УДК: 351.78:004.738.5(497.11)
DOI: https://doi.org/10.22182/pnb.2212022.8
Прегледни рад

Политика националне безбедности
Година XIII, vol. 22
број 1/2022.
стр. 171-188

Ивана Лукнар*

Институт за политичке студије, Београд

ЗЛОУПОТРЕБА ИНФОРМАЦИОНИХ И КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА: ПОЈАМ И УРЕЂЕЊЕ У РЕПУБЛИЦИ СРБИЈИ

Сажетак

Бројни изазови потресају савремену светску сцену. Вишеструка криза (здравствена, економска, еколошка, рат у Украјини и миграције) створиле су тензије на међународном нивоу. Информационе и комуникационе технологије (ИКТ) су оруђе од виталног значаја за функционисање земаља широм света. У постојећим кризним условима безбедност ИКТ још више добија на важности, с'обзиром да се актуелне тензије и сукоби могу лако прелити у сајбер простор. Предмет рада су информационе и комуникационе технологије и њихова могућност злоупотребе. Рад пружа систематски прегледни опис теме и има за циљ да укаже на проблем злоупотребе ИКТ и подстакне размишљање о овом проблему. Методом анализе садржаја приказани су: историјски развој савремених ИКТ, кључни концепти у вези са злоупотребом ИКТ (концепт високотехнолошког криминала, концепт критичне инфраструктуре, сајбер тероризам) и уређење проблема на примеру Републике Србије.

Кључне речи: ИКТ, високотехнолошки криминал, критична инфраструктура, сајбер тероризам, сајбер безбедност

* Контакт: ivanaluknar@gmail.com

РАЗВОЈ ИНФОРМАЦИОНИХ И КОМУНИКАЦИОНИХ ТЕХНОЛОГИЈА

Научно-технолошка револуција је изменила свет у целости. Масовна примена савремених информационих и комуникационих технологија довела је до промена у готово свим друштвеним делатностима, па и у свакодневном животу (комуникације, настанак онлајн заједница и др.). Развој информационих и комуникационих технологија (ИКТ-а) може се посматрати као двоетапни процес (Bezzina&Terrab, 2005, 17).У првој етапи технолошких промена издвојила су се три различита тренда:

1. дигитализација (*digitalization*),
2. компјутеризација (*computerization*) и
3. технологија пакетног преноса (*packet switched technologies*).

Поменути трендови имали су радикалан утицај на ИКТ пејзаж и његов даљи развој и формирање нових технологија.

Дигитализација је основни предуслов за даљи технолошки развој; омогућила је синергију и повезивање ИКТ у цео ланац, проширење ресурса и приступ мрежи на исплатив начин.У „Закону о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању“ стоји: „дигитализација је конверзија документа из облика који није електронски у електронски облик“ („Службени гласник РС“, бр. 94/17, 52/21).Дигитална технологија има широку примену у свакодневном животу. Омогућила је превођење неког објекта као што је: документ, слика, сигнал, звук из аналогног у дигитални облик. Другим речима дигитализација значи „говорити и о виртуелној стварности, дигиталним специјалним ефектима, дигиталном филму, дигиталној телевизији, електронској музици, видео играма, мултимедијима, светским мрежама“ (Гир, 2011, 17).

Примена рачунара несумњиво је представљала историјски корак у развоју савремених ИКТ. Први југословенски дигитални рачунар био је CER-10 (Цифарски електронски рачунар) који је 60-тих и 70-тих годинаXX века производио Институт Михајло Пупин. Воја Антонић је конструисао домаћи рачунар „Галаксија“ за најшири круг корисника у својој кућној радионици. У Институту Михајло Пупин у Београду средином 1980-тих година конструисана је серија TIM-100 микрорачунара чија је основна намена била шалтерска употреба. Употреба рачунара у Републици Србији је у сталном порасту (Табела 1), што потврђују последњи подаци објављени у Стратегији развоја информационог друштва и информационе безбедности у Републици

Србији за период од 2021. до 2026. године („Службени гласник РС“, бр. 86/2021).

