, нападачи су били у могућности да се крећу бочно унутар мрежа банака и да, уз помоћ команди са својих командно-контролних сервера, компромитују администраторске креденцијале и искористе их за напад (Mapoka, Zuva & Zuva, 2019). 4. фебруара 2016. године нападачи су послали тридесет пет лажних захтева за исплату у укупном износу од 951 милион долара ФЕД-у (Bukth & Huda, 2017). ФЕД је био опремљен сигурносним протоколима када су у питању биле СВИФТ трансакције. Од укупног броја пристиглих захтева од стране нападача, тридесет је успешно заустављено, међутим, пет трансакција су успешно обрађене, што је резултирало пребацивањем

81 милиона од стране ФЕД-а на међународне рачуне. Поставља се питање колико је ефикасан био систем контроле захтева за исплату и пребацивање новца. Новац је у веома кратком року прошао токове такозваног прања новца, те је завршио на рачунима казина на Филипинима. Претпоставља се да је пренос новца на Филипине вероватно изабран због строгих закона о банкарској тајности и изузећа казина из закона против прања новца (Bull Jr & Fincannon, 2024). Наравно, последице овог сајбер напада би вероватно биле мање да је контрола трансакција ка Филипинима била строже уређена, нарочито када су усмерене ка казинима и сличним видовима пословања.

Централна банка Бангладеша је у то време поседовала штампач инсталиран и подешен тако да аутоматски штампа све СВИФТ трансакције. Међутим, када су надлежни 5. фебруара 2016. године радили рутинску проверу приметили су да штампач није одштампао ништа од претходног дана. Надлежни су у почетку мислили да је у питању мањи технички проблем, али, даљим сагледавањем ситуације и проблема, открили су поруке трансфера новца послате ФЕД-у (Bukth & Huda, 2017). Као додатна мера опреза и предострожности било би увођење барем још једног штампача за СВИФТ трансакције, те би њихова неусаглашеност слала сигнал да је у питању неправилност, што би предупредило развој сајбер напада на виши ниво. Уложени су напори за ступање у контакт са ФЕД-ом, како би се зауставило плаћање, али због времена напада било је прекасно и банка је изгубила 81 милион долара пре него што су успели да ступе у контакт са њима. Нападачи су искористили слабости у заштити система Централне банке Бангладеша, која је користила јефтине прекидаче од 10 долара за повезивање рачунара са СВИФТ мрежом, а као додатна слабост банка није имала адекватан заштитни зид (Bukth & Huda, 2017). Адекватна, квалитетна опрема која иде у корак са развојем технологије неопходна је како би се сајбер напади попут овог предупредили. Неадекватно конфигурисање заштитног зида само је отворило врата нападачима за улаз у системе банке, те је неопходно било адекватно ажурирати и пратити како физичке тако и сајбер мере заштите. Улагањем у средства и мере заштите финансијске институције се штите од већих трошкова него што би издаци за мере заштите били.

Пљачка Централне банке Бангладеша послужила је као оштар подсетник на важност сајбер безбедности у банкарству и финансијском сектору уопште. Овај догађај је подстакао финансијске институције широм света да преиспитају и побољшају своје мере заштите (Maroka,

Zuva & Zuva, 2019). Централна банка Бангладеша је предузела кораке да ојача своје мере сајбер безбедности и заштите и побољша интерну контролу како би спречила сличне инциденте у будућности (Maroka, Zuva & Zuva, 2019). Инцидент је такође резултирао и заоштравању дипломатских односа између Бангладеша и Филипина. Како је значајан део украдених средстава опран преко филипинских казина, то је довело до међусобних преговора о међународној сарадњи по питању истрага о сајбер злочинима (Karim & Hasan, 2021).

Сајбер напад на банку "Capital One"

Упркос значајним издацима у мере заштите, као и информациону инфраструктуру уопште, компанија "Capital One" је у јулу 2019. године открила да је дошло до сајбер напада, при чему су осетљиви подаци клијената били изложени неовлашћеном приступу. Компанија је у свом јавном саопштењу изјавила како је нападач успео да прибави личне податке клијената путем неовлашћеног приступа, а који су повезани са корисничким кредитним картицама (Novaes Neto et al., 2020). Случај овог сајбер напада показатељ је да је, и поред високих улагања у модерна решења, потпуна заштита од сајбер напада неизвесна. Компанија је навела да су компромитовани подаци исти подаци које банка уобичајено прикупља током процеса отварања рачуна или издавања кредитних картица, укључујући имена, адресе, поштанске бројеве, бројеве телефона, адресе е-поште, датуме рођења и пријављени приход, као и подаци о кредитима, лимитима и слично. Неовлашћени приступ личним подацима погодио је око 100 милиона појединаца у Сједињеним Државама и око 6 милиона у Канади, укључујући и информације малих предузећа. Компанија је открила напад захваљујући свом Програму одговорног откривања података 17. јула 2019. године. Међутим, компанији се замера што напад није био откривен кроз редовне операције у оквиру процедура сајбер безбедности, већ је за то била потребна интервенција спољног лица које је путем е-поште обавестило банку да су подаци клијената доступни на „GitHub" страници (Novaes Neto et al., 2020). Поставља се питање да ли се упад могао открити на други начин, као што су безбедносна скенирања, или преглед и праћење логовања и приступа у системе банке.

Банка је у саопштењу за јавност изјавила да су компромитовани подаци били шифровани, али је такође признала да је услед упада у систем постојала могућност да су подаци дешифровани. Банка није дала изјаву о томе како је до упада дошло. ФБИ је ухапсио Пејџ А. Томпсон, жену из Сијетла, због хаковања сервера које је "Capital One" изнајмио у облаку (Novaes Neto et al., 2020). Истражитељи су утврдили да је Томпсон раније радила у компанији за рачунарство у облаку чији су сервери провађени, а медији су брзо идентификовали компанију као "Amazon Web Services" (AWS), према њеном „LinkedIn" профилу (Sandler, 2019). Томпсон је користила софтверски алат за скенирање, који јој је омогућио да идентификује сервере са погрешно конфигурисаним заштитним зидовима, што јој је омогућило да изврши команде и приступи серверима (Khan et al., 2022). У случају овог сајбер напада, као и у случају напада на Централну банку Бангладеша, може се закључити важност добро конфигурисаног заштитног зида као прве линије одбране од напада.

Након овог инцидента, "Capital One" предузима мере у циљу боље заштите и исправљања ранијих пропуста. Такође, они уводе и осигурање од крађе података за своје клијенте, чиме се даје на значају о свести озбиљности инцидента који се догодио. Систем заштите банке направио је неколико грешака које су омогућиле овај сајбер напад. Поред поменутог лоше конфигурисаног заштитног зида, од великог значаја је ограничити IAM улоге и дозволе које оне носе. Један од основних принципа сајбер безбедности, али и корпоративне безбедности нарушен је увођењем улоге која има изузетно велика права и приступе (Khan et al., 2022). Напомиње се да је од кључних постулата успешне сајбер заштите то да запослени имају приступ само оним подацима, у оном обиму, који су му неопходни за обављање радних задатака.

Сајбер напад на "Travelex"

"Travelex" је компанија специјализована за размену валута и финансијске трансакције основана у Лондону, у Великој Британији. У децембру, 31. децембра 2019. године, компанија доживљава сајбер напад рамсовером, што је довело до великих финансијских, али и губитака у поверењу клијената. Поједини аутори сматрају да је пропуст у одбрани од сајбер напада створен нередовним и неадекватним ажури-

рањем система, што је створило рањивости на систему и омогућило нападачима да изврше упад и крађу података (Lalisang, 2020). Нападачи су за Би-Би-Си тврдили да су преузели пет гигабајта поверљивих информација, укључујући датуме рођења клијената, податке о кредитним картицама и бројеве социјалног осигурања (Novak, 2020), а за откуп докумената су од компаније тражили да плати 6 милиона долара како би се системи омогућили за понован рад и спречило цурење украдених података на мрежу (Nish, Naumann, & Muir, 2022). Разлог успешности напада лежи у закрпи рањивости коју је компанија имплементирала на све сервере и тиме је отворила за упад споља (British Assessment Bureau, 2020).

Како би одбрана од сајбер напада била ефикасна неопходно је применити је свеобухватно на свим уређајима и комплетном мрежном систему. Непримењивањем закрпе за рањивост на свим серверима компанија је такорећи пожелела добродошлицу за све непожељне госте. Санирање рањивости закрпом обављено је неколико месеци пре самог напада, али је то урађено само на једном од сервера компаније. Рањивост на мрежи омогућила је нападачу приступ без налога и лозинке, као и могућност да се вишефакторска аутентификација искључи и дозволи неометана крађа и криптовање података (British Assessment Bureau, 2020). Компанија је услед прекида рада свих система трансакционе операције пребацила на рад оловком и папиром. Утицај напада проширио се на широк спектар банака које су се ослањале на компанијске девизне услуге (Nish, Naumann, & Muir, 2022). Напад је изазвао прекиде у раду у трајању од месец дана, а особље повремено није могло да користи компјутере да прати трговину валутама. Ремећење у раду банака носи ризик од утицаја на функционисање финансијског сектора као дела критичне инфраструктуре. Поставља се питање шта би се догодило да је сајбер напад на компанију имао утицаја на све банке у држави или на више већих глобално с обзиром на то каква је природа рада ове компаније била. Нападачи су користили изузетно ефикасну варијанту рамсовера под називом „REvil", оријентисаног ка финансијским институцијама. Извештаји процењују да је напад на крају коштао компанију скоро 30 милиона долара (Nish, Naumann, & Muir, 2022).

Последице сајбер напада

Сајбер напад на Централну банку Бангладеша уздрмао је свет финансија. Поред огромних финансијских губитака и шока за тржиште финансија, овај напад довео је и до ревизија безбедносних мера и протокола, јачања међународне сарадње и појачаног улагања у напредна технолошка решења за заштиту, како на нивоу институција тако и на пољу њихове међусобне сарадње с обзиром на то да заједно граде високоумрежен систем (Karim & Hasan, 2021). Када се говори о случају сајбер напада на "Capital One", може се рећи да је то прави пример нарушавања приватности података. Несумњиво да данашњи начин функционисања друштва захтева висок ниво поверљивости података, а да се појединци слажу да је заштита њихових података приоритет пословања свих институција, а нарочито финансијских. Нарушавање приватности података носи са собом многобројне последице по финансијске институције, сагледано из више углова (Siddique, 2019). Последице изазване сајбер нападима који су фокусирани на крађу података такве су да је ризик од прекида пословања или немогућности рада финансијских институција изузетно велики. Зависност других сектора критичне инфраструктуре од фунансијског сектора поставља финансијски сектор на такву позицију да је нарушавање рада, или прекид рада овог сектора озбиљнији него што се чини. Иако се не чини да напад на једну финансијску институцију може бити погубан по читав сектор, треба напоменути да су финансијске институције део глобалне мреже финансија и да се рањивости једног система лако могу рефлектовати и на остале институције, а самим тим и на читаву мрежу (George, Baskar & Srikaanth, 2024), што свакако да случај сајбер напада на "Travelex" потврђује. Било да се ради о издвајању средстава за изградњу нових здравствених капацитета, или улагању у заштиту животне средине, у данашњици је новац један од кључних покретача готово сваке активности. Немоћност рада финансијских токова, или компромитовање истих доводи до нарушавања рада осталих сектора, а тиме и угрожавања функционисања државе уопште. Сајбер напади на финансијске институције могу бити изузетно разорни, како за саме институције тако и за шири финансијски систем. Сагледавајући сваку од три студије случаја обрађене у раду, може се закључити да неретко веома ситне грешке и непажња у заштити од сајбер напада доводе до разорних последица. Сајбер напади често доводе до огромних финансијских губитака, нарушавања поверења клијената и зна-

чајних прекида у пословању. Напади попут оног на Централну банку Бангладеша или "Capital One", али и "Travelex" откривају слабости у безбедносним системима, што може покренути ланчану реакцију у финансијском сектору, јер један инцидент може угрозити и друге институције које су део истог међународног система. Ова врста међузависности значи да је једна рањивост у систему потенцијална претња за целу финансијску мрежу. Међутим, сајбер напади такође делују као снажан покретач за финансијске институције да унапреде своје безбедносне мере и јачају међусобну сарадњу. Сајбер напад на Централну банку Бангладеша поспешио је међународну сарадњу, али и свест о потреби за адекватном опремом заштите која прати трендове развоја напада. Такође, напади подстичу банке и друге финансијске институције да уложе више у развој напредних технологија за превенцију и откривање сајбер претњи, као и у обуку запослених у области сајбер безбедности. Случај са нападом на "Capital One", са друге стране, послужио је као оштар подсетник да, и поред модернизације мера заштите, људска улога игра кључан фактор кроз одређивање улога права и приступа у одговарајућој мери. Поред тога, постојање свести о заједничком ризику, попут случаја са "Travelex" компанијом, доводи до побољшане комуникације и координације између институција, што за циљ има развој заједничких стандарда и најбољих пракси у заштити финансијског сектора. Иако сајбер напади носе ризик од прекида пословања и могу озбиљно угрозити финансијске институције, они такође служе као катализатор за трансформацију безбедносних политика и пракси. Финансијске институције постају свесније потребе за заједничким деловањем и улагањем у сигурност система, чиме јачају своју отпорност на будуће претње и доприносе стабилности глобалног финансијског система.

Потенцијално решење за побољшање мера заштите од сајбер напада

Како би мере заштите од сајбер напада биле ефикасне и правовремене потребно је усагласити и развијати више сегмената мера заштите. Неопходно је пратити технолошки напредак и бити у корак са њим колико год је то могуће. Под овим се подразумева и употреба вештачке интелигенције и новоразвијених алата. Застареле технологије, или штедња на квалитету технологија, могу изазвати много више штете

него што би коштала имплементација нових технологија, што можемо видети на примеру сајбер напада на бангладешку банку. Са друге стране, употреба нових технологија и решења мора бити испитана и проверена као сигурна. На примеру сајбер напада на "Capital One" можемо видети да, иако су применили релативно нову технологију складиштења у облаку, сигурност закупљене услуге није била на одговарајућем нивоу. Док је случај са сајбер нападом на "Travelex" показатељ да, без обзира на вид технологије који се користи, уколико се не примени свеобухватно и правовремено не ажурира сигурност од сајбер напада је упитна. Поред улагања у нове технологије и њихово испитивање, кључна је и едукација запослених о сајбер нападима и начинима заштите. Наравно, неизоставно је да су у питању континуиране и правовремене обуке узевши у обзир брз и стални напредак информационих технологија. Развијање свести код запослених и стварање такозване културе нултог поверења (енгл. Zero Trust) представљају основ за успешну заштиту од сајбер напада. На примеру случају сајбер напада на "Capital One" може се закључити да је неопходно размотрити и систематично дедељивати права приступа подацима на основу радне позиције, тако да запослени имају приступ само оним подацима којима је неопходно за обављање радних задатака. Такође, увођење двоструке аутентификације такође се може сматрати за обавезну ставку приликом приступа системима институције. Сарадња и размена информација и знања са институцијама из истог сектора је, као што је већ напоменуто, од изузетног значаја када је реч о сајбер нападима. На примерима бангладешке банке и "Capital One" банке може се видети како недостатак комуникације међу деловима једног система резултује великим последицама, те се стога јачање међусобне сарадње и комуникације истиче као препорука за унапређење мера заштите. "Travelex" случај одличан је пример за схватање увезаности међу финансијским институцијама и потребом да заједно раде на јачању заштите од сајбер напада.

