

Стефан РАШОВИЋ¹

Војска Републике Србије

Докторанд на Факултету безбедности, Универзитета у Београду,

ДОИ: 10.5937/bezbednost2601121R

УДК: 004.89:351.861]:004.056.53

Прегледни научни рад

Примљен: 12. 6. 2025. године

Ревизија: 10. 3. 2026. године

Датум прихватања: 13. 3. 2026. године

Могућности употребе вештачке интелигенције у борби против сајбер тероризма

Апстракт: Четврта индустријска револуција довела је до значајног напретка у развоју вештачке интелигенције, која данас представља незаобилазну технологију у већини савремених области, од аутоматизације процеса и анализе великих количина података, до примене у медицини, индустрији и сајбер безбедности. У раду се разматра употреба вештачке интелигенције у борби против сајбер тероризма, феномена чији је простор одвијања сајбер простор. Циљ овог рада је да покаже на који начин напредни алгоритми разних техника вештачке интелигенције, пре свега машинског и дубоког учења, могу помоћи у детекцији ове претње, али и смањењу утицаја на критичну националну инфраструктуру. У првом делу рада биће представљени корени, дефиниције и карактеристике појма вештачке интелигенције, уз наглашавање значаја машинског и дубинског учења као најприменљивијих области вештачке интелигенције. Други део рада покушаће да пружи један свеобухватни приказ појма сајбер тероризма, елаборирајући његове дефиниције и карактеристике, притом дајући одговор на питање да ли је сајбер тероризам илузија или стварност. Напошетку, завршни део рада повезује ова два појма анализирајући улогу и могућности употребе вештачке интелигенције у борби против сајбер тероризма.

Кључне речи: вештачка интелигенција, машинско учење, дубоко учење, сајбер простор, борба, сајбер тероризам.

¹ stefan.rasovic95@gmail.com, ORCID 0009-0007-5318-0016

Увод

Модерно друштво карактерише четврта индустријска револуција, названа „информатичка револуција”, која је довела до повећане употребе персоналних рачунара, лаког приступа интернету и другим мрежама, али и појаве савремених уређаја информационо-комуникационе технологије. Ове карактеристике изузетно мењају живот појединаца који живе у време поменуте револуције, а долази и до појаве нових појмова као што су сајбер простор, сајбер тероризам, машинско и дубоко учење.

Вилијам Гибсон је сајбер простор дефинисао као „универзум рачунарских мрежа, свет у којем се мултинационалне компаније, друштва и други субјекти боре за освајање података и информација”, док Парсонс сматра да је то „врста заједнице сачињена од мреже рачунара у којој се елементи класичног друштва налазе у облику битова и бајтова, односно простор који креирају рачунарске мреже” (Вулетић, 2017: 174). Сајбер простор се везује за компјутерске или рачунарске мреже и представља вештачку творевину насталу као последицу односа између потребе друштва и разних технолошких иновација. То је нематеријални и неограничени простор креиран од рачунарских мрежа, који пружа велике могућности и у току четврте индустријске револуције представља доминантан начин комуникације.

Проблем код сајбер простора јесте његова безбједност, која се врло тешко остварује због изузетно великог опсега могућих сајбер напада. Они су врло вероватни због великог броја циљева који се налазе у сајбер простору. Коришћење сајбер простора за вршење терористичких акција представља нови заокрет у начину коришћења сајбер напада и долази до појаве појма сајбер тероризма, а у ситуацијама када напади задовољавају дефинисане критеријуме. У научним круговима се данас дискутује о томе да ли је овај феномен илузија или стварност, односно да ли се говори о нечему што тренутно постоји или о нечему што ће тек бити актуелно. Свакако, развој нових технологија које могу да повежу сајбер и физички свет чине претњу сајбер тероризма реалнијом и јако опасном.

Примена вештачке интелигенције може се представљати као „мач са две оштрице”, јер је могу користити сајбер терористи, али се може употребити и против њих. Најразвијеније области машинског, пре свега дубоког учења, омогућавају примену вештачке ин-

телигенције и у области сајбер безбедности, у циљу заштите система од потенцијалних напада сајбер терориста. Комбинујући анализу великих података и напредне алгоритме, вештачка интелигенција омогућава брже и прецизније препознавање претњи, чиме може постати кључни ресурс у борби против сајбер тероризма.

Корени, појмовно одређење и карактеристике вештачке интелигенције

Корени вештачке интелигенције сежу још у далеку 1943. годину када су Ворен Макалок (*Warren McCulloch*) и Волтер Питс (*Walter Pitts*) објавили рад који је званично признат као први из ове области. Они су предложили модел вештачких неурона у којем је сваки од неурона описан као „активан” или „неактиван”, при чему се активација дешавала као реакција на стимулацију довољног броја суседних неурона. Показали су да су рачунарске функције могле бити израчунате помоћу мреже повезаних неурона, као и да су логички конективи – и (*and*), или (*or*), не (*not*) и други – могли бити имплементирани кроз једноставне мрежне структуре. Заступали су став да би одговарајуће неуронске мреже могле и да уче. Током 1949. године Доналд Хеб (*Donald Hebb*) ствара тзв. Хебово учење које се огледало у правилу ажурирања за модификацију јачине веза између неурона, а актуелно је и данас. Следеће године, студенти Харварда Марвин Мински (*Marvin Minsky*) и Дин Едмондс (*Dean Edmonds*) направили су први рачунар заснован на неуронској мрежи (SNARC). Поред њих, као пионири у овој области појавили су се још Кристофер Стрејчи (*Christopher Strachey*), Артур Самјуел (*Arthur Samuel*), Ален Њуел (*Allen Newell*), Херберт Симон (*Herbert Simon*), Алан Тјуринг (*Alan Turing*), Џон Макарти (*John McCarthy*) и други (Russel, Norvig, 2021: 17). Најпознатији међу њима били су Алан Тјуринг, који је у свом чланку „Рачунарска машинерија и интелигенција” (*Computing Machinery and Intelligence*) представио Тјурингов тест, машинско учење, генетске алгоритме и учење уз подстицаје, и Џон Макарти, који је први употребио назив вештачка интелигенција 1956. године током одржавања конференције на Дартмут колеџу (*Dartmouth College*) у САД (Russel and Norvig, 2021: 18).

Макартијева прва дефиниција детерминисала је вештачку интелигенцију као „науку и технологију креирања интелигентних машина, посебно интелигентних рачунарских програма. То је повезано

за сличним задатком употребе рачунара за разумевање људске интелигенције, али вештачка интелигенција не мора бити ограничена на методе које су биолошки видљиве” сматрао је он (McCarthy, 2007: 2). Касније, у дефиницији Минског из 1968. Године, она је одређена као „наука чињења где машине раде ствари за које би била неопходна интелигенција уколико би их радио човек” (Ковачевић, 2023: 160). Расел (Russel) и Норвиг (Norvig) данас дефинишу овај појам као проучавање и дизајн „интелигентних агената” (у овом смислу рачунарских софтвера) који примају перцепције из свог окружења, а потом самостално предузимају акције усмерене на достизање циљева на интелигентан начин, а самим тим и побољшавају своје перформансе учењем и стицањем знања (Russel and Norvig, 2021).

