Овај рад представља наставак чланка од истог аутора, под насловом „**Сајбер одбрана Швајцарске – претње и стратегијски правци деловања"**, који је публикован у *Војном делу*, пролеће/2013, стр. 81–100, као превод на српски језик.

Уредник

DOI: 10.5937/vojdelo1502027V

САЈБЕР ОДБРАНА – КУДА ИДЕ?*

Gerald Vernez**
Генералштаб Швајцарске војске

Перцепције развоја претњи у сајбер простору у последњих неколико година битно су се промениле, иако су њихови суштински елементи остали исти. Сајбер претње и сајбер одбрана нису више маргиналне појаве које се негирају или преувеличавају већ се тичу свих области модерног, дигитално уређеног друштва. Овај рад представља синтезу ранијих радова и нових сазнања о сајбер домену, односно нови фокус војске у овој важној области.

Кључне речи: *сајбер претње, сајбер одбрана, облици угрожавања, национална стратегија, безбедносно-политички аспекти, улога војске*

Шта је до сада урађено

Дана 19. 6. 2012. године Савезна влада усвојила је Стратегију националне одбране Швајцарске од сајбер ризика и претњи,[1] данас познате као „Nationale Cyber Strategie" – *NCS*. Истовремено, влада је наложила Савезном министарству финансија (*Eidgenössische Finanzdepartment – EFD*), а посебно Контролном органу за информатику Савеза (*Informatiksteuerungsorgan des Bundes – ISB*), њено уредно финансирање. План реализације Савезна владе је усвојила 15. 5. 2013. године.[2]

---

* Овај чланак је објављен у часопису швајцарске војске *Military Power Revue* бр. 2/2013, стр. 46-52, под насловом **„Cyber-Defence: Quo vadis?"**. Са немачког језика текст је превео мр Здравко Зељковић, пуковник у пензији.

** Пуковник Жералд Верне (*Gerald Vernez*) и други, Генералштаб Швајцарске војске, шеф Одељења за сајбер одбрану, gerald.vernez@vtg.admin.ch.

[1] Стратегија националне одбране Швајцарске од сајбер ризика и претњи (27.06.2012.године; http:/www.isb.admin.ch/themen/01709/01710).

[2] Стратегија националне одбране Швајцарске од сајбер ризика и претњи, План спровођења NCS (15.05.2013: http:/www.news.admin.ch/NSBSubscriber/message/attacments/30607.pdf). За војску су посебно релевантна следећа два става: члан 1. „NCS експлицитно искључује случај рата и случај конфликата. Војска је одговорна за заштиту и одбрану сопствене инфраструктуре и система у свим ситуацијама. У спектру

Национална сајбер стратегија захтева одговарајуће планове спровођења промењеног правца деловања који посебно карактеришу следећа два аспекта:

– на постојећој јакој руководећој улози Савеза, од које он ипак одустаје. Децентрализоване структуре биће тек изграђене,

– национална стратегија сајбер одбране израђена је према свакодневици и примерена је мирнодопском времену. Поступање у конфликтним ситуацијама или пак операције у оквиру рата стратегијом су експлицитно искључени. Својом одлуком од маја 2013. године, Савезна влада је војсци то само прецизирала.

Даљи развој ове проблематике, а посебно претњи, свакако ће приморати западне државе и Швајцарску да основе својих стратегија редовно актуелизују. Сама Национална стратегија сајбер одбране не нуди одговоре на сва, још увек отворена питања и изазове ,али представља важан корак у правом смеру и наговештава наредне активности на основу развоја ризика и претњи које редовно преиспитује.

Садашње решење

После уложених великих напора последњих година, развијено је садашње решење у Швајцарској, које функционише као прилично одрживо, али се оно ипак још не може оценити зрелим. Без амбиција на свеобухватност, графикон 1 представља сажетак садашњег решења:

– функција „**сајбер безбедност**" контролише се преко Контролном органу за информатику Савеза (ISB) који је потчињен Министарству финансија Швајцарске. Тај орган обезбеђује успешност свога рада углавном преко обавештајног и аналитичког центра (*Melde und Analysestelle Informationssicherung – MELANI*).

