УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ БЕЗБЕДНОСТИ

Безбедносне претње у сајбер простору

ДИПЛОМСКИ РАД

МЕНТОР:

Др Ненад Путник,

ванредни професор

КАНДИДАТ:

Кристина Кришановић 246/16

Београд, јун 2021.

Садржај

1. УВОД

Људска цивилизација је одувек имала потребу и способност комуницирања, па су у ту сврху развијали одређене технолошке форме за размену информација. У ранијим периодима, пре развоја науке и технологије, људи су као средство комуникације користили бубњеве, димне сигнале, бакље, разне записе на керамичким или каменим таблама, као и књиге које су такође служиле и за пренос знања. Средства која су се тада користила зависила су пре свега од раздаљине између комуникатора, исто тако и од временских услова, односно видљивости, амбијенталних услова и слично.

Наука и технологија је достигла убрзани развој, пре свега у другој половини двадесетог века. Након Другог светског рата, са социолошког аспекта, посебно је значајан развој информационе и комуникационе технологије, које су довеле до промена у начину организовања и функционисања друштва, тако што је повећао брзину и обим интеракције у „умреженом друштву“

Достигнућа Треће информационе револуције - настанак персонализованих рачунара, стварање локалних рачунарских мрежа, а затим и глобалне мреже – Интернета, утицало је на промене у економској, политичкој и културној сфери друштвеног живота. Компјутерске мреже постале су централни елемент друштва. Међусобним повезивањем рачунара путем телекомуникационе мреже настао је нови „дигитални“ свет.

Информационо-комуникационе технологије уводе потпуно ново окружење у подручју сукоба и његове регулације – сајбер простор. Сајбер ратовање има специфичну природу као и форму и примену. Оно мења приступ сукобима и ратовању, како у квантитативном тако и у квалитативном погледу. Одвија се у сајбер простору. Начин на који се остварује дејство сајбер напада се мења у складу са брзином развоја и способностима информационо-комуникационих технологија. Примена умрежених информационо-комуникационих технологија у сајбер простору захтева поседовање извесног знања и вештине из различитих области.

Сајбер ратовање је нов феномен, који подразумева употребу информационих технологија за вођење сукоба. Он користи другачија средства ратовања од традиционалних и одвија се без обзира да ли је стање рата или мира. Његови учесници не морају бити војно униформисани. Ратовање представља сукоб интереса који се

остварује применом инструмента моћи. Методи и технике ратовања карактеристичне за средњи век у савременом друштву нису прихватљиве.

2. НОВИ ОБЛИК САВРЕМЕНИХ ДРУШТВЕНИХ КОНФЛИКАТА-САЈБЕР РАТОВАЊЕ

Крај осамдесетих и почетак деведесетих година двадесетог века обележио је, настанак персонализованих рачунара и рачунарске мреже. Распрострањенијом употребом рачунара и рачунарских мрежа, деведесетих година двадесетог века, отворила је могућност за вођење информационог рата. Нови борбени фронт одвијао се у кибернетском простору односно, сајбер простору. Често се користе синоними сајбер ратовање и информационо ратовање, како у научној тако и у стручној литератури.

У последњој деценији двадесетог века, са развојем информационо-комуникационих технологија, уочена је експанзија сајбер ратовања. Сајбер ратовање је ратовање које се води у виртуелном свету, односно кибер простору.

Сајбер простор (енг. cyberspace) представља виртуелни простор, који настаје у контакту човека и рачунара. То представља дигитални свет, који је конструисан уз помоћ рачунарских мрежа – Интернета.

Сајбер ратовање се може дефинисати као подврста информационог ратовања, којој није потребно традиционално бојно поље. На сајбер могу утицати било који друштвени субјекти, било да је реч о колективу или појединцу, који има приступ умреженом рачунарском систему. Сајбер напади, могу бити усмерени на намерно убацивање дезинформација или могу бити усмерени, према мрежној саботажи. Са обзиром, да је друштво постало зависно од информационог система, било какво онемогућавање нормалног функционисања информационог система, може имати озбиљне последице у свим сферама друштвеног живота. Те последице могу бити фаталне, уколико се угрози критична информациона инфраструктура. Основни предуслов како би се могао водити сајбер рат, јесте поседовање софистицираног информатичког знања.

3. САЈБЕР ПРОСТОР

3.1. Значај појма „сајбер“

Информационо – комуникационе технологије данас имају толики утицај на целокупно друштво, оне повезују људе и народе и остварују изузетно дејство између језика. Утицај информационо – комуникационе технологије расте, и разлози за то су комплексност и ширина његове примене. Кључни израз који прати развој информационо – комуникационих технологија јесте појам „сајбер“. „Сајбер“ подразумева употребу информационо – комуникационих технологија у свим областима друштвеног живота, укључујући безбедност и одбрану. Појам „сајбер“ је пореклом из етимолошког корена старогрчке речи *кибернетикос,* чије је значење, управљати и руководити. Сам појам се користи како у српском, тако и у другим језицима, јер пре његове појаве није постојао адекватан појам, односно реч у тим језицима. Шира примена тог термина уочљива је деведесетих година двадесетог века. Појам „сајбер“ је саставни део појма „сајбер простора“. Они се користе за означавање новог, посебног подручја у пракси рачунарских наука и примене информационо – комуникационих технологија у разним областима. Шира примена појма видљива је у војној области са одређеним префиксима: „сајбер ратовање“ , „сајбер рат“, „сајбер сукоб“, „сајбер напад“, „сајбер оружје“ и сл.

У Социолошком речнику сајбер простор је дефинише на следећи начин: „ Сајбер простор јесте виртуелни простор који настаје у контексту човека и рачунара. У свакодневном говору под тим изразом најчешће се подразумева дигитални свет конструисан уз помоћ рачунарских мрежа, попут нпр. Интернета. То место, иако заиста постоји, могло би се описати пре као комуникацијски медиј него као потпуно другачија галаксија, јер се многе од свакодневних пракси и дискурса кроз њега преламају и структуришу га кроз известан однос узајамне повезаности. Иако се сајбер простор најчешће перципира као нематеријално краљевство података или као нека врста виртуелне стварности, он заправо има и сасвим физичку инфраструктуру, сачињену од жица које се налазе изнад и око наших глава, кабловима који леже поред наших ногу и сателита на небу коју круже око наше планете, све то омогућава интеракцију која на нивоу сензација материјализује квалитет нематеријалности, којим сајбер простор најчешће описују његови конзументи. Сајбер простор је нова форма менталне димензије људске егзистенције унутар које настаје симулирана реалност као последица интеракције између људског и

артифицијелног интерфејса. Он представља алтернативну просторну димензију унутар које се успостављају везе између различитих персоналних рачунара, рачунарских мрежа, различитих виртуелних заједница и појединаца који могу, али и не морају да буду њихови чланови. Сајбер простор се налази у перманентном процесу промене и практично може бити бесконачан у „величини“, иако унутар њега просторна и временска димензија често добијају посве померена/измењена значења. Комуникација са и унутар сајбер простора се успоставља тренутно, при чему је физичка локација корисника у највећем броју случајева потпуно неважна…“ (Путник, 2009)

3.2. Порекло сајбер простора

Термин „сајбер“ простор настао је и развио се у САД-у, паралелно са развојем информационо – комуникационих технологија и применом рачунарских наука. Термин „сајбер“ први пут је употребљен од стране научника Норберт Винера у његовим истраживањима, у другој половини двадесетог века. Сајбер простор означава „виртуелно“ окружење, сачињено од дигиталних података.

Писац Вилијем Гибсон је 1984. године, употребио термин „сајбер простор“ у свом роману *Неуромант* . Према њему, сајбер простор је универзум рачунарских мрежа, дигитални свет у којем се друштва, мултинационалне компаније и информатичари боре за освајање података и информација. Након издања поменуте књиге, термин „сајбер простор“ се све чешће употребљавао.

Природа сајбер простора је неразумљива без укључивања војног елемента. Између сајбер простора и војних активности постоји суштинска повезаност. Информационо – комуникационе технологије, рачунари, рачунарске мреже, сајбер простор, који је настао њиховим умрежавањем, развијене су за потребе одбране и војске, пре свега у САД-у. Интернет се данас назива „сајбер простором“.