Вештачка интелигенције је данас дефинисана и на институционалном нивоу, као и од стране компанија које су међу водећима у области информационих технологија. Европски парламент и Савет Европске уније у својој Уредби о утврђивању усклађених правила о вештачкој интелигенцији и измени ранијих уредби (Акт о вештачкој интелигенцији) од 13. јуна 2024. године дефинишу овај појам као „систем заснован на машинама, са циљем да ради са различитим нивоом аутономије, прилагодљив током примене, и способан да на основу улазних примљених података генерише излазне, тачније разна предвиђања, садржаје, препоруке или одлуке које могу утицати на физичко или виртуелно окружење” (Regulation EU 2024/1689, 2024: 46). Компанија Гугл (*Google*), која је тренутно једна од водећих из ове области, под овим појмом подразумева „скуп технологија које рачунарима и машинама дају могућност да извршавају низ напредних функција, односно да размишљају, уче и делују на начин који би обично захтевао употребу људске интелигенције или који укључује податке огромних размера које људи не могу да анализирају” (Google, 2024). Америчка компанија ИБМ (*IBM – International Business Machines Corporation*), тренутно можда и највећа компанија на свету која се бави информационим технологијама, овај појам посматра као технологију која рачунарима и машинама омогућава да симулирају људско учење, разумевање, решавање проблема, креативност, доношење одлука и аутономију (Stryker, Kavlakoglu, 2024).

Дакле, не постоји једна јединствена дефиниција овог појма, што говори о самој сложености али и тешкоћи да се овај појам јасно одреди. То ипак не би требало да нас чуди с обзиром да је вештачка ин-

телигенција „симулација или имитација нечега што и не разумемо у потпуности, тачније људске интелигенције.” Све док не буде постојао концензус око тога шта представља људска интелигенција, немогуће је рећи како се она може вештачки имитирати (Sheikh et al., 2023:16).

Вештачка интелигенција се може поделити на „слабу” (*Weak or Narrow AI*) и „јаку” (*Strong AI*). Слаба вештачка интелигенција обучава се само за одређену област (нпр. препознавање људских лица или особина, ћаскање са другим саговорницима, играње игрица и др.). Уколико се сагледа утицај овог облика данас стиче се утисак да је атрибут „слаба” погрешан (Bory et al., 2024: 3). Неки од примера овог облика су паметни лични асистенти: Еплов Сири (*Apple Siri*), Амазонов Алекса (*Amazon Alexa*), Мајкрософтова Кортана (*Microsoft Cortana*), Гуглов Џеминај (*Google Gemini*) и други, посебни софтвери као што су Чет ГПТ (*Chat GPT*), Вотсон (*IBM Watson*), самоуправљајући аутомобили и друго. С друге стране, јака вештачка интелигенција се дели на општу (*Artificial General Intelligence – AGI*) и супер вештачку интелигенцију (*Artificial superintelligence – ASI*). Прва представља вештачку интелигенцију која је на нивоу људске, док друга подразумева вештачку интелигенцију која је супериорнија у односу на људску. Иако оне тренутно постоје само теоретски, већина аутора сматра да њихово постојање, барем прве, није сувише далеко. Током 2016. године Шејн Лег (*Shane Legg*), један од оснивача Гуглове истраживачке лабораторије „Дубоки ум” (*Deep Mind*) проценио је да ће вештачка интелигенција бити на људском нивоу до средине 2020-их. Марк Закерберг (*Mark Zuckerberg*), главни извршни директор платформе Мета и Фејсбука, истакао је још 2015. године да је у наредних пет до десет година један од циљева бити бољи у односу на људе у свим људским чулима (виду, слуху, језику, општим сазнањима) (Mitchell, 2019).

Циљ вештачке интелигенције јесте опонашање људи и обављање радњи које су сличне људским. Дакле, системи вештачке интелигенције засновани су на алгоритмима који уче из података (Оташевић, Јовановска, 2025: 128). Она не може да размишља већ само да се усавршава учећи кроз сталну обуку; нема самосвест, тежњу ка друштвеној интеракцији и осећања, а ослања се на унос података и дате инструкције, јер само тако може да пружи тражени резултат. Она тежи ка перфекцији јер је заснована на јасно дефинисаним правилима и троши само два вата енергије. Њена предност је што је бржа од људске интелигенције у решавању проблема и што у доношењу одлука не

постоји утицај предрасуда, стереотипа и субјективности. Њени недостаци огледају се у споријем прилагођавању променама, смањеној креативности и иновативности, као и немогућности обављања више задатака истовремено (Димовски и Грујић, 2024: 70–72). Међутим, са употребом вештачке интелигенције долазе и проблеми, нови изазови и опасности. Проблем код употребе вештачке интелигенције јесте могућност њене злоупотребе, али и потенцијална опасност да машине надвладају људе и овладају светом било у облику интелигентних робота или неком другом. У претходним годинама о овим потенцијалним проблемима које не би требало игнорисати, иако је ризик за овако нешто мали, говорили су Бил Гејтс (*Bill Gates*), Елон Маск (*Elon Mask*) и Стивен Хокинг (*Stephen Hawking*) (Schneider, 2018: 92).

Машинско и дубоко учење као најприменљивије области вештачке интелигенције

У свакодневној комуникацији вештачка интелигенција се често меша са машинским учењем (*machine learning*), иако је машинско учење само једна од области вештачке интелигенције. Машинско учење се појавило 80-их година прошлог века и представља способност рачунарских система да генерализују на основу претходног искуства, односно скупа података о појавама или објектима који су предмет анализе, а које системи користе да би одговорили на питања о новим појавама са којима се раније нису сусретали. Уз помоћ интелигентне анализе података, машинско учење омогућава откривање нових и корисних образаца. Закључује се да компјутерски програм побољшава своје перформансе на одређеном задатку Т (*task*), мерењем перформанси преко метрика П (*performance*), стицањем нових искуства Е (*experience*), а то побољшање перформанси указује на процес учења (Ковачевић, 2023: 162).

Конвенционални систем машинског учења садржи следеће компоненте: податке о обуци и алгоритам који обрађује податке, доноси одлуке и предвиђања и користи се за одређивање приоритета, класификацију, повезивање, филтрирање, евалуацију односно оцењивање перформанси алгоритма и давање резултата (Ammar, 2019: 245–246). Постоји већи број техника или алгоритама машинског учења, а неки од најзначајнијих су линеарна и логистичка регресија (*linear and logistic regression*), стабла одлучивања (*decision trees*), К-најближи сусед

(*k-nearest neighbour*), кластеринг или груписање (*clustering*) и случајна шума (*random forest*) (Stryker, Kavlakoglu, 2024).

Машинско учење се према типу процеса одлучивања може поделити на надгледано (*supervised learning*), ненадгледано (*unsupervised learning*) и учење уз подстицај (*reinforcement learning*). У надгледаном учењу, интелигентни агент односно рачунарски софтвер учи пратећи улазне податке за које постоје излазне вредности. Излазне вредности могу бити реални бројеви (регресија) или номиналне вредности (класификација). Уколико су улазни подаци одређене слике, излазне вредности за те податке представљају ознаке (*labels*) које говоре да ли се на пример ради о „аутобусу” или „пешаку”. Задатак рачунарског софтвера јесте да новим улазним подацима предвиди и додели тачне излазне вредности, односно да новим сликама додели одговарајуће ознаке (Russel, Norvig, 2021: 653). У ненадгледаном учењу рачунарски софтвер има само улазне податке без излазних вредности и његов задатак јесте да открије скривене обрасце и законитости у подацима. Пример ненадгледаног учења јесте одређивање конфекцијских величина у виду кластера, а на основу тежине и висине људи, при чему су елементи једног кластера блиски међу собом (Ковачевић, 2023: 162). Учење уз подстицај подразумева да интелигентни агент учи из подстицаја, односно награди или казни, при чему он адаптира своје поступке на основу добијених повратних информација (Russel, Norvig, 2021: 789). Поједини аутори сматрају да поред ове основне поделе постоји и полунадгледано (*semi-supervised learning*), самонадгледано (*self-supervised learning*) и трансферно учење (*transfer learning*). Полунадгледано учење комбинује надгледано и ненадгледано учење коришћењем и означених и неозначених података за обуку модела вештачке интелигенције, док самонадгледано генерише имплицитне ознаке из неструктурираних података, уместо да се ослања на означене скупове података као извор надгледаних сигнала. Трансферно учење омогућава да се знање стечено кроз један задатак или скуп података користи за побољшање перформанси модела на другом повезаном задатку или различитом скупу података (Stryker, Kavlakoglu, 2024).