Табела 1. Употреба рачунара („Службени гласник РС“, бр. 86/2021)

Употреба рачунара	
Домаћинства	коришћење рачунара у домаћинствима у сталном порасту -74,3 % највеће коришћење рачунара у Београду- 91,5% најмање коришћење рачунара у Војводини- 66,8% веће коришћење рачунара у градским срединама-81,6% мање коришћење рачунара у осталим срединама- 62,8%
Појединци	коришћење рачунара код појединаца у сталном порасту-72,4% 19,8% лица никада није користило рачунар 14,8% корисника рачунара има ниже од средњег образовања највише рачунаре користе студенти - 99,8% најмање рачунаре користе остали (пензионери...)- 52,3% највише рачунаре користе млади од 16-24. године 96,2 % користе жене, а 100% мушкарци најмање рачунаре користе старији од 55-74. године и у тој доби постоји разлика између мушкараца 59,6 % и жена 48,9 %

Технологија пакетног преноса омогућила је ефикаснију употребу расположивих технолошких средстава пружајући платформу за испоруку више услуга унутар мреже. Пол Баран (Paul Baran) је развио концепт пакетног преноса који подразумева протокол у којем се одређена информација (порука) раздваја на пакете, а потом шаље различитим путевима широм мреже до жељене дестинације где се делови поруке уједињују (реорганизују) у првобитну информацију (поруку). Баранова „архитектура“ мреже је направљена да омогући несметану комуникацију (Baran, 1964).

Друга етапа технолошких промена се такође може образложити кроз три различита тренда:

1. појава Интернет протокола (the emergence of the Internet Protocol);

2. нове инфраструктуре (new infrastructure) и

3. конвергенције (*convergence*) (Bezzina&Terrab, 2005, 18).

Појава Интернет протокола омогућила је фундаментално раздвајање између слојева преноса (*transmission layer*) и сервисаи апликације. Појава нових инфраструктура: инфраструктурне мреже које нису предвиђене затранспорт комуникација, него да пружају струјну подршку/линију, оне које користе бежичне и жичане везетехнологије (*WiFI*/*WiMAX*), оптичка влакна и хибридне оптичко-електричне инфраструктуре, омогућиле су настанак нове инфраструктурне мреже која служи за транспорт комуникација. Трећи технолошки тренд конвергенција омогућио је превазилажење специфичности

различитих медија, јер пружа могућност употребе истих или сличних материјала. Дигитализација, IP и напредни комуникациони протоколи/технологије омогућавају спајање различитих услуга које припадају засебним мрежама. Конвергенција се може изразити као способност различитих мрежних платформида спроводе суштински сличне врсте услуга и омогућава повезивање потрошачких уређаја као што су телефон, телевизија и персонални рачунар. Конвергенција је омогућила технолошко и тржишно спајање телекомуникацијске и информатичке индустрије и технологије, и из темеља је изменила ове индустријске гране. Упркос томе што су фиксна и мобилна телефонија имале различите развојне путеве, њихова конвергенција је уследила као последица промене корисничких навика. У будућности можемо очекивати нове сервисе који ће омогућити нове побољшане начине пословања, комуникацију, поједноставити приступ информацијама, забави и др.

Технологија не пружа једино услуге већ има и друштвену димензију која се остварује кроз нове начине пословања и интеракције са друштвом. Поводом научно-технолошког развоја у Стратегији националне безбедности Републике Србије („Службени гласник РС”бр. 94/2019) наведено је: „насупрот очекивањима да ће бити повећан ниво одговорности свих укључених субјеката у погледу коришћења научних достигнућа у општем интересу и за добробит читавог човечанства, процењује се да ће развој науке и технологије наставити да буде подложан различитим видовима злоупотреба, што ће доводити до негативних безбедносних импликација“(„Службени гласник РС”бр. 94/2019).

УРЕЂЕЊЕ ИНФОРМАЦИОНОГ ДРУШТВА У РЕПУБЛИЦИ СРБИЈИ

Развој савремених ИКТ производа има двоструки ефекат. Односно, ИКТ истовремено могу да произведу како позитиван тако и негативан ефекат у зависности од начина и сврхе примене. Информационе и комуникационе технологије истовремено представљају средство за извршење, али и откривање криминалних радњи. Јер, поред тога што служе за функционисање и одржавање критичних државних инфраструктура и омогућавају пружање сајбер безбедносне подршке, контроле и превенције; ИКТ истовремено с друге стране омогућавају повезивање, комуникацију и функционисање актера унутар сложених криминалних система, као што су организовани криминал и тероризам.

