УДК: 355.02(494) ; 343.533:004(494)

САЈБЕР ОДБРАНА ШВАЈЦАРСКЕ – ПРЕТЊЕ И СТРАТЕГИЈСКИ ПРАВЦИ ДЕЛОВАЊА*

Gerald Vernez, *Roman* Hüssy и *Riccardo* Sibilia**
Министарство одбране Швајцарске

Сајбер одбрана представља нови безбедносно-политички изазов за нашу земљу, али и глобално. Швајцарска је ту ситуацију одавно схватила, али мере које је до сада предузимала нису биле адекватне брзом развоју претњи. Савезна влада је 10. децембра 2010. године наложила руководиоцу Пројекта сајбер одбране да до краја 2011. године изради Стратегију сајбер одбране Швајцарске. Овај чланак представља први елемент њеног развоја.

Кључне речи: *сајбер простор, сајбер претња, облици угрожавања, сајбер одбрана, национална стратегија сајбер одбране, елементи националне стратегије сајбер одбране*

Увод

Развој информационих и комуникационих технологија (*IKT – Informations-und Kommunikationstechnologien*) за нешто више од 30 година из темеља је променио модерно друштво – нарочито у процесу глобализације; у неком погледу га је ојачао, чак и демократизовао, али га је, истовремено, у другим областима екстремно ослабио. Тако су егзистенција једног човека, успех једног предузећа или напредак друштва као колектива, на безброј начина постали зависни од комплетности и отпорности функционисања критичних инфраструктура. То опет повећава дигитализацију и умрежавање. Дакле, за то се користе информациони и комуникациони технолошки системи који су, како на основу избора технологија, тако и на основу конфигурације, у многим случајевима, у погледу сајбер напада постали још рањивији.

---

* Овај текст је објављен у часопису швајцарске војске ***Military Power Revue*** бр. 1/2011, стр. 3–14, под насловом „**Cyber Defense der Schweiz“**. Са немачког језика текст је превео мр Здравко Зељковић, пуковник у пензији

** Gerald Vernez (Жералд Верне), пуковник, геолог и метеоролог, Конфедерална висока техничка школа, Цирих, заменик руководиоца Пројекта сајбер одбрана, Генерални секретаријат Министарства одбране, заштите становништва и спорта.

Roman Hüssy (Роман Хиси), аналитичар Пројекта сајбер одбрана, Генерални секретаријат Министарства одбране, заштите становништва и спорта.

Riccardo Sibilia (Рикардо Сибилиа), шеф одсека Анализе сајбер претњи, Центар за електронске операције Швајцарске војске.

Безбедносно-политичке консеквенце за једну модерну западну државу као што је Швајцарска далекосежне су. Однос према тим новим облицима претњи је тек крајем 90-тих година озбиљно узет у обзир, иако тежи случајеви напада тада још нису били познати нити објављивани, па зато политичке пouке нису биле ни извучене. Према томе, та проблематика се све до 2010. године није сматрала приоритетном. Међутим, ситуација се потпуно променила након анализе напада на Министарство иностраних послова, укључујући и његове последице и сазнања из случаја STUXNET, тако да је као резултат проистекао „залет“ са безбедносно-политичком димензијом ка решењу тог проблема.

Шта је сајбер простор

Комплексност умрежених информационих структура, као и њихове интеракције са физичким и људским процесима, водила је ка томе да се то заједно више није могло сматрати само пуким гомилањем техничких средстава. Нужно је целовито посматрати те инфраструктуре као засебни простор са сопственим законитостима. Због тога се сајбер простор може дефинисати као: *„оперативни простор у коме се подаци сакупљају, чувају, преносе, обрађују, класификују, кодирају, приказују и претварају у физичке акције“.*

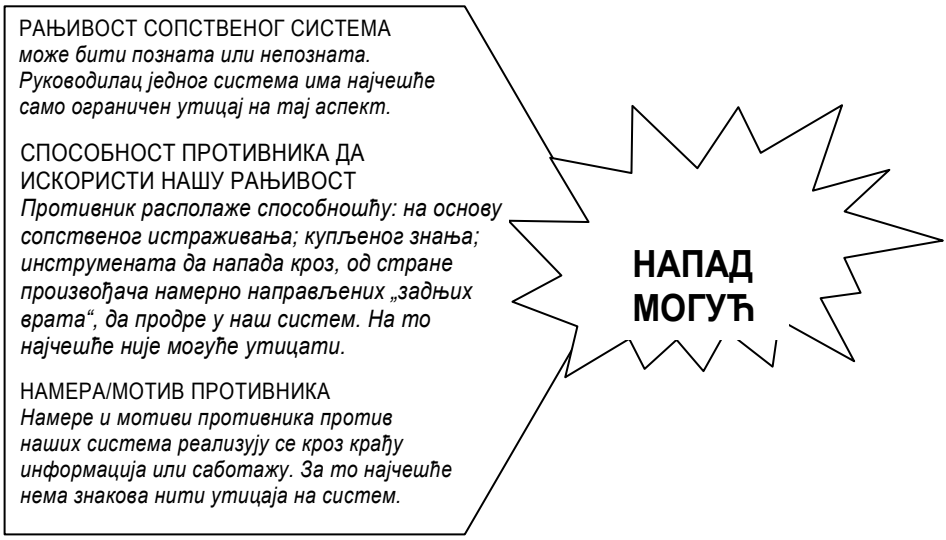
У правној држави релативно брзо и на коректан начин поставља се питање: који органи власти су за њега надлежни, за које случајеве су одговорни и како је уређена сарадња тих органа. Пошто се претња може догодити у року од неколико минута или сати, потребна је брза и енергична реакција. Дакле, суштина је да дискусије о компетенцијама у погледу такве реакције не ометају или чак саботирају елиминисање претње.

Сајбер претња

Традиционално смо се навикли да сајбер претњу посматрамо као случај дириговaног феномена, који се деси само ако се погрешна веб страница посети или отвори *spam* прилог е-поште. Пракса нам је показала да, поред таквих, постоје и претње као планирани и енергични напади који се изводе против људи и система. За то су потребна све професионалнија средства и на интернету се могу прибавити једноставно и са скромним финансијским средствима.

Једна од рушилачких последица циљаног напада може бити нпр. губитак осетљивих информација, што би опет могло значити манипулацију релевантним пословним процесима током више месеци и година. Тај облик претњи у стручном језику је назван *трајна претња због истурености* (*Advanced Persistent Threat*).[1]

[1] „Understanding the Advanced Persistent Thret“, Tom Parker, February 4, 2010, http:/www.usenix.org/event/lisa09/tech/slides/daly.pdf.



