DCAF Geneva Centre for Security Sector Governance

ВОВЕД ВО УПРАВУВАЊЕТО СО САЈБЕР БЕЗБЕДНОСТ – ПРИРАЧНИК ЗА ПРАТЕНИЦИ

ВОВЕД ВО УПРАВУВАЊЕТО СО САЈБЕР БЕЗБЕДНОСТ – ПРИРАЧНИК ЗА ПРАТЕНИЦИ

Автори

Франциска Клопфер

Франциска е Проект координатор во Одделението за Европа и Централна Азија во ДЦАФ.

Ирина Ризмал

Ирина е Проектен асистент во Одделението за Европа и Централна Азија во ДЦАФ.

Милан Секулоски

Милан е Национален проект менаџер во Одделението за Европа и Централна Азија на ДЦАФ.

Тереза Хатцл

Тереза е поранешен Проектен службеник во Одделението за јавно – приватни партнерства на ДЦАФ.

Д-р Драган Младеновиќ

Драган е експерт за сајбер безбедност и сајбер одбрана.

СОДРЖИНА

Вовед

Сајбер безбедноста е едно од најновите подрачја во политиките за национална безбедност кое станува се поважно во безбедносните сектори на европските држави. Креаторите на политики се уште не се во чекор со технолошките новитети кои ги користат различни пријателски и непријателски страни. Ова бара брз и сеопфатен развој на нови правни и политички рамки. Покрај осигурувањето на државната безбедност, безбедните и сигурни мрежи се исто така важни за зајакнување на државната економија и модернизацијата на управувањето со јавниот сектор во државите на Југоисточна Европа (ЈИЕ) (размислете, на пример, за суштинската важност на една безбедна мрежа за доброто функционирање на услугите за е-владеење). Безбедниот сајбер простор е исто така неопходен за да може граѓаните да ги уживаат своите права, како што се пристапот до информации и слободата на изразување. Поради тоа, од суштинско значење е да се биде свесен за можностите, ризиците и заканите кои што ги носи сајбер просторот.

Пратениците имаат витална улога во развивањето на законодавни и институционални рамки за сајбер безбедност, како и во гарантирањето дека принципите на доброто владеење се применуваат во сајбер безбедноста. Покрај одговорноста за усвојување на нови законодавства, тие ја имаат и моќта да ги свикуваат различните заинтересирани страни за дискусии околу политиките, со што се обезбедуваат сеопфатни модели на управување – работа која е од особено значење во сајбер безбедноста. На крајот, пратениците имаат и улога на куче чувар, преку надзор над имплементацијата на законите и политиките за (или поврзани со) сајбер безбедноста.

Имајќи ги на ум овие одговорности, од огромна важност е пратениците да бидат информирани за најновите развои во сајбер безбедноста и да бидат опремени со соодветно знаење и разбирање за да можат да работат на политики и да дискутираат имајки ги при рака сите релевантни информации . Оваа публикација има за цел да им обезбеди на пратениците кои што се вклучени во подготовката на законодавството и надзорот над прашањата на сајбер безбедност, основен преглед на главните прашања, трендови и предизвици во управувањето.

Овој вовед, Прирачник за пратеници, ги објаснува главните елементи на сајбер безбедноста и нејзиното управување: сајбер криминал, сајбер војна, сајбер тероризам, сајбер шпионажа, и хактивизам и предизвиците и можностите со нивното управување. Секое поглавје е дополнето со список на на можни прашања кои што пратениците можат да ги постават во поглед на темата. Прашањата имаат за цел зголемување на отчетноста на владата и други клучни заинтересирани страни во сајбер безбедноста. Тие можат да бидат вклучени во прашања до владата, разгледувани на јавни расправи или за собранискиистраги.

ДЕЛ 1 – КЛУЧНИ КОНЦЕПТИ

Потреби, политики и стратешки цели на сајбер безбедноста

Со појавата на интернетот и се поголемата употреба на интернетот, стана неопходно повторно да се проценат безбедносните ризици и справувањето со нив. Сегашното информатичко доба ги постави информациите и сајбер безбедноста во преден план како важни аспекти на индивидуалната, организациската, државната и меѓународната безбедност. Според ИСО/ИЕЦ стандардот, карактеристики[1] на сајбер безбедноста се „зачувувањето на доверливоста, интегритетот и достапноста на информациите"[2],.

Во концептот на доброто управување со безбедносниот сектор, безбедносните политики имаат за цел не само осигурување на безбедноста на државата, туку и безбедноста на поединецот. Примената на овој пристап кон интернетот значи дека сајбер безбедноста треба да се стреми кон креирање на безбеден интернет простор за сите. За да го постигне ова, политиката за сајбер безбедност мора да покрива голем број на прашања, од заштитата на државниот интегритет и гарантирањето на човековите права, до спроведувањето на законите и спречувањето на кривични дела извршени во, или со користење на сајбер просторот. Според тоа, прашањата на управувањето со сајбер безбедноста треба не само да одговорат на прашањето за одржување на безбедноста и отпорноста на интернет, туку и на градењето безбедност и поттикнувањето можности на интернет.

Според тоа, прв чекор во подготовката на успешна сајбер политика и стратегија е дефинирање на безбедносни цели и одредување што значи одржувањето на безбедноста и градењето на интернет сигурноста за државата и нејзините граѓани. Треба да се дефинираат критичните ресурси кои се суштински во заштитата на нормалното функционирање на државата и општиот интегритет на животот на интернет. Електричните мрежи и клучните интернет услуги се очигледни примери на критични ресурси кои бараат значително внимание и заштита. Истовремено, главните фактори на ранливост во сајбер безбедноста се јавуваат поради човечки грешки и технички дефекти. Неупатените интернет корисници кои одат на погрешен линк се најчестата причина за сајбер инциденти. Образованието и подигањето на свеста на корисниците се според тоа исто толку важни за превенцијата во сајбер безбедноста како што е добрата технологија и поставување на вистински експерти за користење на таа технологија.

---

1 Некои дефиниции на сајбер безбедноста вклучуваат и други карактеристики на информациите, како што се автентичност, отчетност, непобивање и веродостојност, покрај трите горе наведени.

2 Меѓународна организација за стандардизација (2016). ISO/IEC 27000:2016(en) Информатичка технологија — Техники за безбедност — Системи за управување со безбедноста на информациите — Преглед и речник.

Предизвици во управувањето со сајбер безбедноста

Откако ќе се дефинираат целите на сајбер безбедностамора да се постави рамка за управување која ги одредува улогите и одговорностите на различните страни во постигнувањето на целите. Суштински предизвик во управувањето со сајбер безбедноста е фактот дека во меѓународното право и стандарди улогите и одговорностите на различните страни се уште не се јасно дефинирани. Исто така, многу национални правни и политички рамки се уште не ги одразуваат јасно влијанијата на различните страни. На пример, кој ги контролира и кој е одговорен за безбедната инфраструктура или безбедните содржини на интернет? Какви должности или права произлегуваат од оваа одговорност?