Како би се оснажила отпорност на сајбер нападе и самим тим смањио и утицај истих на финансијски сектор критичне инфраструктуре, неопходно је систематично и темељно приступити сегментима сајбер безбедности. Ово захтева интеграцију, односно обједињавање стратешког управљања, технолошке модернизације и промене организационе културе. На управљачком нивоу, финансијске институције и надлежни унутар њих, као што су одбори и извршни тимови, играју кључну улогу у проглашавању сајбер безбедности за стратешки прио-

ритет, обезбеђујући при томе адекватне ресурсе како би се она постигла. Технолошка модернизација подразумева улагање у нове технологије, али и сегментацију мреже ради спречавања бочног кретања, као и вишефакторску аутентификацију за контролу приступа и енкрипцију података. Прелазак са застарелих система и адаптација на нове безбедносне алате у виду платформи поједностављује праћење и реаговање на претње. Оперативно је неопходно осигурати ванмрежне резервне копије и редундантност система како би се обезбедила непрекидност основних услуга у случају сајбер напада. Планирање заштите од сајбер напада подржано тренинзима путем симулација и вежби за реаговање на сајбер нападе омогућава особљу боље усвајање неопходних процедура и знања. Такође, увођење сајбер осигурања такође може помоћи у ублажавању финансијских последица сајбер напада (George, Baskar & Srikaanth, 2024).

Закључак

Експанзија сајбер напада је неизбежна садашњица и будућност, а примери из рада сведоче о њима у прошлости као примерима за развој мера заштите. Како технологија расте и развија се тако расте и развија се и претња од сајбер напада. Софистицираност сајбер напада и домишљатост нападача представљају само једну од препрека у борби са овим претњама. Тежња ка злоупотреби вештачке интелигенције и потенцијално коришћење квантних рачунара неизвесна су, али реална претња по заштиту података и финансија. Циљ истраживања јесте сагледавање утицаја сајбер напада на финансијски сектор критичне инфраструктуре и проналажење решења у виду мера за њихово ублажавање и заштиту од истих. Сајбер напади на финансијске институције, као што су инциденти са Централном банком Бангладеша, компанијом "Capital One" и компанијом за трансфер новца "Travelex", истичу важност развоја свеобухватних стратегија заштите које обухватају како технолошке тако и организационе мере. Иако су последице ових напада биле разорне, оне су такође послужиле као катализатори за унапређење сајбер безбедности у финансијском сектору. Кроз анализу ових случајева, овај рад показује да је смањење утицаја сајбер напада на финансијски сектор критичне инфраструктуре могућ само уз константно улагање у модернизацију технологије, унапређење организационих процедура и промовисање културе безбедности међу

запосленима. Ови напади такође наглашавају потребу за бољом сарадњом унутар сектора, али и спољним релевантним институцијама и разменом информација, као и државама међусобно, како би се финансијски сектор ефикасније одбранио од будућих претњи. Свакако да се као закључак може извући неопходност пажљиве, свеобухватне, детаљне и добро испланиране заштите од сајбер напада на свим нивоима функционисања финансијских институција уз непрекидни мониторинг и будно око над развојем и рапидним растом сајбер напада. Може се закључити да је систем заштите од сајбер напада комплексна слагалица делова од којих сваки мора одиграти своју улогу адекватно како би комплетна слика имала смисла. Сајбер напади циљају рањивости у овим системима, а рањивост само једног дела представља претњу и по све остале, те је добро комбиновање делова и постављање истих на одговарајуће место кључно како би заштита од сајбер напада била успешно примењена. Овај истраживачки рад пружа свој допринос кроз приказ утицаја сајбер напада на финансијски сектор критичне инфраструктуре у виду студије случаја на три финансијске институције сваки специфичан по узроку и последицама. Анализом ових случајева рад нуди решења и препоруке у циљу унапређења заштите финансијског сектора критичне инфраструктуре.

Литература

Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber attacks and its different types. International Research Journal of Engineering and Technology, 6(3), 4849–4852.

British Assessment Bureau. (2020). How the Travelex ransomware attack could have been avoided. Retrieved from https://www.british-assessment.co.uk/how-thetravelex-ransomware-attack-could-have-been-avoided/

Bukth, T., & Huda, S. S. (2017). The soft threat: The story of the Bangladesh bank reserve heist. SAGE Publications: SAGE Business Cases Originals.

Bull Jr, C. L., & Fincannon, C. (2024). Assignment 2.1: The 2016 Bangladesh Bank Heist.

Dumitru, D., Feraru, C. L. (2018). National Security Concept. Annals – Series on Military Sciences, 10(2), 90–101.

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. Partners Universal International Innovation Journal, 2(1), 51–75.

Goldstein, I., Jiang, W., & Karolyi, G. A. (2019). To FinTech and beyond. The Review of Financial Studies, 32(5), 1647–1661.

Karim, Y., & Hasan, R. (2021). Taming the digital bandits: An analysis of digital bank heists and a system for detecting fake messages in electronic funds transfer. In National Cyber Summit (NCS) Research Track 2020 (pp. 193–210). Springer International Publishing.

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the capital one data breach: Critical lessons learned. ACM Transactions on Privacy and Security, 26(1), 1–29.

Lalisang, B. (2020). Cyber-risk and Director's liability: Exploring the Dutch legal framework.

Mapoka, T. T., Zuva, K., & Zuva, T. (2019). Hack the Bank and Best Practices for Secure Bank. International Journal of Computer Science, Communication & Information Technology (CSCIT), 7, 17–21.

National Institute of Standards and Technology (NIST) (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce. Retrieved from https://www.nist.gov/cyberframework

Nish, A., Naumann, S., & Muir, J. (2022). Enduring cyber threats and emerging challenges to the financial sector. Carnegie Endowment for International Peace.

Novaes Neto, N., Madnick, S., de Paula, M. G., & Malara Borges, N. (2020). A case study of the capital one data breach. Stuart E. and Moraes G. de Paula, Anchises and Malara Borges, Natasha, A Case Study of the Capital One Data Breach (January 1, 2020).

Novak, M. (2020, January 7). Travelex shutdown caused by Sodinokibi ransomware attack, reports say. CyberScoop. Retrieved from https://cyberscoop.com/travelex-sodinokibi-ransomware/

Pazarbasioglu, C., Mora, A. G., Uttamchandani, M., Natarajan, H., Feyen, E., & Saal, M. (2020). Digital financial services. World Bank, 54, 1–54.

Sandler, R. (2019, July 29). Capital One Says Hacker Breached Accounts Of 100 Million People; Ex-Amazon Employee Arrested. Retrieved from Forbes: https://www.forbes.com/sites/rachelsandler/2019/07/29/capital-onesayshacker-breached-accounts-of-100-million-people-ex-amazonemployeearrested/

Siddique, N. A. (2019). Framework for the mobilization of cyber security and risk mitigation of financial organizations in bangladesh: a case study.

Somogyi, T., & Nagy, R. (2022). Cyber Threats and Security Challenges in the Hungarian Financial Sector. Contemporary Military Challenges/Sodobni Vojaški Izzivi, 24(3)

Уредба за одређивање критеријума критичне инфраструктуре и начину извештавања о критичној инфраструктури у Републици Србији (Службени гласник РС, бр. 69/2022).

CYBERATTACKS ON THE FINANCIAL SECTOR OF CRITICAL INFRASTRUCTURE

Jovana BRAJOVIĆ
Dejana JOVANOVIĆ POPOVIĆ, Full Professor

Summary

The financial sector of critical infrastructure represents one of the most vulnerable sectors when it comes to cyber attacks, due to its crucial role in the global economy and the nature of business today. The digitalization of finance opens the door to cyber attacks through the wide and pervasive availability of financial services on modern technologies and networks. This paper explores protective measures against cyber attacks in the financial sector by analyzing three significant incidents: the attack on the Central Bank of Bangladesh, the data breach at Capital One, and the ransomware attack on Travelex, a money transfer company. The primary aim of the research is to analyze the impact of cyber attacks on the financial sector of critical infrastructure and to identify effective protective measures that can reduce the risk of similar attacks in the future. By utilizing a review of international literature and case studies, the paper emphasizes the importance of integrating technological and organizational measures, as well as the significance of building cyber resilience through continuous improvement of security protocols and a culture of cyber awareness. The research findings indicate that while cyber attacks pose significant risks, they can also drive financial institutions toward innovation and enhancement of protective measures.

Keywords: *cyberattack, critical infrastructure, financial sector of critical infrastructure, protective measures against cyber attacks, cyber crime.*

Примљено: 07. јун 2024.
Прихваћено: 30. новембар 2024.

УДК 004.738.5:364.632
COBISS.SR-ID 161910537
DOI: 10.5937/ssb2402065P

МОГУЋА РЕШЕЊА ЗА САЈБЕР НАСИЉЕ

Татјана ПЕТРОВИЋ, демонстратор

* Факултет безбедности, Универзитет у Београду, petrovictatjana24@gmail.com

МОГУЋА РЕШЕЊА ЗА САЈБЕР НАСИЉЕ

Сажетак: *У раду су приказана потенцијална решења за сајбер насиље, односно за различите облике насиља који се испољавају у сајбер простору. Рад превасходно отпочиње пружањем осврта на теоријско одређење, кључне одлике сајбер насиља и улоге које особе могу имати у истом. У том контексту, указано је на специфичности сајбер насиља у односу на традиционално насиље, узимајући у обзир карактеристике самог сајбер простора. Посебна пажња је посвећена разматрању штетних последица сајбер насиља, на основу којих је указано на знатну опасност ове појаве и неопходност њеног адекватног сузбијања и спречавања. С тим у вези, у раду ће бити размотрена могућа решења за сајбер насиље која се односе на примену савремених технологија у сајбер простору. Конкретно, биће истакнут значај информационих технологија у борби против сајбер насиља, кроз разматрање њихове примене у детекцији сајбер насиља на основу анализе текстуалног и другог садржаја. Способности вештачке интелигенције и са њом повезаних области, односно технологија које се примењују у сузбијању сајбер насиља, биће илустроване кроз конкретне пројекте и моделе који су развијани у ове сврхе, а који се примењују и у случајевима вршњачког сајбер насиља. Такође, кроз рад ће бити приказани и могући начини употребе високоразвијених технологија за пружање подршке жртвама сајбер насиља.*
Кључне речи: *сајбер насиље, вршњачко сајбер насиље, вештачка интелигенција, машинско учење, обрада природног језика*

Увод

Убрзан развој технологија и интернета последњих деценија са собом уједно повлачи и значајну могућност њихове злоупотребе. Управо је сајбер насиље једно од облика штетног понашања која се везују за сајбер простор.

Сајбер насиље је комплексна појава, која се манифестује на различитим платформама и друштвеним мрежама, односно широко је рас-

прострањена у сајбер простору, при чему конкретне манифестације сајбер насиља попримају различите форме или појавне облике. Услед специфичности сајбер простора, сајбер насиље може потенцијално бити штетније од традиционалног насиља. Такође, сајбер насиље је специфично и по питању улога које особе имају у истом, где се, поред поменутих сајбер насилника и жртава, јавља категорија посматрача, као веома значајна за вршење, односно сузбијање сајбер насиља.

У раду ће посебна пажња бити посвећена штетности сајбер насиља, односно негативним последицама које сајбер насиље изазива код жртава. Кроз разматрање штетних последица биће указано на неопходност сузбијања сајбер насиља, при чему ће у раду акценат бити на потенцијалним решењима сајбер насиља која се примењују у сајбер простору. У том контексту, биће приказана примена информационих технологија као потенцијално решење за сајбер насиље. Поред примене у детекцији, али и превенцији сајбер насиља, уједно ће бити указано и на употребу различитих технологија у сврху пружања подршке жртвама сајбер насиља. У раду ће бити размотрена употреба појединих способности вештачке интелигенције и повезаних области у борби против сајбер насиља, при чему ће превасходно бити разматрана примена машинског учења на друштвеним мрежама. Такође, у раду су представљени и комбиновани модели, који су базирани на комбиновању различитих технологија, односно способности вештачке интелигенције са намером постизања веће ефикасности у борби против сајбер насиља. Такође, у раду ће бити приказани и обрада природног језика, софтвери за родитељски надзор, као и конкретни пројекти за сузбијање сајбер насиља који су имплементирани у образовним институцијама. Поред наведених, биће приказана и поједина решења намењена превенцији сајбер насиља, а која се базирају на слању рефлективних порука.

Сајбер насиље

Када је у питању дефинисање сајбер насиља, неопходно је указати на чињеницу да тренутно не постоји универзално прихваћена дефиниција ове појаве, те да се сајбер насиље (Cyberbullying) најчешће одређује у складу са Олвеусовом (Olweus) дефиницијом, односно као „насиље које се дешава у сајбер простору употребом компјутера, паметних телефона и других електронских уређаја" (Vismara et al., 2022:

3). Додатно, не постоји ни консензус у погледу адекватног термина за означавање овог вида понашања у сајбер простору, при чему се нпр. у српском језику за сајбер насиље симултано користе термини сајбер булинг, електронско насиље, дигитално насиље и онлајн насиље (Milošević i Putnik, 2019).

Сајбер насиље се манифестује, односно спроводи у сајбер простору, при чему оно није везано за једну конкретну платформу или друштвену мрежу. Тачније, насиље у сајбер простору се испољава преко различитих платформи на интернету, од чет-соба, друштвених мрежа и медија па све до компјутерских игрица (Milošević i Putnik, 2019). Конкретни појавни облици сајбер насиља на овим платформама обухватају широк спектар напада, односно штетног понашања – од вређања, узнемиравања и оговарања, све до лажног представљања, недозвољеног саопштавања, као и обмањивања, искључивања, али и прогањања у сајбер простору (Zlatković i Denić, 2019).

Иако су поједине карактеристике сајбер насиља и традиционалног насиља истоветне, специфичности везане за сам сајбер простор утичу на дистинкцију између традиционалног и сајбер насиља. На пример, према Милошевићу и Путнику, за разлику од традиционалног насиља напад у сајбер простору првенствено омогућује нападачу да остане анониман. Дакле, сајбер насилници су у стању да у потпуности прикрију свој идентитет, употребом лажних имена, података и профила, док се жртва, са друге стране, не може сакрити од сајбер насилника. Додатно, размере потенцијалне публике када је у питању сајбер насиље су несагледиве. Такође, постоји директна повезаност између сајбер и традиционалног насиља у случајевима када сајбер насиље заправо представља својеврсну континуацију традиционалног насиља, сада у сајбер простору (2019). Сајбер насиље је специфично и услед самог начина на који се успоставља и одвија комуникација између насилника и жртве. Наиме, сајбер насиље је потенцијално опасније од традиционалног насиља управо због удаљености сајбер насилника од жртве (Dinić, 2022).

Ради свеобухватнијег разумевања феномена сајбер насиља, неопходно је такође размотрити и улоге које особе могу имати у истом, а које се односе на сајбер насилнике, жртве и посматраче. Пре свега, када су у питању сајбер насилници, Ачутан (Achuthan) и сарадници појашњавају да су код ових особа – нарочито деце која спроводе вршњачко сајбер насиље – пре свега присутне психопатске и макијавелистичке тенденције које се повезују са потребом за доминирањем

или показивањем моћи у групи. Додатно, изражено је и присуство агресије, која се испољава у акцијама сајбер насиља које су репетитивне. Притом, емоционална интелигенција и емпатија су недовољно присутни код сајбер насилника, при чему се развијањем управо ових особина значајно доприноси смањењу насилничког понашања у сајбер простору, али и отпорности жртава (2023). Разлози због којих особа врши сајбер насиље се у великој мери повезују са разлозима вршења традиционалног насиља, дакле, најистакнутији мотиви су истоветни и односе се на манифестовање надмоћи насилника над жртвом, стицање одређене позиције у групи, као и одређена негативна осећања и перцепције у вези жртве који су присутни код насилника (Dinić, 2022).