Слика 1 – *Претпоставке за напад*

Претпоставке за напад

Да би један сајбер напад био успешан потребне су, свакако, извесне претпоставке. Ако их нема, онда се у већини случајева то завршава на мање или више очигледном јављању грешке од стране система помоћу једног протокола.

1. Сопствени систем мора показати једну или више рањивости, које на стратегијски начин могу бити искоришћене.

2. Неко мора о томе бити информисан или претпостављати да ова рањивост у систему егзистира, а затим и знати како се то ефективно и у сопствену корист може искористи.

3. Актери морају имати покретачки разлог (мотив) да изведу један такав напад против физичког лица или система.

Чињеница је да модерни информационо-комуникациони системи показују многобројне „безбедносне рупе“, а, истовремено, и знања за њихово искоришћавање су прилично раширена. Истраживање и ширење информација и метода о упаду у ИКС су без ограничења, готово легални. Потребан алат за ту сврху може се лако набавити на тржишту које је врло активно. Међутим, врло је скупо да се та рањивост најпре препозна, а затим да се отклони. Верује се да „нападач“ може сразмерно лако да изведе успешан напад на наше незаштићене системе и податке са лако доступним неопходним *Know How*. Додатни отежавајући фактор јесте да постоје многе рањивости система, а да је то познато свега неколицини потенцијалних нападача. И до данашњег дана недостаје одговор на питање – како да се тај проблем реши. Такве рањивости у стручном језику зову се *O-day Vulnerabilities.*[2] Трошкови

[2] Naraine, Ryan, Anti-Virus Is Dead, D-E-A-D, Dead!, eWeek, December 1, 2006, http/securitywatch.eweek.com/virus_and_spyware/antivirus_is_dead_dead_dead.html.

за куповину једног висококвалитетног *O-day Vulnerabilits* за стицање администраторских права, нпр. код *Windows 7*, или да се уз *Adobe Acrobat Reader* прокријумчари један убачени код данас износи од 10 до 50.000 USA $. У злогласном *STUXNET* црву обједињене су четири такве рањивости.

Осим тога, рањивости система настају и због тога што разне обавештајне службе користе снагу сопствене националне информационе и комуникационе индустрије на тржишту за стратегијске циљеве, нпр. за прибављање информација. Оне располажу детаљним знањима о таквим рањивостима или чак захтевају да у производе буду уграђена „задња врата“. Такве акције увек су повезане са знатним ризицима, јер само један несмотрен поступак са информацијом може имати далекосежне последице све до сајбер криминалитета.

Резултат наведеног јесте да заштита од сајбер напада на техничком нивоу представља једну асиметричну борбу између нападача и систем оператора, што у наредном периоду не би смело тако и да остане. Робусних, на напад отпорних система има мало, тим више што притисак тржишта има тенденцију да функционалност и комфор за кориснике имају предност у односу на безбедност система.

Истовремено, растућа пажња корисника релевантних информационо- комуникационих система помера се од чисте заштите ка одбрани од напада у оперативном смислу, тј. раног препознавања аномалија, али и проверавање актера, укључујући поступке и намере који су данас, у најмању руку, толико важни колико и ажурирање вирусног скенера или одржавање оперативног система. Разуме се, не жели или не може свако предузеће да приушти себи један тако велики трошак. Органи јавне власти повећавају захтеве за преузимање одговорности нарочито код критичних инфраструктура.

ПРЕДГОВОР ДИВИЗИЈСКОГ ГЕНЕРАЛА КУРТА НИДЕГЕРА, РУКОВОДИОЦА ПРОЈЕКТА „САЈБЕР ОДБРАНА“

Нема сличног примера у историји човечанства у којем се у тако кратком времену тако много новог морало асимилирати у промене и знање у друштву као у информационој револуцији. Свет је променио лик који је пресудно и неопозиво зависан од информационих технологија. На овом технолошком развоју благостање је оно што делује повратно, од чега профитирамо ми, како индивидуе, а исто тако и привреда. Истовремено, то благостање зависи од напредовања и ентропије интегритета и способности функционисања информационих и комуникационих система, који управљају свим и свачим. Привредни развитак такође све више зависи од информационих струја широм света, медија (укључујући и друштвене мреже) и мобилних комуникација.

Овакав развој води ка томе да спорење (али и споразумевање) између људи, организација и држава попримо нове облике. Оно је постало брже (информација тече у сајбер простору без временског успоравања и може без губитка бити удвостручена) и анонимније (у сајбер простору свако може са малим трошком (пре)узети други идентитет).

Швајцарска са нивоом сопственог развоја недвосмислено припада том новом свету. Технолошки ми стојимо на предњем фронту и подстичемо развој. Свакако, то претпоставља да из тога произишле ризике свесно прихватимо и у најкраћем времену пронађемо једно стратегијско решење. Јер, већ каснимо! Савезна влада је својом одлуком од 10. децембра 2010. године те чињенице узела у обзир и издала налог за израду Националне стратегије сајбер одбране. При том се показује и значајна синергија са темом „Заштита критичних инфраструктура".

Сајбер одбрана појављује се у разноврсним видовима, али и изван њих. Не само на основу брзог развоја претњи у последње две године, него и на основу са тим повезаних изазова и питања – које суверене задатке држава треба да преузме, а коју личну одговорност сноси руководилац критичних или суперкритичних инфраструктура. Већ се јавља притисак за брзо изналажење добро интегрисаног решења, како у безбедносној политици, тако и у привреди.

У овој публикацији представљене основе скицирају међуфазу промишљања те стратегије. Могле би да уследе још многе измене и прилагођавања. Међутим, једно је неспорно: држава не може сама да отклони ту претњу. Али, она може и мора преузети руководећу улогу на стратегијском и оперативном нивоу и да за то створи правне претпоставке. При томе је потребна сарадња свих учесника, као и оних на које се то односи. Тек тада привреда и друштво могу даље да профитирају од предности технолошког развоја, а да при том не морају доживети „лоше буђење".

Развој претњи

Појмови *сајбер простор* и *сајбер претња* нису нови, тим пре што се већ 80-тих и 90-тих година приметило да растући значај информационе технологије значи и њено умрежавање које се, такође, показало новим безбедносним изазовом. Исто тако, филмска индустрија у Холивуду, као и специјалисти из техничких и безбедносно-политичких области то су проблематизовали. Први рачунарски црв био је програмиран већ 1971. године и проширио се на *ARPANET*-у – претходнику интернета. Први дигитални рачунар на свету, под називом *Colossus-Maschine*, био је израђен 1943. године ради криптоанализе немачких стратегијских порука. Тај важан догађај за британски *Bletchley-Park* из Другог светског рата обелодањен је тек 80-тих година.