Многу клучни услуги во сајбер безбедноста се во сопственишство на приватни актери и се управуваат од истите, додека државата зависи од нивната активна соработка, на пример во обезбедувањето на своите сопствени мрежи и услуги. Според тоа соработката меѓуразличните заинтересирани страни е суштинска за ефективната и ефикасната сајбер безбедност, и дека креирањето на политики за сајбер безбедност е партиципативно и одговорно. На пример, се повеќе се случува јавните и приватните актери да разменуваат информации за подобра превенција и откривање на сајбер инциденти. Истовремено, многу приватни компании често имаат понапредна технологија и знаење од јавниот сектор и можат да ја споделат оваа технологија во обид да ја зголемат севкупната сајбер безбедност во државата за да на крај и нивното работење стане побезбедно. Конечно, сите заинтересирани страни во сајбер безбедноста – владата, законодавците, приватниот сектор, граѓанското општество, техничката заедница и академската заедница – имаат своја улога во процесите на креирање на политики за сајбер безбедност, без оглед дали е тоа во планирањето на политиките, соработка во спроведувањето на политиките или надзорот над целиот процес на креирањето на политики.

Меѓутоа, точниот обем на одговорностите и улогите кои треба да ги имаат овие заинтересирани страни мора да се дефинира во завосност на контекстот на секоја политика. Генерално кредибилитетот и спроведувањето на целиот процес зависи од неговата инклузивност и транспарентност.

Нови сознанија за обезбедување, контрола и надзорот над безбедноста

Сајбер безбедноста мора да биде отчетна. Механизмите за контрола и надзор се често нејасни поради сложената врска меѓу вклучените државни и недржавни актери. Како резултат на тоа мораат да се развијат нови модели не само за соработка туку и за контрола и надзор.

Пратениците треба да играат важна улога во надзорот над управувањето со сајбер безбедноста. Поради тоа што сајбер безбедноста се однесува не само на

безбедносните политики туку и на други политики, надзорот над сајбер безбедноста треба да ги спои, меѓу другите, членовите на комисиите за безбедност и одбрана со членовите на комисиите задолжени за телекомуникации, образование, информатичко општество и човечки права.

Примери на прашања за надзор:

- Дали државата има стратегија со јасно дефинирана визија за сајбер безбедност? Кое министерство или државен орган е одговорно за нејзината имплементација? Дали стратегијата е развиена преку инклузивен процес вклучувајќи ги сите релевантни заинтересирани страни (државни и недржавни)?
- Дали постои список на идентификувана критична информатичка инфраструктура и, ако да, дали е списокот исцрпен? Кој државен орган е одговорен за ажурирање на тој список? Кој е одговорен за контрола на заштитата на критичната информатичка инфраструктура?
- Кои се различните страни вклучени во сајбер безбедноста? Кои се нивните улоги? Кои се нивните одговорности?
- Дали постојат поставени контролни и надзорни механизми за клучните државни и недржавни актери во сајбер безбедноста? Дали функционира контролата и надзорот над клучните државни и недржавни актери? Дали се повикуваат на одговорност како би се осигуриле дека нивните активности не се само ефективни туку и во рамките на законот?

ДЕЛ 2 – САЈБЕР КРИМИНАЛ (КОМПЈУТЕРСКИ КРИМИНАЛ)

Дефиниција

Сајбер криминалот генерално се поразбира како кривични дела каде што компјутери и мрежи се главната цел, истите се користат како орудија за вршење на кривично дело или се место на криминал.

Иако не постои универзално прифатена дефиниција може да се направи разлика меѓу два главни типа на сајбер криминал:

- Сајбер-овозможен криминал, што се однесува на „традиционалните“ форми на криминал кои сега преоѓаат во сајбер сферата, како што се финансиските кривични дела, дела кои што ја нарушуваат безбедноста на децата и младите вклучително и тероризам; и

- Напреден сајбер криминал (познат и како високо технички криминал), кој се однесува на напади против компјутерски хардвер и софтвер.[3]

Важно е пред се, да не се направи забуна меѓу сајбер криминалот и сајбер безбедноста. Двете сајбер закани се разликуваат по мотивот, намерата, употребените средства, целта, обемот, последиците, како и страните вклучени во спречувањето и ублажувањето на заканите. Во пракса сајбер криминалот варира од спам и пишинг емаилови, интернет измами и махинации и лажно претставување, до забранети навредливи и незаконски содржини, кражба на идентитет и материјал со сексуална злоупотреба на деца на интернет. Главната мотивација зад делата на сајбер криминалот, како што е случајот и со „традиционалниот" криминал, генерално е финансиската добивка. Сајбер криминалците се, во суштина, хакери со малициозни намери.

Компјутерите и мрежите како главна цел

Најчесто користените алатки се малициозен софтвер како што се вируси, тројански вируси, адвер и спајвер за добивање на пристап до системи, следење на активности и прибирање на податоци; бот мрежи (ботнет), или киднапирани компјутери кои вршат задачи на далечина без знаење на нивните корисници; и напади за скратување на услуги (Denial of Service (DoS)) кои се насочени кон исцрпување на достапните ресурси во мрежа, апликација или услуги, за да се спречи пристапот на корисниците до нив.

Ефектите на овие напади се многубројни. Физички лица можат да претрпат финансиски загуби, но можат и да бидат жртви на кражба на лични и осетливи информации, како и на идентитет. Фирмите кои се жртви на сајбер криминалните напади се соочуваат со потенцијални финансиски загуби, како и загуби на чувствителни деловни информации, податоци за патенти или лични податоци на нивните клиенти и корисници, што може посредно да доведе до сериозни последици по репутацијата. Јавни институции и непрофитни организации можат да станат жртви на изнуда или кражба на личните податоци на корисниците на нивните услуги.

Компјутерите и мрежите како алатки за извршување на кривични дела

Други кривични дела кои исто така се шират во сајбер просторот вклучуваат недозволена трговија со дрога, оружје и со чувствителни податоци и информации, трговија со луѓе, дури и платени убиства, физички напади и други форми на

3 Интерпол дефиниција за сајбер криминал.

насилство. Генерално таквите договори се случуваат на таканаречениот „даркнет“ (darknet) каде што корисниците делуваат потполно анонимно. Со користење на даркнет, поединците и криминалните организации користат енкриптирани сервиси за праќање пораки и крипто валути за вршење на финансиски трансакции, поради тоа што следењето и идентификацијата стануваат исклучително тешки. Блек-хет хакери (криминалци со технички познавања или технички експерти најмени од страна на криминалците, видете го поглавјето за хактивизам) исто така го користат потенцијалот на даркнетот искористувајќи ги слабите точки кои ги откриле во софтверот и анонимно продавајќи им ги на сите кои што бараат начини да злоупотребат конкретни системи.