Када су у питању жртве сајбер насиља, у контексту вршњачког сајбер насиља, деца из различитих разлога могу бити изабрана од стране сајбер насилника. Између осталог, сајбер насилници су усмерени и на вршњаке који су се тек доселили, на децу која су стидљива и повучена, богатија или сиромашнија од насилника и сл. (Zlatković i Denić, 2019). Поред наведених, жртве су неретко и популарнија деца и деца која имају шири круг пријатеља, а нарочито деца за коју сајбер насилници сматрају да су слабија од њих. Нарочито се истиче виктимизација деце која су у било ком виду другачија од својих вршњака, дакле, може бити речи о деци друге националности, вере или деци која имају физичке или психичке поремећаје (Zlatković i Denić, 2019). Такође, ризик од виктимизације у контексту сајбер насиља је у директној корелацији са количином времена које дете проводи на мобилном телефону или интернету (Kuzmanović i sar., 2016).

Поред поменутог вршњачког сајбер насиља, односно сајбер насиља међу децом, треба напоменути да се виктимизација у контексту сајбер насиља односи и на одрасле особе, како током универзитетског школовања тако и на радном месту (Achuthan et al., 2023).

У погледу виктимизације, али и вршења сајбер насиља, значајно је указати и на супротстављене ставове по питању утицаја пандемије COVID-19 на поменуте трендове. Наиме, пандемија COVID-19 је, између осталог, била праћена и својеврсном инфодемијом и свеукупно повећаним ослањањем на интернет и друштвене мреже. Једна група аутора се слаже да су ове околности, поред ризика од стварања зависности од интернета, односно друштвених мрежа, допринеле и интензивирању сајбер насиља током трајања пандемије (Achuthan et al., 2023). Са друге стране, оваквом ставу су супротстављена мишљења

према којим је пандемија COVID-19 потенцијално позитивно утицала на смањење сајбер насиља, услед схватања да су људи проводили више времена са члановима породице и да су на тај начин уједно имали више подршке уколико су били жртве сајбер насиља (Huang et al., 2024). Наравно, ризик од виктимизације у контексту сајбер насиља је већи код особа које су током пандемије проводиле више времена на интернету, односно на друштвеним мрежама (Huang et al., 2024).

Када су у питању улоге у сајбер насиљу, последња улога се односи на посматраче (bystanders). Наиме, посматрачи могу бити значајни у контексту супротстављања сајбер насиљу, кроз учешће у превенцији и интервенцији. У суштини, посматрачи могу значајно допринети активностима које се односе на сузбијање сајбер насиља, и том приликом они заправо напуштају улогу посматрача и почињу активно да учествују у борби против сајбер насиља. Позитиван утицај посматрача у сајбер насиљу се односи пре свега на могућност да заштите жртву и реагују на уочено сајбер насиље (Abaido, 2019). Са друге стране, особе које посматрају сајбер насиље и које се притом укључе у сајбер насиље, тако што нпр. проследе одређени садржај који је креиран са намером изазивања штетних последица код мете или жртве сајбер насиља, заправо прелазе у улогу насилника (Dinić, 2022). Посматрачи такође могу остати у пасивној улози, односно неретко се неће укључити у сајбер насиље, нити у његово сузбијање (Dinić, 2022).

Сајбер насиље може оставити изразито штетне последице по жртве – како код деце тако и код одраслих особа. Према Јуу (Ju), штетне последице сајбер насиља се најчешће везују за ментално здравље – од изазивања анксиозности и депресије, до суицидалних мисли. У односу на жртве традиционалног насиља, жртве сајбер насиља су потенцијално изложене већем ризику од самоубиства, уколико се узму у обзир разматране карактеристике сајбер насиља, као и чињеница да сајбер насиље није ограничено временом и простором. Поред штетних последица по ментално здравље, сајбер насиље се такође може негативно одразити и на физичко здравље жртве, при чему су најзаступљенији стомачни проблеми и поремећаји сна. Код деце и младих, односно жртава вршњачког сајбер насиља, уочена је и појава поремећаја у исхрани (2023). Сајбер насиље такође доводи и до појаве психосоцијалних проблема код деце, у виду потешкоћа у социјалној интеракцији са вршњацима и ниског степена самопоуздања (Zlatković і Denić, 2019). Додатно, закључено је да су деца која су била жртве сајбер насиља склонија различитим облицима негативног понашања

ван сајбер простора, као што су бежање од куће, или ношење оружја ради сопствене заштите (Chua et al., 2019). Такође, према Ачутану и сарадницима, сајбер насиље значајно отежава и остваривање циљева одрживог развоја услед његових штетних последица по здравље, економију, родну равноправност, мир и правду, при чему се у погледу вршњачког насиља нарочито истичу његове последице на 3. циљ – добро здравље, и 4. циљ, односно квалитетно образовање (2023).

Могућа решења за сајбер насиље

Када се узму у обзир наведене карактеристике сајбер насиља, улоге особа у истом, као и велики потенцијал овог штетног понашања у сајбер простору за изазивање озбиљних последица код жртава, јасно је да је од великог значаја развити одговарајуће начине за решење, односно сузбијање сајбер насиља. У том контексту, у овом делу рада ће бити представљена употреба информационих технологија као потенцијално решење за сајбер насиље, са акцентом на различите примене вештачке интелигенције, као и на неке од актуелних пројеката и модела који се примењују у сузбијању сајбер насиља.

Машинско учење

Машинско учење (Machine Learning – ML) је често представљено као једно од потенцијалних решења за сајбер насиље, услед значајног доприноса машинског учења у детектовању сајбер насиља путем идентификовања кључних речи које су везане за овај феномен. Наиме, машинско учење као грану или област вештачке интелигенције карактерише способност да систем учи и надаље се развија на основу претходног знања и искуства. У односу на степен самосталности у учењу, односно функционисању, можемо разликовати неколико видова машинског учења (Muneer & Fati, 2020). На пример, предложена је употреба модела за детектовање сајбер насиља на Твитеру (Twitter), који би се заснивао на употреби надгледаног машинског учења и којим би биле обухваћене две технике за издвајање карактеристика (Feature Extraction Technique). Након анализе резултата који су добијени применом наведеног модела, закључено је да је CMO класификатор (Sequential Minimal Optimization (SMO) classifier) био најпрецизнији од коришћених класификатора, односно био је успешан

у готово 70% случајева (Muneer & Fati, 2020). Такође, за класификацију текстуалног садржаја у оквиру надгледаног машинског учења често се примењује Classifier Support Vector Machine (SVM) (Muneer & Fati, 2020).

Поред наведеног, развијани су и модели који би се примењивали и на другим друштвеним мрежама, као што је Инстаграм (Instagram), и који би притом детектовали сајбер насиље не само на основу анализе текста (најчешће у форми коментара корисника), већ и на основу анализе слика. У спроведеним експерименталним употребама овог модела уочено је да се анализом различитих врста садржаја побољшава тачност класификације, конкретно у овом случају CBM класификатора (Muneer & Fati, 2020).

Поред великог потенцијалног доприноса у сузбијању сајбер насиља, уједно треба имати на уму да је примена вештачке интелигенције, односно машинског учења и алгоритама за аутоматску детекцију и означавање сајбер насиља на друштвеним мрежама суочено са различитим потешкоћама. Машинско учење се нпр. нарочито на Твитеру суочавало са потешкоћама које се односе на анализу садржаја за који је неопходно разумевање ширег контекста и сарказма. Како би се превазишле наведене потешкоће, даљи развој машинског учења је усмерен и на унапређивање алгоритама за надгледано и ненадгледано учење, као и на проширивање база података карактеристика у вези сајбер насиља које се класификују (Achuthan et al., 2023).

Комбиновани модели

Када је у питању идентификовање сајбер насиља, значајно је такође размотрити и модел који предлаже Ковачевић и који се заснива на комбинованој употреби технике вештачке интелигенције која се назива Web mining и визуелизације (2012). Web mining се може дефинисати као „апликација Data mining-а над садржајем, структуром и коришћењем Web ресурса како би се издвојило релевантно знање из података на Web-у", док је Data mining „итеративни процес тражења нових, скривених информација из велике количине података" (Kovačević, 2012: 229). Са друге стране, визуелизација се у предложеном моделу комплементарно употребљава са Web mining-ом, како би се приказали резултати процеса Data mining-а спроведеног над подацима који се налазе на Web-у (Kovačević, 2012).

Суштина коришћења Web mining-а и визуелизације у контексту решавања проблема сајбер насиља односи се на њихов допринос разумевању података и издвајању значајних информација из њих. Дакле, првенствено се употребом Web mining-а издвајају информације које су садржане у изузетно великом скупу података, при чему се, осим информација, долази и до значајних образаца, односно патерна који су садржани у одређеном скупу података. Затим се коришћењем визуелизације резултати Web mining-а представљају на начин погодан за њихово потпуније разумевање, односно информације и патерни се представљају у визуелној форми. Важно је напоменути да управо визуелизација може имати изузетно велики значај, јер не само што се информације и патерни представљају на пријемчив начин, већ визуелизација доприноси уочавању патерна који можда нису били уочени након Web mining-а. Управо наведене чињенице потврђују велики значај који комбинована употреба Web miming-а и визуелизације може имати у откривању релевантних информација и патерна (Kovačević, 2012).

У случају идентификације сајбер насиља, односно сајбер насилника, у употреби су класификација и кластеризација, као две технике Web mining-а. Применом класификације могуће је разврставање нпр. порука на оне чији се садржај доводи у везу са сајбер насиљем, односно на поруке које не садрже сајбер насиље. Кластеризација, са друге стране, може наћи примену у креирању кластера, односно за кластеризацију особе у односу на њено понашање на друштвеној мрежи, у нпр. насилнике, жртве или посматраче (Kovačević, 2012).

Дакле, у предложеном моделу Web mining се примењује за детектовање насилника, док визуелизација доприноси запажању сајбер насилника (Kovačević, 2012).

Поред претходно разматраног, изузетно значајан „комбиновани" модел за детекцију сајбер насиља развили су и Алмомани (Almomani) и сарадници. Овај модел би се користио за детекцију сајбер насиља које је присутно на друштвеним мрежама, при чему је модел замишљен тако да се комбинује употреба одређених способности дубоког учења (Deep Learning – DL) и машинског учења (Machine Learning – ML) (Almomani et al., 2024). Функционисање наведеног модела се одвија кроз неколико фаза, где на почетку процеса слике са друштвених мрежа пролазе кроз кораке претходне обраде, који подразумевају нпр. промену величине слике. Након тога, модел користи способности учења дубоких конволуционих неуралних мрежа (Deep

Convolutional Neural Networks – CNNs). У ту сврху, користе се претходно обучени модели попут VGG16 и ResNet50 за издвајање карактеристика из садржаја. Ови модели се користе за анализу садржаја, односно у овом случају се анализирају слике са друштвених мрежа које су прошле кроз претходну обраду. Кроз анализу слика ови модели откривају и издвајају унапред одређене карактеристике. Карактеристике до којих се дошло употребом више CNNS-ова се затим комбинују у јединствено заједничко представљање знања. Скуп идентификованих карактеристика се затим користи као инпут за класификаторе машинског учења (нпр. Support Vector Machines или Logistic Regression). На крају, на основу научених образаца, односно карактеристика, модел Алмоманија и сарадника се употребљава за категоризацију слика са друштвених мрежа на оне које се могу или не могу сврстати под сајбер насиље (Almomani et al., 2024). Предвиђено је да постоји потенцијал да се модел даље развија тако да обухвати не само слике, односно податке са слика, већ и да се примењује на садржај који обухвата комбинацију текста, звука и видео снимака са друштвених мрежа (Almomani et al., 2024).

Обрада природног језика

За детекцију сајбер насиља се такође користи обрада природног језика (Natural Language Processing – NLP). Када су у питању конкретне примене обраде природног језика као потенцијалног решења за сајбер насиље, потребно је пре свега истаћи да се обрада природног језика често примењује за функционисање четботова (Chatbots), како би се допринело бољој комуникацији између рачунара и корисника (Baltezarević i sar., 2023). Такође, обрада природног језика је коришћена у видео-игрицама, како би се анализирала комуникација међу играчима која подразумева писани текст или говорни садржај. Циљ употребе обраде природног језика у овом контексту јесте откривање сајбер насиља, односно увредљивог садржаја у комуникацији између играча, при чему у овој комуникацији може учествовати велики број особа. Обрада природног језика се комбинује са употребом машинског учења и за припрему, односно обуку алгоритама користе се подаци који се односе на различите увреде, односно негативне коментаре и сличне садржаје сајбер насиља који су присутни у комуникацији међу играчима видео-игрица (Baltezarević i sar., 2023).

Обрада природног језика је такође развијана у правцу адекватне детекције сајбер насиља у случајевима када се користи неколико језика у једној објави на друштвеној мрежи. Пол (Paul) и сарадници су радили на развоју модела који би се користио за детекцију сајбер насиља током пандемије COVID-19 и који би се примењивао на садржају у коме корисници употребљавају два или више језика, односно прелазе са употребе једног језика на друге (code-switch) у својим објавама. У овом моделу је коришћен Deep Ensemble Learning како би се комбиновале способности, тачније инпути машинског и дубинског учења, чиме је развијен јединствен модел за детекцију сајбер насиља на друштвеним мрежама. Суштина овог модела јесте комбиновање предвиђања различитих метакласификатора који су разрађени употребом неколико алгоритама, како би се свеукупно допринело бољој робусности класификатора (2022).

У контексту употребе обраде природног језика као једног од могућих решења за појаву сајбер насиља, уочено је да се посебан проблем јавља када је у питању идентификовање или сузбијање сајбер насиља које се манифестује у случају слабије коришћених језика (low-resource languages), односно језика који су у мањој мери заступљени на интернету и у литератури (Mahmud et al., 2023).

Софтвери за родитељски надзор

Један од приступа фокусираних на правовремено идентификовање и сузбијање вршњачког сајбер насиља подразумева праћење активности детета на интернету, посебно на друштвеним мрежама. Осим родитеља, школе се такође могу укључити у ову активност, како би се свеукупно побољшала идентификација и борба против сајбер насиља. Неки од софтвера који су развијени у ове сврхе јесу Content Watch Net Nanny и Net Nanny Social, као и Socialshield (Milošević i Putnik, 2019).

За праћење активности детета на друштвеним мрежама у употреби је и вештачка интелигенција која је развијена у склопу IBM Watson-a. Ова вештачка интелигенција је превасходно усмерена на идентификовање знакова да је дете жртва сајбер насиља и обавештавање родитеља о уоченим активностима, при чему ова вештачка интелигенција такође може да саветује родитеље у вези могућих начина решења проблема сајбер насиља у конкретној ситуацији (Rakhmatov, 2022).

Како би сузбијање вршњачког сајбер насиља било ефективније развијају се алгоритми за софтвере за родитељски надзор и софтвере којима се блокира садржај који обухвата неку од кључних речи повезаних са сајбер насиљем, који би алгоритмима омогућили прецизније детектовање, односно обраду текста у којем је употребљен сарказам, као и одређене скраћенице, псовке и увреде, при чему би били обухваћени и случајеви у којима су одређене речи намерно погрешно написане (Rakhmatov, 2022).