Интернет је настао радом научника и инжењера у оквиру пројекта ДАПРА, као и радом истраживача на водећим универзитетима у САД-у, на иницијативу Владе САД, чији је циљ био да се унапреди способност војске за одбрану.

Развојем технологије мења се и сам појам „сајбер простор“. Сајбер простор се развијао дуги низ година, упоредо са развојем технологије.

3.3. Дефинисање сајбер простора

Једна од најважнијих карактеристика сајбер ратовања је то да се оно делом или у целини одвија у сајбер простору, с тога је одређење и разумевање сајбер простора од кључног значаја за разумевање сајбер ратовања. Сајбер простор представља нов појам и сматра се новим подручјем ратовања, поред копна, мора, ваздуха и свемира. Сам израз „сајбер простор“ настао је и развио се у САД-у, паралелно са развојем и применом рачунарских наука и информационо-комуникационих технологија.

У здруженој публикацији Војске САД број 2-01-3, из 2000. године, под називом Здружене тактике, технике и процедуре за здружену обавештајну припрему бојишта, објављена је једна од првих јавно доступних војних дефиниција сајбер простора уопште. По њој, сајбер простор је: „Концептуално окружење у коме дигитализоване информације комуницирају преко рачунарских мрежа“. Ова дефиниција је добила статус званичне дефиниције сајбер простора у Министарству одбране САД објављивањем у Речнику војних и повезаних термина Министарства одбране из 2001. године. (Младеновић, 2016.)

Дефиниција америчког министра одбране може се прихватити као најчитанија у стручној војној литератури: „ Сајбер простор је глобално подручје у оквиру информационог окружења које сачињава међузависна мрежа инфраструктуре информационих технологија, укључујући интернет, телекомуникационе мреже, рачунарске системе и уграђене процесоре и контролоре.“ (Младеновић, 2016)

Сајбер простор представља вештачку творевину, створена активношћу људи, која је настала као резултат друштвених потреба и технолошких иновација. Сајбер простор можемо такође дефинисати и у ужем и у ширем смислу. У ужем смислу, сајбер простор представља скуп информација, рачунарских система и мрежа као и активности између њих. У ширем смислу, сајбер простор поред поменутих елемената обухвата и целокупну инфраструктуру и активности у електромагнетном спектару. Развој технологије и дигитализација информација, воде ка спајању свих електронских активности у сајбер простору.

Раст и развој сајбер простор,а као међусобно зависне мреже инфраструктуре информационих технологија које укључују интернет, телекомуникационе мреже, као и рачунарске системе, доприноси наглом порасту броја злоупотребе информационо-комуникационих технологија, као што су високо-технолошки криминалитет, шпијунажа,

тероризам и сајбер ратовање. Савремени глобализациони процеси померају границе криминалних активности и стварају нове могућности повезивања криминалаца и организованих група, а рачунарске мреже постају место, мета, циљ и средство извршења криминалних активности, док је са друге стране, одговор безбедносних органа на претње у виртуелном свету више реактиван него проактиван.

Аљоша Мимика и Марија Богдановић сматрају да је „сајбер простор нова форма менталне димензије људске егзистенције унутар које настаје симулирана реалност као последице интеракције између људског и артифицијелног интерфејса. Представља алтернативну просторну димензију унутар које се успоставља веза између различитих персоналних рачунара, рачунарских мрежа, различитих виртуелних заједница и појединаца.“(Вулетић, 2017)

Сајбер простор не представља само интернет, већ га чине све информационе мреже, као и све што њих повезује и контролише. То је простор различитих садржаја који је постао саставни део сваког појединца, пословања и функционисања државе. Пружа огромне могућности и у информационом друштву представља доминантни медиј комуникације. Сајбер простор постаје све више домен за извођење криминалних активности, што изискује потребу да се у међународној заједници ускладе ставови у вези са класификацијом малициозних активности у сајбер простору. Анализирајући ставове у сајбер стратегијама развијених земаља, малициозне сајбер активности се могу поделити на:

- Сајбер криминал;
- Сајбер тероризам;
- Сајбер шпијунажа;
- Сајбер ратовање.

4. САЈБЕР СУКОБИ

Сајбер сукоби представљају нову врсту ратовања која се веома брзо развија. Резултат, јесу све чешћи сајбер напади које државе покрећу на противничке циљеве и који имају широк спектар тог дејства, од информационих до физичких уништења циљева.

Сајбер сукоби не подразумевају нужно употребу физичке силе, нити се дешавају искључиво на географском простору.

Након Хладног рата, наступио је нови војно – безбедносни контекст. Њега карактерише задржавање нуклеарне претње и нова прилагођена структура војне организације. Нуклеарна војна технологија се толико развила да су у Хладном рату сукобљене стране могле у потпуности да се униште међусобно.

4.1. Утврђивање природе сајбер сукоба

Упркос растућем броју сајбер напада, у међународној јавности се често може уочити погрешан став о њиховој природи, која се меша са сајбер криминалом, тероризмом, шпијунажом или пропагандом и информационим операцијама. У стварности, број случајева сајбер ратовања је много мањи од укупног броја сајбер напада. Највећи број сајбер напада односи се на сајбер криминал, односно на ситуације у којима је прекршен кривични закон неке државе и међународни прописи кривичног права. У тим случајевима прекршиоци су појединци или криминалне организације које подлежу санкцијама националних и међународних кривичних прописа, у складу са прихваћеним правилима јурисдикције правних система. У начелу, сајбер тероризам је специфичан случај сајбер криминала који представља употребу сајбер простора ради остваривања терористичких циљева, на начин, како то дефинишу национални и међународни прописи. Други специфичан случај сајбер криминала је сајбер шпијунажа, која је у принципу легална у међународним оквирима и забрањена националним прописима уколико ју је покренуо противник, а дозвољена, уколико служи сопственим националним интересима. Кључна разлика између сајбер криминала и ратовања огледа се у томе да ли су у те активности укључени политички актери који имају међународно-правни субјективитет. С обзиром на околности да се за сајбер ратовање и криминал користе иста средства, методе и технике, ради избегавања њиховог мешања неопходно је одредити идентитет учесника сукоба и њихове мотиве. Само у случају да је напад преузео неки субјекат међународног права са намером да почини акт агресије над другим субјектом међународног права, може се сматрати да је реч о ратовању. У томе се крије тренутно највећи проблем одређивања природе сајбер напада, јер је технолошки тешко, или чак и немогуће , у реалном времену утврдити идентитет нападача, његове намере и средства или методе напада. Ако и када се утврде, неопходно је и утврдити непосредне и посредне

последице напада, како би се могло применити међународно право које регулише ратовање. Зато полазне и уједно најважније чињенице при одређивању да ли неки сајбер напад, представља акт насиља и са којом намером је покренут. Одговор на прво питање одређује природу сукоба – да ли је реч о ратовању или криминалу, а одговор на друго питање даје потврду агресије, јер се не може сматрати да је реч о ратовању уколико је до штете по нападнутог дошло ненамерно или без утврђене одговорности државе из које је потекао напад. (Дракулић, Јовановић и Младеновић, 2012)

Природа сајбер ратовања је нова и прилично нејасна, због употребе великог броја различитих термина и одсуства општеприхваћене дефиниције. Како би се схватио појам сајбер ратовања неопходно је да се разуме разлика између термина рата и ратовања. Рат представља стање непријатељства, односно сукоба између држава или нација, чију основу чини оружана борба. Ратовање представља процес који се води између супротстављених страна, употребом оружја и метода за вођење тог процеса. Има и уже и шире схватање. У ширем смислу ратовање подразумева све могуће оружане и неоружане активности које су усмерене против супарника, са циљем да се наметне воља. У ужем схватању ратовање подразумева вођење сукоба у некој области попут: ратовања правом, информационо ратовање, поморско ратовање, космичко ратовање, сајбер ратовање итд. Ратовање није ограничено само на употребу оружја, већ се оно може водити и применом одређених не смртоносних средстава, метода и техника. Сајбер ратовање је неодвојиво повезано за сајбер простор и углавном се његове активности одвијају делом или у целини у њему.