Компјутерите и мрежите како место на злосторството

Криминалните организации до сега исклучително ефективно прејдоа во дигиталната сфера. Тие дури имаат развиено и нови деловни модели кои наликуваат на некои од најнапредните законски претпријатија. Исто како што некои фирми нудат „безбедност како услуга“ и ги развиваат капацитетите за сајбер безбедност на заинтересираните купувачи, криминалните групи нудат „криминал како услуга“ на пазарот на сајбер криминал. Уште една причина за загриженост е потенцијалната соработка меѓу различните малициозни актери. На пример, сајбер криминалците можат да ги нудат нивните услуги на терористички групи или да вршат државно спонзорирани кривични дела во сајбер просторот исклучиво за финансиска добивка. Со други зборови, дигиталната сфера им нуди на криминалните групи нови канали и можности за вршење на незаконски активности кои што инаку можеби не биле достапни.

Трендови и одговори на сајбер криминалот

Генерално сајбер-овозможениот криминал е во брз пораст и во развиените земји и во земјите во развој. По својата природасајбер криминалот е меѓународен криминал којги преминува државните граници. Сторителите не мораат да бидат во истата држава како и жртвите или полицијата која што ги гони. Ова е еден од клучните предизвици во борбата против сајбер криминалот, бидејќи разликите во правните системи и пракси на различните вклучени држави можат да влијаат врз ефикасноста и изводливоста на соработката, како и на размената на оперативни сознанија и докази.

Понатаму, многу малку полиции во светот имаат капацитет независно да се соочат со случаи на сајбер криминал, иако многу од нив имаат посебни единици за сајбер или „компјутерски“ криминал. Како и со другите форми на малициозни активности во сајбер просторот (видете го поглавјето за сајбер шпионажа), постои очигледна асиметрија на вклучените трошоци. Како резултат на тоа традиционалниот пристап

на полициската работа со кривичните дела во одредена мерка се менува во сајбер сферата. Наместо непосредно апсење на сторителите, полициските единици за сајбер криминал главно се фокусираат на прекинување на тековни сајбер кривични дела и решавање на безбедносните пропусти кои биле злоупотребени. Поради еднаквата распространетост на предизвикот на атрибуција во целиот сајбер спектар и долгите и напорни истражни постапки, вклучувајќи го и форензичното испитување на податоци, доаѓањето до правосилни пресуди е исто така побавно во споредба со традиционалните кривични дела.

На државно ниво борбата против сајбер криминалот бара соработка од сите страни. Приватниот сектор е најчестата мета на сајбер криминалците и неговите искуства и интереси треба да се земат во предвид при планирањето на стратегии за борба против сајбер криминалот. Експертите за сајбер криминал од приватниот сектор, како и академската заедница и граѓанското општество, исто така можат да придонесат во планирањето на политики за борба против сајбер криминалот со технички капацитети и знаење. За ефективна борба против сајбер криминалот, владите мораат да негуваат јавно – приватна соработка и да го поддржуваат воспоставувањето на мрежи на доверба. Подеднакво важна е превенцијата на сајбер криминалот и заштитата на индивидуалните корисници. Преку општо подигање на свеста и градење на капацитети, корисниците требаат да научат како да препознаат потенцијално измамнички емаил пораки, малициозни содржини и потенцијално лажни контакти. Дурии релативно едноставни активности можат да имаат големо влијание во спречувањето на сајбер криминало како на пример обуки за за корисниците да одржуваат основна сајбер хигиена и користат силни лозинки, ажуриран лицензиран софтвер и енкрипција,

На меѓународно ниво постигнат е напредок со усвојување на Конвенцијата за компјутерски криминал на Советот на Европа[4], која исто така се нарекува Будимпештанска конвенција. До денес Будимпештанската конвенција е единствениот обврзувачки меѓународен инструмент за сајбер криминал која пропишува упатства за државите за развивање на сеопфатни национални законодавни рамки во борбата против сајбер криминалот и воспоставување на рамка за меѓународна соработка меѓу земјите потписнички. Меѓутоа, со шеесет и една потписничка и уште десет за кои се очекува да се приклучат, истата се уште не е универзален глобален документ. Сепакво последните години можат да се забележат случаи на меѓународна соработка. На пример, меѓународните организации за полициска соработка, првенствено Интерпол и Европол, се вклучени во активности насочени кон јакнење на меѓународните капацитети и создавање на рамки за прекугранична соработка меѓу различните полиции. Поради претходно споменатите високи потреби за одржување на националните единици за борба против сајбер криминал, овие рамки можат да ги надоместат ограничените национални капацитети,

4 Конвенција за компјутерски криминал. Совет на Европа. Договор бр. 185.

вклучително и преку развојот на јавно – приватни партнерства и мрежи на доверба меѓу експертите од различните сектори на општеството.

Примери на прашања за надзор:

- Дали државата има законодавство за сајбер криминал (компјутерски криминал) кое ги идентификува различните типови на сајбер криминал и утврдува добро дефиниран систем на санкции? Во која мерка е истото усогласено со меѓународните конвенции потпишани од државата?
- Дали судството и полицијата се добро опремени во поглед на техничко знаење, стручност и капацитети?
- Кои делови од општеството се најмногу изложени на сајбер криминал? Дали постојат превентивни иницијативи насочени кон тие сектори?
- Дали функционира контролата и надзорот над клучните државни и недржавни актери? Дали се повикуваат на отчетност сајбер капацитетите на безбедносните агенции за да се осигури дека нивните активности не се само ефективни туку и во рамките на законот/не ги прекршуваат гарантираните права на граѓаните за приватност?
- Дали полицијата и судството ги користат сите достапни правни алатки за ефективна меѓународна соработка? Дали законските рамки треба да се изменат за постигнување на поголема ефикасност? Истовремено, кои контролни механизми постојат за заштита на личните податоци на граѓаните кои се разменуваат со трети земји? Дали комуникацијата со приватниот сектор е ефикасна и транспарентна (во нејзината форма, ако не и во содржината која треба да биде доверлива)?