Влада Републике Србије усвојила је различите стратегије, уредбе и акционе планове како би уредила област информационог друштва.У прилогу је дванаест најзначајнијих стратегија које су директно и индиректно обликовале уређење информационог друштва у Републици Србији:

1. „Стратегија за борбу против прања новца и финансирања тероризма за период 2020 - 2024.године“ („Службени гласник РС“, бр. 14/20)
2. „Национална стратегија за спречавање и борбу против тероризма за период 2017 - 2021. године“ („Службени гласник РС“, бр. 94/17)
3. „Стратегија националне безбедности Републике Србије“ („Службени гласник РС“, 94/19)
4. „Стратегија одбране Републике Србије“ („Службени гласник РС“, бр. 94/19)
5. „Стратегија за борбу против високотехнолошког криминала за период од 2019. до 2023. године“ („Службени гласник РС“, бр. 71/18)
6. „Стратегија развоја вештачке интелигенције у Републици Србији за период 2020 - 2025“ („Службени гласник РС“, број 96/19)
7. „Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године“ („Службени гласник РС“, бр. 86/21)
8. „Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године“ („Службени гласник РС“, бр. 68/10)
9. „Стратегија развоја индустрије информационих технологија за период од 2017. до 2020. године“ („Службени гласник РС“, бр. 95/16) чијим објављивањем је престала да важи претходно донешена „Стратегија развоја и подршке индустрији информационих технологија“ („Службени гласник РС“, бр. 25/13)
10. „Стратегија развоја мрежа нове генерације до 2023. године“ („Службени гласник РС“, бр. 33/18)
11. „Стратегија заштите података о личности“ („Службени гласник РС“, бр. 58/10)
12.„Стратегија развоја дигиталних вештина у РС за период 2020 - 2024“ („Службени гласник РС“, број 21/20).[1]

1 Имајући у виду да је ово прегледни рад, као и ограничен број страна, у раду су наведене поменуте стратегије. За детаљнији увид у Стратегије можете погледати наведене web адресе.

У Стратегији националне безбедности Републике Србије („Службени гласник РС"бр. 94/2019) у тачки 2 препознати су негативни ефекти развоја савремених информационих и комуникационих технологија,односно да „њихова присутност у свим сферама друштва има за последицу и пораст високотехнолошког криминала и угрожавање информационо-комуникационих система" („Службени гласник РС"бр. 94/2019).

Република Србија је препознала индикације злопупотребе ИКТ. Међутим, сајбер претња не постоји у вакууму, па одговоре треба формулисати и спровести „у контексту шире глобалне безбедносне политике"(Mandel, 2017). Савремену друштвено-политичку ситуацију карактерише вишеструка криза. У таквој ситуацији питања рањивости ИКТ, сајбер безбедности, високотехнолошки криминал и сајбер тероризам више него икада добијају на својој актуелности и потребно им је посветити посебну пажњу. Ефекти здравствене COVID-19 кризе, драстичне мере изолације и прекид трговине капитала и услуга за време ванредног стања довели су до економске кризе, што уз истовремену енергетску, еколошку кризу, рат у Украјини и миграције производи појачане тензије и ствара климу за различите сукобе. У таквим условима се незадовољство и тензије лако могу прелити у сајбер простор. То има за последицу пораст дела која убрајамо у високотехнолошки криминал и на међународном нивоу повећану претњу од сајбер тероризама (Luknar 2020a; Luknar 2020b).

ВИСОКОТЕХНОЛОШКИ КРИМИНАЛ

У употреби је неколико термина рачунарски криминал, високотехнолошки криминал, сајбер криминал да означе илегалну активност за чије извршење је употребљена рачунарска технологија.[2] Под злоупотребом рачунара подразумева се намерна активност којаје повезана са рачунаримана било који начин, где жртва трпи губитак а извршилац активности остваруједобит.

Високотехнолошки криминал према Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала: „представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. Под

2 Појмови рачунарски криминал и злоупотреба рачунара су први пут дефинисани у Министарству правде САД 1983. године.

производима у електронском облику посебно се подразумевају рачунарски програми и ауторска дела која се могу употребити у електронском облику" („Службени гласник РС", бр. 61/05, 104/09).

Дакле, високотехнолошки криминал подразумева било коју криминалну активност која је извршена посредством мреже и алата савремених информационих и комуникационих технологија и/или унутар сајбер простора, јер се рачунари и рачунарске мреже могу јавити не само као средство већ и као објекат извршења криминалне активности.

Кривичним закоником (члан 298-304) су дефинисана „кривична дела против безбедности рачунарских података:

- Оштећење рачунарских података и програма;
- Рачунарска саботажа;
- Прављење и уношење рачунарских вируса;
- Рачунарска превара;
- Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података;
- Спречавање и ограничавање приступа јавној рачунарској мрежи
- Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података" (Службени гласник РС, бр. 85/05, 88/05- исправка, 107/05- исправка, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19).