Рефлективне поруке

Примена вештачке интелигенције у превенцији сајбер насиља се такође односи и на употребу „рефлективних порука", односно употребу вештачке интелигенције како би се особи послала порука којом се указује да садржај који она намерава да пошаље или објави потенцијално спада у сајбер насиље. Намера овакве употребе вештачке интелигенције јесте навођење особе на преиспитивање да ли заиста жели да постави или објави такав садржај (Milošević i sar., 2022). Једна од апликација која функционише по наведеном принципу јесте BullStop апликација, која се примењује и за детекцију вршњачког сајбер насиља. BullStop је примарно обучавана уз помоћ података који су прикупљени са Твитера и апликација је осмишљена тако да се употребом вештачке интелигенције пре свега уоче и блокирају поруке чији се садржај може означити као сајбер насиље, при чему апликација такође има развијене могућности за слање „рефлективних порука". Такође, замишљено је да BullStop саветује родитеље и особље у образовним установама како да поступају у конкретном случају сајбер насиља (Milošević i sar., 2022).

Rething Words је средство које се користи како би се допринело превенцији сајбер насиља, а које такође функционише по принципу утицања на слање поруке, пре него што се оне пошаљу. Наиме, ова виртуелна тастатура првенствено онемогућава слање поруке у чијем садржају је детектовано сајбер насиље. Особи се затим упућује обавештење да је у питању увредљив садржај и да особа треба да измени поруку. Rething Words неће онемогућити слање поруке, иако особа не измени њен садржај. Међутим, важно је имати на уму да је према подацима истраживања у коме је анализирана употреба наведене виртуелне тастатуре закључено да је у 93% случајева особа изменила садржај поруке након што јој је скренута пажња на потенцијално сајбер насиље (Kovačević i Bajramović, 2018).

CREEP пројекат

У контексту употребе информационих технологија у сузбијању сајбер насиља, а нарочито вршњачког сајбер насиља, значајан је и CREEP пројекат. CREEP пројекат је намењен превенцији вршњачког сајбер насиља и заправо обухвата две врсте технологија – CREEP семантичку технологију (CREEP Semantic Technology) и CREEP виртуелног тренера (CREEP Virtual Coach). CREEP семантичка технологија (CREEP Semantic Technology) је платформа која је намењена за анализу садржаја на друштвеним мрежама. Ова платформа је настала како би се омогућила употреба вештачке интелигенције као средства за детектовање употребе говора мржње и сајбер насиља и пре свега је замишљено да се ова платформа имплементира у школама. Замишљено је да се ова платформа користи као средство за правовремено детектовање појаве сајбер насиља међу вршњацима, како би одговорна лица у школама могла да се укључе и предузму одговарајуће мере (Gabrielli et al., 2021).

Као што је наведено, у оквиру CREEP пројекта за сузбијање, односно детектовање сајбер насиља, развијен је и CREEP виртуелни тренер (CREEP Virtual Coach). У овом случају реч је о апликацији за паметне мобилне телефоне која је намењена комуникацији са младима који су изложени сајбер насиљу. Наиме, апликација се користи како би се младима пружила подршка да нпр. пријаве сајбер насиље и да се лакше носе са његовим штетним последицама. CREEP виртуелни тренер функционише тако што се млади уз помоћ упитника едукују да препознају различите облике сајбер насиља којима су били изложени као жртве или сведоци, односно посматрачи. Након што се идентификује да ли је у питању сајбер насиље, и о ком облику испољавања сајбер насиља је реч, CREEP виртуелни тренер затим саветује младе како да поступају у конкретној ситуацији. Такође, ова технологија пружа подршку младима који су били жртве сајбер насиља кроз прослеђивање различитих едукативних материјала о начинима како се носити са сајбер насиљем и како појачати сопствену отпорност. Апликација се такође примењује у и превенцији, односно пре него што дође до виктимизације младих (Gabrielli et al., 2021).

Закључак

Сајбер насиље је вид штетног понашања којим се злоупотребљава развој нових технологија и перципиране предности сајбер простора, како би се потенцијално нанела значајна штета, односно последице жртвама сајбер насиља. Стога, неопходно је пре свега поседовати релевантно разумевање самог феномена и његових основних одлика, како би се надаље развијала адекватна решења за појаву сајбер насиља. Како је у раду приказано, тренутно је изостала универзално прихваћена дефиниција сајбер насиља, чиме је не само отежано разумевање сајбер насиља, већ и потенцијална шира сарадња на сузбијању ове веома штетне појаве.

Такође, у раду је указано на специфичности сајбер насиља, односно на одређене карактеристике сајбер простора чија злоупотреба доприноси ставу да је сајбер насиље опасније од традиционалног, услед пре свега дистанце између насилника и жртве, као и чињеници да је сајбер насиље присутно на различитим платформама, и да није ограничено просторним или временским факторима.

Услед велике опасности и тешких последица које сајбер насиље изазива код жртава, јасно је да је неопходно развити правовремене и адекватне одговоре на сајбер насиље, те се међу могућим решењима истичу различити модели, пројекти и платформе, односно употреба различитих технологија у сајбер простору.

У раду је посебна пажња посвећена технологијама попут вештачке интелигенције, машинског учења, дубоког учења, обради природног језика и конкретним моделима и платформама као могућим решењима за сајбер насиље. Приказана је примена појединих високоразвијених технологија у детекцији сајбер насиља путем текстуалног садржаја, али су представљени и модели који се односе и на друге садржаје, као што су нпр. слике, при чему је појашњена примена машинског учења и различитих модела за детекцију сајбер насиља на различитим друштвеним мрежама.

Такође, радом су обухваћени и комбиновани модели за сузбијање сајбер насиља, при чему би се у првом моделу користили Web mining и визуелизација, ради детектовања и уочавања сајбер насилника, док се у другом моделу комбинују способности машинског и дубоког учења. Овакав приступ у великој мери доприноси превазилажењу појединих недостатака вештачке интелигенције, односно комплементарном употребом различитих технологија се постиже значајан напредак у

сузбијању сајбер насиља. Такође, као потенцијално решење за сајбер насиље се појављује и употреба обраде природног језика, нарочито када се користи у комбинацији са нпр. машинским учењем.

Када је у питању вршњачко сајбер насиље, у раду је представљено како различити пројекти – попут CREEP пројекта, као и софтвери за родитељски надзор, доприносе сузбијању вршњачког сајбер насиља, са једне стране, и подршци жртвама, са друге.

Напослетку, када се узму у обзир карактеристике и штетне последице сајбер насиља, може се закључити да се као једно од могућих решења истиче употреба информационих технологија, односно њена примена у сајбер простору. Како се нове технологије развијају несагледивом брзином, потребно је, са једне стране, обратити пажњу на могућност њихове злоупотребе, док се такође мора узети у обзир и потенцијал ових технологија за даљи развој одговора на штетна понашања у сајбер простору.

Литература

Abaido, G. M. (2019). Cyberbullying on Social Media Platforms Among University Students in the United Arab Emirates. *International Journal of Adolescence and Youth*, 25(1), 407–420. Retrieved from: https://www.tandfonline.com/doi/full/10.1080/02673843.2019.1669059

Achuthan, K., Nair, V. K., Kowalski, R., Ramanathan, S., & Raman, R. (2023). Cyberbullying Research – Alignment to Sustainable Development and Impact of COVID-19: Bibliometrics and Science Mapping Analysis. *Computers in Human Behavior*, 140, 1–17.

Almomani, A., Nahar, K., Alauthman, M., Al-Betar, M. A., Yaseen, Q., & Gupta, B. B. (2024). Image Cyberbullying Detection and Recognition Using Transfer Deep Machine Learning. *International Journal of Cognitive Computing in Engineering*, *5*, 14–26.

Baltezarević, V., Baltezarević, R. i Baltezarević, I. (2023). Sajber uznemiravanje dece sa posebnim osvrtom na digitalne igre. *Temida,* 26(2), 261–284.

Chua, Y. T., Parkin, S., Edwards, M., Oliveira, D., Schiffner, S., Tyson, G., & Hutchings, A. (2019). Identifying Unintended Harms of Cybersecurity Countermeasures. In: *2019 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 1–15). New York: Institute of Electrical and Electronics Engineers.

Dinić, B. (2022). *Digitalno nasilje*. Novi Sad: Filozofski fakultet u Novom Sadu.

Gabrielli, S., Rizzi, S., Carbone, S., & Piras, E. M. (2021). School Interventions for Bullying-Cyberbullying Prevention in Adolescents: Insights from the UPRIGHT and CREEP Projects. *International journal of environmental research and public health*, 18(21), 1–13.

Huang, N., Zhang, S., Mu, Y., Yu, Y., Riem, M. M. E., & Guo, J. (2024). Does the COVID-19 Pandemic Increase or Decrease the Global Cyberbullying Behaviors? A Systematic Review and Meta-Analysis. *Trauma, Violence & Abuse*, 25(2), 1018–1035.

Ju, B. (2023). Impacts of Cyberbullying and Its Solutions. *Advances in Humanities Research,* 29, 254–258.

Kovačević, A. (2012). Primena web mininga i vizualizacije u otkrivanju sajber nasilja. U: *Reagovanje na bezbednosne rizike u obrazovno-vaspitnim ustanovama* (225–241). Beograd: Fakultet bezbednosti.

Kovačević, A. i Bajramović, J. (2018). Monitoring sajber nasilja. U: *Bezbednost u obrazovno-vaspitnim ustanovama i video-nadzor* (str. 111–126). Beograd: Fakultet bezbednosti.

Kuzmanović, D., Lajović, B., Grujić, S. i Medenica, G. (2016). *Digitalno nasilje – prevencija i reagovanje*. Beograd: Ministarstvo prosvete, nauke i tehnološkog razvoja Republike Srbije i Pedagoško društvo Srbije.

Mahmud, T., Ptaszynski, M., Eronen, J., & Masui, F. (2023). Cyberbullying Detection for Low-Resource Languages and Dialects: Review of the State of the Art. *Information Processing & Management*, 60(5), 1–52.

Milošević, M., i Putnik, N. (2019). Fenomen vršnjačkog nasilja na internetu – izazov za nauku i zakonodavstvo. *Sociologija*, 61(4), 599–616.

Milošević, T., Van Royen, K. & Davis, B. (2022). Artificial Intelligence to Address Cyberbullying, Harassment and Abuse: New Directions in the Midst of Complexity. *International Journal of Bullying Prevention*, 4, 1–5.

Muneer, A., & Fati, S. M. (2020). A Comparative Analysis of Machine Learning Techniques for Cyberbullying Detection on Twitter. *Future Internet*, 12(11), 187.

Paul, S., Saha, S., & Singh, J. P. (2023). COVID-19 and Cyberbullying: Deep Ensemble Model to identify Cyberbullying from Code-Switched Languages during the Pandemic. *Multimedia Tools and Applications*, 82(6), 8773–8789.

Rakhmatov, D. (2022). Methods and Effectiveness of the Use of Artificial Intelligence in the Fight Against Cyberbullying. *Journal of Academic Research and Trends in Educational Sciences*, 1(4), 122–129.

Vismara, M., Girone, N., Conti, D., Nicolini, G., & Dell'Osso, B. (2022). The Current Status of Cyberbullying Research: A Short Review of the Literature. *Current Opinion in Behavioral Sciences*, 46, 1–17.

Zlatković, D. i Denić, N. (2019). Prevencija elektronskog nasilja. U: *Zbornik radova sa 5. međunarodnog savetovanja o upravljanju znanjem i informatici* (str. 65–75). Novi Sad: Visoka tehnička škola strukovnih studija u Novom Sadu.

POSSIBLE SOLUTIONS FOR CYBERBULLYING

Tatjana PETROVIĆ, Teaching Aide

Summary

The paper presents potential solutions for cyber violence, that is, the solutions for different forms of violence that are manifested in the cyber space. The paper begins with an overview of the theoretical framework, key features of cyberbullying and the roles that people can play in it. In this context, the paper points out the specifics of cyberbullying compared to the traditional bullying, while pointing out the relevant characteristics of the cyber space itself. Based on the consideration of the harmful consequences of cyberbullying, the paper points out the considerable danger of this phenomenon, and consequently, the necessity of its adequate suppression and prevention. In this regard, the paper will present possible solutions for cyber violence related to the application of modern technologies in cyber space. In particular, the paper discusses the importance of utilising information technologies in the fight against cyberbullying, through consideration of their application in the detection of cyberbullying based on the analysis of textual and other content. The capabilities of artificial intelligence and its related fields, that is, technologies that are applied in the suppression of cyber violence will be illustrated through specific projects and models developed for these purposes, which are also applied in cases of peer cyber violence. The paper also examines the possible ways of using certain technologies for providing support to victims of cyber violence.

Keywords: *cyberbullying, peer cyberbullying, artificial intelligence, machine learning, natural language processing.*

Примљено: 03. октобар 2024.
Прихваћено: 30. новембар 2024.

УДК 614.84:640.522(497.11)
COBISS.SR-ID 161914377
DOI: 10.5937/ssb2402083N

СПРОВОЂЕЊЕ ПРЕВЕНТИВНИХ МЕРА НА ПЛАНУ СМАЊЕЊА РИЗИКА ОД ПОЖАРА У КБЦ „ДР ДРАГИША МИШОВИЋ – ДЕДИЊЕ”

Јована НИКОЛИЋ*, мастер менаџер безбедности
Милош ТОМИЋ**, доцент

* jovicicj16@gmail.com
** Факултет безбедности, Универзитет у Београду, milos.tomic@fb.bg.ac.rs

СПРОВОЂЕЊЕ ПРЕВЕНТИВНИХ МЕРА НА ПЛАНУ СМАЊЕЊА РИЗИКА ОД ПОЖАРА У КБЦ „ДР ДРАГИША МИШОВИЋ – ДЕДИЊЕ”

Сажетак: *Пожари имају велики потенцијал да угрозе животе људи, имовину, материјална добра и околину, те да прерасту у катастрофе. Опасност од пожара, односно ризика по људе и имовину, посебно расте у јавним објектима, у којима по правилу истовремено борави већи број лица. Бројна искуства су показала да је велики број пожара могао бити спречен или угашен још у почетној фази, поштовањем и применом основних мера заштите од пожара. Ранији приступ заштите од пожара базирао се на мерама које су имале за циљ да сузбију пожар и умање последице, онда када је пожар већ наступио. Савремени концепт смањења ризика од пожара подразумева планирање и примену низа превентивних мера. Превентивне мере једини су ефикасан и економичан начин заштите од пожара, а њима се утиче како на спречавање настанка пожара тако и на знатно умањење негативних ефеката, уколико до пожара дође.*

Кључне речи: *објекти од јавног значаја, пожар, смањење ризика, превентивне мере заштите, заштита од пожара*

Увод

Пожар је видљиви и осетни ефекат процеса сагоревања – посебне врсте хемијске реакције. Ради се о релативно брзој оксидацији материјала у егзотермном хемијском процесу сагоревања, при чему се ослобађају велика топлота, светлост и други различити продукти. Људску историју одувек су пратили пожари, неки са мањим, а поједини и са великим катастрофалним последицама. Овоме је значајно допринео нагли развој индустрије, брза урбанизација и градња великих објеката, који нису увек у складу са мерама заштите од пожара.

У укупној изграђеној инфраструктури једног друштва, објекти од јавног значаја, односно јавни објекти имају велики удео. Такви објекти

имају одређену намену, а у њима је предвиђено окупљање и боравак већег броја људи. Јавни објекти пројектују се тако да своју намену могу испуњавати деценијама, односно да током свог века трајања пре свега буду безбедни и функционални. Са безбедносног аспекта, ови објекти увек захтевају посебну пажњу када је реч о заштити од разних извора угрожавања. Ово је пре свега због великог броја људи на једном месту истовремено, али и због повећане угрожености самог објекта, имовине, инвентара и околине. Опасности од пожара у сваком објекту, али и из његове околине су врло извесне. Велики број пожарних опасности настаје услед кварова и неодржаваних електричних инсталација, грешака при извођењу и руковању разним уређајима, али пре свега због непоштовања и непоступања према основним захтевима заштите од пожара. Не сме се занемарити ни намерно подметање пожара или експлозија. Све факторе угрожавања од пожара, наравно, није могуће избећи. Међутим, адекватним управљањем ризиком од пожара, анализом стања и предузимањем одговарајућих мера – могуће је смањити осетљивост и ублажити евентуалне последице.