4.2. Учесници сукоба у сајбер простору

Учесници могу бити:

- Наддржавне организације као учесници сукоба у сајбер простору;
- Државе као кључни учесници сукоба у сајбер простору;
- Организације као кључни учесници сукоба у сајбер простору;
- Појединци као кључни учесници у сајбер простору.

4.3. Наддржавне организације као учесници сукоба у сајбер простору

Да би се разумео однос између држава у сајбер простору, неопходно је разумети и виши и нижи ниво организовања од државног. Под вишим нивоима организације држава, сматрају се све врсте организованог међународног удруживања, које је засновано на вољи држава. Државе удруживањем остварују различите интересе на основу дељења заједничких ресурса, способности и вредности на биолошким, друштвено – политичким, економским, безбедносним и другим основама. Становништво неких држава може имати идентично национално и религиозно порекло, исти или сличан језик, делити сличне културне вредности и интересовања. На основу свега тога, нације деле заједничку политику у међународним односима и спроводе је кроз заједничке акције и функције. У том процесу степен повезивања зависи од културолошке, друштвено-политичке, економске, војно-безбедносне и других врста повезаности.

Од елемената повезаности, а под дејством националних интереса и метода испољавања моћи у међународним односима, зависи и ангажовање држава у сукобима и ратовима, укључујући и у сајбер простору. У области безбедности и одбране, национална култура није имагинарни фактор, већ стварни и утиче на ангажовање у рату.

У оквиру ЕУ, све државе чланице деле заједничке европске вредности које представљају основне елементе културе. Те вредности у већини држава са разноврсним националним културама, традицијом и језицима, какав је ЕУ, представља важан фактор равнотеже. Оне нису статичке посебно у заједници са више чланова. Мењају се, развијају у складу са временом, глобалним и регионалним догађајима и динамиком међународних односа. Међутим, национални интереси су изнад општих заједничких вредности које деле наддржавне заједнице.

С` обзиром да је ЕУ политичка заједница која је израсла из економске заједнице, логично је да су заједнички интереси њених чланица, првенствено економске природе, а да их заједничка политика подржава. То се одсликава и на заједничку политику у сајбер безбедности и одбрани. ЕУ је усвојила заједничку стратегију сајбер безбедности и формирала је цивилну Европску агенцију за мрежну и информациону безбедност (ЕНИСА). ЕУ нема јединствену војску, нити оперативне капацитете за одбрану како у физичком тако и у сајбер простору. Одбрамбене способности ЕУ се примарно развијају

кроз успостављање заједничке политике одбране и функционисање институција за координацију, интероперабилност и развој војних способности, попут Европске одбрамбене агенције. Та агенција је надлежна и за развој способности ЕУ за сајбер одбрану. Тај развој се односи на обуку и тренинг, подизање свести у подручју информационе безбедности, унапређењу развојно-истраживачких капацитета и развоју специфичних способности у области сајбер безбедности и одбране. Кључна колективна способност ЕУ није оперативна способност колективне одбране од војног напада споља, већ очување мира, учешће у мировним операцијама, превенцији сукоба и јачању међународне безбедности. Одсуством оперативних снага не значи да су државе чланице ЕУ небрањене од претњи у сајбер простору.

Све чланице ЕУ, осим шест војно неутралних држава су део НАТО-а, па чак и те војно неутралне државе остварују политичке, безбедносне и одбрамбене везе са НАТО. Оно се састоји од јединица и припадника националних армија чланица. Финансијске ресурсе за одбрану НАТО-а обезбеђују чланице улагањем у властите одбрамбене капацитете у складу са плановима и заједничким одлукама савеза. У погледу капацитета за сајбер одбрану у оквиру НАТО савеза, уочено је да државе које издвајају највећа средстава за развој и функционисање војних снага су истовремено и државе које имају најразвијеније војне капацитете за извођење војних операција у сајбер простору.

НАТО и ЕУ остварују стратегијско партнерство у области одбране укључујући и сајбер одбрану. У Европи главни центар за развој способности НАТО је Кооперативни центар изузетности за сајбер одбрану у Талину. Кључни циљеви тог центра су обука, развој и истраживање у области сајбер одбране. Снага сајбер одбране држава ЕУ не лежи нити у одбрамбеним структурама ЕУ, нити у НАТО-у , већ у сопственим капацитетима.

Заједница „пет очију“ коју чине: САД, Велика Британија, Канада, Аустралија и Нови Зеланд, је створена на основу низа билатералних и мултилатералних споразума и поседује најразвијеније капацитете и способности за сајбер одбрану, обавештајне активности електронски надзор у свету. Њихове обавештајне програме за електронски надзор у сајбер простору развија и предводе америчка агенција NSA и британске агенције за електронски надзор GCHQ.

Сагледавањем шире слике функционисања заједнице „Пет очију“ може да се закључи да је степен њене структуре, функционалне и оперативне повезаности извођења војних и

обавештајних операција у сајбер простору, много већи него у случају различитих обавештајних агенција унутар многих држава.

ЕУ као економско-политичка заједница држава готово да нема никакве капацитете за сајбер одбрану и обавештајни рад, за разлику од заједнице „Пет очију“. Национални интереси у области безбедности и одбране у сајбер простору су израженији у одбрамбено-безбедносној, него у економско-политичкој заједници.

4.4. Државе као кључни учесници сукоба у сајбер простору

Државе су сложени системи, који имају своју специфичну правну и друштвену традицију, вредности, начин организације, ресурсе, капацитете и националне интересе. Државе су субјекти међународних односа и сукоба. Државе су политички организоване групе људи на одређеној територији, чије границе се могу мењати.

Под структурним деловима државе сматрају се органи, институције и агенције које извршавају неку специфичну државну функцију и/или активност, остваривањем неке државне надлежности, у циљу спровођења централне државне власти у оквиру јединствене надлежности државе. Међународно право оружаних сукоба се бави оружаним сукобима у одговорности политичких субјеката међународног права.

Испољавање националне политике, кроз војну моћ, обележје је државе још од Вестфалског мира. Ратови се од тада не воде између религиозних заједница, већ се искључиво воде између држава. Државе имају кључну улогу у вођењу међународних сукоба и њихово решавање. Држава је централни акт међународног односа и међународног права. Државе су кључни елементи у међународним односима. Међународно право су створиле државе. Оно се односи на сукобе у којима државе учествују. Сукоби се воде специфичним средствима која су карактеристична само за оружане снаге, попут ратних бродова, борбене авијације, тенкова, униформисаних војних јединица, које су у поседу држава.

Државе су и кључни субјекти међународног права оружаних сукоба и сукоба у сајбер простору. Сајбер сукоби се морају регулисати као сукоби који се одвијају у сајбер простору, између држава. Од Вестфалског мира државе су основни фактор међународног права, али то не омета друге да улазе у сукобе, било у име државе или самостално.

4.5. Организације као кључни учесници сукоба у сајбер простору

На поднационалном нивоу друштвене организације истовремено владају интегративне и дезинтегративне силе у разним областима друштвених активности, које су од значаја за безбедност. Као последица тога, издвајају се развој технологије и процес глобализације. Интегративни фактори утичу на то да свет постаје све мањи а нације, заједнице и појединци постају све ближи. Та близина им омогућава да деле ресурсе. Повећана концентрација интереса око ресурса, доводи до нових сукоба.

На црном тржишту могу прикривено да учествују сви, од појединаца преко представника приватног бизниса, па до организација из државног апарата. Таква места су углавном виртуелне природе. Развојем „Тамног веба“, на коме се појављују и нестају разна неформална али развијена и нелегална тржишта, за трговину разним нелегалним стварима, допринео је повећаном обиму трговине. Таква тржишта кратко трају, с обзиром на своју криминалну природу а и саме информације које се размењују не трају дуго, јер се могу искористити за нападе, док не постану опште познате широј јавности. Таква места имају велики потенцијал да информације добију од страних обавештајних и безбедносних агенција. На таква места је могуће приступити анонимно, али исто тако не постоји никаква претходна пракса о квалитету производа или услуга, којима се тргује.