На сајту Министарства унутрашњих послова поред претходно поменутих кривичних дела стоји:

- „кривична дела против интелектуалне својине, имовине и правног саобраћаја код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику
- кривична дела где се рачунари и рачунарске мреже јављају као средство извршења кривичних дела преваре, код злоупотреба платних картица на интернету, злоупотреба у области електронске трговине и банкарства, злоупотребе деце у порнографске сврхе на интернету (тзв. дечја порнографија), говора мржње на интернету (ширење националне, расне, верске мржње и нетрпељивости и сл.)" (Министарство унутрашњих послова, е-извор)

Високотехнолошки криминал је у порасту. Његови учиниоци су током времена све организованији приликом извођења илегалних

онлајн активности и прибегавају све сложенијим врстама напада што нарочитозабрињава све оне који се боре са овом врстом криминала. Еволуција високотехнолошког криминала јестимулисала раст и развој индустрије сајбер безбедности. Предузећа у непрекидној трци са конкуренцијом настоје да одрже и прошире своје тржиште, усвајају иновације. Брзина и ефикасност имплементације технолошких иновација у привреду је критична за безбедност пословања. Јер, предузећа усвајају иновације како би постигле раст продуктивности, економски раст и да би остале конкурентне. Отуда примену савремених технологија треба да прати поузданост и безбедна примена како би крајњи утицај иновације имао вишеструкипозитиванефекат на пословање. Међутим, трошкови које компаније треба да издвоје за одбрану од високотехнолошког криминала из године у годину расту. На пример у САД-у: „порасли су за 62% са 7,2 милиона долара у 2014.години на 11,7 милиона долара у 2017.“ (Schirrmacher et al., 2018).

Потреба за све озбиљнијим улагањем у мере заштите и одбране од ове врсте криминала, као и неједнака могућност корисника ИКТ да поменуте мере заштите обезбеди остављају простора за различите сајбер малверзације. Савремено стање додатно компликује и правна регулатива чије је благовремено прилагођавање и праћење развоја злоупотреба савремених ИКТ упитно. Откривање и доказивање дела високотехнолошког криминала није једноставан посао. Постоје различити изазови са којим се суочава полиција у Србији и тамна бројка учињених дела која убрајамо у област високотехнолошког криминала. Писарић наводи следеће потешкоће за доказивање дела ове врсте криминала: „неусклађеност правне регулативе са савременим облицима извршења кривичних дела; недовољна техничка опремљеност и оспособљеност полицијских службеника везана за откривање извршилаца у онлајн окружењу;недостатак операционалних обука које би омогућиле да полицијски службеници који се баве спречавањем високотехнолошког криминала буду довољно обучени и технички опремљени за вршење ових задатака; потешкоће у откривању извршилаца кривичних дела који користе лажне идентитете у онлајн окружењу, посебно када се у обзир узме чињеница да је у великом броју случајева међународна полицијска сарадња лоша, а да у некима чак и не постоји; потешкоће у откривању тачне локације извршења кривичног дела, пошто се ова кривична дела врше са многих места широм света, а у великом броју случајева извршиоци кривичних дела користе мреже са јавним приступом“ (Писарић, 2016, 54). Због карактеристика ИКТ и услуга које оне

пружају корисницима постоје бројне потешкоће за откривање и доказивање дела високотехнолошког криминала. Потребно је континуирано праћење трендова развоја ИКТ и високотехнолошког криминала, стратешко планирање, усавршавање правне регулативе и техничких процедура на националном и међународном нивоу, континуирана сарадња и размена искустава, оспособљавање кадрова који се овом врстом криминала баве и подизање свести код људи о постојећем проблему.

ПРИМЕНА ИКТ У КРИТИЧНОЈИНФРАСТРУКТУРИ

Сајбер безбедност је значајан предуслов не само за функционисање привреде, него и целокупне државе, друштва. Јер, савремене ИКТ су постале окосница функционисања савремених критичних инфраструктурних система широм света. Појмови критичне инфраструктуре и критичне информационе инфраструктуре се разликују, али су међусобно повезани. Савремено значење синтагме критична инфраструктура је знатно шире од првобитног значења које је преузето из војне терминологије[3]. Критична инфраструктура у Републици Србији дефинисана је Законом о критичној инфраструктури ичине је: „системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно угрозити функционисање Републике Србије“ („Службени гласник РС“, бр. 87/ 2018). Дакле, критична инфраструктура има велики значај за функционисање државе на свим нивоима, јер представља: „скуп мрежа, ентитета, система и структура које могу оштетити одрживост друштвеног поретка или јавне службе када престану да испуњавају своје функције делимично или потпуно“ (Yagli & Dal, 2014, 911).