Поред осталог, то указује на тесну сарадњу између Савезног завода за снабдевање националне економије (*Bundesamt für wirtschaftliche Landesversorgnung – BWL*) и Савезног уреда за цивилну заштиту (*Bundesamt für Bevölkerungsschutz – BABS*). Овај други је надлежан за спровођење Стратегије заштите критичне инфраструктуре (*Die Strategie des Schutzes kritischer Infrastrukturen – SKI*), а основу за наведено представља Национална стратегија сајбер одбране;

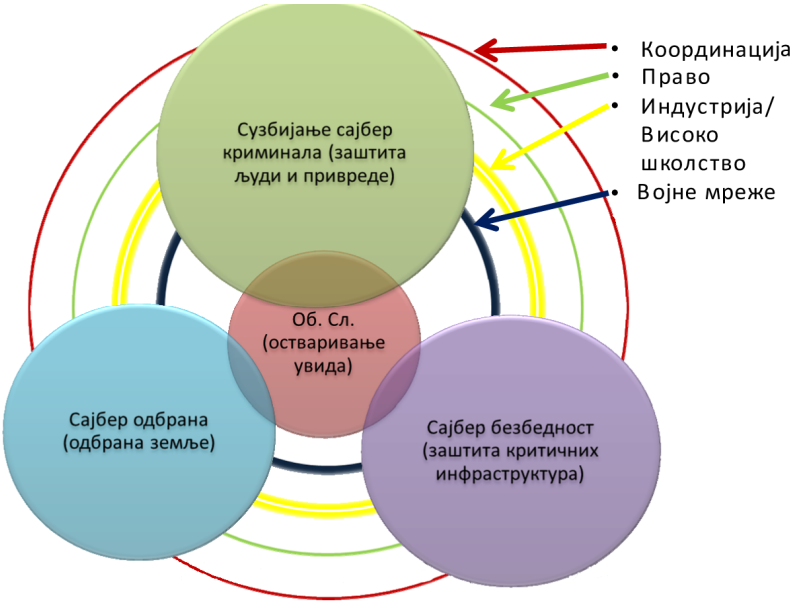
– функција „**сузбијање сајбер криминалитета**" обезбеђена је преко Савезног министарства правде и полиције (*Eidgenossische Justiz und Polizeidepartment – EJPD*) у сарадњи са кантоналним полицијским снагама. Руководећи савезни орган за концепцију и координацију је Савезна криминалистичка полиција (*Bundeskriminalpolizei – BKP*) са Координационим органом за сузбијање интернет криминалитета (*Koordinationstelle zur Bekämpfung der Internetkriminalität – KOBIK*) као најважнијим елементом;[3]

задатака и одговорности војска треба додатно да одлучује о основним поступцима за сузбијање сајбер претњи и да процени њихове консеквенце. Члан 3.3 Помоћна функција војске ... „расположиве (техничке) способности (војске) надлежни локални органи власти могу да уграђују у своје планове, а у случају потребе, они им могу и приступити. То и одговара већ испробаној и провереној помоћи војске друштву...".

[3] Координациони орган за сузбијање интернет криминалитета (*KOBIK*) даје изванредне резултате, али се, све до скоро, бавио искључиво сузбијањем порнографије. Поред надзора интернета тај орган има обавезу и обавештавања органа за кривично гоњење.

– функција „**обавештајна служба**" је задатак Савезне обавештајне службе (*Nachrichtendienst des Bundes – NDB*) која у тесној сарадњи са другим службама (поред осталих са Војном обавештајном службом (*Militärnachrichtendienst – MND*) контролише ту област. Нови Закон о обавештајним службама (*Nachrichtendienstgesetz – NDG*) који је недавно донесен, дефинисаће обавештајним службама неопходне оквире како би сајбер претње на националном нивоу биле благовремено откривене. Војска подржава ову функцију у техничком и аналитичком смислу, коришћењем постојеће синергије;

– функција „**сајбер одбрана**" осигурана је преко групе „Одбрана", Министарства одбране, цивилне заштите и спорта (*Ministerium für Verteidigung, Bevölkerungsschutz und Sport – VBS*). Њена средства ће се примарно користити за заштиту сопствених информационо-комуникационих техничких система и инфраструктуре, као и за очување способности деловања војске у свим ситуацијама. Наведеном одлуком Савезне владе од 15. 3. 2013. године, од војске се додатно очекује да у случају конфликта или/и рата преузме значајну помоћну улогу. Шта то тачно значи, како војска своју улогу треба да испуни и који ресурси ће јој за то бити потребни, мораће се, поред осталог, прецизирати у следећем безбедносно-политичком извештају.