Захваљујући анонимности оваквих мрежа, постоји и могућност да владине агенције, неке државе учествују у оснивању и организовању рада таквих организација, са циљем да на лак начин дођу до важних информација о рањивостима и нападима. Такве информације се касније могу користити у активностима везаних за безбедност и одбрану, попут офанзивних операција у сајбер простору.

У војном и технолошком погледу, способност актера да изведу напад у сајбер простору, зависи од врсте и дубине релевантног знања, за извођење напада и од ресурса да се то знање развије и примени.

Многе терористичке организације изграђују организациону структуру и способности које им омогућавају да прикривено изводе терористичке операције, упркос свеобухватном надзору у електронском и сајбер простору који изводе многобројне државне полицијске, војне и безбедносно-обавештајне агенције. Пример за то је напад Ал-Каиде, који се догодио 11. септембра 2001. године у САД-у. Државе саме изнајмљују приватне организације за развој система и способност активности у сајбер простору, у

складу са националним законима када то раде јавно, и прикривено, када то раде ради извођења специјалних и шпијунских активности, према другим државама. Постоји велики број приватних компанија које су развиле способност истраживања у области информационе безбедности и специјализоване су за истраживање рањивости и продор у информационе системе. Оне продају информације, знање, услуге и производе државним агенцијама које их користе за извођење напада у сајбер простору.

4.6. Појединци ако кључни учесници у сајбер простору

Појединци, такође учествују у вођење сукоба у сајбер простору и то не само као чланови државних и корпоративних институција, него и самостално. Црно тржиште, екплоит и криминалне хакерске услуге су створени од стране криминалаца и њима су и намењени. Али такође, то има утицаја на вођење сајбер шпијунажа и сукоба између држава. Међународно право оружаних сукоба односи се на активности, радње и поступке у међународним сукобима између држава и других субјеката међународног права. Међународно право се односи и на појединце, организације и групе за извршење кривичних дела у међународном окружењу, током оружаних сукоба. Могуће је да се утврди одговорност појединца за кривична дела, која су учињена у току међународних сукоба на основу међународног права, за која не постоји одговорност држава. Сајбер сукоби се морају регулисати као сукоби који се одвијају између држава у сајбер простору који достиже ниво тј. последице оружаних сукоба.

5. САЈБЕР РАТОВАЊЕ

5.1. Појам сајбер ратовања

Анализирајући ставове у сајбер стратегијама развијених држава, малициозне сајбер активности можемо поделити на: сајбер криминал, сајбер тероризам, сајбер шпијунажу и сајбер ратовање. Све ове активности често изгледају исто или слично.

Опште прихваћена дефиниција сајбер ратовања још увек не постоји. Оно се често поистовећује и меша са терминима сајбер криминал, шпијунажа или електронско

ратовање. Да би било реч о сајбер ратовању, неопходно је да има карактер организоване агресије једног субјекта међународног права на други, односно једне државе на другу.

Сајбер ратовање је ратовање у сајбер простору, засновано на примени информационо-комуникационих технологија. То је специфичан облик међународног сукоба, који се од традиционалног ратовања разликује по средствима, методима и учесницима. Традиционални сукоби одвијају се у физичком простору, док се сајбер ратовање одвија у сајбер простору. По техникама, методи и процесу напада се не разликује значајно од криминалних, шпијунских или терористичких активности. За разлику од традиционалних сукоба у физичком окружењу који представља организовану примену ексклузивног и специфичног наоружања, сајбер ратовање је процес, а не употреба „сајбер оружја“. Тај процес подразумева намерно нарушавање информационе безбедности нападнутог система у сајбер простору у војне сврхе.

Широка примена информационо-комуникационих технологија у сајбер простора у сврху вођења сукоба на међународном нивоу последица је њихове велике заступљености у свим сегментима људског живота. Права моћ сајбер ратовања управо лежи у непрекидном развоју информационо-комуникационим технологијама, а не у тренутним ефектима сајбер напада,

Основне области примене сајбер ратовања јесу шпијунажа, информационе операције и онеспособљавање система друштвене инфраструктуре. Оно представља идеално средство технолошке манифестације мрежноцентричног и асиметричног ратовања. Своје потенцијале ће показати тек у будућности.

Војно присуство у сајбер простору је несумњиво, многи експерти сматрају да сајбер напад може имати велики утицај на борбену способност јединице, пре свега напади на информационе инфраструктуре, као што су систем телекомуникација или напајање електричном енергијом. Природа сајбер ратовања је нова и специфична. У сајбер простору је тешко некада и немогуће да се утврди идентитет учесника као ни њихове мотиве. Само у случају да је напад преузео неки субјекат међународног права, са намером да почини акт агресије над другим субјектом међународног права, може се сматрати да је реч о ратовању. Сајбер ратовање подразумева примену офанзивног и дефанзивног сајбер оружја и информација, које су покренули или организовали државни акти.

Сајбер ратовање је врста непријатељске активности преузета против рачунарске мреже, рачунарских система и база података које имају за циљ да униште противнички циљане системе.

Сајбер ратовање се дефинише и као неовлашћени упад од стране владе у рачунаре или мреже, али исто тако и преузимање других активности, којима се утиче на рачунарски систем, попут додавања, измене, фалсификација података или прекида или уништења рачунара, мрежних уређаја или објекта контроле рачунарских система.

Сваки сајбер напад који је изведен од стране неког ентитета против државе и њеног друштва, представља сајбер ратовање. Актер који организује ратовање може бити државни или недржавни. Дакле, сајбер ратовање представља облик информационог ратовања, који се састоји од низа активности, којима се прекидају или уништавају информациони и комуникациони системи противника.

Активности сајбер ратовања, како неки аутори сматрају, не морају бити ограничени, ипак, само на сферу војних активности. Индивидуални корисници информационо-комуникационих технологија, као и политички мотивисане друштвене групе, користе тактике и стратегије, како би тачно одредиле мете напада у сајбер простору и тако постигли своје циљеве. Они на око могу бити неприметни а у реалном животу, односно физичком свету, резултовати људским жртвама и материјалним разарањима.

Методи сајбер ратовања су тактике, технике и процедуре које примењују зарађене стране. Сајбер оружја су она средстава ратовања која су направљена, користе се или намеравају да се користе у сукобу и која су способна да проузрокују, повреде или смрт лица, односно оштећење или уништење објеката.

5.2. Карактеристике сајбер ратовања

Основне карактеристике сајбер ратовања:

- сајбер ратовање представља примену информација, информационих средстава и сајбер простора у сврху вођења међународних сукоба;
- одвија се у потпуности или делимично у сајбер простору или кроз сајбер простор;

- директно дејство сајбер напада нема природу кинетичког дејства, али његове последице (посредно дејство) могу бити и физичко уништење средстава и рањавање или убијање људи;
- сајбер напади могу имати тренутно или одложено дејство;
- операције сајбер ратовања могу остати неоткривене и након што остваре дејство;
- нападачи су најчешће прикривени и није позната њихова природа (не морају бити припадници оружаних снага, већ и цивили или унајмљени информатички стручњаци);
- сајбер ратовање замагљује разлике између цивила и бораца и по питању нападача и по питању цивила;
- средства којима се врше сајбер напади најчешће имају основну мирнодопску намеру;
- напади могу имати дистрибуиран извор, али и циљ;
- у већини случајева је тешко или немогуће утврдити државну одговорност за покретање сајбер напада;
- сајбер ратовање може имати ниску цену примене у односу на остварене ефекте напада у поређењу са традиционалним ратовањем;
- има мрежноцентрично и асиметрично дејство;
- оно се не одвија у засебном подручју као искључиво војна активност, већ великим делом има пресек са сајбер криминалом и шпијунажом, од којих га разликује само намера покретача напада, а не средства, методе и технике;
- природа, средства и последице сајбер ратовања се брзо мењају у складу са технолошким развојем;
- не постоји међународно прихваћен став шта конструише сајбер ратовање, нити међународне правне регулативе.

Наведене карактеристике сајбер ратовања чине га специфичним у односу на друге врсте сукоба. (Дракулић, Јовановић и Младеновић, 2012)

5.3. Шта омогућава сајбер ратовање?

Фактори који омогућавају примену сајбер простора са циљем ратовања су:

- друштвени;

- технолошки;
- војно-стратегијски.