Ова технологија се користи у многим областима, као што су категоризација текста (по теми, осећањима или ставовима), машинско превођење, разумевање говорног језика, препознавање лица, сегментација тржишта, откривање безбедносних упада у мрежу и друго. С обзиром да се два и по квантилиона података дневно креира на гло-

балним мрежама и да је немогуће да толико података прегледају људи, машинско учење може имати ефикасну употребу у брзом и ефикасном генерисању, симулацији и процени адекватних и неопходних решења из обимне количине података. Суштински, сам алгоритам машинског учења користи се за предвиђање, што није нимало јединствена метода, при чему је врло тешко у многим ситуацијама објаснити логику добијених резултата јер често не постоји узрочна веза између улазних и излазних података. Непредвидиву природу оваквих система, поједини аутори називају „друштво црне кутије” (Ammar, 2019: 243).

Данас се све чешће помиње и појам дубоког учења (*deep learning*). Дубоко учење јесте област машинског учења која је заснована на вишеслојним дубоким неуронским мрежама које симулирају моћ доношења одлука људског мозга. Дубоке неуронске мреже се обично састоје из улазног слоја, више стотина скривених слојева и излазног слоја, за разлику од неуронских мрежа у класичним моделима машинског учења, који имају само један или два скривена слоја. Ови вишеструки слојеви могу да аутоматизују издвајање карактеристика из тих великих, неозначених и неструктурираних скупова података и самим тим предвиде шта ти подаци представљају. Развој дубоког учења омогућио је употребу полунадгледаног, самонадгледаног и ненадгледаног учења, учење уз подстицај и трансферно учење (Stryker, Kavlakoglu, 2024). Способност дубоког учења да аутоматски генерише сложене приказе или обрасце без потребе за ручним одабиром скупа карактеристика ставља га испред традиционалних алгоритама машинског учења. Овај процес доношења сложених одлука директно из извора информација означио је дубоко учење као *end-to-end* алгоритам, при чему се процес решавања неког проблема врши од почетка до краја без потребе за ручним интервенцијама корисника. Алгоритам сам закључује који су најважнији аспекти за задатак који решава (Millar et al., 2019: 104).

Технике машинског, пре свега дубоког учења, могу се користити за напад и за одбрану у сајбер простору. У смислу одбране, ове технике се могу користити за унапређење одбрамбених стратегија, чинећи их интелигентнијима и ефикаснијима, омогућавајући им да спрече или ублаже последице које напади могу изазвати, док се у смислу напада користе за унапређење софистицираности самих напада у циљу заобилажења одбрамбених стратегија. Ти напади могу бити усмерени и на саме моделе машинског и дубоког учења па се онда говори о су-

парничким нападима (*adversarial attack*). Методе ових техника се могу користити за детекцију упада, откривање малициозних софтвера, сајбер-физичке нападе, заштиту приватности података (Nguyen, Redd, 2021:1). Поставља се питање да ли се и на који начин могу користити у борби против сајбер напада који би се могли класификовати као сајбер тероризам. Пре дефинисања њихове улоге, неопходно је прво дефинисати појам сајбер тероризма са карактеристикама и дати одговор на питање да ли се говори о феномену који постоји само у теоријском оквиру или је у будућности могућа и његова примена од стране сајбер терориста.

Појмовно одређење сајбер тероризма

Сајбер тероризам представља кованицу коју је сковао Бери Колин (Barry Collin), виши истраживач на Институту за безбедност и обавештајне послове (*Institute for Security and Intelligence*) у Калифорнији још средином осамдесетих година 20. века (Collin, 1997). Центар за стратешке и међународне студије (*Center for Strategic and International Studies – CSIS*) у Вашингтону је у оквиру свог пројекта 1998. године објавио извештај под насловом: „сајбер криминал, сајбер тероризам, сајбер рат: спречавање електронског Ватерлоа”, што је био први велики искорак у овој области. Центар је сајбер тероризам дефинисао као политички мотивисане и унапред осмишљене нападе на информационе и компјутерске системе, компјутерске програме и податке, с циљем узроковања насиља над цивилним метама, чији су извођачи били појединци, поднационалне групе или кландестини актери, тачније тајни агенти (Berner, 2003).

Један од пионира изучавања овог појма била је и професорка Дороти Е. Денинг (*Dorothy E. Denning*) која је сајбер тероризам дефинисала као интеграцију сајбер простора и тероризма. Према њеним речима, овај појам се односио на политички мотивисане хакерске операције чији је циљ био изазивање економске штете или губитка људских живота, а као потенцијални пример навела је упад у систем контроле ваздушног саобраћаја и намерно узроковање судара два авиона. Она је нагласила квалификацију дела сајбер тероризма, при чему, да би неки напад био тако дефинисан, мора да има утицај у стварном свету, односно да превазилази утицај на оштећење података и информационе технологије (Denning, 2001: 2). „Није сваки

сајбер напад сајбер тероризам” говорила је Денинг (Denning, 2001: 21). Дефиниције Мауре Конвеј (*Maura Conway*), професорке на Универзитету Даблину, и Марка Полита (*Mark Pollit*), бившег директора Федералног истражног бироа (ФБИ), врло су сличне и усклађене са дотадашњим наративом, при чему је за њих овај појам представљао политички мотивисане нападе на информационе компјутерске системе, програме и податке извршене од стране поднационалних група или тајних агената, чија је последица насиље над цивилним метама (Broeders et al., 2021: 4).

Све поменуте дефиниције биле су комплементарне дефиницији тероризма која је важила у САД. Другим речима, сајбер тероризам је био повезиван са традиционалним терористичким тактикама, али се могао посматрати као нова стратегија која користи нове алате и искоришћава нове зависности, па према томе обједињава и два значајна страха, страх од технологије и страх од тероризма (Conway, 2007: 1).

С друге стране, постојали су аутори који су имали другачији приступ у дефинисању овог појма. Аналитичар Еван Колман (*Evan Kohlmann*) под појмом сајбер тероризма подразумевао је сваку примену тероризма на интернету, односно читав низ онлајн терористичких активности као што су комуникација, регрутовање, координација, планирање и прикупљање обавештајних података (Broeders et al., 2021: 4). Анализирајући дефиницију Дороти Денинг, Сара Гордон (*Sarah Gordon*) и Ричард Форд (*Richard Ford*) у свом делу „Сајбер тероризам?” креирали су два појма, и то „чист сајбер тероризам”, који је представљао нападе терориста на рачунаре, мреже и информације похрањене у њима, и појам „традиционалног сајбер тероризма” под којим се подразумевала ситуација када терористи користе различите факторе и способности виртуелног света у циљу извршења своје мисије (Gordon, Ford, 2002: 637). Поједини аутори су уместо овог термина користили термин информатички тероризам, при чему се Тимоти Томас (*Timothy Thomas*) сматрао творцем ове кованице. Међутим, његова дефиниција информатичког тероризма, као и начин манифестовања, није се поклапала у потпуности са дотадашњим концептом сајбер тероризма, па се може рећи да овај појам скоро и није заступљен (Дамњановић, 2009).