Током 90-тих година, а посебно од 2000. године, „лансирани" су бројни компјутерски црви и вируси. Иако се ту радило само о „игралишту" за аматере, ипак су у појединачним случајевима проузроковане знатне штете. Вирус *ILOVEYOU* је један од најпознатијих примера из тог времена.

Професионализација и подела рада у сајбер криминалу почела је у првој половини последње деценије 20. века. Већ тада је било јасно да је први пут развијена једна претња глобалних размера. Из тога произилази да сајбер криминалитет своје порекло вуче са периферије бившег СССР-а, Кине, Јужне Америке или неког великог града у САД. Циљани напади до средине последње деценије били су релативно ретки.

Данашњи облици претњи

Погрешно би било закључити да се та претња у сајбер простору редуковала само на чисто информатичко-безбедносне случајеве. Много је важније починиоце и њихове мотиве идентификовати, како би значај њихових напада на време био препознат.

Следи илустрација седам облика претњи и прецизирање њихове генеричке форме. Циљ је да се сазнања из те анализе искористе за развијање Националне стратегије сајбер одбране. Та подела се не сматра закљученим листингом могућих степена претњи, јер се, свакако, морају узети у обзир и мешовити облици, међустепени и временска еволуција.

Вандализам

Посебни догађаји, политичке или привредне напетости, незадовољство или позив на протест појединаца воде ка томе да они, или мање групе, намеравају да нападну државно јединство или инфраструктуру, да би дестабилизовали земљу или неку организацију и њене репрезентативне симболе и да их једном „сајбер казном" приморају да обуставе рад. То је био случај у Естонији 2007. године, када је одлучивано о уклањању једног споменика подигнутог у време постојања СССР-а. Због тога се земља нашла више седмица под јаком „паљбом" сајбер нападача. Такви напади против приватног предузетништва чињени су у скорије време у Швајцарској, али они не представљају ништа ново. Услед великог пораста мобилизаторског потенцијала дигиталних друштвених мрежа, као што су *Twitter* или *Facebook*, које већ имају преко 600 милиона чланова, таква догађања добијаће на значају.

Логика и динамика маса развија се тамо где ће неко други понудити нешто више. Мотивација за таква настојања могла би да добије финансијски карактер или чак друштвену награду (признање). Такви напади могу да проузрокују значајне штете имиџу и изазову застоје у функционисању инфраструктура. Колатералне штете које, пре свега због комплексних веза, настају у инфраструктури, нажалост нису реткост и стално расту.

Са пратећим физичким акцијама против делова постојећих инфраструктура у спектру од_простих „ознака" (исписивања) па све до разарања, мора се, такође, имати у виду. Сасвим је могуће да појединци и организације у оквиру таквих вандалских аката намеравају да открију поверљиве, односно заштићене податке. Непосредне последице настале из таквих аката могу проузроковати грађанкама и грађанима, као и предузетницима, знатне сметње и штете (расположивост услуга, штете на имиџу, губитак новца и продуктивности итд.) Такве акције могу, потрајати данима и недељама са различитим временским шпицевима.

У будућности се може рачунати са порастом броја таквих напада у сајбер простору, бар из два разлога: прво, јер се добро виде и, друго, медијски су веома атрактивни. Они, такође, изазивају и знатан притисак на доносиоце одлука и, на крају, потребна средства једноставно треба набавити или изнајмити (*Bot-Netze*, *Denial of Service Tools*, итд.).

Чињење таквих деликата из угла државе није сасвим непроблематично. Иако та дела недвосмислено испуњавају критеријуме кажњивог дела, извођење доказа и идентификација коловођа („људи из позадине“) веома је тешко. То поред осталог и због тога што маса нападнутих људи са различитим пореклом, мотивима, инструментима, занимањима, итд., могу починиоце кривично-правно гонити само уз енормне трошкове. Ни већина држава то не може себи да приушти! Често, као решење остаје да се те махинације благовремено открију и прате, а штете што је могуће више ограниче.

Криминалитет

Појединци или организације могу из више криминалних мотива (превара, крађа, уцена, клевета, фалсификовање итд.), из сопствених интереса, или по налогу трећег лица, ангажовати целокупне информационе методе и ресурсе. Позадина тих криминалних аката може бити финансијске природе, личне фрустрације, али и конкуренције.

Дискретно учешће држава у позадини таквих случајева, све до налога ради шпијунаже или пропаганде није нимало необично.

Криминалци су често врло мобилни и добро организовани; изналазе и користе на иновативне начине све суптилности права. Граница према терористичким организацијама, које такве методе такође користе да би осигурале сопствено финансирање није оштра ни јасна. Поступци нападача су врло специфични и непосредно су усмерени ка циљу. Насупрот вандализму, такви случајеви немају циљ да утичу на постојећи систем или да буду видљиви сем код појединачних, типованих напада на поједине особе. Што су напади комплекснији, то ће бити потребно више инсајдерског знања и вероватније да ће те акције најчешће остати сакривене. Ако пак буду откривене, оне се, по правилу, не могу приписати ниједном одређеним починиоцу. Гро успеха криминалних актера заснива се на „фактору човек“ који је истовремено једна од највећих слабости, наводно безбедних организација. Све методе „друштвеног инжењеринга“ и даље се, све до психичког насиља (телесне повреде, провале, застрашивања итд.), користе за то. Криминалне акције трају прилично дуго, како би остале профитабилне (често месецима па и годинама) и углавном буду касно препознате. Али, криминалне организације су стално под притиском императива успеха и времена, што их на срећу води ка томе да почине грешку, а то је од значаја и органима за кривично гоњење.

Шпијунажа

Сајбер напади на информационе инфраструктуре изводе се са циљем да се дође до осетљивих података и информација и на тај начин постигне предност у преговарању; постигну привредне, односно политичке предности. Стога починиоци користе све методе обавештајних служби и своје акције планирају врло педантно. Актери могу бити државе, предузећа и приватна лица, који делују аутономно или по налогу.

Сајбер напади су по дефиницији врло суптилни, циљани и добро организовани. Ти деликти су успешни тек тада ако остану неоткривени и не доспеју у јавност. У случају да актери у својим намерама ипак буду компромитовани, они морају своје

организаторе и спонзоре да прикрију, односно да истражне органе одведу на један или више погрешних трагова. Због тога је истрага таквих напада готово „немогућа мисија“, а кривично гоњење актера по правилу неуспешно.