Графикон бр. 1 – Генеричка представа швајцарског сајбер одбрамбеног плана

Као саставне делове овог решења, треба узети у обзир још и одређене елементе. То су:

– **координација**: према Националној стратегији сајбер одбране, укупна координација се остварује преко Контролног органа за информатику Савеза – ISB. Сарадњу Савеза и кантона усмерава Безбедносни савез Швајцарске (*Sicherheitsverbund der*

Schweiz – SVS), а на међународном нивоу она се одвија преко Министарства иностраних послова (*Eidgenossisches Department für Auswärtige Angelegenheiten – EDA*);

– **право**: да би се могла осигурати ефикасност ланца кривичног гоњења починилаца кривичних сајбер дела неопходан је један солидан правни оквир. Инволвиране инстанце предузеће одговарајуће напоре како би се постигла хармонизација и подигла ефикасност правних органа и затвориле празнине;

– **индустрија и високо школство**: у квантитативном и квалитативном смислу Швајцарска располаже одличним компетенцијама и способностима. Међутим, проблем је у томе да се те компетенције при отклањању сајбер ризика свуда и флексибилно повежу;

– **војне мреже**: добро уређена и изванредно густа мрежа у и између војних састава представља један веома широк и посебан инструмент.

Ово скицирано решење се још дограђује и, у односу на оперативну хармонизацију и интероперабилност, још много тога треба урадити. Разноликост и комплексност одговарајућих мера захтева време, али и искуство. Дуж овог стрмог пута засигурно ћемо доживети још многе промене. Швајцарска може бити „fit" за борбу против сајбер претњи и у томе успети, али не само са брзим „проналажењем" једноставних техничких и персоналних решења. Феномен, који је изазван владајућим агресивним „сајбер рекламирањем" („Cyber-Hype") неће моћи надоместити темељан оперативни рад и стручну компетентност у сопственим редовима.

Карактерисање сајбер претњи

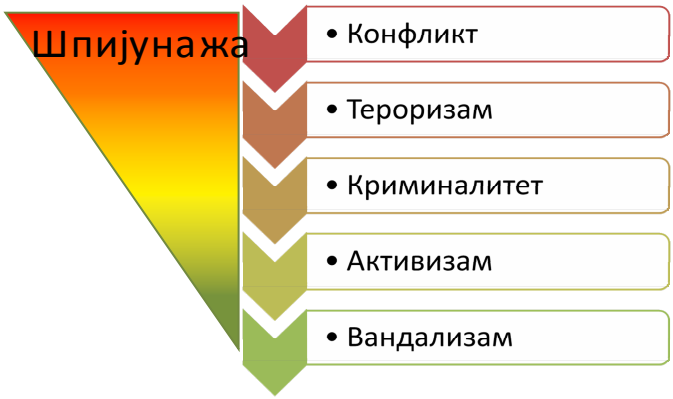
Актуелни развој сајбер претњи швајцарска војска процењује из два угла: први, на основу могућих мотива и, други, на основу квалитета и способности актера претњи.

Класификација облика претњи

На основу бројних искустава, анализа и ранијих радова, на графикону 2 сажето су приказани облици сајбер претњи, који су и релевантно степеновани. Овај графикон приказује еволуцију сајбер претњи елаборираних у бројним ранијим радовима, али су основна идеја и правци деловања остали исти.

Шпијунажа је облик претње, која по свом домету и интензитету може бити варијабилна. Она претходи осталим облицима претњи, али и систематски их прати. Шпијунске активности и криминалне радње често иду руку под руку и, по правилу, између тих категорија није могуће направити оштру поделу. Иако је ту реч о нападима у и око сајбер простора, било би погрешно сајбер нападе посматрати изоловано. Напади у сајбер простору не претпостављају само примену логичких метода. Коришћење физичких, електромагнетних или семантичких метода такође се мора узети у обзир (нпр. провала у рачунски центар, „прислушкивање" зрачења монитора, манипулисање веб страницама ради ширења малвер (*Malware*)[4] софтвера, итд.