ДЕЛ 3 – САЈБЕР ВОЈНА

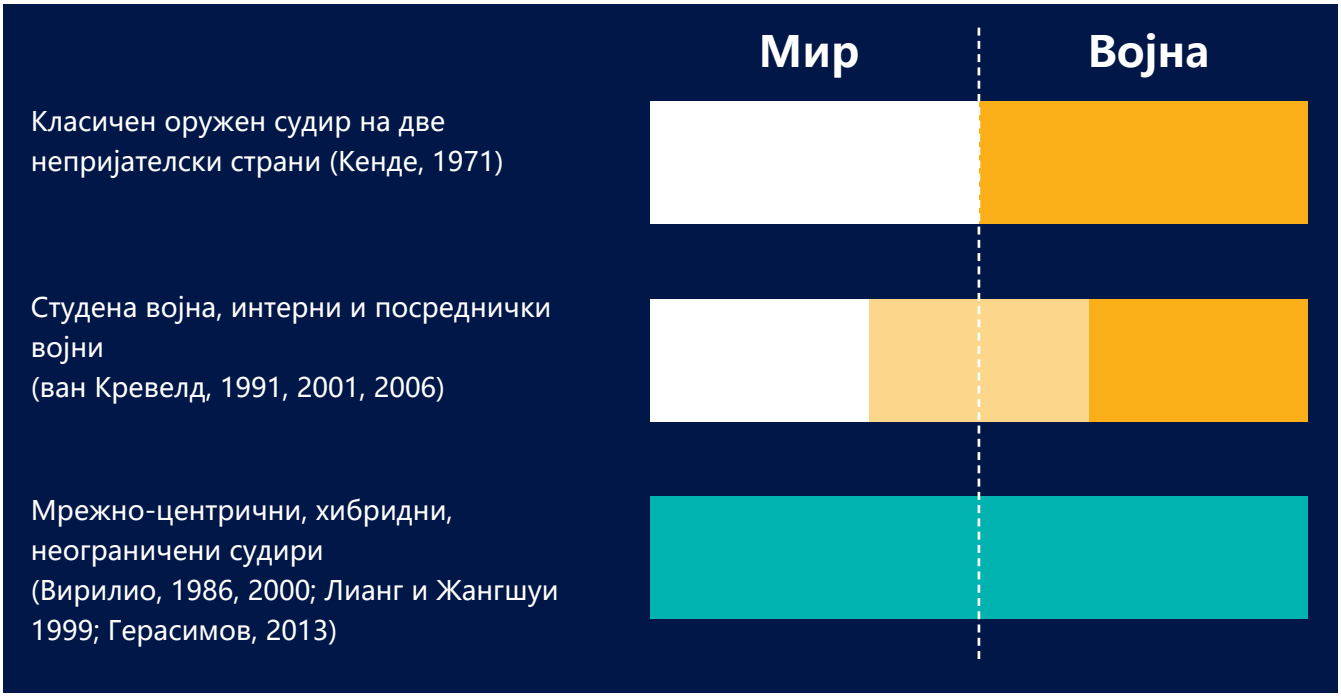
Дефиниција

Сајбер војната може да се дефинира како чин на „војување во сајбер просторот или преку сајбер просторот". Тоа е нов специфичен начин на војување[5] кој користи информатичко комуникациски технологии (ИКТ) за постигнување на воени цели

5 Војување е процес на водење на меѓународен оружен судир. Војната е оружен судир меѓу не помалку од две непријателски оружени сили кои имаат најмалку централна организација и команда, додека барем едната страна е претставена со некој вид на власт (како редовна војска или полиција, или нередовна паравоена сила), кој се води во континуитет, во согласност со единствен план и стратегија на непријателските сили. Традиционалните војни се водат на копно, море, во воздух и во вселената.

и ефекти во физичките, информатичките и сајбер домени. Воените ефекти можат да бидат еднакви со ефектите на кинетички, нуклеарни, биолошки или хемиски оружја.

Меѓутоане постои меѓународен договор за тоа како треба да се дефинираат содржината, методите, техниките, средствата и целите на сајбер војувањето. Меѓународната заедница се уште се нема согласено околу мерките за градење на националните капацитети и меѓународната доверба или како да го примени постојното меѓународно право на сајбер војувањето.



Проблеми во регулирањето на сајбер конфликти

Новите технологии со офанзивни капацитети се јавуваат побрзо отколку што поединте држави се способни да ги развијат потребните одбрани од нив. Зад нив заостанува и способноста на меѓународната заедница да изнајде решенија за регулирање на сајбер конфликтите.

Сторителите на сајбер нападите често работат прикриено, а ефектите на нивните сајбер напади често имаат одложено дејство. Можат да поминат неколку години меѓу сајбер експлоатацијата и откривањето на нејзините ефекти. Напаѓачите можат да бидат владини единици или органи, приватни компании, криминални организации, терористи или неформални групи или поединци.

Наспроти конвенционалното војување, ефектите на сајбер конфликтите често не го достигаат прагот на „чин на агресија“[6], „употреба на сила“[7], „оружена сила“[8] или „оружен напад“[9] според дефиницијата на Повелбата на Обединетите Нации, поради

6 Повелба на Обединетите нации, 24 октомври 1945. Обединети нации. 1 UNTS XVI, член 39.
7 Исто, 1 UNTS XVI, член 2, став 4.
8 Исто, 1 UNTS XVI, Преамбула.
9 Исто, 1 UNTS XVI, став 51.

што е тешко да се применат правилата ius ad bellum и ius in bello на Меѓународниот закон за оружени судири.

Дополнително, повеќето држави немаат доволни капацитети за:

- прецизно откривање на сајбер напади;
- идентификација и атрибуција на напаѓачите; и
- навремена, прецизна и правна реакција на сајбер нападите.

Меѓународни активности за регулирање на сајбер војувањето

Недостатокот на правни прописи остава простор за потенцијална злоупотреба на сајбер нападите, која што може да доведе и до појавата на меѓународни и регионални кризи, особено во региони обременети со хронични политички тензии.

Меѓународната заедница се уште се обидува да постигне договор околу начините за регулирање на сајбер војувањето. Постојат различни предлози, од кои еден е Прирачникот од Талин[10], подготвен од група академици во НАТО Центарот за заедничка сајбер одбрана во Талин, Естонија.

Меѓународни правни одговори на сајбер војната

Можен практичен одговор на сајбер заканите може да биде усвојувањето и примената на мерки за градење на капацитетите и довербата на национално, регионално и меѓународно ниво.

За оваа цел, Обединетите нации основаа Група на владини експерти за новитетите во полето на информации и телекомуникации ко контекстот на меѓународната безбедност (ОН ГВЕ). Групата се има состанато пет пати во периодот меѓу 2004 и 2017 година за да разгледува постојни или потенцијални закани; норми, правила и принципи на одговорно однесување на државите; и мерки за градење на капацитетите и довербата. Во Извештајот од 2013 година, ГВЕ заклучи дека „Меѓународното право, а особено Повелбата на Обединетите нации, е применливо и суштинско во одржувањето на мирот и стабилноста и промовирањето на отворено, безбедно, мирно и пристапно ИКТ опкружување".11

10 Шмит, Мајкл Н. 2017 Талин прирачник 2,0 за меѓународното право кое се применува на сајбер операции (Schmitt, Michael N. (ed.) 2017.Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press).

11 Извештај на Групата на владини експерти за новитетите во полето на информации и телекомуникации ко контекстот на меѓународната безбедност. 24 јуни 2013 година, Генерално собрание на ОН. Резолуција A/68/98.