Војска и органи јавне власти су посебно угрожени и п(р)озвани. Војска као стратегијска ресурс Конфедерације обучена је и задужена да штити информације о инфраструктурама и поступке дуж спектра њене употребе да би их у правом тренутку, како и када је предвиђено, употребила, односно могла употребити. Зато посебна пажња мора бити посвећена протоку информација које се односе на дугорочне тајне, а које су од далекосежног политичког и стратегијског значаја.

Саботаже

Саботажа може бити политички, привредно или друштвено мотивисана. Кроз ометање информатичких, телекомуникационих система и система за управљање, са њима повезани процеси исто тако могу бити ометани, па и прекинути. У екстремним случајевима то се постиже физичким разарањем инфраструктурних елемената. Због једноставности и ефикасности у првом плану су удари нпр. на инфраструктуре у области логистике и транспорта, енергетике или привреде. Починиоци то раде првенствено због тога да постигну привредну или техничку предност у односу на конкуренте. Такође, пружају и подршку војној акцији или служе да се имиџ једне институције ослаби, односно да се углед једног органа власти уништи или, у екстремном случају, да се изазове колапс једног друштва или његових делова. Такве акције могу да буду изведене само са високопрофесионалним и увежбаним снагама које располажу солидном логистичком подршком. Мање организације или појединци који располажу поузданим информацијама и јаким мотивима за успешан напад, такође, могу да причине знатне штете. Такозвана „величина“ нападача и бројност његових средстава нису више, како се класично схвата, релевантни. *Паметни људи* (*Smart people*) су исто тако опасни ако не и опаснији од пуке масе употребљених средстава.

Тероризам

Политички мотивисане и за насиље спремне групе, религиозни или политички екстремисти могу, ради утицаја на циљне групе, користити терористичке методе. Такве акције могу бити усмерене на државе, физичка лица, симболе или институције, а често могу бити и насумичне. Рањивост нашег друштва и његових инфраструктура у односу на сајбер нападе води ка томе да се и сајбер тероризам са једним незанемарујућим потенцијалом нуди као ефикасна алтернатива или као „пратња“ нападима експлозивом (варијанта: конвенционални напади).

Стицање техничких компетенција преко млађе генерације у оним слојевима становништва у којима има мало или уопште нема перспективе, представља велики и опасан потенцијал, јер се ти млади људи могу лако регрутовати и употребити за такве акције.

За терористичке организације интернет има посебно високу вредносну позицију. За остатке разбијених терористичких организација из Авганистана, Јемена итд., интернет је постао посебно драгоцена алтернатива за мобилизацију подмлатка. Та

платформа је од суштинског значаја за регрутацију, финансирање, обуку као и руковођење терористичким активностима. Уосталом, интернет је за терористе централно ехо-средство и пропагандни медијум за представљање њихових акција. Ипак, не би се смело заборавити да су им и даље примарни циљеви терористички напади.

Конфликти

Данас би једна држава или једна организација могла водити стратегијску сајбер кампању против критичних инфраструктура других држава успешно и без посезања за дипломатским или војним средствима. У сенци једне готово апсолутне анонимности и без опасности од казне тако се могу реализовати сопствени политички/стратегијски интереси на рачун друге државе. Ова посебно опасна варијанта често се означава као сајбер рат (*Cyberwar*). Раније су је стручњаци контрадикторно тумачили, јер је само у малом броју случајева било познато да то отприлике том облику претње и одговара. Због чињенице да је наша држава, као и друге модерне државе јако рањива, не можемо себи дозволити да тај сценарио из анализе искључимо. Због тога то мора бити узето у обзир приликом израде стратегије.

Као вероватнији сценарији морају се ипак узети они код којих државне, а посебно информационе и комуникационе инфраструктуре војних противника у оквиру кризе, непосредно пре или за време конфликта, буду нападнуте са циљем да њихове способности за отпор буду редуциране или чак парализоване. На тај начин могу се постићи стратегијске, оперативне или тактичке предности, а кинетичка средства уштеђена.

Генерално посматрано, то је развојни тренд модерних оружаних снага у правцу утврђивања умреженог управљања ради подизања ефикасности и ефективности. Примењене технологије једва да се разликују од истих оних које се користе нпр. у приватном предузетништву. Притом су средства и методе за напад на те системе исти они које су познати из сајбер криминалитета. Због тога се мора, у оквиру свих ових сценарија ангажовања, поред познатих конвенционалних кинетичких метода и претњи, сајбер нападима придавати велики значај.

Марфи као противник

Информационе и комуникационе инфраструктуре, које управљају свакодневним процесима нашег друштва нису много статичне, робусне и стабилне. Оне су подложне сталним променама и један велики број непредвидивих и кроз случај управљаних ризика може прекинути њихово функционисање. Актуелни развој технологија повезан увек је са све већим недостацима код инжењерског и техничког персонала и води ка осетној редукцији квалитета у архитектури, дизајну, развоју и одржавању система и, на крају, ка значајном порасту броја слабих тачака и ризику од незгода, такорећи ка једној „мирољубивој“ претњи.

Из угла сајбер одбране, непредвиђени, случајни догађаји могу имати катастрофалне консеквенце на које се мора реаговати, слично као на праве сајбер нападе. Злонамерни актери могу и један несрећан случај да искористе за извођење напада или за његову припрему.

Строги захтеви по критичне инфраструктуре за одбрану од сајбер напада могли би бити предност, јер би они вероватно могли пружити заштиту и од „мирољубивих“ случајева.

Сајбер претња не може се схватити у једној коначној и систематичној форми. Узајамно деловање актера и знатан пораст поделе задатака у свету сајбер криминалитета и сајбер напада то не допуштају. Ипак, за развој стратегије важно је да од грубих категорија угрожавања проистекне развој одговарајућих реалистичних основних сценарија. Такође, што се тиче криминалне или безбедносно-политичке релевантности једног актера или једног догађаја не може се повући једна оштра линија поделе. У случају напада против естонских инфраструктура 2007. године, технички пре свега, може се говорити о вандализму. Наравно, на основу контекста, скривени актери су, без икакве сумње, били од извесне безбедносно-политичке релевантности.

Тренд

Сајбер претња развија се у тесној вези са технолошким напретком у области информационо-комуникационих технологија. Тако су из данашњег угла гледања препознатљива четири важна тренда.