У Републици Србији, област противпожарне заштите регулисана је пре свега Законом о заштити од пожара и бројним подзаконским актима, који из њега произлазе. Субјекти заштите од пожара, који подразумевају и јавне објекте, имају законску обавезу да поступају према одредбама Закона, а то подразумева најпре примену прописаних мера заштите од пожара. Када је реч о пожарној безбедности, односно смањењу ризика од пожара, подразумевају се, у првом реду, превентивне мере заштите. Циљ мера превенције јесте да спрече појаву пожара, или да његово испољавање сведу на најмању могућу меру. Уколико до пожара ипак дође, превентивне мере имају за циљ гашење пожара у почетној фази, спречавање ширења пожара, безбедну и сигурну евакуацију људи и материјалних добара и слично (Гавански и сар., 2011).

Искуство и пракса показали су да у великом броју случајева пожара, посебно оних у већим стамбеним, пословним и јавним објектима, постоје само минималне мере за ублажавање опасности од пожара. Савремени извори угрожавања и проблеми опасности од пожара често се не узимају у обзир, што условљава и неадекватан ниво заштите. Традиционални, односно класични приступ систему заштите од пожара подразумевао је реактиван приступ, односно сузбијање пожара и ублажавање негативних ефеката, након што је већ дошло до испољавања пожарне опасности. Савременим приступом, односно

смањењем ризика од настанка нежељеног догађаја, предвиђа се читав низ превентивних мера у заштити од пожара. Повећање отпорности, односно идентификовање и умањење слабости, од кључног је значаја, посебно када је реч о јавним објектима, објектима у којима постоје процеси који укључују запаљиве материје, и слично. То је могуће постићи једино адекватном проценом ризика и спровођењем превентивних мера, још у фази пројектовања и градње објекта. Осим тога, опрема објекта савременим системима за дојаву и гашење пожара још једна је од неопходних превентивних мера смањења ризика од пожара.

Угроженост објеката од јавног значаја пожаром

Објекти од јавног значаја, односно јавни објекти, јесу посебно пројектовани простори или површине, унутар или ван насеља, а разликују се према својој намени. Њихов значај може бити локални, регионални, па и глобални (Бркљач и др., 2018). Према Правилнику о класификацији објеката (2015), објекат јавне намене јесте објекат који има више од 80% корисне површине намењене окупљању и боравку људи. Овде спадају: угоститељски објекти за исхрану и пиће; угоститељски објекти намењени за смештај; културни, образовни, здравствени, спортско-рекреативни, религијски и други објекти; пристаништа; железнички и аутобуски објекти; авио терминали и друго.

Јавни објекти имају знатног удела у изграђеној инфраструктури заједнице, и имају велику улогу у друштвено-економском и социјалном развоју. Велики број објеката пројектује се тако да трају више деценија, те да током овог дугог временског периода буду пре свега безбедни и функционални. Последњих година, инфраструктура широм света све више је погођена природним непогодама (земљотрес, цунами и слично), али и опасностима чији је изазивач у великом броју случајева човек, као што су пожари и експлозије. Осим што представљају велику претњу по живот, инфраструктуру, имовину и животну средину, пожари у највећем броју случајева погођене објекте остављају делимично или потпуно уништеним. Осим директних, такво онеспособљавање великог броја објеката са собом носи и велики број индиректних губитака (Kodur et al., 2020). Вероватноћа избијања пожара зависи од бројних фактора, односно пожарна угроженост објекта

утврђује се на основу: грађевинских карактеристика, локације, степена угрожености технолошког процеса који се у објекту одвија и слично (Јованов и др., 2000).

На територији Републике Србије, највећи број објеката од јавног значаја или објеката јавне намене, уколико према другом критеријуму нису сврстани у I категорију угрожености од пожара, спада у објекте са повећаним ризиком од избијања пожара, односно у II категорију угрожености, јер се у њима у највећем броју случајева окупља 200–500 лица. Власник или корисник објекта са повећаним ризиком од избијања пожара према Закону је обавезан да спроведе превентивне мере заштите од пожара, као и стално дежурство са потребним бројем лица, која су стручно оспособљена за спровођење мера заштите од пожара. Поред тога, субјекат је у обавези да обезбеди уређаје за гашење пожара и адекватну опрему.

Уређаји и ручни апарати за гашење пожара намењени су гашењу свих врста почетних пожара, а посебно су погодни за гашење пожара у радним и сличним просторијама. Када се такви апарати благовремено и правилно употребе пружају врло ефикасну помоћ и спречавају ширење и разбуктавање пожара, до доласка ватрогасних јединица (Костић и др., 1970). Одржавање ручних апарата и уређаја за гашење пожара, у јавним објектима, од кључног је значаја, а такви објекти, по Закону, обавезни су да формирају Службу заштите од пожара са руководиоцем и довољним бројем лица на сталном дежурству који су стручно оспособљени да спроводе мере заштите од пожара. Сви запослени у служби морају поседовати Уверење о положеном стручном испиту за раднике који раде на пословима заштите од пожара.

Анализирајући интервенције од 2010. до 2022. године у којима је учествовала ватрогасно-спасилачка бригада града Београда, закључује се да, на годишњем нивоу, око 22% од укупног броја пожара настаје у јавним објектима. Од овог броја, највише пожара настаје у угоститељским објектима, тржним центрима и већим трговинским објектима, а остало су пожари настали у болницама, школама, трафо постројењима ЕДБ Београд, и други.

Најзначајнији корак управљања ризиком од пожара, и саставни део Плана заштите од пожара, према Закону, јесте процена ризика. Проценом ризика од пожара заправо се одређује ниво угрожености конкретног објекта од пожара. Како би се успешно проценио ризик, односно одредио ниво угрожености од пожара, користе се разне методе за процену ризика (Комљеновић и др., 2017). Бројне методе за

процену ризика од пожара често користе програме у којима се симулира: сам развој и ширење пожара, пожарне ситуације које могу наступити, поступци људи у случају избијања пожара, безбедна евакуација, успешност гашења и слични сценарио. За разлику од раније праксе, где се заштита од пожара базирала на идентификацији ризика, нови приступ омогућава успешно предвиђање, оцену и доношење најоптималнијих одлука у заштити од пожара (Кокић Арсић и Мишић, 2014).

Заштита од пожара захтева мултидисциплинарни приступ и подразумева познавање: технологије објекта, грађевинских материјала, конструкције објекта, карактеристика саобраћајница, машинских инсталација, електричних инсталација слабе и јаке струје, инсталација водоводне мреже, гасних инсталација и других елемената (Секуловић и др., 2012). Управљање ризиком од пожара у свим делатностима неопходно је, пре свега, како би се смањио број пожара и број жртава, умањиле материјалне штете и постигла економична заштита, а то је могуће једино превентивним мерама.

Превентивне мере у циљу смањења ризика од пожара

Превентивне мере смањења ризика од пожара у оквиру одређеног субјекта заштите не могу се одвојити од целокупног система заштите од пожара, и његов су саставни део. Из овог разлога, сама заштита од пожара дефинише се као скуп активности и мера, пре свега превентивног карактера, у циљу спречавања избијања и ширења пожара, смањења негативних ефеката, ефикасног гашења пожара, утврђивања узрока пожара и евентуалне одговорности (услед непоштовања прописаних заштитних мера) (Јазић, 2023). Треба истаћи да за оптимално решење и примену превентивних мера заштите од пожара у обзир треба узети сложену интеракцију људи, објеката (посебно оних у којима борави или се окупља већи број лица) и самих пожара. У том смислу, дизајн и конструкција објекта, његово одржавање и имплементација превентивних мера у фази пројектовања и изградње од кључног су значаја за саму заштиту од пожара, али и за безбедну евакуацију и спречавање ширења пожара, у случају његовог испољавања (Нукић и Марковић, 2020).

Надлежни орган који контролише спровођење мера превенције у области заштите од пожара јесте Министарство унутрашњих послова Републике Србије. Другим речима, МУП реализује активности које укључују спровођење превентивних мера, којима се спречава избијање пожара, као и мера којима се ублажавају последице уколико до пожара ипак дође. За област заштите од пожара најважније тело у надлежности Министарства јесте Сектор за ванредне ситуације, у чијем оквиру постоји неколико управа, од којих је у области превентивне заштите од пожара најзначајнија Управа за превентивну заштиту (Јазић, 2023). Како би се смањила учесталост таквих нежељених догађаја, приликом пројектовања градње нових објеката предузима се низ превентивних мера, почев од саме локације објекта. Када се врши одабир локације за изградњу новог објекта, у контексту заштите од пожара, посматрају се два аспекта. Прво се води рачуна у којој мери будући објекат може угрозити околину, и, повратно, у којој мери околина (суседни објект) угрожавају будући објекат. Надаље се разматра материјал од којег ће објекат бити изграђен, као и израда унутрашњости објекта. То подразумева, поред архитектонских, естетских, економских, функционалних и других услова, и обавезно испуњавање захтева заштите од пожара (Секуловић и др., 2012). Сагласност на техничку документацију у вези мера заштите од пожара издају јединице државне управе у чијој надлежности се налази заштита од пожара.

За објекте који подлежу законским одредбама о заштити од пожара обавезна је и израда Главног пројекта заштите од пожара, као и прибављање сагласности на тај пројекат. Уз пројекат, субјекти заштите од пожара обавезно прилажу и Елаборат о заштити од пожара. Елаборат заштите од пожара, у том случају, јесте саставни део техничке документације и прилаже се уз захтев за издавање дозволе за градњу или реконструкцију објекта. Елаборат израђује лице које је лиценцирано у складу са прописима којима је уређен систем заштите од пожара (Драганић и др., 2020). Техничка документација у свом саставном делу садржи посебно Главни пројекат заштите од пожара. Законом је дефинисано да Главни пројекат заштите од пожара може израдити само привредно друштво које је регистровано за израду техничке документације и које има посебно овлашћење Министарства по питању израде Главног пројекта заштите од пожара. То подразумева да привредно друштво које израђује Главни пројекат има запослена лица која поседују одговарајућу лиценцу за израду техничке документације и пројеката заштите од пожара.

Испитивање грађевинских материјала и конструкција са аспекта реакције на ватру, и отпорност према ватри, само је један у низу захтева заштите од пожара, али и основни услов смањења ризика од пожара. Треба истаћи и да начин понашања материјала према извору топлоте зависи и од саме површине, облика, технике обраде материјала, као и од намене коју има у градњи (да ли је носећи или преградни елемент и слично). Степен отпорности према пожару утврђује се за објекат у целости или за део објекта који чини јединствену техничко-безбедносну целину. СОП се одређује онда када је потребно оценити како ће се конкретни објекат понашати у случају испољавања пожара. Овај степен се базира на процени ризика од пожара, за лица која се налазе у објекту, као и за сам објекат, посебно ако је он од већег значаја за друштво. СОП треба да буде најмање такав да се омогући безбедна евакуација свих лица која се у нормалним условима могу наћи у објекту (Секуловић и др., 2012).

Да би се осигурала безбедна евакуација људи за време пожара од изузетног је значаја да у објекту постоји одговарајући број излаза правилних димензија. Распоред излаза треба да буде такав да се свим присутним лицима омогући да напусте објекат на време. Број, величина и распоред излаза одређују се према максималном броју лица која се могу наћи у објекту, па је и различит за поједине врсте објеката, у односу на њихову намену (Секуловић и др., 2012). Посебна пажња се посвећује одређивању и распореду излаза у јавним објектима, и код лоцирања излаза посебно се утврђује удаљеност коју треба савладати приликом напуштања објекта. Адекватна процена времена које је потребно за евакуацију од посебног је значаја за објекте у којима се окупља или борави већи број људи, као што су велики стамбени, пословни и јавни објекти, који припадају I или II категорији угрожености од пожара. У нашој држави, према инжењерској пракси и законским одредбама, примењује се рачунски модел према којем се одређује време потребно за евакуацију критичним путем, односно од најудаљеније тачке објекта до крајњег излаза, док су брзине кретања лица дефинисане стандардом (Лабан и др., 2015).

Најефикаснији начин и најкраће време снабдевања водом за гашење пожара обезбеђује се из градских водоводних мрежа, из водоводних мрежа насељених места или пак из индустријских водовода. То се најчешће изводи тако што се за ове основне системе, поред осталих потрошача, везују и противпожарне, односно хидрантске водоводне мреже (Јованов и др., 2000). Хидрант мора бити увек доступан, а

простор око њега слободан. Капацитет хидранта зависи од капацитета потребног за гашење пожара и броја млазева који се користе, а потребан број хидраната различит је за стамбене зграде, јавне и индустријске објекте.

Савремени вид техничке заштите подразумева детекторе пожара, јер врше функцију јављања пожара у почетном стадијуму, као и функцију локације, односно адресе на којој се пожар јавио (Радишић, 2017). Према начину активације разликују се ручни и аутоматски детектори пожара. Ручни системи су врло једноставни и раде тако што се притиском на дугме алармира опасност од пожара, али то значи да је за њихово коришћење потребан човек, односно активацију детектора врше људи. Доста значајнију примену имају аутоматски детектори пожара, који се фиксирају на одређеним местима, где постоји повећана опасност од пожара, а када региструју промену детектори се укључују аутоматски и алармирају опасност. Детектори региструју пожар у почетној фази, на основу појава које прате јављање пожара, као што су дим, температура, зрачење и друго.

Стабилни противпожарни системи могу бити полуаутоматски и аутоматски. Полуаутоматске системе активира човек са даљине, док аутоматски системи делују без учешћа човека. Данас су у употреби најпре стабилни системи са аутоматским деловањем, а њихов развој условљен је општим технолошким развојем, у којем долази до значајног повећања опасности од пожара (Имамовић и др., 2022). У најефикасније стабилне системе за гашење пожара убраја се спринклер инсталација, која се данас највише и примењује. Ради се о аутоматској инсталацији која ради на бази распрскавајућег млаза воде. Изведени цевоводи, путем којих вода долази до млазница, морају бити под сталним притиском воде или ваздуха. У припремном стању, пре активације, млазнице су затворене, а на одређеној температури аутоматски се отварају и активирају. Када се региструје пројектована температура долази до пуцања ампуле на млазници спринклера, и на тај начин се води отвара излаз. Док излази из млазнице, вода удара у посебан дефлектор и тако се распршује, правећи круг и покривајући површину која се штити од пожара (Радишић, 2017).

Спровођење превентивних мера у КБЦ „Др Драгиша Мишовић – Дедиње"

Велики број различитих здравствених објеката, као што су клинички центри, болнице, домови здравља, амбуланте, рехабилитациони објекти и други, подразумевају константан боравак великог броја људи, од којих многи могу бити тешко здравствено угрожени, непокретни и слично. Њихов смештај и кретање отежано је чак и у нормалним условима функционисања, док у ситуацијама као што су земљотреси, пожари и слично може бити врло комплексно, често и неизводљиво. У здравственим објектима пацијенти су најчешће стационирани у собама, у обичним или посебним медицинским креветима. Они се крећу сами, или уз помоћ особља. У таквим случајевима евакуација се мора извести уз помоћ болничког особља под надзором лица које спроводи мере заштите од пожара, и то посебно пројектованим евакуационим путевима (Јевтић, 2019).