Организацијата за безбедност и соработка во Европа (ОБСЕ) вложи дополнителни напори преку усвојувањето на Мерките за градење на доверба за зачувување на меѓународниот мир и стабилност (МГД).12 МГД се фокусираат на размена на информации и дијалог; заштита на критичните инфраструктури и националната безбедност; и промовирање и подобрување на соработката меѓу јавниот и приватниот сектор.

Меѓутоа, обете иницијативи се доброволни (не се задолжителни за земјите членки на ОН и ОБСЕ) и нивното постоење не е директна и цврста гаранција за постигнување на мир и безбедност во сајбер просторот на меѓународно ниво.

Можно решение можат да бидат билатерални и мултилатерални договори меѓу различните држави. Овие договори можат да ги дефинираат нормите, стандардите и принципите на мирно однесување; да воспостават правила и процедури во случај на сериозни сајбер инциденти; да ја олеснат соработката и создавањето на заеднички капацитети за откривање на сајбер напади, идентификација на напаѓачите и атрибуција.

Примери на прашања за надзор:

- Дали се дефинирани стратешките цели за сајбер одбрана?
- Постои ли проценка за свесноста околу ситуацијата? Дали ги зема предвид сите елементи во државата кои требаат да бидат заштитени?
- Кои се главните ранливости и ризици? Дали истите редовно се идентификуваат, ревидираат и решаваат?
- Колку се развиени постојните национални капацитети за сајбер одбрана?
- Кои се различните актери, на државно и меѓународно ниво, кои придонесуваат кон сајбер одбраната?
- Какви рамки за соработка постојат меѓу одговорните страни? Како истите се организирани и колку се отчетни, транспарентни и ефективни?
- Дали се доволни чести и доволно обемни обуките за персоналот?
- Дали државата учествува во регионални и меѓународни обуки и вежби? Колку често се случуваат истите?

12 Одлука бр. 1106. Првична збирка на Мерки за градење на доверба на ОБСЕ за намалување на ризикот од конфликти кои произлегуваат од употребата на информатички и комуникациски технологии. 3.12.2013. Организација за безбедност и соработка во Европа. PC.DEC/1106. Одлука бр. 1202. Мерки за градење на доверба на ОБСЕ за намалување на ризикот од конфликти кои произлегуваат од употребата на информатички и комуникациски технологии. 10.3.2016. Организација за безбедност и соработка во Европа. PC.DEC/1202.

ДЕЛ 4 – САЈБЕР ШПИОНАЖА

Дефиниција

Сајбер шпионажата се дефинира како чин кој се презема тајно или под лажни претпоставки, и користи сајбер капацитети за собирање (или обид за собирање) на информации со намера да се пренесат на спротивставената страна.[13] Пристап се добива кога лицето лажно се претставува како легитимен корисник, или преку употребата на софистицирани целни напади (како што е социјалниот инженеринг), преку кои се манипулираат легитимните корисници со што им отвораат пристап на лицата кои имаат за цел добивање на неовластен пристап.

Специфични предизвици на сајбер шпионажата

Една од основните карактеристики на сајбер шпионажата е единствената асиметрија на вклучените трошоци. Трошоците за заштита и одбрана против сите ранливости се диспропорционално високи во споредба со трошоците на напаѓачот, кој треба да открие и злоупотреби една единствена слаба точка. Понатаму, земајќи го во предвид потребното време за откривање на упад, сајбер шпионажата претставува ефективна офанзивна алатка за извлекување на информации од системи, процеси и поединци. Се проценува дека потребното време за откривање на упад е меѓу еден и три месеци[14], во кое време напаѓачот може да добие пристап до големи количества на чувствителни информации. Поради обемот на присутност на интернет и мрежни услуги во општествата низ целиот свет, сајбер шпионажата нуди многу поголеми можности за добивање на чувствителни информации за некој противник.

Прифатливо однесување, сајбер криминал или чин на агресија?

Постои се поголема согласност дека сајбер шпионажата генерално станува неиздржлива. Меѓутоа, одлучуката за тоа што претставува прифатливо однесување а што треба да се санкционира е сеуште голем предизвик. Фактот дека традиционалната шпионажа од страна на државите во минатото се сметала за прифатливо однесување довела до тоа денешната сајбер шпионажа исто така да не биде регулирана. Следствено во пракса влегувањето во компјутерски систем и нарушувањето на неговата доверливост сеуште се смета за прифатливо. Меѓутоа,

13 Според горенаведениот Прирачник од Талин.

14 Мандиант извештајот (2013) проценува дека просечното време на одржување на пристап до мрежата на жртвата е 356 дена. Глобал Спејс (2013) проценува дека просечен упад останува неоткриен 90 дена, во просек. Форин Полиси (2015) проценува дека во просек на жртвата и треба 205 дена да открие дека била инфицирана. Понемон Институтот (2015) открил дека упадите остануваат неоткриени 46 дена, во просек. Крепс, Флечер и Грифитс (2016) проценуваат дека упадите остануваат неоткриени во просек 3 месеци.

нарушувањето на интегритетот или достапноста на системот, што може да настане како резултат на тој упад се смета за неприфатливо. Според тоа, шпионажата се смета и за прифатлива и за неприфатлива, во зависност од нејзините последици.

Дополнително се јавува предизвикот на правење разлика меѓу активностите за собирање на информации и активности со малициозни намери кои можат да претставуваат чин на агресија. Ова исто така зависи од користењето на собраните информациите. Според тоа, тенка е границата меѓу чиновите чија примарна цел е сајбер шпионажата и оние кои можат да се сметаат за непосредни сајбер напади. Поради ова исклучително е тешко да се утврдат меѓународни принципи и режими со кои се регулира идејата за сајбер шпионажа која, за сега, останува релативно нерегулирана.

Од безбедносна гледна точка се смета дека сајбер шпионажата може потенцијално да се преклопи со идејата за сајбер криминал. Во таа смисла, сајбер криминалците можат да бидат најмени од трети страни да вршат и/или овозможат дела на шпионажасо задача да продрат во владини и/или корпоративни системи и извлечат чувствителни информации.

Посредници, приватни армии и хибридни конфликти

Друг предизвик се државно спонзорирани кампањи за сајбер шпионажа, каде што државите можат посредно да спонзорираат страни кои имаат капацитети за продирање во системите на нивните противници. Во оваа смислахакерите станаа потенцијални приватни шпионски армии во дигитална доба на располагање на најбогатиот купувач. Подемот на сајбер шпионажата исто така додаде уште еден елемент во новата идеја за хибридни конфликти и асиметрично војување, каде што судирите веќе не се црно-бели, туку се јавуваат во различни форми и интензитет. Преку вклучување во сајбер шпионажа државите сега се во можност да развијат хибридни односи со нивните противници. Тоа ефективно значи дека односите во реалниот свет остануваат нормални, додека непријателските активности и судири се случуваат во дигиталниот домен преку користење на сајбер шпионажа заедно со хакирање и хактивизам, сајбер криминал и офанзивни сајбер активности.