Трајна претња због истурености (Advanced Persistent Threat)

Интеграција система унутар предузетништва, али и растућа употреба кроз службе ван безбедносног надзора, воде ка комплексној размени података. Истовремено ће праг за спречавања отицања осетљивих и чуваних података изван сопствене контролисане мреже бити нижи. Тако се нападачима пружају нове бројне могућности за инсталацију „тројанских коња“ и неприметан рад током дужег времена. Често се дешава да се током освежавања животног циклуса (ажурирања софтвера) одстрањује штетни програм, тзв. *Malware*, да би се одстранила грешка у функционисању. Тако се може одговорити на промену окружења циљаног система. Осим тога, могу се накнадно уградити нове функције. Код *Advanced Persistent Threats* противничка страна располаже веома детаљним знањима о инфраструктурама или циљним системима, као и о људима који их одржавају.

Мобилни апарати

Такозвани *Malware* на мобилним апаратима је тема о којој се све више дискутује. Свакако, он се сада налази још у зачетку. Велики број места „пресека“ и сензора у модерним мобилним апаратима и чињеница да оне „иду“ са власницима нуди безброј могућности за шпијунирање (крађа података, одређивање позиције, прислушкивање разговора, снимање тона и слике без знања власника, итд.). И платформе чије су архитектуре јавно мало познате, као нпр. *Blackberry*, могле би кроз *Revers-Engieneering*, уз веће напоре професионалне хакерске заједнице, постати знатно рањивије у погледу сајбер напада.

Крађа идентитета

Способност да се сопствени идентитет прикаже у мрежи (ауторизација) добија на значају. Ту се ради, с једне стране, о сталном расту коришћења интернета у финансијама, привреди и трговини (плаћање са мобилних телефона ће ускоро бити свакодневици, чак ће и физички новац бити истиснут као и кредитне картице) али и о широкој комуникацији са јавним службама које захтевају идентитет (*Single-Sing-On* код друштвених мрежа, *Online Gaming* и слично, електронско банкарство, контакти са органима власти). Нажалост, крађа идентитета доживеће даљи развој. Компромитација система фирме *RSA* са циљем прибављања детаљних информација о надалеко чувеном производу *SecureID* само је један предзнак таквог развоја (актуелан је напад на *SSL-Zertifikate* од *COMODO*).

Напади на системе за управљање

Разјашњен је потенцијал прецизних напада са *STUXNET* на контролне системе. Такви системи су у све већем броју циљ потенцијалних нападача.

Редовно се откривају и публикују нове рањивости система, од тзв. *Supervisory Control and Data Aquisition (SCADA)* система. Погубно је да се све више информација о таквим „безбедносним рупама“ нуди на продају на црном тржишту. Из тога произилази да би оне већ данас могле бити употребљене за напад.

СРЕДСТВА ЗА САЈБЕР НАПАДЕ

У бављењу темом сајбер одбране развио се један специфичан језик, који све више улази у дневне медије. Због тога је корисно објаснити најважније појмове.

Даљински подухвати (*Remote Exploits*) јесу програми који користе рањивост организација, служби или апликација у циљаним системима и омогућавају недозвољене операције или продор у систем.

Инфицирани документи изазивају погрешно извршавање неке апликације услед специфичних кодних грешака (нпр. *Microsoft Word*, *Adobe Acrobat* или *Kaspersky Antivirus*) и омогућавају да се изврши један нежељени, штетни код/наредба. Тиме ће се циљани систем компромитовати.

Друштвени инжињеринг је циљано и планирано коришћење погрешног поступања корисника (укључујући одавање осетљивих података о архитектури система) како би се провалило у његов систем.

Тројански коњи су програми који омогућавају извршење недозвољених/нежељених функција у циљаном систему, односно осигуравају истрајност напада у том систему. Они ће се помоћу нпр. *Remote Exploits*, инфицираних докумената или медија за архивирање, као и преко друштвеног инжињеринга „ушуњати“ у циљани систем и на тај начин моћи даље „прескакати“ у друге системе у датој мрежи.

Напади путем одбијања услуге (*Denial of Service*) јесу напади који имају за циљ преоптерећење система путем преобимног саобраћаја подацима или поновљеним позивима погрешних функција чиме се ограничава расположивости система или се чак и обара. На тај начин функције и процеси постају недоступни за овлашћене кориснике.

Botnetze су мреже са хиљадама, па и милионима заражених рачунара, које користе нападачи за нападе типа *Denial of Service*.

Стражња врата у софтверима и тзв. Firmware су механизми које су произвођачи система (или инфилтриране особе) уградили у софтвер или *Firmware,*[3] да би у неком каснијем тренутку недозвољено и неприметно ушли у сам систем или га паралисали. На пример, кроз једну тастер комбинацију *Login* екрана може се пренети или са једним специјалним пакетом података преузети веза са неком спољном апликацијом.

(Из)манипулисани хардвер је измена на хардверу, тако да је могућ приступ са удаљености, јер под извесним условима функција неће бити коректно извршена.

Како се то одражава на војску

Војска и руковођење војском

Као и у другим областима друштва, информационе и комуникационе технологије у војсци и руковођењу војском такође покривају широк спектар делатности. Од највишег кадра, па до појединачних сарадника, обичан радни дан најчешће почиње пријављивањем (логовањем) у канцеларијски аутономни систем, да би се прочитала е-пошта и отворили интернет странице. У милицијској војсци то изгледа слично, осим што поред службених система знатан део одлази на ангажовање приватних средстава. Скоро је немогуће накнадно установити или контролисати да ли се нпр. за руковођење обрађују и достављају релевантне информације преко приватних или војних информатичких средстава.

Паметни телефони (*Smart*) овде су од великог значаја, јер они физички, као и операционално, једва да се могу ограничавати. То показују најсвежији примери немира на северу Африке. Према томе, немогуће је контролисати да ли се свуда примењују исти безбедносни стандарди: највероватније је да то није случај. У уређењу информационе области имамо сличну амбивалентну ситуацију, а поред тога и незадовољавајућу ситуацију око правних основа које су превазиђене, компликоване, непотпуне, па зато, најчешће, и неефикасне.

Из визуре једног нападача, таква ситуација је оптимална: што су хетерогенији безбедносни стандарди код релевантних организација и лица, утолико је лакше наћи слабу тачку, која се може искористити да се боље заштићени системи „пробију“ ради добијања информација о особама, стању, намерама, логистици и руководству или, још горе – да би послужиле за манипулисање.

Полазећи од тога да војска представља најважнију ставку у савезном буџету, њено директно угрожавање, као безбедносно-политичког инструмента, постаје претња и пословно-финансијским процесима. Добијање профитабилног уговора са војском могао би да подстакне неку организацију да прибегне сајбер нападу ради повећања сопствених шанси као добављача.

[3] *Firmware* је специјални вид софтвера који је уграђен у мале апарате (нпр. рутере, штампаче итд.) и врло ретко се користи. Ти софтвери су посебно погодни за добро прикривање „стражњих врата“.