Током историје забележени су бројни пожари који су се јављали у болницама и здравственим центрима, неки са мањим, а поједини и са катастрофалним последицама. Како би се најефикасније спречили или минимизирали такви догађаји потребно је добро познавати претње које могу угрозити нормално функционисање таквих објеката, и у складу са тим планирати мере заштите. Претходни случајеви пожара и њихове последице могу послужити као основни сценарио у циљу сагледавања узрока и последица, те спречавања таквих догађаја у будућности (Илић и др., 2021).

Здравствени објекти, посебно болнице, често се пројектују као неколико одвојених зграда или објеката, међусобно повезаних спољним или подземним ходницима. Такви објекти, у складу са својом наменом, имају велики број различитих просторија, од соба за смештај пацијената, лабораторија, шок соба, интензивне неге, све до техничких просторија и посебних остава за медицинска средства. У таквим објектима, са безбедносног аспекта, постоји велика угроженост, како пацијената тако и особља, имовине и околине. Опасност расте када се узме у обзир здравствено стање пацијената, њихова немогућност кретања, неопходна помагала и слично. Најчешћи начин муњевитог ширења пожара у здравственим објектима јесте преко запаљивих материјала који се користе у ентеријеру објекта (дрво, врата, прозори, кревети и слично), а посебно су опасне боце са кисеоником које, у случају пожара, могу довести и до експлозије (Јевтић, 2019).

Правилним избором опреме и техничких решења, редовним и адекватним одржавањем и контролом опреме и инсталација значајно се смањује вероватноћа појаве извора паљења и настанка пожара услед неисправности опреме или инсталација. Постављањем одговарајућих знакова упозорења и забране, адекватном обуком запослених и адекватним радним процедурама смањује се опасност од пожара. Адекватном заштитом од атмосферског пражњења, статичког електрицитета и правилним складиштењем робе склоне самозапаљењу смањена је и опасност од природних узрочника. Могућност настанка пожара у објектима КБЦ „Др Драгиша Мишовић – Дедиње" постоји и у помоћним и технолошким просторијама. Поједине просторије, као на пример оне у којима се чувају запаљиви гасови или разне запаљиве течности и енергенти за употребу у техничке и медицинске сврхе, лабораторије, болничка апотека, просторије са боцама са кисеоником и другим медицинским и техничким гасовима, су места са повећаним ризиком од пожара и о њима се мора водити посебна брига и предузимати мере заштите од пожара.

Посебна ставка на коју треба обратити пажњу је чињеница да су у већини објеката уграђени и неки синтетички материјали, било као грађевински материјали или као опрема и инвентар просторија (подови, делови спуштеног плафона и сл.). Ти материјали у случају пожара горе и при томе могу пренети пожар у виду запаљених капи (пренос пожара капљањем) или у виду жара, а при томе развијају отровне гасове и стварају велику задимљеност просторија и коридора за евакуацију.

Примењене превентивне мере заштите од пожара у објекту

Објекти КБЦ „Др Драгиша Мишовић – Дедиње" се разврставају у категорију II угрожености од пожара. Послови заштите од пожара у КБЦ су организовани у оквиру Службе за техничке и друге сличне послове, у оквиру ког је формиран Одсек за заштиту од пожара. Рад запослених на пословима физичко-техничког обезбеђења и запослених на пословима непосредног гашења пожара је организован у смене, чиме се заокружује 24-часовно радно време, тј. дежурство. Запослени на пословима физичко-техничког обезбеђења и запослени на пословима непосредног гашења пожара су лоцирани у пријавницама на главним улазима и поред централа за дојаву пожара. У појединим

објектима комплекса КБЦ изведене су стабилне инсталације за аутоматску дојаву пожара са извршним функцијама. Такође, у објектима постоји спољашња и унутрашња хидрантска мрежа.

Прилазне саобраћајнице објектима КБЦ обезбеђују неометан приступ свим врстама возила. Није омогућен приступни пут средњем делу објекта центра за збрињавање ургентних стања – ургентном центру између две пасареле. Главни улази у комплекс су у свакодневној употреби, а улази у објекте комплекса се користе у складу са потребама. Ватрогасно возило може нормално да уђе и изађе на главни улаз у ул. Хероја Милана Тепића бр. 1. Поред објеката КБЦ пролазе и јавне и интерне саобраћајнице које се могу користити и као пожарни пут, пут за интервенцију у случају пожара и за евентуални прилаз ватрогасних возила у случају интервенције.

На објекту се примењују и превентивне мере заштите приликом пројектовања, изградње и коришћења објекта. Приликом изградње објекта коришћени су материјали одговарајуће ватроотпорности. КБЦ „Др Драгиша Мишовић – Дедиње" поседује План заштите од пожара и Програм обуке запослених радника на који је добијена сагласност Управе за ванредне ситуације у Београду. Такође, обука запослених радника и провера знања се редовно спроводи. Има формирану службу са потребним бројем извршилаца на пословима сталног дежурства са положеним стручним испитима из области заштите од пожара. Сва мобилна опрема и уређаји за почетно гашење пожара, електроенергетска постројења и инсталације ниског напона, општег напајања електричном енергијом, инсталације развода електричне енергије и заштитни уређаји који су саставни део ових инсталација, инсталације за заштиту објекта од утицаја атмосферског пражњења и стабилни системи за дојаву и гашење пожара контролишу се и одржавају редовно. Сви објекти се редовно контролишу и у случају откривања незаконитости у раду налажу се мере за отклањање незаконитости са предвиђеним роковима за њихово отклањање.

Поред свих примењених превентивних мера, 24. октобра 2009. године, у касним вечерњим часовима, дошло је до пожара на објекту клинике хирургије. У гашењу пожара учествовало је 80 ватрогасаца-спасилаца и 27 ватрогасних возила. Упоредо са гашењем пожара, ватрогасци-спасиоци вршили су евакуацију пацијената која је била приоритет. Значајну помоћ у евакуацији пружили су припадници Полицијске бригаде, Жандармерије и медицинско особље КБЦ-а. На основу евиденције из КБЦ-а, евакуисано је 300 пацијената, без погор-

шања општег здравственог стања. Пацијенти су систематски изношени на плато и травњак, где се вршила тријажа од стране медицинског особља, на основу које је одлучивано који ће пацијенти и у коју медицинску установу бити по приоритету транспортовани колима хитне помоћи.

Закључак

Повећању учесталости пожара који настају у разним објектима, и катастрофалнијим последицама, највише је допринела: брза градња, нагла урбанизација, градња великог броја високих објеката и други фактори. Оштећење, онеспособљавање или уништавање објеката у случају пожара доводи до губитка живота људи, нарушавања опште безбедности и сигурности, значајних директних и индиректних новчаних и материјалних губитака и бројних других негативних ефеката. Опасност од пожара у објектима се може представити као могућност случајног или намерног пожара, који прети да угрози животе људи, конструкцију објекта, имовину и околину (Kodur, Kumar, Rafi, 2020). Сваки објекат мора бити заштићен од пожара, у складу са својом наменом, бројем лица који бораве у њему и другим значајним условима. Објекти треба да буду пројектовани и изведени тако да издрже дејства идентификованих опасности, уз што мање последице.

Пожари су посебна група угрожавања безбедности, јер у кратком року могу изазвати катастрофалне последице. Озбиљан проблем јесу пожари у великим и јавним објектима. То није само због чињенице да је у таквим објектима присутан велики број људи, већ и због чињенице да је у таквим случајевима најизвеснија паника, отежана евакуација, брзо ширење дима, па ситуација лако прераста у катастрофалну. У том смислу, таквим објектима потребне су посебне безбедносне мере, а систем заштите од пожара веома је озбиљно питање, посебно у јавним објектима. Процена ризика од пожара основни је предуслов планирања и извођења адекватних превентивних мера, јер се једино превентивним мерама може утицати на само умањење ризика настанка пожара. При процени ризика од пожара у обзир треба узети сва лица која бораве или посећују јавни објекат, укључујући и запослена лица, конструкцију објекта, његову намену, процесе који се одвијају, опрему, инсталације и друге факторе од значаја. У циљу што ефикаснијег смањења ризика од пожара, умањења жртава и материјалних

губитака потребно је обезбедити такав систем заштите који ће пре свега имати задатак спречавања пожара, и у случају настанка спречавања ширења пожара.

Приликом пројектовања сложених објеката неопходно је узети у обзир бројне елементе од значаја. Овде се подразумевају превентивне мере у пројектовању и градњи објекта, односно у избору таквих материјала који ће обезбедити заштиту од пожара. Одабир ватроотпорних конструкционих елемената спречава ширење пожара у објекту и ван њега, дозвољава додатно потребно време евакуације и доприноси много мањем оштећењу објекта. Неке од најзначајнијих превентивних мера које се данас спроводе су: категоризација технолошког процеса, дефинисање и извођење пожарних сектора, прорачун пожарног оптерећења, те извођење заштитних мера у складу са прорачуном.

Како би се постигло што ефикасније смањење ризика од пожара, ове пасивне мере заштите потребно је комбиновати са активним мерама, које имају за циљ сузбијање пожара у почетној фази. Комбинација ових мера доприноси потпунијој заштити, спречавању избијања и ширења пожара, заштити људи и имовине, што и јесте циљ заштите од пожара као јединственог, законски уређеног система.

Литература

Бркљач, Д., Милинковић, А., Вукајлов, Љ. (2018). Значај јавних објеката за социјални развој заједнице. У: М. Бешевић (ур.), *Зборник радова 'Савремена достигнућа у грађевинарству'*, (563–571), Суботица: Грађевински факултет.

Гавански, Д., Миланко, В., Крњетин, С. (2011). Имплементација оцене спроведених мера заштите од пожара. *Заштита материјала,* 52*(2),* 115–122.

Драганић, С. и сар. (2020). Енергетска рехабилитација и безбедност од пожара фасада високих зграда. У: М. Лабан и др. (ур.), *Безбедност зграда од пожара – Приступ и пракса западног Балкана,* (175–195), Нови Сад: Факултет техничких наука.

Илић, С. и сар. (2021). Заштита од пожара здравствених објеката. У: В. Миланко, М. Лабан и Е. Мрачкова (ур.), *Зборник радова са међународне конференције о заштити од пожара и експлозије 'Безбедносни инжењеринг',* (30–35), Нови Сад: Висока техничка школа струковних студија.

Имамовић, А., Агић, Д., Оруч, М. (2022). *Утврђивање и надзор заштите од пожара.* Зеница: Институт за привредни инжењеринг.

Јазић, А. (2023). Уређење превентивне заштите од пожара у Републици Србији. У: М. Томић и др. (ур.), *Савремене студије безбедности,* 4/2023, (67–84), Београд: Факултет безбедности.

Јевтић, Р. (2019). Евакуација здравствених објеката са присуством непокретних особа. *Здравствена заштита,* 48(1), 61–68.

Јованов, Р. и сар. (2000). *Основи превентивне заштите од пожара и експлозија*. Београд: Виша школа унутрашњих послова.

Kodur, V., Kumar, P., Rafi M. (2020). Fire hazard in buildings: review, assessment and strategies for improving fire safety. *PSU Research Review*, 4(1), 1–23.

Кокић Арсић А., Мишић, М. (2014). Модел управљања ризиком од пожара. У: С. Арсовски, М. Лазић и М. Стефновић (ур.), *41. национална конференција о квалитету,* (31–36), Крагујевац, 22–23.5.2014.

Комљеновић, С., Стојановић, Д., Марковић, С. (2017). Имплементација методе „Густав Пурт" у процени ризика од пожара у војним објектима. *Војно дело,* 69(5), 290–302.

Костић, В., Танасковић, С., Опачић, В. (1970). *Противпожарна заштита у рату.* Београд: Народна армија.

Лабан, М. и сар. (2015). Перформансе путева евакуације и безбедност зграда од пожара. *Техника – наше грађевинарство,* 69(4), 599–606.

Нукић, Е., Марковић, Ј. (2020). Инжењерство безбедности од пожара. У: М. Лабан и др. (ур.), *Безбедност зграда од пожара – Приступ и пракса западног Балкана,* (2–43), Нови Сад: Факултет техничких наука.

Правилник о класификацији објеката, „Сл. гласник РС", бр. 22/2015.

Радишић, Д. (2017). *Заштита од пожара и спасавање*. Бања Лука: Независни универзитет „NUBL".

Секуловић, З., Богнер, М., Пејовић, С. (2012). *Превентивна заштита од пожара.* Београд: „ЕТА".

IMPLEMENTATION OF PREVENTIVE MEASURES FOR REDUCING THE FIRE RISKS IN UHMC "DR. DRAGISA MISOVIC – DEDINJE"

Jovana NIKOLIC, master security manager
Milos TOMIC, Assistant Professor

Summary

Fire have a great potential to threaten people's lives, property, material goods, and the environment, and turn into disasters. The danger of fire, i.e. the risk to people and property, increases especially in public buildings, in which, as a rule, a large number of people are staying at the same time. Numerous experiences have shown that a large number of fires could have been prevented or extinguished at the initial stage, by observing and applying basic fire protection measures. Earlier approach to fire protection was based on measures aimed to suppress the fire and reduce its consequences, when the fire had already started. The contemporary concept of fire risk reduction involves planning and implementing a series of preventive measures. Preventive measures are the only effective and economical way to protect against fire, and they affect both the prevention of fire occurrence and the significant reduction of negative effects, if a fire occur.

Keywords: *objects of public importance, fire, risk reduction, preventive protection measures, fire protection.*

ОСВРТИ

DOI: 10.5937/ssb2402103T

др Милош ТОМИЋ, доцент*

ЦИВИЛНА ЗАШТИТА И РИЗИК ОД УПОТРЕБЕ ОРУЖЈА ЗА МАСОВНО УНИШТЕЊЕ: АКТУЕЛИЗАЦИЈА УПОТРЕБЕ ДВОНАМЕНСКИХ СКЛОНИШТА У СРБИЈИ

Специјална војна операција коју је Руска Федерација започела на територији Украјине 24. фебруара 2022. године са собом доноси низ проблематичних питања не само из домена војних наука већ сада све конкретнијих наука безбедности (енергетска безбеност, еколошка безбедност, безбедност хране, здравствена безбедност). Наиме, ескалацију насиља карактерише велики број цивилних жртава на обе стране, нарочито због употребе одавно међународно забрањених система наоружања и ратне технике (нпр. касетне бомбе), као и ракетних система велике разорне моћи са раздаљином далеко изван линије фронта. Захваљујући научно-техничким достигнућима, ракетно наоружање може имати веома велику девастирајућу снагу, што намеће потребу предузимања мера оптималне заштите целокупног становништва, њихове имовине, материјалних и културних добара изузетне вредности и значаја. Сходно томе, многе европске земље (нпр. Норвешка, Швајцарска, Шведска) улажу значајне напоре у изградњи и одржавању склоништа за скоро сваког становника како би се осигурала њихова заштита од ратних опасности, као и последица техничко-технолошких акцидената и елементарних непогода. Треба напоменути да су економски услови једна од кључних детерминанти у контексту изградње и одржавања склоништа, односно све је више заговорника да заштитне објекте треба градити искључиво са двонаменском функцијом, и то: права *мирнодопска*, када се они користе као места за обављање неких комерцијалних активности (теретане, коц-

* Факултет безбедности, Универзитет у Београду, milos.tomic@fb.bg.ac.rs

карнице, оставе, магацини, продавнице, клубови) и друга, најбитнија јесте *заштитна* функција, када се они релативно лако претварају у склоништа (у року од 24 часа). Такође, изградња склоништа за већи број људи мора да буде у складу са сложеним грађевинским стандардима који прописују низ специфичности у погледу просторија, опреме (нпр. санитарна мрежа, противпожарна заштита, осветљеност) и поседовања различитих филтро-вентилационих уређаја.