Савремена информациона и комуникациона технологија је омогућила повезивање, односно умрежавање различитих инфраструктурних елемената, али и њихову већу међузависност. На тај начин је критична инфраструктура постала обимнија и сложенија. Критична инфраструктура у Републици Србији, како је наведено у члану 6 Закона о критичној инфраструктури сачињена је од осам

3 У војној терминологији означава све оно што је неопходно за функционисање војног система ради очувања сопствених објеката, мрежа и система током војних сукоба, али и за онеспособљавање војних система на противничкој страни.

сектора: „1) енергетика; 2) саобраћај; 3) снабдевање водом и храном; 4) здравство; 5) финансије; 6) телекомуникационе и информационе технологије; 7) заштита животне средине; 8) функционисање државних органа“ („Службени гласник РС“, бр. 87/ 2018).

Критични инфраструктурни систем садржи критичну информациону инфраструктуру која пружа функционалну информациону подршку која је потребна за рад поменутог система. Међутим нефункционисање критичне информационе инфраструктуре може да узрокује прекид и озбиљно угрози функционисање целокупне критичне инфраструктуре. Истовремено рад критичне инфраструктуре може да угрози низ других фактора који су невезани за њену информациону инфраструктуру.

Средства за очување безбедности националне критичне инфраструктуре су од приоритетног значаја. Поменута средства су се током времена развијала. Национална критична инфраструктура је средином педесетих година била штићена интерним радом безбедносних служби (полиција, безбедносне и обавештајне службе) и обухватала је сва државна предузећа. Од друге половине седамдесетих година XX века, поред унутрашње службе безбедности уведен је и систем друштвене самозаштите свеобухватном мрежом који је обезбедио два додатна степена заштите[4] критичне инфраструктуре, односно државне или јавне имовине у тадашњој Југославији. Поменути концепт друштвене самозаштите имплементиран је у периоду од 1973. до 1990. године и временом је усавршаван усвајањем различитих закона, одредби и уредби.(Вучинић & Милосављевић, 45).

Упркос томе што су препознати позитивни технолошки ефекти и могућности примене савремене ИКТ за остварење заштите критичног инфраструктурног система, потребно је развијати и унапређивати заштиту од инцидената у ИКТ системима органа власти. Такође је потребно,,додатно уредити критеријуме за утврђивање критичне инфраструктуре са становишта информационе безбедности, критеријуме за карактеризацију напада применом информационих технологија на такву инфраструктуру у односу на класичне облике напада, као и услове заштите у овој области“ (Вучинић & Милосављевић, 2021, 51)

Безбедност критичне инфраструктуре је од виталног државног значаја. Левис указује да је сајбертероризам значајна претња којој треба посветити посебну пажњу јер може озбиљно да угрози критичну инфраструктуру неке земље, јер подразумева

4 Унутрашња финансијска контрола и контрола удружених радника.

„употребу компјутерских мрежа и интернет алата за ометање критичних националних инфраструктура (као што су енергија, јавни превоз, владине активности) или застрашивање или присиљавање влада једне земље или њених грађана“ (Lewis, 2002, 1). Последице сајбертерористичког напада на критичну националну инфраструктуру могу да буду катастрофалних размера, без обзира да ли је у питању један напад, или серија координираних наизглед независних напада(Wilke, 1999).

САЈБЕР ТЕРОРИЗАМ

Сајбер тероризам је посебна форма тероризма за чије извршење се користе савремене ИКТ било као оруђе или као мете напада ради остварења неког политичког мотива. У дела сајбер тероризма убрајамо „незаконите нападе и претње напада на рачунаре, мреже и информације које се тамо чувају“ како би (подвукла Лукнар) „застрашили или приморали владу или њен народ да ради на остварењу политичких или друштвених циљева“ (Manap & Tehrani, 2012, 409).

Домаћа литература о сајбер тероризму је оскудна. Термин сајбертероризам се први пут помиње крајем двадесетог века (Collin, 1997, 15). Шиндер у дефинисању сајбер тероризма даје посебан осврт на разорност последица ове врсте напада. „Напади на компјутере и рачунарске мреже могу се дефинисати као сајбертероризам уколико су њихови ефекти довољно деструктивни толико да изазвају страх који је упоредив са физичким терористичким актом“ (Shinder, 2002, 19).

