Сајбер безбедност

ИНТЕРН

ОПАСНО ОРУЖЈЕ У РУКАМА ТЕРОРИСТА

Знање у области информационих технологија један је од примарних ресурса савременог друштва. Услед све већег ослањања виталних државних инфраструктура на рад технологије, сајбер тероризам постаје још актуелнија форма тероризма.

Пише др Ивана ЛУКНАР, аутор монографије *Сајбер тероризам – мере за сузбијање и превенција*, у издању Института за политичке студије у Београду

ЕТ

Развој технологије и примена савремених технолошких иновација, нарочито информационих и комуникационих технологија, изменили су начин на који функционише свет. Генерално посматрано, савремена друштва се у значајној мери ослањају на интернет, нарочито услед глобализације и пандемије ковида 19. Она, дакле, нису у истој мери „везана" за свој географски положај, државу или нацију као претходна, јер постоје у сајбер простору кроз различите системе комуникација и умрежавања. Интернет је знатно изменио функционисање целокупног друштва и његових кључних националних и међународних структура, а изменио је и начин пословања и свакодневног живота. Поред бројних предности, развој технологије изнедрио је нове опасности и форме криминала. Криминалне групе се такође служе погодностима интернета за спровођење различитих малверзација и злоупотреба. Док је широм света расла примена интернета и паметних уређаја, сајбер инциденти су постајали све учесталија и значајнија претња. Таква ситуација у први план поставила је проблем сајбер безбедности.

САЈБЕР АКТИВИЗАМ

Информационе и комуникационе технологије поједноставиле су комуникацију и пружају бројне могућности појединцима и осталим групним актерима. Интернет има потенцијал за мобилизацију и оснаживање друштвено искључених и мање привилегованих појединаца и група. Кориснику интернета омогућено је да врши претраживање и лако пронађе друштвену групу, политички субјект или покрет који је у складу са његовим интересовањима и ставовима, независно од садржаја који су локално расположиви. Као последица тога настају виртуелне (сајбер) заједнице, чији чланови осећају припадност групи исто као и чланови било које друштвене

групе која постоји у реалном физичком свету. Интернет је омогућио корисницима да критикују или промовишу одређене политичке идеје, искажу апел или незадовољство постојећим системима моћи. На тај начин је отворен простор за нову форму активизма, тзв. сајбер активизам, који, иако се одиграва у онлајн окружењу (сајбер простору), може значајно да утиче на актуелна дешавања у реалном друштвено-политичком животу. Тако се знатан део друштвено-политичке арене смешта у сајбер простор, који је постао далеко конкретнији простор за друштвено-политичке борбе од класичних националних политичких система. Таква ситуација олакшава појаву нових типова политичких субјеката, који постоје изван формалног политичког система, а имају значајну подршку јавности (инфлуенсери, телевизијска лица, спортисти и др.). Интернет нуди и алтернативне садржаје због којих је интересантан различитим друштвено-политичким актерима и може да буде опасно оруђе у рукама терориста.

ТЕРОРИСТИ И ИНТЕРНЕТ

Између тероризма и интернета постоји вишеструка веза. Познато је да се терористи служе интернетом (dark web, chat room) обављајући своје активности, као што су: интерна комуникација, ширење пропаганде, вођење кампање психолошког ратовања, промовисање идеја, слање порука мржње, радикализовање регрута путем различитих видеа и порука. Такође, на интернету постоје снимци обука терориста и учињених дела насиља који треба да скрену пажњу светске јавности и изазову панику широких размера. Опасност од тероризма је константна, а он се временом мењао. Савремени тероризам је попримио толико опасне и широке размере да се сматра једном од највећих опасности данашњице. Терористи се служе различитим средствима, отуда се тероризам јавља у различитим облицима. С обзиром на технолошки развој и актуелна дешавања у свету, једна од најактуелнијих врсти тероризма управо је сајбер тероризам. Такође, временом су се мењале и тежње терориста. „Традиционални" терористи углавном су били усмерени против тековина савремене демократске државе и њених структура моћи, док је савремени тероризам углавном усмерен против постојећег поретка моћи и економско-енергетских система, како у националним, тако и у међународним оквирима. Без обзира на облик у којем се јавља, тероризам подразумева насиље које је политичко-идеолошки мотивисано против неке или нечије власти. Такође, може да подразумева и насиље неких држава које су означаване као спонзори тероризма.