Питање склоништа у Републици Србији већ неколико година након НАТО агресије 1999. године не налази се у друштвено-политичком фокусу што се може објаснити евидентно ниском безбедносном културом, јер, како се често може чути, „неће то код нас да се деси". Од 1992. године сви послови око изградње, одржавања и контроле склоништа поверени су Јавном предузећу за склоништа, које запошљава преко 100 људи различите струке. У делокругу рада овог предузећа налазе се и двонаменска склоништа као најрентабилнији облик грађевине са обрамбено-заштитном функцијом. Према неким подацима, само је у периоду од 1992. до 1996. године од издавања јавних и блоковских склоништа остварено око 30,1% укупног прихода Јавног предузећа за склоништа. Интересантно је да се поменуто предузеће не финансира из буџета РС већ управо на основу издавања објеката у закуп, при чему је 2012. укинута обавеза грађевинског инвеститора да уплати накнаду 2% од укупне процењене вредности новоизграђеног објекта. Од момента доношења ове одлуке ЈП „Склоништа" послују са великим губицима, што се одражава на целокупан систем цивилне заштите, тј. отежано је спровођење мера реконструкције и одржавања (текуће и инвестиционо) свих јавних и блоковских склоништа унутар 48 локалних самоуправа широм РС. О томе сведочи и податак да је од укупно 1442 јавна склоништа којима газдује ово предузеће више од 951 ван функције јер се налазе на неприступачним местима (укопана неколико метара испод површине земље), без одговарајуће опреме и уређаја. Други проблем са којим се суочава ово предузеће представља недостатак стручног особља (у просеку преко 35% непопуњених радних места) надлежног за спровођење мера одржавања и техничке контроле склоништа (сагласно Правилнику о техничким нормативима за склоништа контрола се спроводи једанпут годишње). Да је стање у погледу одржавања склоништа више него забрињавајуће констатује се у Извештају Државне ревизорске институције, који је објављен 2023. године. Као један од закључака, инспектори наводе да се склоништа у Србији користе као оставе, при чему су станари зграда својим неса-

весним деловањем оштетили опрему и уређаје који треба да обезбеде функционалност и ефикасност мера склањања становништва од последица употребе оружја за масовно уништење.

На крају, треба нагласити да не постоји јасна формално-правна регулатива, а последично и одсуство санкционисања, затим инкопатибилност државних органа и недовољна стручност снага система цивилне заштите (повереници ЦЗ и Сектор за ванредне ситуације). Услед наведених проблема тренутно није могуће испунити одбрамбено-заштитну функцију склоништа, иако су реалне потребе Србије по том питању нарочито изражене имајући у виду геостратешки положај и близину актуелних ратних дешавања на истоку европског континента (нпр. удаљеност Кладова и Одесе је нешто више од 650 километара). Дакле, основна препорука научно-стручне јавности тиче се предузимања неопходних нормативних, материјалних и других мера и поступака у контексту оснаживања система цивилне заштите у ужем, односно цивилне одбране у ширем смислу, ради испуњења стратешки важног задатка, а то је заштита становништва, материјалних и културних добара од све опасније и сложеније физиономије савременог рата, али и разорнијих последица природних непогода.

DOI: 10.5937/ssb2402107K

др Душан КЕСИЋ, доцент*

ПОВРАТАК ОБАВЕЗНОГ СЛУЖЕЊА ВОЈНОГ РОКА

Традиција служења обавезног војног рока у Србији свој заметак налази у периоду друге половине 19. века. Стицање независности Кнежевине Србије на Берлинском конгресу утрло је пут развоја народне стајаће војске 1883. године. Тиме је и српска држава кренула стопама великих сила Европе 19. века, које су увеле народне стајаће војске. Увођење обавезног војног рока било је подстакнуто растућим националним заносом, како у случају великих сила тако и у случају Србије. Народна стајаћа војска постала је симбол државности и независности Србије, и израз њене вишевековне борбе за слободу. Следствено томе, служење војног рока представљало је праксу која је имала далекосежне ефекте, његова функција надилазила је просту војну обуку. Специфичан израз служења војног рока било је јачање националне свести и особеног етоса српског народа.

Улога војске и ослободилачке борбе у стицању независности српске државе обликовала је њен симболички значај за колективни идентитет. Српски национални идентитет током 19. века свој доминатни израз нашао је кроз народну војску, а потом и служење војног рока, као моделе који су симболизовали „обнављање" српске нације. Војни успеси, како током ослободилачке борбе тако и током балканских ратова, само су појачавали симболички значај народне војске за колективну самоспознају. Војска је својим победама непрестано (ре)афирмисала темељне елементе националног идентитета, истицањем карактеристичних идеала у виду слободе, независности и државности. Стога је веза националне и војне културе била практично нераскидива, односно потоња

* Факултет безбедности, Универзитет у Београду, dusan.kesic@fb.bg.ac.rs

култура је била један од стубова колективног идентитета у периоду 19. и прве половине 20. века. Специфична веровања, вредности, представе и симболи колективног идентитета рефлектовани су кроз народну војску. Наиме, редовно служење војног рока подразумевало је усвајање ових чинилаца националног идентитета, са идејом да се код војника развије национална свест и пробуди свесна жеља за служењем отаџбини. Свеукупно, елементи националне културе уграђивани у народну војску омогућили су креирање кохерентног система веровања и вредности унутар српског народа. Исходи тако компонованог колективног менталитета исказани су кроз солидарност у херојским жртвама и подвизима приликом остваривања националних циљева током 19. и 20. века. Дакле, свеукупност чинилаца националне и војне културе пронашла је свој израз кроз особен приступ српског народа рату и употреби силе, као и вођењу одбрамбене и спољне политике. Тако обликована српска стратешка култура рефлектовала се кроз самоспознају, националне интересе и расположива средства и методе њиховог остваривања. Међутим, период Друге Југославије дезавуисао је вредности српске националне и војне културе, привилеговањем идеолошких идеја и вредности у концепцији нове државе. Унутар таквог система, улога војске и служења војног рока није била афирмативна по српски национални идентитет. Напротив, војска је постала један од водећих симбола комунистичке идеологије, рефлектујући партијски поглед на заједничку државу и друштво. Дакле, током овог периода српски национални идентитет изгубио је своје важно упориште – народну војску. Последице таквих промена у културном обрасцу довеле су до слабљења националне самоспознаје.

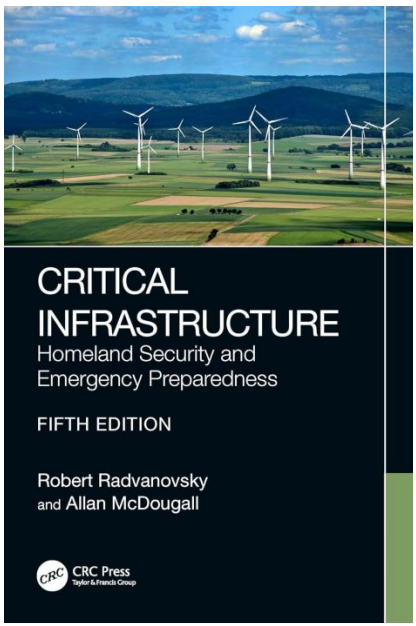
Период деведесетих означио је прве покушаје обнове националног идентитета у магновењу идеолошких преламања и ратова. Служење војног рока било је обавезно, а војска је све више попримала некашњу функцију, да кроз војну обуку рефлектује националне идеје и вредности. Ипак, са демократским променама овај процес изгубио је свој замајац, а са „замрзавањем" служења војног рока 2011. године наступило је „гашење" ове традиције, која је за неговање српског националног идентитета била прекопотребна. С тим у вези, вести о повратаку обавезног служења војног рока представљају повратак коренима, како српске војске тако и српског националног идентитета. Обавезно служење војног рока може, као што је то био случај у прошлости, помоћи у јачању националне свести и промовисати националне вредности и интересе.

ПРИКАЗИ КЊИГА/BOOK REVIEWS

Јана МАРКОВИЋ, сарадник у настави*

ЗАШТИТА КРИТИЧНЕ ИНФРАСТРУКТУРЕ КАО УСЛОВ ОЧУВАЊА ЖИВОТА И ОПСТАНКА ДРУШТВА

Robert Radvanovsky, and Allan Mcdougall. *Critical Infrastructure: Homeland Security and Emergency Preparedness*, Fifth Edition. CRC Press, 2023, 294 pp.



Књига *Критична инфраструктура: Државна безбедност и спремност за ванредне ситуације*, која се налази пред читаоцем, представља пето издање и наставак дугогодишњег истраживања. Аутори Роберт Радвановски (Robert Radvanovsky), стручњак у области безбедности, управљања ризицима, континуитета пословања, планирања опоравка од катастрофа и сајбер безбедности, и Алан МекДугал (Allan McDougall), стручњак у области заштите имовине и безбедности, настоје да кроз дванаест поглавља дају одговоре на следећа питања: Да ли је инфраструктура неопходна за очување живота или опстанак заједнице? Да ли инфраструктура функционише у веома ограниченом контексту или у много ширем контексту, односно да ли је инфраструктура

* Факултет безбедности, Универзитет у Београду, markovicfb22@gmail.com

специфична само за локалну заједницу, или се повезује са другим заједницама како би створила много већу заједницу? Да ли инфраструктура функционише као појединачна или јединствено организована целина, или је то заједница координисаних напора које улаже неколико страна? Чини се да аутори настоје да, поред приказа тренутног стања, понуде увиде за сагледавање трендова у домену заштите критичне инфраструктуре и њеном значају за националну безбедност. Таква сазнања би значила истраживачима, студентима, стручњацима, заинтересованим странама у индустрији, попут власника и оператера критичне инфраструктуре било у приватном, јавном или непрофитном сектору.

Прво поглавље аутори користе да читаоце упознају са значењима одређених појмова и понуде објашњења за феномене без чијег разумевања даље читање овог штива не би имало смисла. Објашњени су развој, појам и елементи критичне инфраструктуре, њена заштита, приватни и јавни сектор као власник критичне инфраструктуре и улога ових сектора у њеној заштити, као и незаобилазно јавно-приватно партнерство приватног и јавног сектора у области заштите „физичких и логичких система који су неопходни за минималне операције привреде и владе". Кроз књигу се провлачи прагматичан приступ разумевању супротстављених интереса јавног и приватног сектора око заштите критичне инфраструктуре.

Критична инфраструктура има одређена својства или карактеристике. Једно од својстава јесте капацитет одређен као „способност система да производи, дистрибуира и испоручује услуге". Међутим, у конкурентном окружењу, за успех система није довољан само капацитет, већ и уверење или сигурност да ће ти капацитети задовољити потражњу. Онда када капацитет система задовољи потражњу онда се каже да је систем у равнотежи. Са друге стране, систем ван равнотеже може да доспе у стање крхкости и дестабилизације, или чак да изгуби могућност комуникације и координације између својих активности, што систем води до фрагментације и распадања. Друго поглавље, поред одређених карактеристика, указује и на подложност критичне инфраструктуре утицајима који могу деловати на међузависности, као и поремећајима унутар њеног умреженог окружења.

Трећи део књиге посвећен је међународном карактеру критичне инфраструктуре, а у првом реду међународним стратешким интересима и ланцима снадбевања као једном виду економских веза који повлаче за собом и уједно захтевају кретање изван националних ка

међународним оквирима. У таквом окружењу, аутори подвлаче да „владе задржавају *de facto* коначни ауторитет … али оне више нису водећи играч на сцени". Тада на сцену ступају међународни споразуми који не обавезују само на дељење информација, већ и на заједничке захтеве по питању одређених активности као што су управљање ризиком и ланцима снабдевања који прелазе међународне границе. Посебно питање које се отвара јесте и подела одговорности између влада као јавног сектора (сектора који регулише) и приватног сектора (сектора који се регулише).

Јавно-приватно партнерство у области заштите или осигурања критичне инфраструктуре долази у први план у наредном поглављу где се, поред одређења и врста јавно-приватног партнерства, повлачи паралела између улоге влада и улоге приватног сектора у тој заштити, а посебно у областима успостављања нових капацитета и одржавања постојећих.

Пето поглавље посвећено је улози коју подаци и информације имају у заштити критичне инфраструктуре. Подаци, као основна запажања, након што се обраде постају информације које се интелигенцијом даље синтетизују у функцији доношења одлука, а све то уважавајући контекст. Аутори не само да разматрају нове трендове када су у питању прикупљање, коришћење и заштита информација и обавештајних података већ разматрају и употребу такозваног облака (енгл. *Cloud*) за складиштење података или повезивање поуздане рачунарске базе и корисничких заједница за размену података, уз указивање на евентуалне ризике коришћења истог и могућа решења. На крају, у ери све бржег развоја отворених извора података (енгл. *Open Sources*), истраживачи треба да воде рачуна између информација које се само преписују и знања које је генерисано.

Функционисање сваке заједнице почива на основним услугама, које су све више резултат конкуренције на отвореним тржиштима. Улога владе јесте да заштити пружање тих услуга и уједно заштити безбедност и економско благостање својих грађана. И на овом месту аутори указују на кључну разлику између јавног и приватног сектора, усмерености на јавно добро и усмерености на профит кроз теме као што су балансирање јавне безбедности и пословних операција и балансирање отпорности и финансијске одговорности.

Шта је отпорност? Шта она значи за критичну инфраструктуру? Да ли је довољно чекирати контролне листе и строго се придржавати правила и „добре праксе" да бисмо били сигурни да је критична инфра-

структура коју штитимо заиста заштићена и осигурана. Суштина заштите критичне инфраструктуре јесте обезбедити да „услуга очувања здравља, безбедности или економског благостања буде присутна, у употребљивом стању, када је то потребно и по разумној цени". Како томе треба приступити? Одговоре на ова, али и друга повезана питања могуће је пронаћи у седмом поглављу ове књиге, где аутори дају критички осврт на строго поштовање стандарда и уско посматрање контекста и ризика који се у њему јављају.

Поред отпорности, значајно место у разумевању критичне инфраструктуре има њена међузависност, којој аутори посвећују наредно поглавље. Аутори упозоравају на то да, с обзиром на растућу међусобну повезаност инфраструктуре, „способност да се идентификује, процени, управља и надгледа комплетан пакет зависности и међузависности било које организације постаје све сложенији и изван домета било којег самосталног ентитета". У овој ери „повећаног груписања инфраструктура" од изузетне је важности регулисање и усаглашавање међузависности, а посебно у четири кључна сектора: енергетике, транспортних система, комуникација и финансијских услуга… У супротном, може се догодити „савршена олуја" – потпуни колапс неколико инфраструктура на најмање регионалним нивоима.

Стручност и искуство аутора у областима физичке и сајбер безбедности огледа се и у размишљању о конвергенцији физичких и сајбер претњи критичној инфраструктури. Док су сајбер претње, односно сајбер безбедност обухваћени кроз више поглавља, аутори су разматрању физичке безбедности посветили девето поглавље књиге. Физичка безбедност, која се протеже на стратешком, оперативном и тактичком нивоу, није изгубила на значају услед јачања сајбер безбедности. Разумевање топографије мреже која пружа критичне услуге, процена ризика, која омогућава разумевање ризика, поштовање прописа и стандарда, а тек онда пројектовање и имплементирање мера физичке безбедности елементи су успешног одговора на ризике са овог аспекта заштите.