[4] Термин *Malware* (малвер) обухвата све врсте злонамерних софтвера намењених оштећењу рачунара или мрежа. Тзв. *Malware* на мобилним апаратима је тема о којој се све више дискутује. Свакако, он се сада налази још на почетку развоја. Велики број места „пресека" и сензора у модерним мобилним апаратима и чињеница да оне иду са власницима нуди безброј могућности, да њих и њихово окружење шпијунирају (крађа података,



Графикон бр. 2 – Облици сајбер претњи

Због тога се овде представљени облици претњи морају „читати" не само као просто узимања у обзир ових елемената, него као интегрални поглед на нападне и одбрамбене реакције, односно противмере.

Према томе, да би разумели сајбер претње, увек морамо узимати у обзир контекст (политичке и привредне напетости, кризе и конфликте свих врста).

Квалитативна класификација актера претњи

Актери претњи могу се грубо разврстати у 5 група (претње П1-П5) – погледати графикон 3.

Графикон бр. 3 – Категорије претњи

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 на сајбер нападе постати знатно рањивије.

Комплексност напада и за то потребна знања и искуства расту одоздо нагоре. Али, вероватноћа да ће се она догодити и причинити штету ипак опада.

Ниже категорије претњи могу се реализовати и са средствима која су доступна на тржишту по веома ниским ценама, а која данас не захтевају велике персоналне ресурсе. Ипак, највиши ниво претњи захтева специјалне стручне компетенције, а делимично и способности да се примене у сопственој режији развијене мере.

– *Категорија П1*: „корисник хакерског алата" (Anwender von Hacking-Tools) (Script-Kiddies): актери без посебних специфичних стручних знања користе софтверски алат преузет са интернета, дају e-mail или IP-адресу и посматрају шта се дешава. До сада, ови углавном несистематични поступци причињавали су само мање штете, али понекада и веће. Пораст употребе таквих алата кроз ситан криминал израженији је у последње време.

– *Категорија П2*: „програмери рањивости, мотивисани хакер" (Entwickler von Verwundbarkeiten, motivierte Hacker). Особе које су укључене у истраживање и развој нападачких метода у индустрији или академским круговима могли би трећим лицима омогућити приступ новим алатима и методама. Осим тога, те особе могле би на неки начин да воде двоструки живот – да поред свога истраживачког и „развојног" посла буду активни и као хакери и да неовлашћено упадају у системе других и на тај начин даље континуирано развијају свој софтверски алат.

– *Категорија П3*: „Професионалне организације и сајбер криминал" (Professionelle Organisationen und Cyber – Kriminelle). Овај сегмент претњи развија се и користи за пословне моделе, квалитативно највише процесе и алате, како би помоћу сајбер напада и за њих примереним технологијама зарадили новац или шпијунирали. Нарочито се финансијска индустрија и њени клијенти, који најчешће и чине најслабију карику безбедносног ланца, налазе у фокусу ове претње. Истовремено, неке фирме на тржишту нуде технологије које омогућавају несметан приступ заштићеним системима. У неким земљама такво понашање је нелегално, док у другима није. Понуда је глобална, па зато локална законодавства имају скромне могућности утицаја. Генерално, овај сегмент претњи јесте једно велико тржиште развоја у криминалној, сивој али, такође, и у легалној зони. То данас представља главну полугу претњи.

– *Категорија П4*: „Специфични и непрепознатљиви актери претњи" (Gezielte und nicht erkennbare Bedrohungsagenten) („Advanced Persistent Threats").[5] Под овим обликом претње подразумева се брижљиво одабран циљ, веома прецизно поступање како би се, колико год је то могуће, дуже остало непримећен. Актери упадају што је могуће неприметније у заштићене системе (понекад и коришћењем погрешног понашања сарадника) и труде се да што дуже остану непримећени, како би, с

[5] *Advanced Persistent Threat* (трајна претња због истурености). Интеграција система унутар предузетништва, али и растућа употреба кроз службе ван безбедносног домашаја, воде ка томе да се догоди комплексна размена података. Истовремено ће праг за спречавања отицања осетљивих и чуваних подататка, изван сопствене контролисане мреже, бити нижи. Тако се нападачима пружају нове и бројне могућности за инсталацију тројанских коња и неприметан рад током дужег времена. Често се дешава у току животног циклуса актуелизација једног штетног програма, тзв. „*Malware*" да би се грешка одстранила. Тако се може реаговати на промену околине код циљног система. Даље, нове функције се могу накнадно позвати. Код *Advanced Persistent Threats* супротна страна располаже веома детаљним знањима о инфраструктурама или циљним системима, као и оним људима који их одржавају.