Слика стања сајбер простора

Са војском која постаје све мања, поставља се питање како њене способности могу даље да расту уз помоћ примене модерних технологија и како обука и њена употреба могу бити оптимизиране. У умреженом руковођењу војском управо је то препознато као врло велики потенцијал.

Истовремено, претходно смо већ закључили да тај пут собом носи врло велики ризик. Сајбер простор ће за војску бити још више релевантан операциони простор. Према томе, неизбежно је да се тај простор узима у обзир приликом процене стања, планирања и руковођења свим активностима и на свим нивоима. Тешкоћа лежи у стручном језику актера, који треба коректно превести и покрити различите временске односе између оперативних простора.

У процени демографског развоја треба узети у обзир да ће нашем друштву у будућности недостајати стручно особље. То ће се убрзо показати проблематичним управо у војсци. Сасвим је легитимно питање да ли ћемо бити у ситуацији да купимо, одржавамо и употребљавамо савремену опрему и наоружање. Потребан је брзи одговор на то, јер је важан за одлучивање о још отвореним питањима о даљем развоју војске.

Изазов за одбрану од сајбер претњи

Одлука Савезне владе од 10. 12. 2010. године о оснивању оперативне групе (*Task Force*) и именовање руководиоца пројекта за дефинисање и развој Националне стратегије сајбер одбране изазвали су јавну дискусију и поларизовали друштво. Неки су те одлуке поздравили, наглашавајући да је Национална стратегија од суштинског значаја за сајбер одбрану. Други су, опет, страховали да се ту ради само о „алиби вежби“ и да то коначно води ка нултом решењу. Неспорно је да ће тај новостворени пројекат бити конфронтиран са неколико изазова.

Он није усклађен са релевантним постојећим компетенцијама, али се руководи, пре свега, комплексношћу и временским роковима једне такве претње, односно једног ефективног напада, који прикривено вреба из реалних опасности и који би приликом реализације могао имати катастрофалне последице за цело друштво. Развитак правне државе и оружаних снага резултат је дугогодишњег процеса који се током столећа руководио принципима *trial-and-eror* и временом се оптимизирао. Иако су родови војске, као нпр. артиљерија и авијација, револуционирали бојно поље, а одређени проналасци, као нпр. струја или мотор са унутрашњим сагоревањем из темеља променили наш живот, ипак ниједна наведена област није извршила тако широк преокрет као развој информационих технологија и опасности које она собом доноси. За мање од 25 година, до тада важеће политичке, временске и географске границе нестале су и више не представљају истински лимитирајући фактор. И даље су актери најчешће непознати и у случају неког деликта углавном остају некажњени. Сада је важно да се решења, колико год је то могуће, једноставније дефинишу и да се могу применити. Ако је икако могуће, то би требало да се деси без ограничавања обима. То је у супротности са ставовима оних аутора који су се усудили да тврде да „сајбер одбрана“ буде изједначена само са „Информаци-

оном безбедношћу“. Сајбер одбрана поприма безбедносно-политичку димензију која се може реализовати само помоћу националног и међународног умрежавања. Трагични земљотрес који је 11. марта 2011. године погодио Јапан показао нам је да последице често указују на начине решавања, који су до тада често и на погрешан начин тумачени као немогући или ирелевантни. Због тога они никада нису ни били унесени у планове збрињавања или проигравани на вежбама.

Интегрални приступ

Из наведених разматрања произлази да је проблем сајбер одбране комплексан и да се у његовој димензији и динамици према њему мора интегрално односити. Поред осталих, мора се отпочети са следећим аспектима:

– **Унутрашња политичка раван**. Не смемо се ограничити само на ниво федерације, већ и кантоне и општине узети у обзир у смислу паритетног узајамног деловања. То уноси елемент различитости због њихове величине, значаја и компетенција.

– **Спољнополитичка раван**. Међународна димензија и неопходност једне тзв. сајбер дипломатије постаје све значајнија. Зато морамо са нашим суседима и међународном заједницом тесно да сарађујемо као поуздани савезници и да у текућем раду учествујемо у изградњи међународног правног оквира.

– **Инструменти безбедносне политике**. У пројекту понуђена решења морају бити интегрални део система швајцарске политике безбедности. Она се не смеју градити као независна творевина. Претња је вишедимензионална! Због тога, „заједничка игра“ између политике, права, полиције, обавештајних служби, заштите становништва, снабдевања земље и војске у вези са сајбер претњом мора бити јасно дефинисана. Међународна компонента овде је такође релевантна, поготово због тога што ће се употреба информације као стратегијског оружја у ратоводству покушати прецизније уредити.

– **Критичне инфраструктуре**. Зависност нашег друштва од малог броја умрежених критичних инфраструктура континуирано се повећава. Примарно секторска природа тих инфраструктура, брза дигитализација управљачких процеса, притисак цена преко тржишта и регулаторних тела, као и далекосежне последице једног краткотрајног испада малог дела суперкритичних инфраструктура захтева скуп софистицираних прописа. Мора се наћи равнотежа између сопствене одговорности и извршавања суверених задатака државе.

– **Привредна позиција Швајцарске**. Стратегија сајбер одбране се не сме схватити као ограничавајућа мера. Привреда може од једне добре и промишљене стратегије, како краткорочно тако и дугорочно, профитирати. Земље које су своје задатке у тој области решиле, у кооперативном сусрету са глобалном претњом биће боље повезане, а за друштво и привреду постиће бољу почетну позицију у сајбер простору.

– **Постојеће не заборавити.** Досадашњи напори Швајцарске против сајбер претњи заснивају се на стратегијској Генералштабној вежби 1997. године (*Strategische Führungsübung – SFU 97*). Она је реализована под надзором америчке *Tink Tank RAND* корпорације према методи *The Day After*. Претње нападима информационратне врсте нашле су тада важно место у безбедносно-политичком извештају 2000 (*SIPOL B 2000*).

сензуализирајући ефекат те вежбе, након које су следиле вежбе *INFORMO 2001* и *InformOren 2002*, као и пратећи безбедносно-политички извештаји, није био довољан да дâ решење, које би оправдало високу вероватноћу те претње и пратећих ризика. Расположиви ресурси су недовољни по обиму, ефективности и кохерентности. То је од изузетног значаја када треба да постане релевантно са политиком безбедности.

– **InfoSurance**. Та установа покушава да омогући и ојача сарадњу унутар сектора критичних инфраструктура, између сектора, као и између појединих сектора и федерације. Препирке између појединих њених чланова у вези финансирања и њене улоге довело је до снижавања њеног значаја на ниво обичног удружења, и своју првобитну сврху, углавном, више и не испуњава.