Како и со другите форми на одбрана и заштита против малициозни активности во сајбер просторот, сајбер шпионажата го содржи предизвикот на откривање и атрибуција. Дополнително сајбер шпионажата не мора секогаш да се врши од страна на државите или државно спонзорираните актери. Таа може да биде искористена и од сајбер криминалците, како и од приватниот сектор за едноставно добивање на финансиска добивка.

Одговор, регулирање и противмерки на сајбер шпионажата

Според тоа, најдобрата одбрана против сајбер шпионажата – барем сега за сега – е одвраќањето. Ова наведува на зголемување на реалните или претпоставените трошоци од потенцијалниот напад за противникот. Покрај градењето на посилна одбрана, ова исто така значи и промовирање на билатерална и мултилатерална соработка за постигнување на договори и/или кодекси на однесување со кои се регулира прашањето на сајбер шпионажа, покрај другите видови на однесување во сајбер просторот. Навидум успешен пример на ова е договорот од 2015 година меѓу САД и Кина за економска шпионажа, кој утврдува дека ниту една држава нема да врши или свесно да поддржува сајбер овозможени кражби на интелектуална сопственост со цел обезбедување на конкурентски предности на фирми или сектори во стопанството.

Меѓутоа, сајбер шпионажата со цел добивање на разузнавачки информации за национална безбедност се уште не е регулирана. Поради оваа причина, постојат се повеќе иницијативи од државите за дискусии во поглед на правото на 'одмазда', или повратно хакирање кога ќе се открие упад во системот, како поубедлива форма на одвраќање. Една од најскорешните земји која им се приклучи на овие дискусии е Германија, каде што државната разузнавачка заедница бара да и биде дадено правото да користи активна одбрана. Ова имплицира право на уништување податоци кои се украдени или преместени од германски сервери, како и компромитирање на странски сервери за зајакнување на националните капацитети за надзор. Идејата за овие иницијативи е одвраќање на потенцијалните напаѓачи преку заканата од одмазда.

Примери на прашања за надзор:

- Што се прави за да се заштитат граѓаните и нивните податоци од сајбер шпионажа? Кои министерства или државни органи се одговорни за борба против сајбер шпионажата?
- Дали постои проценка на ранливоста и потребите на државата во поглед на сајбер шпионажата и какви противмерки се преземаат?
- Како може подобро да се дефинира и регулира сајбер шпионажата во националното законодавство и на меѓународно ниво?

ДЕЛ 4 – САЈБЕР ТЕРОРИЗАМ

Дефиниција

Сајбер тероризмот ги вклучува двата највпечатливи развои на настани во светот: се поголемата зависност на општеството од интернет и заканата од меѓународен

тероризам.[15] Анонимната, лесно достапна и често нерегулирана природа на интернетот го чини особено подложен на експлоатација и злоупотреба од страна на терористички организации и други недржавни страни. Меѓутоа, додека употребата на интернетот за терористички цели претставува предизвик за меѓународната заедница, истата дава и нови средства за борба против тероризмот.

Сајбер тероризам наспроти употребата на интернетот за терористички цели

Иако не постои универзално признаена дефиниција на сајбер тероризам, повеќето дефиниции на различните држави зборуваат за напад кој користи електронски средства за да навлезе во и/или сериозно и попречи на критичната национална инфраструктура.[16] На пример, Организацијата за безбедност и соработка во Европа (ОБСЕ) го дефинира сајбер тероризмот како „сајбер поврзан тероризам или, поконкретно, [...], терористички напади врз сајбер инфраструктурата, а особено на контролните системи на критичната ненуклеарна енергетска инфраструктура".[17]

Сценаријата на закани од сајбер тероризам вклучуваат парализирање на важни урбани подрачја, секторот на јавното здравство или нарушување на финансискиот сектор со „менување на неколку единици и нули".[18] Подемот на Интернетот на нештата[19] претставува уште една важна опасност која што лесно можат да ја искористат терористичките организации за вршење на чинови на сајбер тероризам. Чиновите на сајбер тероризам кои ќе резултираат со реално физичко уништување се сметаат за помалку веројатно и, поради тоа, како помал предизвик за државитепоради огромното количество на ресурси потребни за извршување на таквите активности.[20]

Понатаму, многу терористички организации го користат интернетот за вршење на класични кривични дела како што е измама, неовластен пристап и недозволено мешање во компјутерски систем. Ова резултира во преклопување меѓу сајбер криминалот (видете го поглавјето за сајбер криминал), сајбер нападите (видете

15 Ленц, Кристофер Е. Ленц. 2010.Обврската на државата да спречи и одговори на чинови на сајбер тероризам Чикаго журнал на меѓународно право 10 бр. 2.

16 Националните критични инфраструктури се ресурси или системи витални за одржувањето на суштинските општествени функции, кои, ако се надвор од мрежата подолг период, можат да доведат до сериозни ризици по јавното здравје, стопанството, граѓаните и државната безбедност.

17 Добри пракси за заштита на ненуклеарната критична енергетска инфраструктура од терористички напади со фокус на закани кои доаѓаат од сајбер просторот. 2013. Организација за безбедност и соработка во Европа. бр. 16.

18 Ген. Вотел, Јозеф Л., јули 2015.Разбирање на тероризмот денес и утре. ЦТЦ Сентинел 8. Издание 7, стр. 2–6.

19 Речникот Кембриџ го дефинира поимот „Интернет на нештата" како предмети кои содржат сметачки и кои се способни да се поврзат едни со други и разменуваат податоци преку интернет. Интернетот на нештата се повеќе се провлекува низ националната критична инфраструктура.

20 Вајман, Габриел, март 2004. https://www.usip.org/publications/2004/03/wwwterror-net-how-modern-terrorism-uses-internetwww.terror.net:%20How%20Modern%20Terrorism%20Uses%20the%20Internet. Специјален извештај бр. 116. Институт за мир на Соединетите Држави.