Сајбер тероризам данас нема јединствену дефиницију, па се најчешће може рећи да истраживачи дефинишу овај појам у складу са ставом који заступају везано за тероризам. Велики број дефиниција

указује на тешкоће при теоријском дефинисању, а то може утицати и на препознавање у пракси. Додатан проблем у анализи претњи сајбер тероризма представља ослањање на јавно доступне информације из отворених извора. Наиме, веома мало се зна о истраживањима која спроводе националне и међународне обавештајне службе, посебно када су у питању намере, мотивација и способности противника. Медији, штампа и средства јавног сервиса додатно усложњавају ситуацију називајући различите акте сајбер терористичким, пре свега због неразумевања проблема, као и потребе за увећањем профита продајом већег броја тиража са сензационалистичким насловима, текстовима, најавама и друго. Сензационализам додатно драматизује ситуацију, шири страх и панику међу становништвом и оставља утисак да је проблем све присутнији (Путник, 2012: 327).

Често постоји проблем и у дистинкцији појмова, јер није сваки сајбер напад препознат као сајбер тероризам, па је битна дистинкција појмова: сајбер тероризам, компјутерски или сајбер криминал и сајбер напад или сајбер инцидент. Појам компјутерског односно сајбер криминала јесте карактеристика савременог дигиталног доба и примене нових информационих технологија и он се односи на нове облике криминалног понашања који укључују поменућу злоупотребу компјутера, компјутерских система, мрежа, информационих технологија и интернета, али се односи и на традиционална кривична дела извршена коришћењем компјутера или као средства или као објекта (Грујић, 2018). Компјутерски односно сајбер криминал обухвата кривична дела везана за компјутерске мреже, где се оне користе као циљ напада (нападају се сервиси, функције, садржаји), као средство напада (онлајн продаја сексуалних услуга, људских органа, продукција и дистрибуција недозвољеног садржаја као што су дечја порнографија, нацистичке, расистичке и идеје верских секти) и као окружење за реализацију напада (мреже прикривају криминалне радње). Не постоји једна дефиниција која се односи на овај појам, али је заједничко постојање три елемента дефиниције, и то: средства извршења (рачунари или компјутери, рачунарски или компјутерски системи, мреже и подаци), начина извршења (злоупотреба компјутера или рачунара и других средстава) и последица дејства (имовинског, неимовинског или комбинованог карактера) (Павловић и Тошић, 2017).

Сајбер напади се, како наводе Фарат (*Farhat*), Макарти (*McCarthy*) и Рајсман (*Raysman*), могу дефинисати као сваки напади

иницирани рачунарима усмерени на веб-локацију, рачунарски систем или рачунар, при чему угрожавају поверљивост, интегритет и доступност рачунара или информација на њему (Giantas, Stergiou, 2018: 5). Правило 30 Талинског приручника о применљивости међународног права на сајбер ратовање (*Tallin Manual on the International Law Applicable to Cyber Warfare*) дефинише сајбер нападе као офанзивне или дефанзивне сајбер операције за које се може сматрати да ће довести до смрти или рањавања лица или уништења и оштећења објеката (Путник и Милошевић, 2017).

Може се рећи да сајбер тероризам има за циљ да изазове прекид у функционисању државе или њених виталних компанија, али и да изазове код јавног мњења изузетан осећај страха и несигурности. Као последица настаје забринутост за националну безбедност, јер сајбер тероризам може бити усмерен и на угрожавање критичне националне инфраструктуре, што би била једна од његових најопаснијих варијанти употребе. Изузетно озбиљни сајбер напади терориста на критичну националну инфраструктуру, који могу да доведу до физичког оштећења, уништења или смрти људи, а притом имају политичку конотацију, могу се сматрати сајбер тероризмом (Јонев, 2016). У САД је још Клинтонова администрација дефинисала „осам кључних инфраструктурних система коју могу бити мета напада: телекомуникације, банкарство и финансије, електрична енергија, дистрибуција и складиштење нафте и гаса, водоводни систем, саобраћај, владине и хитне службе” (White House, 1998).

Свеобухватно гледајући, може се рећи да су главне одлике сајбер тероризма следеће:

1. постоји употреба информационих или компјутерских технологија као оружја;
2. изражена је политичка, идеолошка, верска усмереност;
3. постоји оријентација ка симболици и публицитету;
4. материјална штета или људске жртве или претња тим последицама;
5. настанак и ширење страха изузетно великих размера.

Сајбер тероризам – илузија или стварност?

Сајбер тероризам је у многим западним земљама препознат као један од проблема националне безбедности, без обзира што у ака-

демским заједницама не јењава дискусија да ли је то манифестована или потенцијална претња, и колико је реална ако је потенцијална (Путник, 2012: 327). Бери Колин, креатор овог појма, сматрао је да су већ почетком 21. века постојали сценарији сајбер терористичких напада који су били технички могући. Потенцијалне мете будућих напада могле би да буду фабрике за прераду хране, фармацеутска постројења, постројења за производњу електричне енергије (термо, хидро и нуклеарне електране) као и нафтна постројења, системи за контролу ваздушног и железничког саобраћаја, цивилне путне комуникације, војна опрема и системи. Он је сматрао да ће сајбер терористи моћи да изазову ситуације у којима људи неће моћи да се хране, да се крећу и преживе, и да притом неће моћи да буду упозорени и да спрече нападача, који би се могао налазити било где (Collin, 1997).

Терористички напади који су се догодили у свету, а било их је поприлично, показали су да је ситуација врло напета и да од тероризма није безбедан нико. Већ је речено да би сајбер напади, уколико задовоље критеријуме сајбер тероризма, довели до несагледивих последица и прекида функционисања државе услед слома критичне инфраструктуре. Међутим, да би се закључило да ли се ради о сајбер тероризму или не, неопходно је разумети мотиве извршилаца односно терориста, као и то да ли су оспособљени за нападе које би квалификовали као сајбер тероризам и који би довели до потенцијалне штете.

Центар за изучавање тероризма и неконвенционалног ратовања дефинисао је факторе због којих се одређена терористичка група може одредити за сајбер тероризам, али и факторе одвраћања од употребе сајбер тероризма. Фактори који одређују употребу указују на то да сајбер тероризам има предност као стратегија пре свега због коришћења глобалних мрежа као што је интернет и велике зависности коришћења развијених информационих технологија, због трошкова за извођење напада који су нижи, али и због постојећег проблема на глобалном нивоу око међународне сарадње и неусклађености закона на пољу сајбер тероризма, па сајбер терористи могу проћи несанкционисано (Nelson et al., 1999: 24–31). С друге стране, аргументи за одвраћање од употребе односе се на то да терористи често имају више стратегија за употребу пре сајбер тероризма, да ови напади не могу да изазову деструкцију на светском нивоу као напади традиционалног тероризма, да су њихови ефекти непредвидиви, да су одбрамбени

системи жртве већ припремљени на напад због учесталости претходних напада, као и да пре долази до финансијских или губитака поверљивих и приватних информација него до губитака живота (Nelson et al., 1999: 32–35).