Предности које информационе и комуникационе технологије пружају својим корисницима такође погодују терористима и свим осталим корисницима који прибегавају различитим врстама злоупотреба ИКТ. Превасходно се мисли на: 1) могућност корисника да сачувају своју анонимност ангажовањем у сајбер простору помоћу креираног, односно виртуелног (сајбер)идентитета, 2) однос причињене штете у реалном (физичком) свету и напора, тј. конкретних улагања за извршење сајбер напада. 3) извршење поменутих дела поред знања из IT области и технолошке опремљености не захтева неке додатне организације и ризике. Управо због поменутих предности сајбер криминал и сајбер тероризам превазилазе традиционалне облике тероризма и криминалашто их чини актуелним формама у савременом друштву.

Сајбер тероризам и сајбер криминал су тесно повезани, али се разликују. Основне одредице којима се прецизно дефинише сајбертероризам и јасно разликује од осталих сајбер злоупотреба су:

а) правни контекст (Разликује се по намери извршења чина; заверe; претње);

б) употреба сајберпростора за спровођење напада, док истовремено сајбер простор може бити мета(циљ) напада;

в) подразумева злонамерни поступак који садржи неку врсту насиља са тежњом за остварење далекосежних психолошких ефеката код циљаног аудиторијума;

г) намера за извршење је у складу са дугорочним циљевима терористе или терористичка група, као што је нпр. тежња за остварење друштвене или политичке промене, утицај на политичко одлучивање“ (Akhgar, Staniforth&Bosco, 2014, 13).

Дамњановић наводи пет основних одредница сајбертероризма: „1. употреба информационих/компјутерских технологија као оружја (а не само као логистичке подршке, средства комуникације или мете) 2. политичка мотивација 3. оријентација ка симболици/спектакуларности/публицитету 4. значајна материјална штета и/или људске жртве, или претња таквим последицама, што доводи до 5. ширења страха већих размера.“ (Дамњановић, 2009, 244). Дакле, оно што разликује сајбер тероризам од осталих врсти сајбер напада је политички мотив. Сајбер терористи неретко прибегавају извршењу осталих врсти сајбер напада како би прибавили неку корист за себе, која им даље омогућава једноставнији и бржи долазак до коначног циља.

СМЕРНИЦЕ ЗА ОЧУВАЊЕ САЈБЕР БЕЗБЕДНОСТИ

Смернице за очување безбедности сајбер простора се могу сумирати у три основне категорије:

1. Превенција - подразумева сајбер’хигијену’ која служи да подигне свест о различитим врстама сајбер претњи и злоупотреба, едукује кориснике и радну снагу ради пружања заштите и достизања адекватног нивоа безбедности.

2. Технике детекције, одбране и кажњавања - развијена сензорна технологија на различите врсте сајбер грешака и упада, развијен систем сајбер одбране са мамцима за диверзију, едукованим кадром, развијена правна регулатива сензибилна за поменуте врсте сајбер злоупотреба.

Сајбер одвраћање је стратегија којом држава која се брани

настоји да одржи status quo сигнализирајући своје намере да одврати непријатељске сајбер активности с циљем да утиче на противников апарат за доношење одлука како би се избегле деструктивне сајбер активности и избегла већа одмазда од стране почетног агресора. Углавном се примењују два типа стратегије одвраћања: одвраћање казном и одвраћање одбијањем (Iasiello, 2014, 55). Сајбер одвраћање је захтевно за спровођење и да би било успешно захтева испуњеност одређених параметара: комуникација, сигнализирање, приписивање и пропорционалност (Iasiello, 2014, 55). Могућност комуникације са извршиоцем напада пружа се онда када извршиоци напада обезбеде директан канал за обављање размене података (информација) (Falco, Noriega& Susskind, 2019). Суочавање са сајбер нападачима изискује тзв. „*the Wade and seek method*" (Wade, 2021) који је комбинација традиционалне методе преговорања са таоцима и терористима, која садржи базичне поставке дизајниране за решавање спорова које су прилагођене за рад у сајбер окружењу. Дакле, за успешно сајбер преговарање неопходно је урадити евалуацију трошкова и ризика, и применити интердисциплинаран приступ који комбинује технике решавања спорова и терористичке талачке кризе узимајући у обзир специфичности онлајн окружења.