> Кориснику интернета омогућено је да врши претраживање и лако пронађе друштвену групу, политички субјект или покрет који је у складу са његовим интересовањима и ставовима, независно од садржаја који су локално расположиви. Као последица тога настају виртуелне (сајбер) заједнице, чији чланови осећају припадност групи исто као и чланови било које друштвене групе која постоји у реалном физичком свету.

САЈБЕР ТЕРОРИЗАМ

Савремене државе света утркују се у развијању нових технологија и у њиховој примени. Отуда је њихова инфраструктура, поред традиционалних физичких средстава, великим делом сачињена од средстава у онлајн (сајбер) простору, док је знање, нарочито у области информационих технологија, постало један од примарних ресурса савременог друштва. Та чињеница има за последицу рањивост државне инфраструктуре у сајбер простору коју је потребно свести на минимум. Сајбер тероризам је форма тероризма која са применом савремених информационих и комуникационих технологија постаје све актуелнија. Услед све већег ослањања виталних државних инфраструктура на рад технологије, сајбер тероризам постаје још актуелнији. Истовремено, рат између Русије и Украјине, економска и енергетска криза стварају тензије које подстичу извођење различитих сајбер активности. Најмоћније државе света издвајају велика финансијска средства за наоружање и технолошки развој, чиме се енормно увећавају капацитети за уништење планете и нарушава глобална безбедност.

Сајбер тероризам представља озбиљну претњу. У поређењу са традиционалним облицима тероризма релативно је лак за извршење и осим знања из ИТ области и технолошке опремљености не захтева додатну организацију и ризик по извршиоца. Извршиоцу пружа анонимност, односно могућност да изврши напад под лажним профилом, виртуелним идентитетом, са лажне адресе, без улагања великог физичког напора и употребе конкретног оружја, без обзира на реалну удаљеност од мете напада. Истовремено, акт сајбер тероризма може да причини штету великих размера и губитке људских живота. Владини званичници и представници одбране сајбер тероризам одређују шире, као било који напад у виртуелном (сајбер) простору којим се угрожава безбедност. Ту спадају и напади на компјутере и рачунарске мреже, уколико су њихови ефекти у толикој мери деструктивни да изазивају страх који је упоредив са физичким терористичким актом. Сајбер тероризам може да узрокује и прекид рада критичних националних инфраструктура (као што су енергија, јавни превоз, владине активности).

За извођење напада сајбер терористи служе се различитим методама које се мењају и развијају упоредо са технологијом. Можемо их класификовати у три основне категорије. Прву категорију представља класичан физички напад који је усмерен против компјутерске опреме, објекта или далековода чији је циљ да омета и онемогући правилан рад и функционисање, ремети поузданост опреме. За ову врсту напада сајбер терористи углавном примењују конвенционално оружје (нпр. ватрено оружје или експлозив). Другој категорији припада електронски напад који подразумева употребу електромагнетне енергије, односно електромагнетног пулса који је усмерен против компјутерске опреме с циљем да онемогући, омете или угрози пренос и интегритет података (прегревање струје или ометање комуникација). Трећој категорији припада напад на компјутерске мреже (CNA – Computer Network Attack) који подразумева сајбер напад који је усмерен на рачунарски процесни код, његову логику и инструкције или податке.

САЈБЕР ТЕРОРИЗАМ И САЈБЕР НАПАД

Као комплексан и динамичан проблем, сајбер тероризам захтева добро познавање и разумевање. Како разликовати сајбер тероризам од сајбер напада? Сајбер напад подразумева сукоб који се одвија у виртуелном (сајбер) простору и може да буде вођен самостално или као вид подршке неком другом сукобу. Сајбер тероризам може да се посматра као посебна врста сајбер напада и, истовремено, посебна врста тероризма. Оно што јасно разликује сајбер тероризам од осталих онлајн злоупотреба је употреба информационих – компјутерских технологија као оружја или мете напада. Карактеришу га и политичка мотивација и тежња ка симболици, спектакуларности, публицитету. Намера сајбер терористе је, као и код осталих форми тероризма, да се причини значајна материјална штета и/или људске жртве, или претња таквим последицама. Његов циљ је извођење злонамерног поступка који садржи неку врсту насиља са далекосежним психолошким ефектима код циљаног аудиторијума. Дакле, намера је комбинована са дугорочним циљем (нпр. друштвене или политичке промене, утицај на политичко одлучивање) којем тежи терориста или терористичка група, као и ширењем страха већих размера.