го поглавјето за сајбер војна) и сајбер тероризмот, поради што на крај е тешко да се направи разлика меѓу нив. Резолуцијата 1566 на Советот за безбедност на Обединетите нации нуди одредени упатства по ова прашање, бидејќи го потенцира политички мотивираниот елементи ги идентификува „терористичките чинови“ како:

> “[...] кривични дела, вклучително и против цивили, извршени со намера да се предизвика смрт или тешки телесни повредни, или за земање заложници, со цел предизвикување на состојба на терор [...], застрашување на населението или принудување на влада или меѓународна организација да изврши или да се воздржи од извршување на некое дејство, што претставува прекршок во рамките на и според дефинициите во меѓународните конвенции и протоколи кои се однесуваат на тероризмот [...].”[21]

Дополнително, терористичките организации го користат интернетот секојдневно за различни активности како што се пропаганда (вклучувајќи и радикализација, наведување на тероризам, врбување), финансирање, обука и планирање (вклучувајќи и преку тајни комуникации и информации од отворени извори), како и извршување на сајбер напади.[22] Додека употребата на интернетот за пропагандни цели зема голем замав во меѓународната заедница, повикувањето на посилни партнерства, вклучително и со технолошката индустрија,[23] како и предизвикот на употребата на интернетот за финансиски цели доста често се занемарува. Во меѓувреме, со општиот премин кон употребата на технологија во меѓународната трговија го трансформираше интернетот во средство за перење пари и пренос на средства на терористичките организации.[24]

Следствено, полициските и разузнавачки органи се повеќе следат сомнителни финансиски трансакции на интернет и развиваат средства и вештини за проактивна превенција, откривање и одговарање на терористичките активности кои го вклучуваат интернетот. Владите исто така започнаа да реагираат на употребата на интернетот за пропагандни цели преку стратешки комуникации како алтернативни приказни и против мерки и регулирање на содржините.[25] Меѓутоа, секоја активност против тероризмот на интернет бара заеднички напори меѓу државите, приватниот сектор и граѓанското општество за ефективна одбрана кон овие нови предизвици.

---

21 Одлука на Советот за безбедност 1566 (2004) за Заканите по меѓународниот мир и безбедност предизвикани од чинови на тероризам. 8 октомври 2004. Совет за безбедност на Обединетите Нации. Резолуција S/RES/1566. Оп. став 3.

22 Видете:Употребата на интернетот за терористички цели. 2012. Канцеларија на Обединетите нации за дроги и криминал.

23 Видете:СЦ Комисија за борба против тероризам; Технологија против тероризам; Глобален интернет форум за борба против тероризам.

24 Џејкобсон, Мајкл. Јуни 2009. Финансирање на тероризмот преку интернет. ЦТЦ Сентинел 2. Издание 6, стр. 17–20.

25 Видете:Цирих-Лондон Препораки за спречување и борба против насилен екстремизам и тероризам на интернет. 2017. Глобален форум за борба против тероризам.

Прашања за владеење на правото

Генерално, активностите за борба против тероризам кој го вклучува интернетот можат да имаат влијание врз повеќе човечки права (вклучувајќи ја приватноста и слободата на изразување, здружувањето, мирното собирање и религија или вера). Во поглед на употребата на интернетот за пропагандни цели, владите усвоија нови мерки од побивање на активностите за оправдување или величање (апологетика) на терористички чинови до законски забрани за наведување на вршење на истите.[26] Меѓутоа, треба да се забележи дека говорот кој е морално одбивен, шокантен, вознемирувачки или навредлив не претставува сам по себе кривично дело; но "но такви се барањата на плурализмот, толеранцијата и слободоумноста без кои не постои 'демократско општество'."[27] Меѓутоа, предизвикот е во идентификација на точката во која полемиката или критиката се претвораат во говор на омраза, величање (апологетика) или наведување на вршење терористички чинови. Не е секогаш лесно да се идентификува оваа точка.

Во суштина, важно е владите јасно да ги дефинираат релевантните кривични дела во кривичните законици на нивните држави, за да им се овозможи на граѓаните да ги предвидат последиците поврзани со одредени активности и да се избегне преголемото регулирање и последователното „ладење" на човечките права. Гаранциите за исполнување на соодветниот процес, како што се пресумпција на невиност и правото на фер судење, се клучни во осигурувањето дека мерките за борба против тероризмот се ефективни и го почитуваат владеењето на правото. Понатаму, ефективниот надзор над страните во јавниот сектор вклучени во борбата против тероризмот (на интернет и вон него) се суштински во промовирањето на реформски процеси во борбата против тероризмот кои ги почитуваат човечките права.

Примери на прашања за надзор:

- Дали постои усвоена јасна правна рамка со која се дефинираат забранетите активности на интернет?
- Дали правото на слобода на изразување и правото да не се биде подлегнат на субјективно или незаконско мешање во нечија приватност се гарантирани со Уставот?
- Дали некоја собраниска комисија има правен мандат да ја надзира работата на државните органи за борба против тероризмот?

26 Видете: Побивање на приказните на терористите. 2017. Совет за безбедност на Обединетите нации S /RES/2354 (2017). Преамбула став 12, и Забрана за наведување на терористички чинови. 2005. Совет за безбедност на Обединетите нации S/RES/1624 (2005). Преамбула став 4 и оперативен став 1(а).

27 Хендисајд против Обединетото Кралство. 4 ноември 1976. Совет на Европа: Европски суд за човекови права. 5493/72, оп. цит., став 49

- Дали законодавството ги регулира активностите за борба против тероризмот на интернет, внимавајќи на стандардите за човечки права? Дали законодавството се усвојува по јавен и инклузивен процес на консултации?
- Какви се можностите за Собранието да ги надзира приватните претпријатија во поглед на нивното собирање на лични информации од своите корисници?

ДЕЛ 5 – ХАКТИВИЗАМ

Дефиниција

По дефиниција, хактивизам е спој меѓу хакирање и традиционален активизам. Самиот збор го немаат присвоено „хактивистите“, туку им бил припишан од истражувачите, новинарите и стручњаците за сајбер безбедност во обид да ги разликуваат од другите актери во сајбер просторот. Хактивизмот овозможува нови облици на мобилизација за активистите на интернет во нивната борба за одредена кауза (пр. човечки права, слобода на говор, итн.). Тој овозможува активности на далечина и мобилизација од големи размери со само еден клик на глушецот. Во поглед на последиците, самиот хактивизам генерално предизвикува мали штети, поради што многу малку случаи доаѓаат до точката на кривичен прогон, особено поради дополнителниот предизвик на атрибуција кој е подеднакво присутен тука како и во секој друг тип на активност во сајбер просторот.

Мотиви на хактивистите и разликата од сајбер криминалот и сајбер тероризмот

Во суштина, хактивизмот се смета за нарушувачки, а не деструктивен. Тоа го разликува од другите злонамерни активности во сајбер просторот, како што се сајбер криминалот и сајбер тероризмот. Хактивистите главно се потпираат на тактики како ширење црви и вируси, Дистрибуирани напади за скратување на услуги (Distributed Denial of Service (DDoS)), интернет нагрдување и слично. Обемот во кој хактивистите вообичаено се сметаат за минорна закана се гледа во вообичаената карактеризација дека нивните DDoS напади се еднакви на мирните седечки протести од 1960-те години.

Меѓутоа, хактивистите исто така се вклучуваат во активности како што се преземање на Твитер кориснички налози и Фејсбук страни, како и крадење и/или откривање на чувствителни и лични информации на и од системите во кои што влегуваат.