3. Сарадња (национална, регионална и међународна) - Континуирано праћење актуелних стратегија одбране, развоја технологије и техника је неопходно за адекватну сајбер одбрану и очување сајбер безбедности. Суочавање са изазовима у области сајбер безбедности изискује активно праћење развоја различитих злоупотреба ИКТ, критично сагледавање могућности да се пружи адекватан одговор и превентивно делује.

ЗАКЉУЧАК

Употреба савремених информационих и комуникационих технологија широм света прожима готово сва поља друштвеног постојања. Основне државне структуре и индустрије (струја, гас, вода,железница и телекомуникације) своје функционисање ослањају на савремене информационе и комуникационе технологије. Глобална претња од различитих врсти сајбер малверзација и злоупотреба расте. Разматрање могућности злоупотребе ИКТ је комплексан проблем чија анализа захтева интердисциплинаран приступ.

У првом делу рада приказан је развој савремених информационих и комуникационих технологија. Потом је посебна пажња посвећена проблему високотехнолошког криминала. Подршка

коју савремене ИКТ пружају у раду критичних националних инфраструктура чини сајбер безбедност питањем од прворазредног значаја, док, актуелна друштвено-политичка ситуација у свету упућује на евентуалну претњу од сајбер тероризама. У раду су понуђене три основне смернице за очување сајбер безбедности. Питање безбедности савремених информационих и комуникационих технологија је изазов садашњости који ће засигурно бити актуелан у будућности.

ЛИТЕРАТУРА

Akhgar, B., StaniforthA. &Bosco F. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook*, USA: Elsevier Inc.

Baran, P. (1964). On Distributed CommunicationsXI. Summary Overview, RAND Corporation. Aviable at: https://www.rand.org/pubs/research_memoranda/RM3767.html (25.2.2022)

Bezzina, J. &Terrab, M. (2005). Impacts of New Technologies on Regulatory Regimes, *Communications & Strategies*, Special Issue, 15-30.

Collin, B. (1997).The Future of Cyberterrorism, *Crime and Justice International*13(2),15-18.

Falco, G., Noriega, A., & Susskind, L. (2019). Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. Journal of Cyber Policy, 4(1), 90e116. Geller, E., & Matisha.

Iasiello, E. (2014). Is Cyber Deterrence an Illusory Course of Action?Journal of Strategic Security 7 (1), 54-67.

Lewis, A. J. (2002, December). *Assessing the Risks of Cyber Washington DC, Terrorism, Cyber War and Other Cyber Threats*. Washington DC: Center for Strategic and International Studies. Retrieved from: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (10.1.2018)

Luknar, I. (2020a). Cyber Terrorism Threat and the Pandemic. In:Cane T. Mojanoski (Ed. in chief), *The Euro-Atlantic values in the Balkan countries*, Vol. 3 (p. 29-38). Bitola: University "St. Kliment Ohridski", Skopje: Faculty of Security.

Luknar, I. (2020b). Cybercrime – Emerging Issue. In: S. Jaćimovski (ed.), *Archibald Reiss Days.Vol. 10. International scientific conference* (621-628). Beograd: Kriminalističko-policijski univerzitet.

Manap., N.A., & Tehrani, P.M. (2012). Cyber Terrorism: Issues in Its Interpretation and Enforcement. *International Journal of*

Information and Electronics Engineering, 2(3), 409-413.

Mandel, Robert (2017). *Optimizing Cyberdeterrence : A Comprehensive Strategy for Preventing Foreign Cyberattacks*. Washington, DC: Georgetown University Press.

Schirrmacher, N. B., Ondrus, J., & Tan, F. T. C. (2018). Towards a response to ransomware: Examining digital capabilities of the WannaCry attack. In Proceedings of the 2018 Pacific Asia Conference on Information Systems. Atlanta, GA: Association for Information Systems.

Shinder, L. D. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. USA; Rockland, MA: Syngress Publishing Inc.

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace, Business Horizons 64, 787-797.

Wilke, A. Clifford. (1999, 5 March). *Infrastructure Threats from Cyber-Terrorists*. Retrieved from:https://www.occ.gov/news-issuances/bulletins/1999/bulletin-1999-9.pdf (8.6.2021)

Yagli, S.&Dal, S. (2014). Active Cyber Defense within the Concept of NATO's Protection of Critical Infrastructures, *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*8 (4). Retrieved from: https://pdfs.semanticscholar.org/959c/817cd8d725a3e37feb3b251b18a1c951e1cf.pdf (22.7.2021)

Вучинић, Д., Милосављевић, Б. (2021). Одос према критичној инфраструктури у Републици Србији, *Војно дело* 73(4), 42-56.