САЈБЕР ТЕРОРИЗАМ И ОРГАНИЗОВАНИ КРИМИНАЛ

На путу до остварења свог примарног циља, који је готово увек идеолошке природе, терористи се неретко служе разним криминалним радњама. Иако између тероризма и организованог криминала постоје сличности, ова два облика криминалних делатности се јасно разликују. Организовани криминал је комплексна криминолошка појава која постоји у различитим облицима широм света. Као и тероризам, представља константну опасност која се различито тумачи у националним законодавствима, тешко га је препознати и на

НАЦИОНАЛНИ СИСТЕМ ЗА СУПРОТСТАВЉАЊЕ ТЕРОРИЗМУ

Република Србија има развијен и модеран антитерористички национални систем, чији су институционални капацитети један од подсистема унутар националног система Републике Србије. Национални систем за супротстављање тероризму постоји од када постоји и тероризам на подручју наше земље, карактеришу га динамичност и константно усвршавање и реорганизовање с циљем превенције и што ефикаснијег суочавања са делима тероризма. Влада Републике Србије је препознала претње које произлазе из сајбер простора и нормативно-правно их регулисала.

њега адекватно реаговати. Оно по чему се сајбер тероризам суштински разликује од организованог криминала је његов идеолошко-политички карактер. Примарни циљ организованог криминала је стицање профита и моћи. Чак и када садржи политичко-социјалну компоненту, као што је деловање у сарадњи са терористичким групама, герилским организацијама или сарадња са разним друштвено-милитантним покретима, он не подразумева криминалне активности чији је примарни циљ политичко-идеолошке природе. Тада је у питању прибављање тренутне користи или интереса кроз разне активности, као што су: прање новца, организовање трговине људима, отмица, производња и дистрибуција различитих наркотика, формирање лоби група итд. Односно, организовани криминал је неидеолошко удружење једног броја лица која међу собом остварују врло блиске друштвене интеракције с циљем стицања профита или моћи.

Између тероризма и интернета постоји вишеструка веза. Познато је да се терористи служе интернетом (dark web, chat room) обављајући своје активности, као што су: интерна комуникација, ширење пропаганде, вођење кампање психолошког ратовања, промовисање идеја, слање порука мржње, радикализовање регрута путем различитих видеа и порука.

САЈБЕР КРИМИНАЛ

Починиоци сајбер криминала служе се разноврсним средствима унутар рачунарских система да би прибавили противправну корист за себе или учинили штету неком физичком или правном лицу. Сајбер криминал, високотехнолошки криминал или компјутерски криминалитет су синоними и служе да означе широк спектар криминалних поступака, те не обухватају само нападе који се могу извести употребом телекомуникационих мрежа, него и нападе на саме информационе системе. Употреба компјутерских технологија за извршење кривичних дела отворила је многа питања, стога је појму општег криминалитета придодат и компјутерски криминал. Карактерише га прогресивност, те се државе широм света суочавају са изазовом да прилагоде своју правну регулативу и пропишу адекватне мере кажњавања за поменуто противправно деловање. Сајбер криминал је дело учињено зарад неке личне користи, док се сајбер тероризам односи на злочине који подразумевају употребу информационих технологија у политичке сврхе. Софистицирани напади нове генерације навели су државе широм света да развијају стратегије и мере одбране у сајбер простору. Једино добро познавање и разумевање савремене ситуације може да доведе до адекватног реаговања надлежних органа и правног система, ефикасног откривања и доказивања кривичних дела која спадају у овај облик криминалитета. Неопходна је и континуирана сарадња и познавање међународних правних регулатива.