Друштвени и војно-стратегијски разлози примене сајбер ратовања проистичу из нових друштвених околности. Основни симболи тих околности су глобализација, наступајућа мултиполарност светског поретка, доминација англосаксонског правног система, слабљење принципа вестфалског суверенитета држава, синтетисање нових, универзалних моралних начела попут демократије и људских права, експлозија развоја информационе технологије, настанак сајбер простора и глобалног умрежавања људи.

Тренд решавања међународних проблема ослањањем на војну и технолошку моћ отварања пута ка настанку нових облика светских сукоба у свим подручјима, па и у сајбер простору. Ти модерни сукоби показују тенденцију смањења броја међународних учесника, раст броја недржавних учесника сукоба, смањење броја директних жртава сукоба, повећање значаја информационе сфере сукоба и доступности информационих технологија. Трошкови сукоба су све виши, па је изузетно значајан захтев за вођење ефикасних и оптимално осмишљених војних операција за остваривање војног циља са минималним ангажовањем снага. Доступност информација је битно повећала брзину ратовања и смањила време припреме и извођења операција. То доводи до ситуације у којој се рат води у времену уместо у простору.

Технолошки разлози постојања сајбер ратовања су најбројнији и могу се сврстати у групу недостатака који проистичу из архитектуре самих мрежа, недостатке који проистичу из несавршености хардвера и софтвера и недостатке који су последица отвореног приступа подацима. Недостаци садржани у архитектури сајбер простора, уграђени су у његову основу, па их је стога могуће злоупотребити, без обзира на степен његовог технолошког развоја. Недостаци у дизајну хардвера и софтвера. То је вероватно најважнији од свих узрока који омогућавају сајбер ратовање. Битно је нагласити да се за сајбер ратовање користе исти алати, средства и методе као за сајбер криминал или тероризам. Карактеристичан пример искоришћавања слабости хардвера и софтвера у војно-политичке сврхе јесте дизајнирање и подметање рачунарског црва *Stuxnet.* Он је циљано нападао специфичне електронске уређаје компаније у нуклеарним постројењима. Иако је његово присуство откривено у више држава света, стручњаци су утврдили да је његов основни циљ била нуклеарна централа у изградњи у граду Бушер у Ирану.

Stuxnet је постао познат као први рачунарски софтвер који је коришћен као сајбер оружје. Познати *Stuxnet* напад је заједнички реализован од стране Израела и САД-а против иранског програма развоја нуклеарног наоружања, оне су једино могле логистички да организују операцију таквог обима. Он је добар пример где је сајбер оружје експресно направљено и употребљено за сајбер рат.

5.4. Војни аспект кибер ратовања

Modus operandi кибер ратовања проширен је у односу на конвенционално информационо ратовање низом активности, усмерених на софтверско угрожавање информационе инфраструктуре, док је пропагандни аспект информационог ратовања попримио форму злоупотребе Интернета. Кибер простор је постао не само циљ напада већ и моћно средство у рукама високообразованих „информатичких ратника“. Борбе у будућности ће се водити искључиво у сајбер простору, а већина држава се увелико припрема за такву врсту вођења ратова. Употреба термина кибер ратовања за описивање савремених сукоба у сајбер простору, може се чинити непримереном у односу на традиционално поимање рата као организованог конфликта између држава, етничких и верских група или класа средствима оружаног насиља у циљу остваривања одређене политичке, војне или друге добити.

Неопходно је да се редефинише појам „рат“ онда када пракса потврди да рачунарски напад, може погодити системе контроле који су „срца“ критичне инфраструктуре свих развијених држава. Ти системи пружају повезаност између реалног и виртуелног света. Било који хакерски напад на системе могао би имати озбиљне последице.

Рачунарски напад који је трпела Естонија 2007. године, довела је до разматрања појма „рат“ и да се прилагоде новим друштвеним приликама. Тај напад у Естонији је био први случај да су политички, медијски и економски елементи унутар земље били истовремено мета, доводећи до привремене парализе државе. То је био први случај да је конфликт у сајбер простору попримио политичку димензију која је могла да ескалира у „класични“ ратни сукоб. То је такође био први случај да је суверенитет државе био директно угрожен рачунарским нападом који је био спроведен од стране недодирљивог непријатеља.

5.5. Друштвено - социјетални аспект кибер ратовања

Као битно обележје кибер ратовања може се сматрати и тенденција његовог померања изван војних граница на индивидуалну, друштвену и комерцијалну раван. Док је појмовно одређење информационог ратовања истицало његову војну димензију, данас се истиче његово проширење, ван војних области. Проширење изван војних активности је, у технолошком смислу , омогућено дифузном и децентрализованом структуром глобалне рачунарске мреже – Интернета.

Информационо-комуникационе технологије на глобалном нивоу увећавају улогу држава, организација, мултинационалних компанија, невладиних организација, транснационалних криминалних организација, а и појединаца. Савремене технологије омогућавају ширење информација, али исто тако и дезинформација. Природа сајбер простора је таква, да се токови информација тешко ограничавају и контролишу. Може се рећи да сајбер простор не познаје границе.

Оне државе које се ослањају на информационе технологије изложеније су, а исто тако и рањивије на било који облик штетне преправке, прекида или уништења технологија од којих зависе информациони токови.

Са друге стране неједнака доступности и способност коришћења информационих технологија, продубљује јаз између богатих и сиромашних друштава. Тај јаз присутан је и на међународном и унутар-државном нивоу. Уколико би тај јаз наставио да се шири, осећај усклађености код сиромашних популација могао би изазвати унутар-државне и међународне тензије.

Државе које су мање зависне од технологија не само да су мање рањиве, већ могу да искористе рањивост развијених држава за постизање својих стратешких циљева. Развијање офанзивних стратегија у сајбер простору не захтева високе инвестиције и стога оне су доступне великом броју актера. Кибер оружје могу развијати појединци или групе, за које су им једино потребно знање и мотивација. То омогућава државама којима до сада није придаван значај у стратешком контексту, да теже другачијој позицији у сајбер простору, где знање одређује равнотежу моћи.

У сајбер простору је мање изражена веза између безбедности и територије. Више није неопходно физички ући у неку територију, нити је напасти кинетичким оружјем. Комплетна контрола ваздушног и копненог простора не гарантује више безбедност

једној држави. Неопходно је развити нове стратегије одбране националне инфраструктуре, што је посебно тешко због природе сајбер напада.

Ако је сајбер напад извршен професионално , врло је тешко да се одреди порекло извршиоца и мотивације и то из више разлога:

- врло је лако сачувати анонимност у сајбер простору;
- напад се може извршити из било ког дела света, па чак и из више тачака;
- последице напада не морају бити видљиве одмах, већ се могу манифестовати тек након неког временског периода;
- тешко је открити средства и актере;
- технологија, која се користи је једноставна за коришћење;
- инструменти и технике за извршење напада се лако могу наћи у сајбер простору;
- успех напада је све већи – један напад може изазвати тешке последице.

Претња сајбер рата није лако уочљива, нити се актери могу категоризовати лако. Не постоји јасна идентификација актера. Непријатељске државе, војни савези, терористи, незадовољни радници, криминалне организације су само неки од примера, могућих актера. Сваки актер је мотивисан различитим циљем, ограничен ресурсима, сопственим могућностима и могућностима система да се брани. Тешко је пронаћи доказе у вези са непријатељским намерама, могућих нападача и да се изврши процена њихове реалне способности напада.

У прошлости информационо ратовање сматрало се искључиво војним питањем. Настанком сајбер простора проширује се скуп активности које подводе под појам информационог ратовања и уводи се употреба термина сајбер ратовања. Различити видови сукобљавања, сукобљавање између различитих актера помоћу специфичног, информационог оружја, промовисали су феномен сајбер ратовања у друштвено питање. Појам сајбер ратовања се употребљава, као збирни назив за свеукупност поменутих активности и тенденција. Појам сајбер ратовање се употребљава да опише широк распон активности на индивидуалном, друштвено - социјеталном, корпоративном-економском и војном нивоу.