Гир, Ч. (2011). *Дигитална култура*. Београд: Clio.

Дамњановић, И. (2009). Постоји ли сајбертероризам, *Политичка ревија* 19 (1), 237-254.

Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, Службени гласник РС, бр. 94/17. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2017/94/4/reg (15.11.2021)

Закон о критичној инфраструктури, «Службени гласник РС», бр. 87/ 2018. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/8 (22.2.2022)

Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, Службени гласник РС, бр. 61/05, 104/09. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/61/7/reg (24.2.2022)

Кривични законик, Службени гласник РС, бр. 85/05, 88/05- исправка, 107/05 – исправка, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 и 35/19. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2005/85/6/reg (15.9.2019)

Министарство унутрашњих послова Републике Србије (е-извор). Кривична дела која обухвата високотехнолошки криминал. Преузето с http://www.mup.gov.rs/wps/portal/sr/gradjani/saveti/visokotehnoloski+kriminal/krivicna+dela+koja+obuhvata+visokotehnoloski+kriminal (24.2.2022)

Национална стратегија за спречавање и борбу против тероризма за период 2017-2021. године, Службени гласник РС, бр. 94/17. Преузето chttp://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2017/94/1/reg (30.12.2017)

Писарић, М. М. (2016). *Посебности доказивања дела високотехнолошког криминала*, Београдски Универзитет: Правни факултет.

Стратегија за борбу против високотехнолошког криминала за период 2019-2023. године, Службени гласник РС, бр. 71/18. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/71/1/reg (19.11.2021)

Стратегија за борбу против прања новца и финансирања тероризма за период 2020-2024. године, Службени гласник РС, бр. 14/20. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2020/14/1/reg (27.11.2021)

Стратегија заштите података о личности, Службени гласник РС, бр. 58/10. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2010/58/1 (17.10.2019)

Стратегија националне безбедности Републике Србије, „Службени гласник РС”бр. 94/2019. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/strategija/2019/94/2 (25.2.2022)

Стратегија одбране Републике Србије, Службени гласник РС, бр. 94/19. Преузето с https://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/strategija/2019/94/1 (25.11.2021)

Стратегија развоја вештачке интелигенције у Републици Србији за период 2020-2025, Службени гласник РС, број 96/19. Преузето chttps://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2019/96/1/reg (27.11.2021)

Стратегија развоја дигиталних вештина у РС за период 2020-2024, Службени гласник РС, број 21/20. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2020/21/2/reg/ (18.10.2021)

Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године, Службени гласник РС, бр. 68/10. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/reg/viewAct/df3fb65a-6acc-4e90-bd0f-f69066f6e0aa (19.11.2017)

Стратегија развоја индустрије информационих технологија за период од 2017. до 2020. године, Службени гласник РС, бр. 95/16. Преузето с http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2016/95/1/reg (12.1.2017)

Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године („Службени гласник РС“, бр. 86/2021). Преузето с: http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2021/86/1/reg (25.2.2022)

Стратегија развоја мрежа нове генерациједо 2023. године, Службени гласник РС, бр. 33/18. Преузето chttp://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/vlada/strategija/2018/33/1 (3.4.2019)

Ivana Luknar

Institute for Political Studies, Belgrade

ABUSE OF INFORMATION AND COMMUNICATION TECHNOLOGY: CONCEPT AND REGULATIONINREPUBLIC OF SERBIA

Resume

Numerous challenges are shaking modern world scene. Multiple crises (health, economic, environmental, war in Ukraine and migration) have created tensions at the international level. Information and communication technologies (ICT) are vital tool for thefunctioning ofcountriesworldwide.In current crisis conditions, ICT security has become even more importantbecause current tensions and conflicts can easily replace into cyberspace. The subject of this paper is ICT and its abuse. The paper provides a systematic overview of the topic in order to pay attention on ICT abuse and to encourage thinking about this issue. Through content analysis method there are conceptualized: the historical development of modern ICT, key concepts of ICT abuse (cybercrime, critical infrastructure, cyberterrorism) and its regulation in Republic of Serbia. The conclusion is that cyber security should be consider as one of the primary issues. The paper offers three main cyber securityguidelines.

Keywords: ICT, cybercrime, critical infrastructure, cyber terrorism, cyber security