Важно је и разликовати сајбер тероризам од активности терориста у сајбер простору. У активностима у сајбер простору до сада је предњачила терористичка организација Исламска држава (ИСИС), ширећи разне религијске идеје, чиме је инспирисала мноштво напада широм света. ИСИС је пионир у вршењу сајбер напада у терористичке сврхе, при чему су у прошлости комбиновали сајбер нападе са физичким нападима. Пример за то је да су терористи након физичког напада на објекте француског сатиричног листа Шарли Ебдо (*Charlie Hebdo*) у Паризу напали и 19 хиљада француских веб-сајтова, а све због тога што им се није свидела карикатура бога Алаха (Giantas, Stergiou, 2018). Међутим, ИСИС није једина терористичка организација која дејствује у сајбер простору. О дејству терориста у сајбер простору говорило се још од 1998. године, када је Калид Ибрахим (*Khalid Ibrahim*) члан организације Харкат-ул-Ансар (*Harkat-ul-Ansar*) покушао да купи војни софтвер од хакера који су га украли из рачунара Министарства одбране. Привремена ирска републиканска армија (*PIRA*) која је сматрана терористичком организацијом, користила је услуге хакера с циљем набављања обавештајних података полицајаца и обавештајаца како би испланирала њихова убиства (Дамњановић, 2009: 247–248). Војно крило Ирске републиканске армије, Шин Фејн (*Sinn Féin*), шокирало је свет још 1997. године информацијом да ће са конвенционалних дејстава прећи на неконвенционалне облике дејстава укључујући и сајбер тероризам (у смислу напада на владине и пословне рачунарске системе) (Јевтовић, 2016: 102).

Један од специфичних напада који се догодио, а могао је имати и последице по критичну националну инфраструктуру, јесте напад на иранска нуклеарна постројења за обogaћивање уранијума у Натанзу између 2009. и 2010. године. Напад је постао познат под називом Стакснет (*Stuxnet*), како је назван малвер програм који га је изазвао, а имао је циљ да уништи системе за обogaћивање уранијума како би се ограничили капацитети Ирана за производњу нуклеарног оружја. У овој ситуацији Иранци нису ни били свесни да проблеми који су наступили нису случајно настали, већ да су они жртве сајбер напада (Мухић, 2019). На основу анализе, велики број извора је сматрао да

политичка позадина напада постоји и да иза напада стоји америчко-израелска сарадња, иако ниједна страна званично није признала злочин. Њујорк тајмс је чак објавио да су овај малвер развили САД и Израел због заједничких циљева, а на основу поверљивих информација бивших припадника служби безбедности. Стакснет напад је касније назван и првим светским сајбер дигиталним оружјем (Путник, 2022: 121–122). Међутим, и поред постојања политичке позадине, страх није наступио због касног откривања проблема те овај напад није био препознат као сајбер тероризам.

Министарство одбране САД било је најближе да докаже сајбер тероризам 2016. године, када је држављанин АП Косова и Метохије Ардит Феризи (*Ardit Ferizi*) осуђен на двадесет година затвора због неовлашћеног приступа заштићеним рачунарима и мрежама како би прикупио информације од важности за терористичку организацију ИСИС. Он је успео да упадне као систем администратор на сервер америчке компаније и при томе прибави личне информације десетине хиљада клијената, при чему око 1300 војних и владиних појединаца, а потом их проследи Јунеиду Хусеину (*Juneid Husein*), једном од најпознатијих пропагандиста ИСИС-а на друштвеним мрежама (Soesanto, 2020).

С обзиром да извршење напада у технолошком смислу није једноставно, поставља се питање да ли би терористи овај напад могли да изведу према плану и да исконтролишу штету. У логистичком смислу и даље је лакше уништити зграду експлозивном направом него запосести рачунаре непријатеља. За све то би терористи морали бити адекватно оспособљени и организовани (Путник, 2012). Такође, поставља се питање и да ли је неопходно да влада толики страх од помена сајбер тероризма данас. Сингер (*Singer*) и Алан Фридман (*Allan Friedman*) упоредили су у својој књизи овај појам са ТВ програмом „Недеља ајкула” (*Shark week*), чији је закључак био да је већа вероватноћа да се несрећа догоди у тоалету него да је изазове ајкула. И поред разумних закључака, људи се ипак више плаше ајкула, при чему су главни кривци медији који својим сензационалистичким вестима и драматизацијом шире панику и страх међу људима. Иста ситуација је и са појмом сајбер тероризма, сматрају поједини истраживачи (Papathanasakis et al., 2020: 335–336).

Општеприхваћено научно мишљење јесте да до данашњег дана није било сајбер терористичких напада и поред активности терориста

у сајбер простору и поменутих покушаја који су могли да доведу до оштећења критичне националне инфраструктуре. Један од главних разлога због чега није дошло до сајбер тероризма јесте ограничење капацитета сајбер простора да има директне узрочне последице у физичком свету. Раније поменути Талински приручник о међународном праву примењивом на сајбер ратовање заступао је овакав став у правилу 11, сматрајући да ниједан сајбер напад није достигао ниво физичке употребе силе. С обзиром да сајбер напади до сада нису имали физичке последице, они се нису могли сматрати сајбер тероризмом, сматрала је научна већина (Henschke, 2021: 73). Још један од разлога може бити и недостатак знања, средстава или мотивације код терориста (Путник, 2012).

Међутим, не може се рећи да је претња сајбер тероризмом илузија у данашњем мултиполарном свету. Поједини аутори сматрају да примена концепта интернет ствари (у даљем тексту: *ИоТ*)² данас чини појам сајбер тероризма смисленијим, пре свега јер овај концепт представља сајбер-физички систем. Многи елементи *ИоТ*-а успевају да остваре директну везу између кода и актуатора, односно елемента који ће након добијене команде кодом донети промену у физичком свету. Пример могу представљати даљински активирани браве на вратима паметног аутомобила, при чему ће комуникација између мобилног телефона власника аутомобила и аутомобила утицати да се врата откључају због команде кода (Henschke, 2021: 74). Приметна је и употреба вештачке интелигенције код аутономних *ИоТ*-а што додатно олакшава њихову примену (Henschke, 2021: 81–82). Овакви типови *ИоТ*-а се често могу наћи и у системима аутоматизованог даљинског

² Феномен *ИоТ* подразумева физичке предмете из нашег окружења који су повезани на интернет и могу да шаљу или примају податке. Фасцинантно је то да се било којој физичкој ствари може доделити *IP* адреса која ће јој омогућити слање података, а *IPv6* протокол омогућава велики број адреса. Сензори који су уграђени у овај систем најчешће имају више функција, и то од мерења и прикупљања података везаних за одређене параметре, преко слања тих података путем интернета до покретања акција на основу њих, али један сензор не може обављати све функције. С обзиром да се прикупља велика количина података, они се складиште и обрађују на облаку односно „клауду”. Треба напоменути да постоји разлика између „конвенционалних” *ИоТ* система, који подразумевају учешће људи и њихову анализу, и аутономних *ИоТ* система који имају способност да заобиђу људе и представљају комбинацију са коришћењем вештачке интелигенције (*AI*), где објекти осмишљавају податке, уче из њих и једни од других и мењају своје понашање (Milivojević i Radulski, 2020).