5.6. Активности и иницијативе на међународном и националном нивоу

НАТО је организација која препознаје опасност од сајбер ратовања, званично посматра сајбер простор као подручје ратовања. Поред Америке, Русије, Кине, Велике Британије,

Израела, Ирана и Северне Кореје које се сматрају „сајбер силама“, појавиће се и други односно нови, како државни тако и недржавни актери са респектабилним капацитетима за деловање у сајбер простору. Око 120 држава има или развија офанзивну способност за сајбер напад. Сајбер одбрана је постала саставни део Процеса планирања одбране НАТО-а омогућујући лакши заједнички приступ развоју способности. Успостављање узајамно дефинисаних циљних области развоја способности који ће бити у складу са брзим променама претњи.

Све учесталији сајбер напади, стратегије и технологије сајбер ратовања доводе до стварања стручних сајбер центара. Ти центри се формирају у оквиру приватних компанија, националних ентитета као што су немачки National Cyber - Abwehrzentrum и међународних ентитета као што су NATO`s Cooperative Cyber Defence Center of Excellence – CCDCOE у Естонији и Европска организација за сајбер безбедност у Белгији.

Министарство одбране САД је формирало Сајбер команду 2009. године, као заједничку команду која управља и у којој се налазе представници свих видова. Сајбер команда се налази у оквиру Стратегијске команде. Процењује се да Стратегијска команда у свом саставу има негде око 6200 сајбер ратника.

Северна Кореја селектује студенте у основној школи за будуће сајбер ратнике. Ти студенти пролазе кроз средње и високо образовање, након чега аутоматски уписују Command Automation University у Пјонгјангу. Фокус образовања на том универзитету је упадање у рачунарске системе противника. Реализују се редовне обуке и вежбе сајбер ратовања. Процењује се да Северна Кореја има негде између 600 и 1000 лица за сајбер ратовање.

Мера способности за сајбер ратовање , поред офанзивног аспекта подразумева и дефанзивни аспект. Дефанзивни аспект односи се на способност да се преузму акције одбране уколико је дошло до напада, акције којима ће блокирати или ублажити напад.

6. БЕЗБЕДНОСНЕ ПРЕТЊЕ У САЈБЕР ПРОСТОРУ

6.1. Појам безбедносне претње у сајбер простору

Порекло сајбер претњи везује се за период настанка рачунарских мрежа. Интензивније се о сајбер претњама почело говорити тек, појавом глобалне рачунарске мреже – Интернета.

Информациони системи су изложени како класичним претњама тако и специфичним, односно новим претњама, попут електронских и сајбер напада. Оне претње за чије манифестовање је неопходно постојање рачунарске мреже на пољу сајбер безбедности, називају се сајбер претњама, тј. безбедносне претње у сајбер простору. Под појмом „сајбер претња“ подразумева се злонамерна употреба технологије које припадају сајбер простору, као инструмената претње и као циљева од стране великих броја актера попут криминалаца, терориста, држава и сл.

Сајбер претње су попут традиционалних, исто усмерене на информационо-комуникациони систем и информације које су садржане у њима, али су извори као и средства извршења, везана за сајбер простор.

6.2. Врсте претњи

Безбедносне претње у сајбер простору можемо поделити на:

1. Сајбер напади
    - Сајбер напади уз коришћење обмане:
      -Социјални инжењеринг;
      -Фишинг.
    - Сајбер напади техничког типа:
      -Напади помоћу малициозних програма (енг. Malwere)
      -Напади усмерени на опструкцију услуга (енг. Denial of Service Distributed и Denial of Service)

2. Злоупотреба сајбер простора као средство масовне комуникације:
    - Информационо ратовање;
    - Пропаганда;
    - Психолошки рат;
    - Обавештајна делатност.

6.3. Сајбер напади техничког типа

Сајбер напади користе било који облик слабости или рањивости система жртве. Уколико су изазвани људским фактором, реч је о социјалном инжењерингу, а уколико су наклоњени техничким рањивостима, њих називамо „технички напади“.

Јако је тешко набројати све нападе техничког типа. Реални напади се често изводе комбинацијом различитих техника, што додатно отежава њихову класификацију.

Сајбер нападе техничког типа можемо поделити на:

- напади који се изводе уз помоћ малициозних кодова и
- напади усмерени на опструкцију услуга циљаног рачунарског система

6.4. Напади помоћу малициозних кодова

Термин „malware“ означава посебну категорију информационих програма. Он има за циљ да оштети рачунарски систем корисника. Малициозни код оштећује рачунарски систем уз помоћ неауторизованих и неочекиваних процеса. Постоји више врста малициозних кодова и ту спадају: вирус, црв, споредна врата, тројански црв, програми за неауторизовано праћење активности корисника, програми за праћење и снимање оперативног рада корисника рачунара на нивоу микрооперације и отмичари. Инсталирањем малициозних програма је техника којом се инсталирају разне врсте програма којима се долази до података и информација или у ређим случајевима до уништења одређених информација или фајлова.

6.4.1. Вирус

Вирус је део сложенијег кода. Он се шири унутар једног рачунара или рачунарске мреже. То је програм који се „прикачи“ за други рачунарски програм и шири се између рачунара разменом фајлова. Такође се може активирати отварањем неког инфицираног фајла. Након инсталације софтвера, вирус је у стању да саморепликацијом зарази и остале фајлове у рачунару или рачунарској мрежи, без знања корисника. Има за циљ да изврши мали број операција и да притом остане невидљив. Неки проузрокују само мања узнемиравања, док други праве деструкцију или краду податке. Главна сврха је да се реплицира и копира што више може. Секундарни циљ је да успори мрежу, приказује узнемиравајуће поруке и уништава фајлове или садржај хард диска.

6.4.2. Црв

Црв се реплицира сам, без људске интервенције, за разлику од вируса коме је неопходна људска интервенција. Активира се аутоматски и шири захваљујући мрежи и не везује се за друге програме и фајлове да би се ширио и умножавао. За транспорт овакве врсте инфекције користи се електронска пошта или мрежа. Црв углавном користи технике социјалног инжењеринга како би навео примаоца да отвори поруку. Преко мреже се шири, тако што се у датотеке које размењују корисници, инфилтрира и наводи кориснике да преузму те фајлове на рачунар и инсталирају. Он може да оштети заражени систем а исто тако и да буде преносилац других малициозних програма.

6.4.3. Споредна врата

Споредна врата представља програм, који омогућава неауторизовани приступ систему. Он се шири најчешће у комбинацији са црвом или тројанским коњем. Међутим, може се и намерно инсталирати на рачунару од стране ауторизованих корисника. Намерна инсталација подразумева заобилажење сигурносних процедура у хитним случајевима.

6.4.4. Тројански коњ

Тројански коњ представља врсту злонамерног кода, који не може да се самореплицира. Састоји се од кода, који углавном извршава одређене злонамерне активности. Углавном је он убачен у неку апликацију, где у позадини извршава своју функцију и на тај начин је много теже да се детектује. Он мора бити послат намерно. Може бити прикачен уз апликацију или програм или да се шаље уз вирусе и црве. Тројански коњ се користи за

прикупљање података или наношење штете. Углавном се користи за прикупљање поверљивих информација, података, докумената, података о кредитним картицама, података везаних за шифре и адресе електронске поште.

6.4.5. Програми за неауторизовано праћење активности корисника

Програм за неауторизовано праћење активности софтвера представља софтвер, који се користи за прикупљање информација из система на ком је инсталиран. То је шпијунски програм који информације које је прикупио, шаље заинтересованом кориснику. Такође се може, као и тројански коњ, користити техникама социјалног инжењеринга и инсталирати на рачунар без знања корисника. Активира се у тренутку покретања инсталираног програма.

6.4.6. Програми за праћење и снимање оперативног рада корисника рачунара на нивоу микрооперација

Оваква врста програма меморише сваку команду откуцану на тастатури и израђује слике радне површине нападнутог рачунара. За инструменте који прате и снимају целокупан рад на рачунару, користи се назив *keylogger*. Постоји хардверски и софтверски *keylogger.* Хардверски се физички повезује, каблом између тастатуре и рачунара или са тастатуром рачунара. Јако лако се инсталирају. Софтверски *keylogger* је програм који контролише и меморише редослед типки које корисник притиска и шаље их другом рачунару. Он се углавном преноси преко тројанског коња или црва.