У десетом поглављу главна тема јесте промена парадигме управљања критичном инфраструктуром изазвана догађајима попут пандемије. Низ „тренутака из којих се може учити" произвео је промене у радној снази, измешта „локације" управљања, увећава значај дигиталне инфраструктуре, отвара питања заштите критичних информација и мрежа, као и сертификације у функцији свеобухватне процене управљачких, оперативних и техничких контрола неког система.

Наредно, или једанаесто поглавље се надовезује на промену парадигме обухватајући неке аспекте које би та промена парадигме требало да обухвати.

Последње поглавље аутори су посветили климатским променама као једној од претњи по критичну инфраструктуру и изазову за оне који се баве њеном заштитом. Неизвесности које доносе климатске промене, те неповољни временски услови условљавају управљање ванредним ситуацијама неизоставним елементом заштите критичне инфраструктуре. Способност да се издржи (да се идентификују критичне услуге на сваком нивоу стратешког, тактичког и оперативног нивоа), способност да се реагује и способност да се опорави три су кључна елемента у суочавању са елементарним непогодама. Аутори, избегавајући политичку дебату која постоји око ове теме, пишу још и о ПООД петљи (енгл. *OODA Loop*), која укључује посматрање, оријентисање, одлучивање и деловање, а може се користити у процесу доношења одлука.

Аутори су користили јасан језик за писање, што је садржај ове књиге учинило лаким за читање. Ова књига представља корисно штиво за заинтересоване читаоце како у научним тако и у стручним круговима, у јавном и приватном сектору, који желе да разумеју заштиту критичне инфраструктуре и импликације, те заштите на националну безбедност.

Значајан сегмент ове књиге јесу прилози у виду линкова значајних владиних и јавних интернет страница који омогућавају читаоцима да дубље истражују питања која их интересују. Међутим, имајући у виду брзу промену Интернет ресурса, као и могућност нестанка интернет адреса аутори су обезбедили секундарни извор референтног материјала како би се обезбедила конзистентност онога што је написано. Уз то, садржај књиге је употпуњен и мноштвом примера које аутори користе да поткрепе изнете ставове.

УПУТСТВО ЗА АУТОРЕ

Савремене студије безбедности је научни часопис на листи Министарства просвете, науке и технолошког развоја Републике Србије, у којем се објављују научни и стручни чланци из уже научне области наука безбедности, као и текстови из других друштвених наука и дисциплина, ако се у њима теоријски или емпиријски обрађују безбедносна питања или проблеми у вези са истраживањима у области безбедности.

Рукописи се достављају електронски преко система *SCIndeks* путем опције „Пријави рукопис".

УПУТСТВО ЗА АУТОРЕ

Факултет безбедности Универзитета у Београду[1]

Часопис *Савремене студије безбедности/Contemporary Security Studies* (раније Годишњак Факултета безбедности) је истакнути национални часопис на листи Министарства просвете, науке и технолошког развоја Републике Србије, који има за циљ да на динамичан и тематски фокусиран начин информише и пружи најновија сазнања из теорије и праксе у области студија безбедности. Часопис објављује актуелне и квалитетне научне чланке који се баве развојем идеја и побољшањем безбедносне праксе са фокусом на теоријским, методолошким и емпиријским истраживањима у следећим подобластима наука безбедности – глобалној/међународној, регионалној и националној безбедности, са подтемама као што су: стратешка, урбана, људска, корпоративна и еколошка безбедност.

Часопис излази два пута годишње, при чему су крајњи рокови за достављање рукописа 1. јун и 1. октобар.

АУТОРИ СУ ДУЖНИ ДА СЕ У ПРИПРЕМИ РУКОПИСА ПРИДРЖАВАЈУ СЛЕДЕЋИХ УПУТСТАВА:

Рукописи треба да буду обима једног ауторског табака, који износи 28.800 словних знакова са размацима, у Word-у (*.doc i .docx*). Прикази не треба да буду дужи од 8.000 словних знакова са размацима. У обим рада нису урачунати апстракти, референце и прилози. У изузетним случајевима може се објавити и рад већег обима, уколико уредништво процени да је такав обим неопходан.

---

[1] Факултет безбедности, Универзитет у Београду, Београд, godisnjakfb@fb.bg.ac.rs.

Рукописе треба писати ћириличним писмом, фонтом *Times New Roman* величине 12, са пагинацијом у доњем десном углу.

Наслов треба што верније да опише садржај чланка и пожељно је коришћење речи прикладних за индексирање и претраживање. Наслов писати великим словима, задебљано (*bold*), величина слова 14.

Испод наслова текста стоји име и презиме аутора чланка у *Italic*-у, величина слова 14.

Уз име и презиме, у виду фусноте аутор наводи назив институције у којој је запослен, њено седиште и своју електронску адресу. У овој фусноти аутор може да укаже читаоцима да поједини погледи изнети у чланку одражавају његов лични став, а не институције у којој је запослен. У овој фусноти аутор може да укаже читаоцима да је рад настао у оквиру одређеног пројекта, при чему је потребно навести назив и број пројекта.

Испод наслова стоји апстракт на српском језику обима 150–200 речи, који треба да пружи кратак информативан приказ чланка представљањем основних хипотеза, циља, метода и резултата истраживања и то тако да се може користити приликом индексирања у референтним периодичним публикацијама и базама података. Испод апстракта аутор прилаже највише 5 кључних речи на српском језику које најбоље описују садржај чланка. Подсећамо да је добар избор кључних речи предуслов за исправно индексирање рада у референтним периодичним публикацијама и базама података.

Основни текст треба да буде поравнат у складу са опцијом *justify*, фонт *Times New Roman*, величина слова 12, са проредом *single* и без прореда између пасуса.

Поднаслови се пишу великим словима, док се под-поднаслови пишу малим словима у *italic*-у; у оба случаја величина слова је 12. У оба случаја користити опцију *center*. Потребно је поставити проред пре и након (*paragraph-spacing*) на 6pt. Сваки пасус увући користећи опцију *paragraph-indentatiton first line* – 1.27cm.

Латинске, старогрчке и друге неенглеске речи и изрази у тексту наводе се у *italic*-у (нпр. *status quo, a priori, de facto*, итд).

Страно име и презиме треба писати у српској транскрипцији, с тим што се приликом првог помињања у тексту мора у загради навести како гласе у оригиналу (нпр. Џон Миршајмер (*John Mearsheimer*)).

У тексту користити само следећи облик наводника — „и". Када се унутар ових знакова навода налазе и додатни, унутрашњи наводници треба то учинити на следећи начин: ’и’.

Фусноте је неопходно писати на дну стране (опција *Footnote*), а ознаке за фусноте стављати искључиво на крају реченице. Текст фусноте треба да буде поравнат у складу са опцијом *justify*, фонт *Times New Roman*, величина слова 10, са проредом *single* и без прореда између фуснота.

Навођење референци

Референце се наводе у складу са АПА стилом (Publication Manual of the American Psychological Association).

У тексту се референца наводи у загради и то презиме аутора, година издања и број стране/страна: (Минин, 2021: 30) или (Močnik, 2015, str. 17–20).

Уколико је аутор организација наводити: (United Nations Development Program, 1994).

Уколико је реч о легислативи наводити: (Krivični zakonik, 2005, čl. 40).

МОНОГРАФИЈЕ

Навођење монографије треба да садржи презиме и иницијале имена аутора, годину издања (у загради), наслов монографије (курзивом), место издања и издавача.

Минин, Е. М. (2021). Хашки трибунал: поглед из Москве. Београд: Факултет безбедности.

Buzan, B., Ole Wæver, O., & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers. U tekstu: (Buzan, Ole Wæver & de Wilde, 2013: 55).

ЗБОРНИЦИ РАДОВА

Уколико се као референца наводи зборник радова у целини користити следећу форму:

Dragišić, Z., Mladenović, M. i Jeftić, Z. (Ur.) (2014). *Sadržaj bezbednosnih izazova Srbije na početku XXI veka*. Beograd: Inovacioni centar Fakulteta bezbednosti.

Томич, М. (2019). Актуальные проблемы безопасности и жизнедеятельности. Москва: Московский государственный областной университет.

ПОГЛАВЉА У КЊИЗИ И ЧЛАНЦИ У ЗБОРНИЦИМА РАДОВА

Поглавље у књизи или зборнику радова, као и рад у зборнику с научних конференција наводити на следећи начин:

Milošević, M., Banović, B. i Putnik, N. (2014). Projektovanje integralnog sistema školskog obezbeđenja – smernice i dileme. U Z. Dragišić, M. Mladenović, i Z. Jeftić (Ur.) (2014). *Sadržaj bezbednosnih izazova Srbije na početku XXI veka* (str. 81-89). Beograd: Inovacioni centar Fakulteta bezbednosti.

Tomic, M., Dinic, J., and Priorova, E. (2020). Security aspects of urban planning and design – "The european model". In: 7th International Academic Conference on Places and Technologies (p. 26). Belgrade: University of Belgrade – Faculty of Architecture.

ЧЛАНЦИ У НАУЧНИМ ЧАСОПИСИМА

Научни чланак треба да садржи презиме и иницијале имена аутора, годину издања (у загради), наслов чланка, пун назив часописа (курзивом), волумен (курзивом), број (у загради) и странице.

Kopanja, M. (2020). Geopolitička misao Sola Bernarda Koena: između prevaziđenosti i nedovoljne iskorišćenosti. *Међународни проблеми*, *72* (1), 61–100.

Dragišić, Z. (2010). Nacionalna bezbednost – alternative i perspektive. *Srpska politička misao, 28*(2), 217–232.

Кесић, Д. Б., Џелетовић, М., & Томић, М. (2020). Презентација криминалитета у медијима. *Социолошки преглед*, *54*(4), 1415–1436

Уколико се часопис издаје искључиво у електронској форми референца би требало да садржи исте елементе као и референца из штампаног часописа, али се након броја страница наводи "Retrieved from" (за стране референце), односно „Преузето са" (за домаће референце) и интернет адреса.

Said, A. A., & Funk, N. C. (2002). The Role of Faith in Cross-Cultural Conflict Resolution. *Peace and Conflict Studies, 9*(1). Retrieved from http://www.gmu.edu/programs/icar/pcs/ASNC83PCS.htm.

ЧЛАНЦИ У ДНЕВНИМ НОВИНАМА И ЧАСОПИСИМА

Уколико је у штампаној форми: Навођење ове врсте чланака треба да садржи презиме и иницијале имена аутора, датум када је објављен (у загради), наслов чланка, назив новина или часописа (курзивом), број стране.

Влаховић, Б. (02. новембар 2018). Трамп и Путин своде рачуне. Новости, стр. 8.

Уколико је у електронској форми: Навођење ове врсте чланака треба да садржи презиме и иницијале имена аутора, датум када је објављен (у загради), наслов чланка, назив новина или часописа (курзивом), УРЛ адресу.

Уколико нема аутора: Навођење ове врсте чланака треба да садржи назив новина или часописа, датум када је објављен (у загради), наслов чланка (курзивом), УРЛ адресу.

Milman, O. (June 08, 2023). Air pollution in US from wildfire smoke is worst in recent recorded history. *The Guardian*. https://www.theguardian.com/environment/2023/jun/08/air-quality-record-smoke-hazard-wildfire-worst-day-ever-canada-new-york.

Политика. (09. јун 2023). За сат времена вулкан Анак Кракатау два пута избацивао пепео. https://www.politika.rs/scc/clanak/556990/erupcija-vulkan-anak-krakatao-indonezija.

НАВОЂЕЊЕ ДОКУМЕНАТА

American Psychological Association (1973). *Ethical principles in the conduct of research with human subjects*. Washington, DC: American Psychological Association, Ad Hoc Committee on Ethical Standards in Psychological Research.

United Nations Development Program (1994). *Human Development Report*. New York: Oxford University Press.

International Organization for Standardization (2018). *Occupational health and safety management systems – Requirements with guidance for use* (ISO Standard No. 45001:2018).

Krivični zakonik (2005). Sl. glasnik RS, br. 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

НАВОЂЕЊЕ ИЗВОРА СА ИНТЕРНЕТА

За извор пронађен на Интернету треба навести тачан датум када му је аутор приступио, пошто се адресе садржаја повремено мењају. Након наведене референце навести:

... Преузето 09.06.2023. са ... / ... Retrieved 09.06.2023. from ...

Додатне напомене

Уколико се у тексту наводи више страница користи се средња црта без размака пре и после (... стр./pp. 15, 25, 30) или (... стр./pp. 15–17).

Уколико има више од три аутора користити „и др." за референце на српском језику, односно, „et al." за референце на страном језику.

Уколико страни зборник радова има само једног уредника, уместо скраћенице „Eds.", наводи се једнина „Ed.".

Чланак може садржати табеле и друге прилоге (попут географских карата, графикона, и сл.), с тим што је неопходно да се наведе њихов број и потпун наслов (нпр. Табела бр. 1. Разлика између рутинских и системских ризика или Прилог бр. 3. 2. Economic loss in 2021 from natural events by hazard). Уколико је прилог преузет од неког другог аутора или из неког документа неопходно је навести извор.

На крају чланка аутор даје списак коришћене литературе, а референце наводи према претходно представљеним правилима за цитирање извора. Редни бројеви се не стављају испред. Редослед референци на списку литературе утврђује се према првом слову презимена аутора или наслова документа. Уколико се у литератури наводи неколико референци чији је први аутор исти, најпре се наводе по хронолошком реду (од године објављивања рада) референце у којима је тај аутор једини аутор, а затим референце у односу на азбучни ред првог слова презимена другог аутора (уколико има коаутора). Уколико се наводи више референци једног аутора из исте године потребно је године означити словима а, б, в (нпр. 2014а, 2014б, 2014в).

Након списка коришћене библиографије аутор даје резиме на енглеском језику обима до 300 речи и кључне речи.

ПОСЕБНЕ ОБАВЕЗЕ АУТОРА РУКОПИСА

Аутори гарантују да приложени рукопис представља њихов оригиналан допринос, да није објављен раније и да се не разматра за објављивање у другој публикацији.

За сваки рукопис проверава се да ли је плагијат.

Рукописи који нису усаглашени са смерницама садржаним у Упутству за ауторе биће враћени аутору на исправку, а уколико ни након исправке не буду усаглашени неће бити узети у поступак рецензирања.

Рукописи се достављају преко система за онлајн уређивање часописа Асистент Српског цитатног индекса (SCIndeks), за који је потребно регистровати налог.

Уређивачки одбор

Универзитет у Београду
ФАКУЛТЕТ БЕЗБЕДНОСТИ

Београд, Господара Вучића 50
www.fb.bg.ac.rs

За издавача
Проф. др Младен МИЛОШЕВИЋ

Главни и одговорни уредник
др Милош ТОМИЋ

Секретар часописа
ма Јана МАРКОВИЋ

Лектор и коректор
Оливера ВЕЛИЧКОВИЋ

Графички дизајн
Биљана ЖИВОЈИНОВИЋ

Тираж
50 примерака

Припрема и штампа
ЧИГОЈА ШТАМПА

ISSN 3009-3759
ISSN 3009-3767 (Online)

CIP – Каталогизација у публикацији
Народна библиотека Србије, Београд

355/359

САВРЕМЕНЕ студије безбедности = Contemporary Security Studies / главни и одговорни уредник Милош Томић. – [Штампано изд.]. – 2023, бр. 1- . – Београд : Универзитет у Београду, Факултет безбедности, 2023- (Београд : Чигоја штампа). – 24 cm

Годишње. – Је наставак: Годишњак Факултета безбедности = ISSN 1821-150X. – Друго издање на другом медијуму: Савремене студије безбедности (Online)= ISSN 3009-3767

ISSN 3009-3759 = Савремене студије безбедности (Штампано изд.)

COBISS.SR-ID 123804681