управљања (SCADA системи), који представљају такозвана „срца“ критичне инфраструктуре, али и системима за контролу индустријских процеса (ISC, DSC системи, нпр. у нуклеарним реакторима) (Ђекић, 2017). Комуникациона веза ових система заснована је на TCP/IP протоколу, што омогућава управљање са великих удаљености, али их чини рањивијим на сајбер нападе, које терористи све чешће изводе на ове системе, па и на сајбер тероризам (Путник, 2022: 94). Озбиљност ситуације показује и број ИоТ-а који се тренутно процењује на преко 18,8 милијарди, што је раст од 13,3% у односу на прошлу годину (IoT Analytics, 2024).

Закључује се да је претња од сајбер тероризма у будућности реална и да је не треба потценити. Сајбер терористи ће у будућности бити још немилосрднији са разноврснијим тактикама за остварење циљева, а сајбер простор ће у 21. веку бити још веће бојно поље, тако да постоји потенцијална опасност пре свега и због боље повезаности сајбер-физичког света. У прилог томе говори податак да се у свету дневно догоди и преко 14 милиона сајбер напада, што је изузетно велики број (Checkpoint, 2024). У складу с тим, државе би требало да буду свесне потенцијалне опасности, да се припреме превентивно за одбрану, да заштите своје становнике и да санирају штету. Поставља се питање да ли им у томе могу помоћи и савремени алати вештачке интелигенције, да ли би они брже открили потенцијалне сајбер претње и могли да их неутралишу, али и да спрече потенцијалне нападе сајбер тероризма у будућности.

Улога вештачке интелигенције у борби против сајбер тероризма

У данашњем времену се велики број активности, попут ширења мржње и подела, пропагандних активности и индоктринације, регрутовања, комуникације и координације, извршења екстремистичких и терористичких активности, одвија на интернету. Сматра се да је томе значајно допринела пандемија ковида 19 (COVID-19), при чему су процене да се данас и преко 40% састанака у екстремистичким и терористичким мрежама одвија виртуелно (Laytouss, 2022: 5). Неопходно је разумети како те групе функционишу, шта оне могу учинити у сајбер простору, да ли њихови сајбер напади могу начинити штету и задовољити критеријуме сајбер тероризма у будућности.

Сајбер напади вођени вештачком интелигенцијом знатно су бржи, непредвидљивији, могу да користе већи део сајбер простора и ресурса од оног који би човек могао да ангажује, па је веома битно да постоји јака сајбер безбедност у циљу одбране, пре свега критичне националне инфраструктуре. Овакви напади због својих карактеристика и алгоритама заснованих на техникама машинског и дубоког учења могу проћи неопажено, а у рукама сајбер терориста били би веома јако оружје и претња безбедности (Guembe et al., 2022).

С друге стране, вештачка интелигенција може знатно повећати ефикасност омогућавајући бржу и прецизнију идентификацију активности које представљају потенцијалну претњу. У борби против сајбер тероризма технике вештачке интелигенције могу се користити за: обраду слика, препознавање лица, транскрипцију и прислушкивање сајбер терориста, откривање аномалија односно *outliera*, предвиђање и откривање сајбер напада, надзор друштвених мрежа с циљем сузбијања екстремистичког и терористичког садржаја у сајбер простору. Обрада слика и препознавање лица могу довести до идентификације познатих или сумњивих лица за које се може сматрати да су сајбер терористи, и то у реалном времену и у различитим окружењима. Технологија скенира лица и упоређује са базама података познатих појединаца. Системи за откривање аномалија користе се како би се открили подаци који су значајно различити у односу на остале податке у оквиру постојећег скупа података и могу се користити у откривању сумњивих финансијских трансакција за потребе сајбер терориста, сумњивих образаца и онлајн комуникација (Akilili, 2024).

Развијени предиктивни модели на принципима машинског и дубоког учења могу се искористити за рано откривање и спречавање сајбер претњи. Ове технике могу играти кључну улогу у предвиђању будућих сајбер терористичких активности, анализирајући мрежни саобраћај, али и велике количине података. Алгоритми који подржавају предиктивне моделе самостално се програмирају, они уче из великог скупа података, прилагођавају своје параметре и уочавају специфичне обрасце понашања који могу бити карактеристични за сајбер терористе (Nadjia, 2023: 221). Конволуционе неуронске мреже (CNN), једна од варијанти вештачких неуронских мрежа, могу имати значајну употребу у области сајбер безбедности и управљању мрежним саобраћајем, иако се првенствено користе у области класификације слика, звука, обраде сигнала и друго. Оне се могу користити у

откривању и класификацији малициозног и необичног саобраћаја на мрежама, па и оног насталог од сајбер терориста, тако што омогућавају статистичке анализе метаподатака саобраћаја и анализе садржаја порука (Millar et al., 2019: 104). Метаподаци представљају информације о подацима, а у случају мрежног саобраћаја информације о томе одакле подаци долазе, где иду, колико су велики пакети података, који се протоколи користе. Статистичком анализом метаподатака може се утврдити да ли постоји нешто необично, јер уколико се појави велика количина саобраћаја непознатог извора, то може указивати на потенцијални сајбер напад. Анализа садржаја порука се односи на податке који се преносе преко мреже, као што су текст у е-пошти, код веб-странице или порука у апликацији за ћаскање. Њиховом анализом се могу препознати обрасци, речи или фразе које могу указати на малициозне намере, или пак структуре које одговарају познатим нападима. Примена конволуционих мрежа омогућава да се велике количине података које пролазе кроз мрежни саобраћај анализирају аутоматски, без потребе за ручним прегледом, што штеди време и ресурсе.

Веома битна активности јесте и анализа података са друштвених мрежа, пре свега у циљу сузбијања екстремистичког и терористичког садржаја у сајбер простору. Службе безбедности користе аналитику друштвених мрежа у циљу откривања оваквих садржаја. Проблем је што популарне друштвене мреже као што су Фејсбук (*Facebook*), Јутуб (*YouTube*), Твитер (*Twitter*), Инстаграм (*Instagram*) и Тик ток (*Tik Tok*) чине свега 16% интернет мреже, док се иза кулиса скрива паралелан свет такозване „дубоке мреже” (*Deep Web*) и њеног најмрачнијег дела „мрачне мреже” (*Dark Web*), који су према проценама већи око петсто пута од интернета (Јевтовић, 2016). Сајбер терористи и те како користе поменуте друштвене мреже уз још пар шифрованих апликација за размену порука као што су Телеграм (*Telegram*) и Там там (*Tam Tam*), али и анонимне клауд платформе за складиште података, па чак и „дубоку и мрачну мрежу” (Weimann et al., 2024: 18). Обрасци у коришћењу друштвених мрежа и интеракцијама могу обезбедити увиде у намере, припадност и потенцијалне планове појединаца, што га чини адекватним средством у превентивном решавању сајбер претњи (Akilili, 2024).

Треба напоменути да данас постоје и софтверски алати вештачке интелигенције засновани на принципима машинског и дубоког учења, развијени од стране појединих компанија. Они могу имати

разне намене, од идентификације сумњивих образаца до проактивног лова на претње. Ови алати нуде интелигентан и проактиван механизам одбране од сајбер напада притом превазилазећи традиционална решења сајбер безбедности. Ово се такође односи и на потенцијалне сајбер нападе који би могли да задовоље критеријуме сајбер тероризма. Најбољи и најефикаснији алати који се данас користе јесу *Dark Trace*, *Crowdstrike*, *SentinelOne*, *Check Point*, *Fortinet*, *Zscaler*, *Trelix*, *Vectra AI*, *Cybereason*, *Tessian*, *Palantir* и други (Rinko, 2024).