6.4.7. Отмичар

Отмичар је посебна врста програма, којим се преузима контрола над апликацијама за навигацију у мрежи и изазивање аутоматског отварања нежељених веб страница. То су малициозни програми који преузимају контролу над програмима за приступ интернету.

6.5. Напади усмерени на опструкцију услуга

Лишавање услуге (DoS) и дистрибуирано лишавање услуга(DDoS) су сајбер напади, који имају за циљ да онемогуће коришћење услуге рачунарских мреже или информационих ресурса. Нападају системе који омогућавају те услуге. То је врста напада која циља на доступност информација, а не на њихову поверљивост. Њихов циљ није крађа информација. Штета која се проузрокује нападом DoS испољава се у времену које је

неопходно да би се поново покренуо систем. Уколико су мета напада, економске организације, за њих би то представљао и велики економски губитак.

DDoS напад се започиње тако што нападач присваја контролу над првим рачунаром, који постаје „мастер“ напада. Потом се преко њега инфицирају остали рачунари, црвом или bot-ом. Инфицирани рачунари могу истовремено да покрену напад DDoS против циља који је изабрао нападач.

6.6. Сајбер напади уз коришћење обмане

6.6.1. Социјални инжењеринг

Социјални инжењеринг користи везу и односе између људи за постизање циља, путем различитих метода убеђивања. Нападач покушава комуникацијом да наведе мету напада да прекрши безбедносне норме или процедуре, а да притом не примети да је изманипулисана.

Социјални инжењеринг је једна од најбољих техника напада, фокусира се на слабост људског фактора. Крајни циљ социјалног инжењеринга је долажење до информација која се користи у различите сврхе које су штетне, по власника те информације.

Особе које врше социјални инжењеринг су веома интелигентне и креативне. Поседују добре комуникативне и манипулаторске вештине, добри су познаваоци психологије. Делују тимски или самостално. Напади социјалног инжењеринга користе комуникацију како би се жртва преварила и урадила неку компромитујућу ствар, попут откривања личних информација.

Социјални инжењеринг може да се подели у односу на постојање или непостојање комуникације и контакта између мете напада и нападача и то на:

- Извршење контактом (директни контакт, контакт телефоном или преко социјалних мрежа);
- Извршење без контакта (помоћу малициозних софтвера, постављањем интернет адресе на форум или подметањем неког меморијског медија)
- Комбиновани начин извршења

Технике које користи социјални инжењеринг су:

- Техника лажног представљања,
- Техника обрнутог социјалног инжењеринга,
- Техника искоришћења немара, непажње и незнања мете напада.

Посебна врста напада који користи технике социјалног инжењеринга јесте фишинг.

6.6.2. Фишинг

Крајњи циљ социјалног инжењеринга је долажење до одређене информације, што је и крајњи циљ фишинга. Фишинг подразумева илегално прикупљање информација добијених обманом у сајбер простору. Нападач шаље електронску пошту потенцијалним метама, убеђујући их да посете интернет-страницу која им звучи познато да би решили неки измишљени проблем. Фишинг је техника социјалног инжењеринга која се извршава без контакта преко електронске мреже.

Напад се започиње тако што нападач настоји да усмери жртву ка одређеној интернет страници и на њој оставља личне поверљиве информације. На тај начин нападач преузима идентитет жртве, да би извршио незаконите радње односно незаконите финансијске трансакције. Мета напада трпи значајне финансијске губитке, а исто тако и губитак електронског идентитета.

Фишинг представља глобални проблем нарочито због флуидности мреже и података који се путем ње могу разменити. Фишингом су највише погођени сектор финансијских услуга, интернет-сервис-провајдери и трговински ланци. Напади су базирани на недостатку безбедносне културе информатизованих маса. Интернет корисници нису спремни да се самостално и на адекватан начин, суоче са претњама у сајбер простору. Масовна распрострањеност финансијског пословања „из фотеље“ у комбинацији са неискуством корисника у области сајбер безбедности, до сада су осигурали лаку зараду „електронским“ криминалцима.

7. САЈБЕР ОРУЖЈЕ

Сукоби су део људске природе, а друштва су их одувек водила у складу са својим искуством, вештинама, знањем и расположивим ресурсима. Исто тако их и данас воде у складу са новим технологијама и друштвеним односима.

Људи су одувек користили оружје, прво ради лова а касније, са ширењем друштвених сукоба и у вођењу ратова. Оружје се дефинише као средство, инструмент којим се извршава напад, или се користи за остваривање неког циља везан за сукоб са другом страном. Тај циљ је повезан са ефектима дејства оружја, тј. убијање, повређивање људи, уништење или оштећење техничких система или објеката, при чему је довољно да се оствари бар неки од ефеката на циљ.

По *Оксфордском речнику* појам „оружје“ обухвата „инструмент било које врсте, употребљен у ратовању или у борби ради напада и савладавања непријатеља“. Ова дефиниција истиче постојање циља при примени оружја у сврху савладавања противника, што, у суштини, представља вођење сукоба. Међутим није свако оружје средство којим се води сукоб или рат. *Мериам-Вебстер* речник, оружје дефинише као „нешто што се користи за борбу или напад на неког или за властиту одбрану када неко напада“, односно, „нешто што је употребљено да се победи у такмичењу или да се нешто постигне“. У *Речнику српскохрватског језика Матице Српске* термин „оружје“ обухвата било које оруђе за напад или одбрану, укључујући сопствени део тела и опреме или неки екстерни инструмент чија основна сврха не мора бити повезана са актом нападања и са циљем да се озледи или убије противник, односно да се уништи или онеспособи објекат напада. (Младеновић, 2016)

Организација за економску сарадњу и развој (ОЕБС) дефинише сајбер оружје на следећи начин:

„Сајбер оружје обухвата: неауторизован приступ системима, вирусе, црве, тројанце, нападе ускраћивање сервиса, дистрибуиране нападе ускраћивањем сервиса, рутките и употребу социјалног инжењеринга. Резултати напада могу укључивати: нарушавање поверљивости/крађу тајни, крађу идентитета, нарушавање веб-презентација, уцену, преузимање система или блокирање сервиса. Сајбер оружје се употребљава индивидуално, у комбинацији и симултано са конвенционалним „кинетичким“

оружјима, као мултипликатор њихове моћи. Поуздано се може предвидети да ће сајбер оружје ускоро постати свеприступно“. (Младеновић, 2016)

Ово одређење обухвата средстава и технике сајбер напада и њихове циљеве, због чега се може сматрати да је потпуно. Набрајање постојећих врста злонамерних система, техника и метода напада не може да пружи добар основ за дефинисање појма сајбер оружја. Технологија сајбер напада се брзо мења и њен развој доводи до појаве нових система и техника. Дефиниција наводи могућност комбинације употребе информационих система и традиционалних средстава напада и предвиђа развој сајбер оружја у складу са развојем технологије.

Сукоби у сајбер простору се извршавају извођењем сајбер напада. Њихово средство и циљеви су информациони системи и процеси. Примена информационо-комуникационих технологија у савременим друштвима је комплетна и њихов значај за функционисање људи и система је велики и значајан. Информациони системи се користе и у војним и у цивилним организацијама. Информационо-комуникационе технологије се у друштву користе за све савремене функције, укључујући и оне од критичне важности за безбедност и одбрану. Војне организације их користе као основу процеса командовања, подршке и извођења војних операција. Дакле, сајбер оружје и сајбер нападе је неопходно анализирати заједно, са обзиром да је њихова природа повезана на нивоу истих технологија, и у оквиру истог процеса вођења сукоба у сајбер простору.