– **Центар за анализу информација и обавештавање (*MELANI*)** кадровски је прилично слабо попуњен и смештен у два министарства. Сви партнери су задовољни његовим квалитетом рада, али замерају му квантитет и обим.

– **Координациони центар за интернет криминал (*KOBIK*)** даје изванредне резултате. Али, он се све до скоро бавио искључиво сузбијањем порнографије. Поред надгледања интернета он има и обавезу обавештавања органа за кривично гоњење.

– **Специјални информациони штаб (*SONIA*)** формиран је током вежбе *INFORMO,* али никада није правилно обучен нити структуиран. Постоји само на папиру и приморава савезне органе у случају напада на *ad hoc* решења.

– **Војска** је 2005. године имала озбиљну концептуалну студију „Информационе операције“ која је требало да јој омогући способност подршке сопственим операцијама и постизање делимичне информатичке надмоћи. Иако је значај претњи у савременом конфликту препознат, тренутна расположива средства нису довољна.

Ова разматрања усмерена су на безбедносно-политичке инструменте. Међутим, ти ставови нису релевантни и за приватна информационо-безбедносна средства, јер су она, логично, у домену сопствене одговорности. Приватно окружење узима сајбер претње у обзир на врло хетерогене начине. Према функцији информатичког система и безбедност поприма различита значења. На пример, у случају неког немарног поступања у некој ствари, у безбедносном смислу, настале последице биле би у домену ограничене привредне штете. Насупрот томе, немарност у нпр. једној болници проузроковало би тешке последице. Један погрешан поступак може проширити *Malware* програм и створити повољне услове да рачунари постану део *Botnet*-а и на тај начин искоришћени за извођење сајбер напада. Због тога стратегија мора, такође, да садржи и елементе за редуковање опасности у важним секторима приватне делатности.

Визија

Сајбер претња је у порасту и опасна је. Она може угрозити, како егзистенцију и постојање Швајцарске, тако и њену инфраструктуру. Данашњи одбрамбени диспозитив из различитих разлога још није у стању да тај изазов обузда. Због тога једна стратегија националне сајбер одбране не сме пристајати на компромисе.

За постизање циља биће формулисане неке тезе, које нису упитне, као нпр.:

– апсолутна неопходност јасних политичких и правних оквира,

– консензус свих учесника о томе да су развојна решења сразмерна постизању циља,

– дефинисање ефективног стратегијског и оперативног процеса одговорности и процеса руковођења, који је финансијски и технички остварив,

– ризико и кризни менаџмент омогућио је себи да се робустним одговорима концентрише на праве проблеме и фокусира у првој линији на критичне инфраструктуре и привреду,

– набавка професионалних инструмената и ресурса, који се могу модификовати; који су издржљиви и обезбеђују континуитет свакодневице, као и приликом сајбер напада,

– стављање на располагање довољно персонала, који може компетентно да се носи са таквим облицима претњи.

Ове тезе заживеће због комплексности ствари, разноликости актера, а даљи развој претњи неће бити једноставан. То је од суштинског значаја како би се знало: за шта се ми залажемо, која је сврха сајбер одбране и, на крају, чиме ћемо наше ангажовање оправдати. Одговор налазимо у члану 2 Савезног устава који каже: „*Швајцарска Конфедерација штити слободу и права народа и брани независност и безбедност земље. Она унапређује заједничко благостање, трајан развој, унутрашње јединство и културну разноликост земље. Стара се, колико је могуће, за што већу једнакост шанси између грађанки и грађана и залаже за трајно очување природних животних основа и за мирољубив и праведан међународни поредак“.*

Овде је јасно како је претња дефинисана (снага, простор, време) и како изгледа крајње стање којем стремимо (слобода, благостање, безбедност). Зато нашу визију сајбер одбране формулишемо на следећи начин:

„Ми ћемо виталне функције на којима се базира стабилност, безбедност и просперитет Швајцарске, трајно штитити од сајбер претњи помоћу: правног, динамично превентивног, антиципирајућег, одвраћајућег, заштитног и интервентног диспозитива“.

Слика 3 – *Важност елемената визије*

На слици 3 приказана је важност различитих елемената визије. Тежиште ће се ставити на антиципацију, превенцију и заштиту. Истовремено, одвраћање нема великог значаја, а интервенција би требало, пре свега, да се концентрише на способност за кризно „домаћинско“ управљање.

Ниво амбиције и опције деловања

Кључно питање националне стратегије сајбер одбране је не само спектар задатака и одговорности државе већ и одређивање приоритета као нивоа амбиције.

Да би се добио одговор било је међусобно упоређивано 10 сектора критичне инфраструктуре и њихових подсектора (сходно основној стратегији савезне владе за заштиту критичних инфраструктура) са 7 облика угрожавања на нивоу највишег кризног менаџмента. Путем такве анализе може се сазнати који су сектори, са становишта сајбер одбране, посебно критични или имају нарочито висок утицај на остале секторе, на привреду и друштво као целину. Тај корак водио је ка уочавању тежишних задатака и приоритета, али још нису наведени нивои амбиције у домену различитих задатака.

Као други инструмент анализе коришћена је „морфолошка кутија“[4] да би се сачинио профил од многих тешко представљивих и хетерогених критеријума.[5] Желело се уочити како се ти критеријуми понашају међусобно при промени њиховог узајамног утицаја. Данашњи профили упоредиви су са једним минималним и једним идеалним профилом са уочљивим финансијским, персоналним, политичким и правним последицама.

Могући елементи националне стратегије сајбер одбране

Већ данас су активни бројни чиниоци на различитим нивоима у заштити Швајцарске од сајбер напада. Иако тренутни ресурси и постојеће организације по својој прилици нису довољни да би претња постала изводљива, не сме се ићи на то да се постојећа решења о ангажовању игноришу или чак да се све почне из почетка.

Поред затварања видљивих „рупа“ у стратегији, првенствено би требало допунити и консолидовати ланац постојећих процедура и средстава за покривање потреба свакодневице са аспектима безбедносно-политичке релевантности. Тај посао мора да се обави у тесној сарадњи са кантонима, најважнијим градовима, предузећима критичне и суперкритичне инфраструктуре, као и у дијалогу са изабраним иностраним партнерима и међународним организацијама (поред осталих УН, ЕУ, НАТО и ОЕБС).

Са данашњег становишта већ се распознају одређени елементи наше стратегије.

[4] Fritz Zwicky, Morphologie and Policy Analysis, Tom Ritchey, Defence Rasearsh Estabilisment, S-17290 Stockholm, Sweden.