Иако примена вештачке интелигенције у борби против сајбер тероризма пружа значајне предности, постоје и изазови у вези с њеном употребом, који се односе на заштиту приватности и људских права, могућу злоупотребу и потребу за транспарентношћу у доношењу одлука. Алгоритми могу понекад бити пристрасни или подложни злоупотреби, што захтева пажљив развој регулаторних оквира и етичких стандарда. Неопходно је и успоставити баланс између безбедносних потреба и основних људских права, како би примена вештачке интелигенције остала у складу са принципима правде и транспарентности.

Закључна разматрања

У данашњем дигиталном свету, вештачка интелигенција постаје полако кључни фактор у борби против сложених изазова, међу којима су и сајбер напади који у будућности могу задовољити критеријуме сајбер тероризма. Разматрање појмовног одређења сајбер тероризма указало је на његову сложеност као феномена и неразумевање шта тачно овај појам подразумева. Дефинисањем основних одредница и карактеристика отклоњена је свака дилема, при чему је кроз анализу дат и одговор да сајбер тероризам данас не представља илузију, нарочито не услед развоја модерних система као што су аутономни ИОТ системи, који спајају сајбер и физички свет, а притом су и засновани на примени вештачке интелигенције. Њихова примена у *SCADA*, *DSC*, *ISC* и другим системима који представљају „срца критичне националне инфраструктуре” указује на потенцијалне опасности у будућности. Иако сајбер терористичких напада није било до данашњег дана, то свакако не значи да их неће бити у будућности.

У раду су истражене и могућности примене вештачке интелигенције у оквиру области сајбер безбедности, при чему су обрађени

њени основни концепти, технолошке могућности и специфична примена у овој области. Посебан акценат је стављен на примену напредних алгоритама машинског и дубоког учења, који омогућавају обраду слика, препознавање лица, транскрипцију и прислушкивање сајбер терориста, детекцију аномалија у мрежном саобраћају и предвиђање будућих сајбер напада, анализу друштвених мрежа, препознавање образаца у финансијским трансакцијама и аутоматизован одговор на претње. Примена дубоких неуралних мрежа омогућила је употребу више типова учења, од ненадгледаног па до учења уз подстицај. Ове могућности значајно су унапредиле ефикасност безбедносних система и смањиле време реакције на нападе. Треба напоменути да данас постоји велики број алата вештачке интелигенције развијених од стране компанија из области сајбер безбедности, а које, у циљу заштите у сајбер простору, користе друге компаније, организације, корпорације и државне службе.

Са непрекидним развојем технологије, очекује се да ће вештачка интелигенција наставити да игра централну улогу у заштити сајбер простора и очувању глобалне безбедности. У складу с тим, употреба вештачке интелигенције у овој области захтева и постојање одговарајућих етичких оквира и регулатива како би се обезбедила заштита приватности и људских права. Уколико тога нема, постоји ризик од злоупотребе технологије, што би могло нарушити поверење у њену употребу и угрозити легитимност њене употребе у борби против сајбер тероризма, чиме би се значајно умањила њена ефикасност и допринос глобалној безбедности.

Литература

1. Akilili, E. (2024). Artificial Intelligence in Counterterrorism: Navigating the Intersection of Security, Ethics and Privacy. <https://www.setav.org/en/assets/uploads/2024/04/P73En.pdf>. доступан 08.06.2025.
2. Ammar, J. (2019). Cyber Gremlin: social networking, machine learning and the global war on Al-Qaida-and IS-inspired terrorism. *International Journal of Law and Information Technology*, 27(3): 238–265. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3488894. доступан 04.06.2025.
3. Berner, S. (2003). Cyber-terrorism: reality or paranoia? *South African Journal of Information Management* 5(1): 1-5. <https://www>.

- researchgate.net/publication/228400022_Cyber-terrorism_reality_or_paranoia. доступан 07.05.2025.
4. Bory, P., Natale, S. & Katzenbach, C. (2024). Strong and weak AI narratives: an analytical framework. *AI & Society*. <https://link.springer.com/article/10.1007/s00146-024-02087-8#citeas>. доступан 01.06.2025.
 5. Broeders, D., Cristiano F., Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. *Studies in Conflict & Terrorism*, 46(12): 2426–2453. <https://www.tandfonline.com/doi/epdf/10.1080/1057610X.2021.1928887?needAccess=true>. доступан 08.05.2025.
 6. Checkpoint (2024). *Threatmap*. <https://threatmap.checkpoint.com/>. доступан 28.05.2025.
 7. Collin, B. (1997). Future of Cyberterrorism: The Physical and Virtual Worlds Converge. *Crime and Justice International* 13(2): 15-18.
 8. Conway, M. (2007). *Cyberterrorism: hype and reality*. In: Armistead, Leigh, (ed.) Information warfare: separating hype from reality. Potomac Books Inc, pp. 73-93. https://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf. доступан 08.05.2025.
 9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>. доступан 01.06.2025.
 10. Denning, D.E. (2001). Activism, Hacktivism, and Cyberterrorism: the Internet As a Tool for Influencing Foreign Policy. <https://faculty.nps.edu/dedennin/publications/Activism-Hacktivism-Cyberterrorism.pdf>. доступан 08.05.2025.
 11. Giantas, D., Stergiou, D. (2018). From Terrorism to Cyber-Terrorism: The Case of ISIS. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135927. доступан 28.05.2025.
 12. Google. (2024). What is Artificial Intelligence (AI). <https://cloud.google.com/learn/what-is-artificial-intelligence>. доступан 01.06.2025.
 13. Gordon, S., Ford, R. (2002). Cyberterrorism. *Computers & Security* 21(7): 636-647. <https://www.sciencedirect.com/science/article/abs/pii/S0167404802011161>. доступан 10.05.2025.

14. Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Sanz-Fernandez, L., Pospelova, V. (2022). *The Emerging Threat of Ai-driven Cyber Attacks: A Review*. *Applied Artificial Intelligence* 36(1). <https://www.tandfonline.com/doi/full/10.1080/08839514.2022.2037254?scroll=top&needAccess=true#abstract>. доступан 07.06.2025.
15. Henschke, A. (2021). *Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat*. In: Henschke, A., Reed, A., Robbins, S., Miller, S. *Counter-Terrorism, Ethics and Technology: Emerging Challenges at the Frontiers of Counter-Terrorism*. Springer pp. 71-88. <https://link.springer.com/book/10.1007/978-3-030-90221-6#bibliographic-information>. доступан 15.05.2025.
16. IoT Analytics (2024). *State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*. <https://iot-analytics.com/number-connected-iot-devices/>. доступан 19.05.2025.
17. Laytouss, B. (2022). *The Usage of Artificial intelligence (AI) in the Fight Against Modern Terrorism: Opportunities and Challenges*. Brussels International Center. <https://www.bic-rhr.com/sites/default/files/inline-files/The%20Usage%20of%20Artificial%20intelligence%20%28AI%29%20in%20the%20Fight%20Against%20Modern%20Terrorism%20%20Opportunities%20and%20Challenges%20-%20282%29.pdf>. доступан 06.06.2025.
18. McCarthy, J. (2007). *What Is Artificial Intelligence?*. Technical report. Stanford University. <https://www-formal.stanford.edu/jmc/whatisai.pdf>. доступан 07.06.2025.
19. Millar, K., Cheng, A., Chew Gunn, H., Lim, C.C. (2019). *Using Convolutional Neural Networks for Classifying Malicious Network Traffic*. In: Alazab, M., Tang, M. *Deep Learning Applications for Cyber Security*. Springer pp. 103-126. https://www.researchgate.net/profile/Mingjian-Tang/publication/331247533_Deep_Learning_Applications_for_Cyber_Security/links/5fb7e94ca6fdcc6cc6537873/Deep-Learning-Applications-for-Cyber-Security.pdf. доступан 08.06.2025.
20. Milivojević, S., Radulski, M. (2020). The "Future Internet" and crime: towards a criminology of the Internet of Things, *Crimen*, 11(3): 255-271.
21. Mitchell, M. (2019). *Artificial Intelligence: A guide for Thinking Humans*. Farrar, Straus and Giroux, US. <https://melaniemitchell.me/aibook/>. доступан 05.06.2025.