једне стране, истраживали информације (пример „Red October") или, с друге стране, извели акте саботаже (пример „Stuxnet").[6]

– *Категорија П5*: „Топ 5" – Организације и службе земаља које могу да врше велики утицај на сопствену индустрију информационо-комуникационих технологија и с њом повезани сектор услуга чине најређи и тешко препознатљив, али зато најозбиљнији облик угрожавања. Ови актери имају могућност да изврше свеобухватне припреме, како би провалили у најважније системе, који се данас могу набавити на тржишту. Разумљиво, елиминисање ове претње са којом се сусрећу све државе, па и оне са знатно већим ресурсима од Швајцарске, немогуће је. Трошкови за тестирање свих компоненти важних система су превелики. Али, код посебно осетљивих система мора се поставити важно питање – како се жели и треба елиминисати овај облик претње. Нажалост, то често захтева велике финансијске и кадровске инвестиције.

Остали актери ризика

– „*Стапање*" *приватних информатичких средстава и инфраструктура информационо-комуникационих технологија* (ИКТ) и предузетништва (поред осталог познатог под именом „Bring Your Own Device") знатно повећава ризике од претњи П1 до П5. То, пре свега, због штедњама мотивисаних разлога и од индустрије изразито пропагиране стратегије онемогућавања доследног спровођења континуиране и адекватне ИКТ безбедности, а са тим и одбране од претњи на нивоу мреже и система.

– *Преношење пословних процеса на мобилне апарате* носи велике предности, али такође садржи и нове ризике. Сигурно је да је пословни модел свих произвођача смарт телефона и таблета у противречности са добром праксом („Best Practices") безбедности у којој се корисницима сугерише инсталирање софтвера нових апликација који би могли да компромитују интегритет апарата. Такође, повезивање мобилних апарата на предузетничку мрежу узрокује слабљење безбедносних процеса (тако се нпр. са једном смарт картицом може фингирати аутентичност). Да ли и које осетљиве податке корисници поседују на својим мобилним апаратима препуштено је њима самима, на сопствену одговорност и то се више не може контролисати.

– *Клауд* (*cloud*, енг. облак) *стратегије* воде ка томе да предузећа и јавна управа своје податке све више поверавају спољним менаџерима ИКТ инфраструктура и на тај начин избегавају и смањују сопствене трошкове. Како то последњих година показују сензационална открића (случај Сноуден), ови подаци се и те како налазе у домену интересовања обавештајних служби. У будућности ће се, вероватно, приватним агенцијама које нуде услуге „клауда", рекламни простор и претраживаче, морати поклањати више пажње него државним актерима. Анализом корелација и циљане употребе, подаци који су обрађивани у „клауду" могу се даље развијати изван сваке демократске контроле у врло уносне пословне моделе који су у крајњем случају у противречности са нашим схватањем приватне сфере.

[6] STUXNET је био сајбер напад на Министарство иностраних послова Швајцарске.

– *У повременим кампањама за образовање корисника* поједини корисници се узимају на одговорност због непридржавања бројних правила понашања, чиме се шансе за успех сајбер напада знатно смањују. Генерално, успех тих мера не доводи се у питање, али оне ипак симболично указују на немоћ једног предузетника у односу на сајбер претње. Уколико успешна заштита сопствених инфраструктура зависи од коректног односа свих сарадника (нпр. неотварање непознатих или сумњивих e-mail-ова, медија заражених Veb-страница, коришћење сигурних лозинки итд.) утолико је њена рањивост већа. Ако се главни циљ састоји у томе да безбедно обрађујемо осетљиве податке, тада без сумње морамо набавити системе који ће сарадницима онемогућити чињење погрешних радњи. Најзад, то би могло водити ка томе да се коришћење приватних ИКТ средстава буде морало битно ограничити.