Вајт, Греј и Блек-хет хакери

Земајќи предвид дека, во суштина, хактивистите се хакери со кауза, конкретните активности што ги превземаат кога ќе влезат во еден систем ја прават разликата меѓу различните видови на хакери. Тие се:

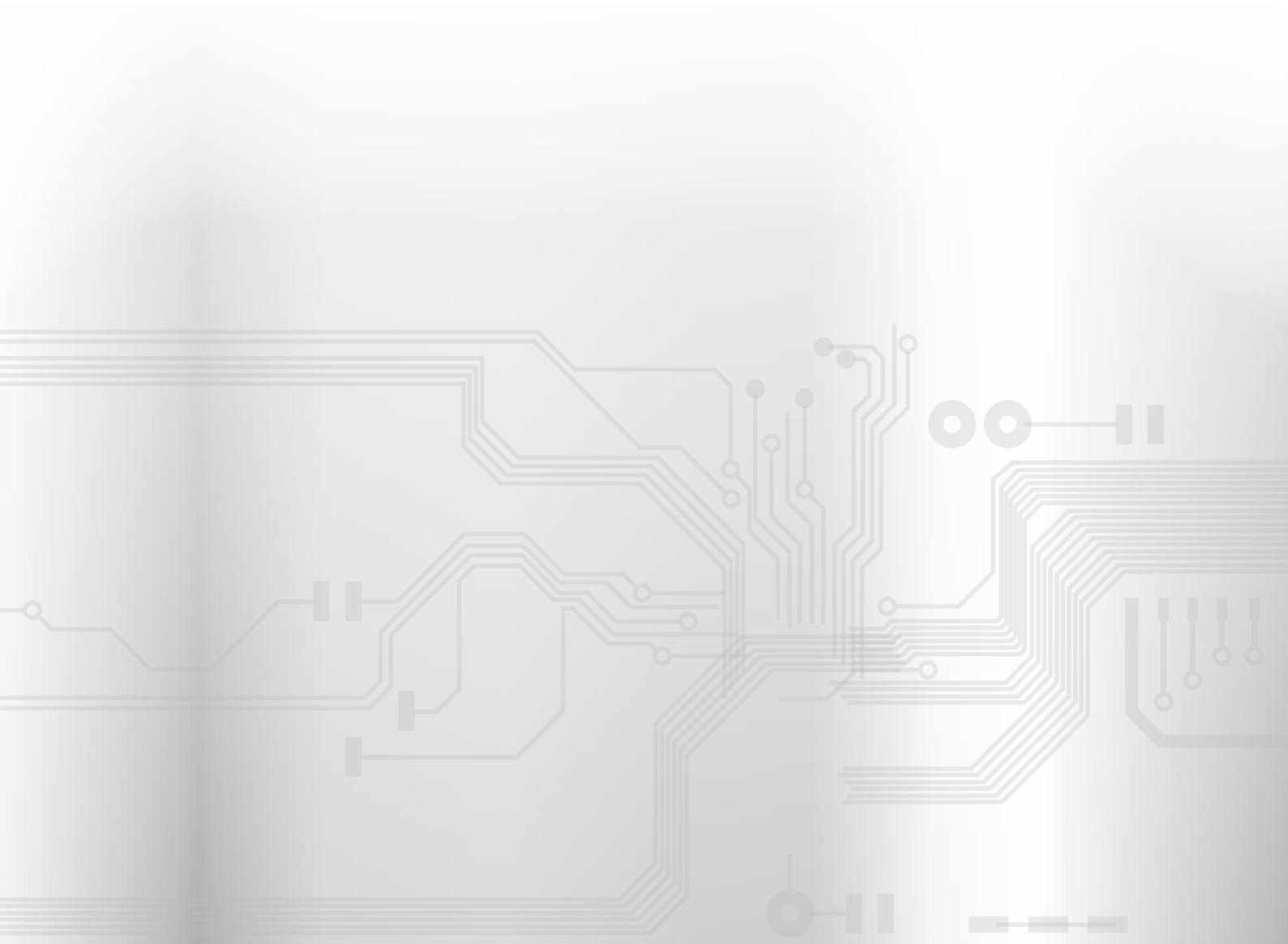
- Вајт-хет (бели) хакери се оние кои кога ќе откријат слаби точки во системите и им ги пријавуваат истите на системските проектанти за да се развијат конкретни исправки и да се подобри севкупната безбедност на системот. Вајт-хет хакерите исто така се опишуваат како „етички хакери".
- Греј-хет (сиви) хакерите исто така ги пријавуваат откриените слаботи на системските проектанти, но можат да бараат финансиски надоместок или некоја друга награда за информациите кои што ги дале.
- Блек-хет (црни) хакерите не ги пријавуваат директно слабите точки на системските проектанти туку имаат за цел да профитираат од истите или преку директна експлоатација или преку продажбата на тие информации на црниот пазар на други страни, како што се сајбер криминалците.

Постои многу тенка граница меѓу хактивизмот и вистинските напади во сајбер просторот. Хактивистите, во некои случаи, можат да соработуваат со сајбер криминалците. Дополнително, директните јавни закани дадени од групи на хактивисти против различни влади, претпријатија и поединци можат потенцијално да доведат до паника и страв меѓу цивилното население, а тоа е еден од основните елементи во дефиницијата за тероризам. Конечно, најновите дискусии се концентрираат на зголемувањето во државно спонзориран хактивизам, кој е практично невозможно да се докаже во пракса, иако можат да се направат разумни претпоставки за неговото постоење.

Примери на прашања за надзор:

- Кои се капацитетите на органите за спроведување на законите да идентификуваат хактивизам и да го разликуваат од другите форми на сајбер закани? Дали се доволни?
- Дали релевантното законодавство јасно дефинира кои активности вклучени во терминот „хактивизам"се нелегални (т.е. кога ќе ја преминат границата на слобода на говор)?
- Што може да направи владата за да ги подржи „вајт-хет хакерите" или да избегне да ги меша со „греј" или „блек-хет" хакерите? Дали некои од механизмите за заштита на свиркачите се применливи на „вајт-хет хакерите"?

- Што се прави за да се идентификуваат потенцијалните хактивисти и да се спречи криминалното однесување? Дали постојат правни и оперативни заштитни мерки за спречување на безбедносните служби од злоупотреба на овластувањата и подривање/оневозможување на легитимниот активизам?
- Што се прави за да се подобри меѓународната соработка во борбата против малициозниот хактивизам?



DCAF Geneva Centre for Security Sector Governance

DCAF Geneva
P.O. Box 1360
CH-1211 Geneva 1
Switzerland
Tel: +41 (22) 730 94 00
Email: info@dcaf.ch

DCAF Brussels
/ EU SSG Facility
24 Avenue des Arts (boîte 8)
1000 Brussels
Belgium

DCAF Ljubljana
Gospodinjska ulica 8
1000 Ljubljana
Slovenia

DCAF Ramallah
Al-Maaref Street 34
Ramallah / Al-Bireh
West Bank, Palestine

DCAF Beirut
Gefinor Bloc C
Office 604, Ras Beirut
Lebanon

DCAF Tunis
Rue Ibn Zohr 14
1082 Tunis
Tunisia