22. Nadjia, M. (2023). The role of artificial intelligence in combating cyber terrorism. *IUS ET SCIENTIA*, 9(2): 211-227. https://institucional.us.es/revistas/Ius_Et_Scientia/vol9_2/IUS_et_Scientia_vol_9_2_10_nadja.pdf. доступан 08.06.2025.
23. Nelson, B., Choi, R., Iacobucci, M., Mitchel, M., Gagnon, G. (1999). *Cyberterror: Prospects and Implications*. Center for the Study of Terrorism and Irregular Warfare, Monterey. <https://apps.dtic.mil/sti/tr/pdf/ADA393147.pdf>. доступан 18.05.2025.
24. Nguyen, T.T., Reddi, J.V. (2021). Deep Reinforcement Learning for Cyber Security. *IEEE Transactions on Neural Networks and Learning Systems*. <https://arxiv.org/abs/1906.05799>. доступан 05.06.2025.
25. Otašević, J., Jovanovska, M. (2025). Artificial Intelligence as a Support for Independent Living of People with Disabilities. *Srpska politička misao*, 94(6): 121-134.
26. Papathanasaki, M., Dimitriou, G., Maglaras, L., Vasileiou, I., Janicke, H. (2021). *From Cyber Terrorism to Cyber Peacekeeping: Are we there yet?* In: Proceedings of the 24th Pan-Hellenic Conference on Informatics (PCI '20). Association for Computing Machinery, New York, pp. 334–339. <https://dl.acm.org/doi/abs/10.1145/3437120.3437335>. доступан 30.05.2025.
27. Rinko, S. (2024). 10 Best AI Security Tools for 2024: Next-Gen Cyber Solutions. https://www.eweek.com/artificial-intelligence/best-ai-security-tools/?utm_source=chatgpt.com. доступан 09.06.2025.
28. Russel, S., Norvig, P. (2021). *Artificial Intelligence: A modern approach* (4th edition). Pearson Education, Inc., London. <https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf>. доступан 06.06.2025.
29. Sheikh, H., Prins, C., Schrijvers, E. (2023). *Mission AI: The New System Technology*, Springer, Cham. https://www.researchgate.net/publication/367606557_Mission_AI_The_New_System_Technology. доступан 05.06.2025.
30. Soesanto, S. (2020). Cyber Terrorism: Why it exists, why it doesn't, and why it will. *ARI* 47: 1-7. <https://media.realinstitutoelcano.org/wp-content/uploads/2021/11/ari47-2020-soesanto-cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will.pdf>. доступан 18.05.2025.

31. Stryker, C., Kavlakoglu, E. (2024). What is artificial intelligence (AI)?. IBM. <https://www.ibm.com/think/topics/artificial-intelligence>. доступан 05.06.2025.
32. Weimann, G., Pack, A., Sulciner, R., Scheinin, J., Rapaport, G., Diaz, D. (2024). Generating Terror: The Risks of Generative AI Exploitation. *Ctc Sentinel*, 17(1): 17-24. <https://ctc.westpoint.edu/generating-terror-the-risks-of-generative-ai-exploitation/>. доступан 08.06.2025.
33. White House. (1998). *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/white-paper-clinton-administrations-policy-critical-infrastructure#0-0>. доступан 15.05.2025.
34. Вулетић, Д. (2017). Сајбер безбедност. *Интегрална безбедност Републике Србије*, 169-184.
35. Дамњановић, И. (2009). Постоји ли сајбер тероризам?. *Политичка ревија*, 8(1): 237-254.
36. Димовски, Д., Грујић, З. (2024). Могућности употребе вештачке интелигенције у превенцији криминалитета. *Безбедност*, 66(2): 67-88.
37. Ђекић, М. (2017). Безбедност интернет ствари. *Техника – квалитет ИМС, стандардизација и метрологија*, 17(2): 309-312.
38. Грујић, З. (2018). Компјутерски криминалитет: специфичности и савремени изазови. *Зборник радова Правног факултета у Нишу*, 46(80): 325-346.
39. Јевтовић, З. (2016). Улога друштвених мрежа у промоцији сајбер тероризма. *Политика националне безбедности*, 1/2016: 99-119.
40. Јонев, К. (2016). Сајбер тероризам и употреба сајбер простора у терористичке сврхе. *Безбедност*, 58(2): 206-222.
41. Ковачевић, А. (2023). *Машинско учење и сајбер безбедност*. У Зборник радова: „Стратешки и нормативни оквир Републике Србије за реаговање на савремене безбедносне ризике”, Факултет безбедности Универзитета у Београду, Београд, стр. 158-173.
42. Мухић, Е. (2019). Сајбер тероризам као нови облик ратовања: Секундарна анализа случаја „STUXNET” и теоретски оквири сајбер тероризма. *Криминалистичке теме* 19(5): 227-243.
43. Павловић, М., Тошић, Д. (2017). Кривичноправна заштита безбедности рачунарских података. *Часопис из области економије, менаџмента и информатике БизИнфо*, 8(1): 41-53.

44. Путник, Н. (2012). *Кибер ратовање – нови облик савремених друштвених конфликта*. Докторска дисертација. Факултет безбедности, Београд.
45. Путник, Н., Милошевић, М. (2017). Сајбер безбедност и заштита од високотехнолошког криминала у Републици Србији – стратешки и правни оквир. *Култура полиса*, 14(33): 177-191.
46. Путник, Н. (2022). *Сајбер рат и сајбер мир*. Иновациони центар Факултета безбедности, Београд.

Potential Applications of Artificial Intelligence for Countering Cyberterrorism

Abstract: *The Fourth Industrial Revolution has led to significant progress in the development of artificial intelligence, which today represents an indispensable technology across various modern fields, ranging from automated data analysis and process automation to applications in industry and cybersecurity. This paper examines the potential applications of artificial intelligence for countering cyberterrorism, a threat located primarily in cyberspace. The aim of this paper is to demonstrate how advanced algorithms from various artificial intelligence techniques, particularly machine learning and deep learning, can aid in detecting this threat while also mitigating its impact on critical national infrastructure. The first part of the paper outlines the origins, definitions, and key features of artificial intelligence, emphasizing the importance of machine learning and deep learning as its most widely applied branches. The second part offers a comprehensive overview of the concept of cyberterrorism, assessing its definitions and characteristics while addressing the question of whether cyber terrorism is an illusion or a reality. Finally, the concluding section of the paper links these two concepts by analysing the role and potential applications of artificial intelligence in countering cyberterrorism.*

Keywords: *artificial intelligence, machine learning, deep learning, cyberspace, counter, cyberterrorism.*