[5] На пример, могућност централизованог или децентрализованог ангажовања, одговорност за процесе, руковођења сајбер одбраном, компетенције главних компоненти, обезбеђење ресурса, циљна група, посвећеност сајбер одбране инфраструктурама, прилагођавање правних основа, интензитет сарадње унутар земље и са иностранством, итд.

Повољне претпоставке за стратегијски кризни менаџмент

За постизање тог циља потребна је мрежа руководећег персонала из свих сектора, која омогућава сталну размену информација и усклађивање мера. Под савезним руководством, поред осталог, мора се:

– вршити размена информација стратегијског значаја о претњи, догађајима и трендовима,

– ускладити рад на дефинисању кохерентних мера и планирања збрињавања и поступања у случају сајбер напада, као и

– преиспитивање постојећих мера посредством вежби или ревизије.

Повезивање националних и техничких средстава одбране

За то је потребно створити платформу (опет у форми једне мреже) са циљем да се, колико је то моће, свим учесницима омогући брз приступ информацијама, решењима, анализама итд. да би се обезбедио успех у случају напада. Та платформа треба да буде спремна за употребу и да функционише 24 сата, 365 дана у години и да:

– даје националну „сајбер оперативну слику“,

– може да изводи сваки облик анализе софтвера, мрежа, система,

– буде национална техничка сертификацијска инстанца.

Подизање знања и обезбеђивање довољно стручног персонала

Швајцарска већ данас има важну међународну улогу у истраживању и развоју информационо-комуникационих и безбедносних технологија најразличитијих врста. Развој и истраживања најчешће иду преко *Swissnes* и запажени су на тржишту као посебно сигурни и вредни поверења. Данашњи ниво може се одрж(ав)ати и повећати само ако тој тематској области припадне одговарајућа висока вредносна позиција у истраживању унутар кантона. Динамична размена сазнања између сајбер одбрамбене заједнице, истраживачких станица индустрије и високих школа може поједноставити брзо прихватање иновација у „реалном свету“.

Обезбеђивање подмлатка – специјалистичке стручне снаге (како квалитативно, тако и квантитативно) суштински је задатак. То мора обезбедити нашем друштву успешно овладавање нарастајућом технологијом. Ми немамо намеру да преко страног, тешко контролисаног особља или фирми штитимо најважније функције државе и наших критичних инфраструктура. Безбедност је један суверени задатак који не подноси импровизације. Због тога се мора форсирати децидирана образовна политика.

Редуковање људских слабости

Тврдња да је човек „слаба тачка“ у борби против ове претње није флоскула. Сви учесници, индивидуални и колективни, морају бити у стању да смање ризике – мора се одржавати широка и тематски циљана сензибилност.

Такође, персонал директно ангажован у процесу сајбер одбране мора бити обучен и увежбан за савладавања кризе.

Из перспективе Националне стратегије већ се ради на томе да се заједно са већ постојећим инструментима државе и приватног предузетништва прилагођава, развија и реализује адекватна обука.

Прилагођавање правне норме

Поред прилагођавања постојећих правних основа, вероватно ће бити нужне и нове, у складу са усвојеним нивоима амбиције. Са данашњег становишта следеће области заслужују посебну пажњу:

– дефинисање минималних захтева за безбедност критичних информационо- комуникационих технолошких система, а пре свега суперкритичних инфраструктура;

– дефинисање могућности деловања државе у превенцији и раном препознавању претњи, као и примени мера реакције;

– утврђивање механизма политичког надзора и контроле над поменутим функцијама;

– доношење норми за јачање међународне сарадње и за узајамно признавање безбедносне провере лица;

– стварање норми и инструмената за право државног вета у спречавању неконтролисаног и штетног одласка, односно одлива важних особа, добара, фирми и знања, који припадају суверености одговорности државе.

Међународна димензија

У глобалној и међународној тематској области врло је важно усвајање кодекса понашања у различитим ситуацијама. Тако анонимност код сајбер напада представља пре правило него изузетак, а и не постоји „државни монопол“ у домену те претње. У циљу развоја динамичне сајбер дипломатије неминовно је доношење специфичног кодекса. Али, све идеје не морају бити оне које воде ка циљу. На пример, обавезујући уговор у области хуманитарног и међународног ратног права за забрану сајбер напада могао би се пре контрапродуктивно одразити, јер злоупотреба позива „неучествујућег трећег“ могла би нашкодити. Осим тога, свеобухватна контрола сајбер оружја могла би бити и тешко примењива, јер све компоненте једног програма, који би као целина можда био означен као сајбер оружје, појединачно не би био правно санкционисан. Тако се за посматрача са стране ни на који начин не разликује нпр. рад једног развојног софтвер-тима који развија сајбер оружје од делатности једног тима који развија безбедносна решења.

Глобални карактер проблема условљава и да се на свим нивоима ефективно развијају билатерални или мултилатерални модели сарадње учесника. Они егзистирају и већ дају вишак вредности за све учеснике. Али, могу се још више побољшати.

Закључак

Најважнија тема о којој још мора бити речи је улога војске у контексту сајбер одбране. Да би њено будуће ангажовање могло бити реализовано, она мора да располаже одређеним способностима, а сајбер простор као оперативни простор мора бити потпуно интегрисан у њену доктрину. То ангажовање може бити упоредиво са значењем суверености у ваздушном простору за копнене операције у једном одбрамбеном сценарију.

Са друге стране, војска још увек не располаже потпуним правним или оперативним претпоставкама како би се употребила у целом спектру рачунарских оперативних мрежа.

Осим тога, већ смо разјаснили да се претње којима је војска изложена готово не разликују од оних које се односе на критичне инфраструктуре. Нема шарених ни црвених, плавих или жутих *Malware*. Због тога се поставља питање – да ли би малобројни специјалисти надлежни за сајбер одбрану војске морали бити концентрисани, не само због синергијског ефекта, са специјалистима из цивилних области у једну јединствену организацијску јединицу. Јер, ако се код реакције на напад заиста ради о минутима и сатима, а не о данима и месецима, онда је такво решење за једну државу са малим ресурсима неминовно. Другачије формулисано: Швајцарска не може себи дозволити такав луксуз да има два или више технички компетентних центара за одбрану од сајбер претњи.

Време за израду националне стратегије сајбер одбране врло је кратко. Она захтева прагматична и разумљива решења. И поред пратећег *Top Down* ангажовања, стратегија не сме бити „диктат из Берна“. Она много више треба да представља основу за јачање националне сарадње у тој области. Стратегија не сме оставити слободан простор када се ради о дефинисању одговорности и о улогама државе, односно приватног предузетништва за заштиту од сајбер претњи. То смо дужни нашем становништву.