Сајбер ратовање подразумева вођење сукоба између нација и то у сајбер простору применом информационо-комуникационих технологија. Природа сајбер ратовања зависи од примене информационо-комуникационих технологија. За разлику од традиционалног сукоба, учесници у сукобу нису наоружани нити су организовани у борбене јединице. Довољно је да имају циљ и интерес, да делују на противничке системе, да располажу са информацијама о рањивостима информационог система противника и знањем да открију и искористе те рањивости. Сајбер напад зависи од постојања рањивости у систему, од способности да је нападач искористи за неовлашћени упад и знањем да се креира скуп инструкција којим ће се остварити дејство на противнички систем. Уколико нема рањивости или информација о рањивости, као ни неопходног знања нападача да ту рањивост искористи, напад се не може извести. На тај начин, оружје у традиционалном сукобу се може употребити са поседовањем информације, знањем и вештином да се оно искористи. Иако се за сајбер напад често користи припремљен софтвер , суштина сајбер напада није у малверу као производу, већ у

организацији, вештини и знању да се напад оствари. Дакле, сваки сајбер напад је процес који се састоји од проналажења и искоришћења рањивости у нападнутом систему и остваривања жељених ефеката на циљ.

Употреба информационих технологија се шири. Технологија постаје све сложенија, самим тим се повећава и број и озбиљност могућих сајбер напада. Нови концепти попут манипулације великом количином података, квантног рачунарства, опште умрежености, дистрибуиране производње средстава омогућене информационим технологијама, роботике и вештачке интелигенције, доносе нове облике сајбер напада. Међутим, сви они се налазе у основи информационе безбедности, па се сајбер ратовање може назвати и применом информационе безбедности у сврху вођења сукоба.

8. САЈБЕР БЕЗБЕДНОСТ

Сајбер безбедност представља релативно нов појам, који се односи на информациону безбедност у сајбер простору.

По ISO/IEC 27032:2012 стандарду, сајбер безбедност је „очување поверљивости, интегритета и доступности у сајбер простору“. (Младеновић, 2016)

По Међународној телекомуникационој унији, сајбер безбедност представља: „скуп алата, политике, безбедносних концепата, безбедносних мера, упустава, приступа управљању ризиком, акција, тренинга, најбољих пракси, обезбеђења и технологија које могу бити употребљене за заштиту сајбер окружења и организационих и корисничких ресурса“. (Младеновић, 2016)

По EastWest институту, сајбер безбедност је, „својство сајбер простора које представља способност супростављања намерним и/или ненамерним претњама, одговара на њих и опоравка“. (Младеновић, 2016)

По Инструкцији америчког Министарства одбране 8500.01, сајбер безбедност је „превенција од штете на, заштита од, и обнова рачунара, електронских комуникационих система, електронских комуникационих сервиса, жичаних комуникација и електронских комуникација, укључујући и информације у њима, са циљем да се обезбеди доступност, интегритет, аутентичност, поверљивост и непоречивост. (Младеновић, 2016)

По Концепту стратегије сајбер безбедности Руске Федерације, сајбер безбедност представља „скуп услова под којим су све компоненте сајбер простора заштићене од максималног броја претњи и утицаја са нежељеним последицама“. (Младеновић,2016)

По Речнику за национално информационо обезбеђење, Комитета за националне системе, као и по Речнику кључних термина информационе безбедности НИСТ института, сајбер безбедност је „способност заштите или одбране употребе сајбер простора од сајбер напада“. (Младеновић, 2016)

На основу претходних дефиниција може да се утврди да се сајбер безбедност односи на примену, стање или способност успостављања информационе безбедности у сајбер простору, који настаје умрежавањем појединачних информационих система.

Иако се често користи термин информациона безбедност како би се означила сајбер безбедност, реч је о потпуно два различита појма. Са обзиром да информациона безбедност представља очување поверљивости, интегритета и доступности информација, а сајбер безбедност се односи на информациону безбедност у сајбер простору.

9. ЗАКЉУЧАК

Сајбер ратовање је ратовање у сајбер простору. Оно се разликује од традиционалних облика ратовања која су се водила у физичком простору. Да би се разумео појам сајбер ратовања неопходно је прво да се дефинише сајбер простор. Сајбер простор представља дигитални свет који је конструисан помоћу рачунарске мреже-Интернета.

Сајбер ратовање је ограничено на сајбер простор и да би се оно могло извести, неопходна је примена информационих система. Присуство информационо-комуникационих система у физичком и друштвеном окружењу ствара услове за преузимање сајбер сукоба или ратовања. Да би се циљ могао постићи, неопходно је да у информационим системима и сајбер простору постоје уграђени недостаци. Уколико су ти недостаци познати нападачу оне постају рањивост система и могу се искористити за напад на информациони систем жртве. Оружје које се користи за сајбер напад није материјалне природе. Оно је процес проналажења рањивости система и искоришћење тих рањивости, како би се пробило, или заобишли безбедносни механизми заштите система.

Сваки сајбер напад који је изведен од стране неког ентитета против државе и њеног друштва, представља сајбер ратовање. Актери који организују ратовање могу бити државни или недржавни.

Дакле, сајбер ратовање представља облик информационог ратовања, који се састоји од низа активности којима се прекидају или уништавају, информациони или комуникациони системи противника. Сајбер напади могу имати одложено или тренутно дејство. Операције сајбер ратовања могу остати и неоткривене након што се дејство оствари. Нападачи, односно актери сајбер ратовања су анонимни и у већини случајева тешко је или немогуће утврдити државну одговорност, за покретање сајбер напада. Природа, средства и последице сајбер ратовања се мењају у складу са развојем технологије.

Што се тиче капацитета за сајбер одбрану и ратовање, на примеру ЕУ,НАТО и заједници „Пет очију“, дошло се до закључка да је основ за испољавање националне моћи у сајбер простору, заснован на снази и усмерености националних интереса, а не на величини и обиму заједнице и расположивих материјалних ресурса.

Сајбер ратовање од настанка до данас показало је велику моћ еволуције и развоја. Оно се првенствено огледа у капацитетима за остваривање дејства на противника и

последицама дејства на циљ. Може се очекивати да ће се оно брзо еволуирати у нове, знатно опасније и разорније форме.

10. ЛИТЕРАТУРА

1. Вулетић, Д. В. (2017). Употреба сајбер простора у контексту хибридног ратовања. Војно дело, 69(7), 308-325.
2. Вулетић, Д. В., Миленковић, М. Р., & Ђукић, А. Р. (2021). Сајбер простор као подручје сукобљавања- случај САД- Иран и Северна Кореја. Војно дело, 73 (1), 1-14.
3. Младеновић, Д. Д., Јовановић, Д. М. & Дракулић, М. С. (2012). Технолошки, војни и друштвени предуслови примене сајбер ратовања. Војнотехнички гласник, 60(1), 70-98.
4. Младеновић, Д. Д., Јовановић, Д. М., & Дракулић, М. С. (2012). Дефинисање сајбер ратовања. Војнотехнички гласник, 60(2), 84-117.
5. Младеновић, Д. Д., Дракулић, М. С., & Јовановић, Д. М. (2012). Међународно право и сајбер ратовање. Војно дело, 64(1), 9-39.
6. Младеновић, Д. Д., Дракулић, М. С. & Јовановић, Д. М. (2011). Неутралност и сајбер ратовање. Војно дело, 63(3), 189-220.
7. Митровић, М. (2018). Јавна дипломатија у парадигми хибридног концепта сукоба. Војно дело, 70(2), 309-325.
8. Младеновић, Д. Д. (2016). Мултидисциплинарни аспекти сајбер ратовања. Докторски рад. Београд: Факултет организационих наука
9. Милашиновић, Р., Милашиновић С., & Путник Н. (2012) Теорије конфликата. Београд: Факултет Безбедности, стр. 253-268.
10. Мандић, Ј. Г. (2015). Системи обезбеђења и заштита правних лица. Београд: Факултет безбедности, стр. 272-298.
11. Путник, Н. (2009). Сајбер простор и безбедносни изазови. Београд: Факултет безбедности, стр. 69-89.
12. Путник, Н., & Миљковић, М. (2012). Злоупотреба кибер простора као средства масовне комуникације. Војно дело, 64(3), 157-183.
13. Путник, Н., Милошевић, М., & Бошковић, М. (2017). Стратешко планирање сајбер одбране- ка адекватнијем правном оквиру и новој концепцији процене ризика, изазова и претњи. Војно дело, 69(7), 174-185.
14. Ђукић, А. (2018). Организовани високотехнолошки криминал – појам, развој и основне карактеристике. Војно дело, 70 (3), 128-156.