– *Инсајдер ризици и ризици од „цурења података*" („Data Leakage"). Једноставном набавком јефтиних меморијских медија, клауд-сервиса уз истовремено смањење улоге информационих технологија повећавају се инсајдерски ризици.

Случајеви великог отицања података, како у јавном, тако и у приватном сектору, последњих су година и у Швајцарској вишеструко порасли. Због тога је неминовно предузети адекватне мере и унутар система, а не само на прелазу ка другим системима или интернету. Основ за то чине технологије као што су и менаџмент идентитета, приступа (*Access*) и маркирања (етикетирање) података. Даље, како код мрежног саобраћаја, тако и унутар система, постојеће способности и пропусти у понашању корисника морају се идентификовати.

Посебне и ванредне ситуације у сајбер области

Посебне и ванредне ситуације биће дефинисане преко средстава потребних за превладавање кризе. Овај метод може бити примењен и у сценаријима који би се заиста могли десити у сајбер области. Ево неколико могућих сценарија:

– *Напад на поједине секторе критичних инфраструктура:* сектори као што су снабдевање струјом, шински саобраћај, транспорт нафте и гаса, финансијска индустрија, ваздушни саобраћај итд. указују на велику инхерентност и рањивост широм земље. То значи да се више координираних малих застоја може кумулирати у велики поремећај и водити до потпуног застоја у раду целог сектора, нпр. и на европском нивоу. Посредством координираних сајбер напада, а делимично и преко тривијалних физичких напада на кључне елементе, такви ексцеси данас се налазе у домену МОГУЋЕГ. Али, просечан нападач тешко може да процени какве ће последице имати његов напад, иако је јасно да и мали напади могу водити ка великим штетама. Мотиви за такве нападе могу се налазити како у политичкој (нпр. терор), тако и у финансијској (конкуренција) сфери.

– *Трговински рат између мултинационалних компанија и земаља:* међународно трговинско окружење носи печат растуће конкуренције за ресурсе који постају недовољни и стратегијских трговинских путева. Као примере навешћемо само аспирације на Арктик или на Јужно кинеско море као и пловни пут кроз Персијски залив. До сада су се таква надметања водила за приступ територијама, пре свега са финансијско-привредним средствима или демонстрацијом силе („Show of Force"). Следећи пример

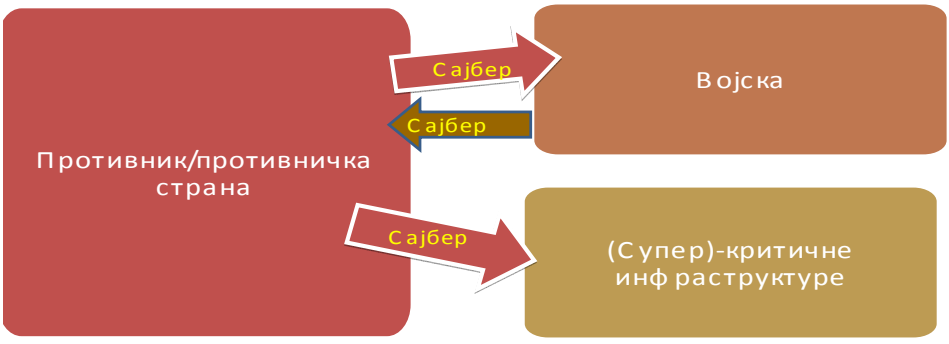
је све већа конкуренција између финансијских центара у време финансијске кризе, која се проширила и на политичку позорницу. У пољу ових зона напетости расте притисак на актере, па је сасвим разумљиво да се користе и сајбер средства. Већ данас је сајбер шпијунажа ствар избора, како би се намере и интереси конкуренције помно пратили. Примена таквих средстава ради саботаже или чак потпуне парализе пословних процеса једног или више предузећа данас је у домену ИЗВОДЉИВОГ. На тај начин фирмама и државама могу се нанети високи финансијски губици или велике штете на угледу, чак толике да буду истиснуте са тржишта.

– *Политичке или привредне уцене посредством сајбер напада против једне земље*: државни или недржавни актери данас могу помоћу сајбер напада на критичне инфраструктуре једне земље да испоље толики негативан утицај и угрозе њене поједине секторе да се попуштање политичким или привредним захтевима не може избећи. Један такав сценарио био је проигран у оквиру „Стратегијске вежбе 2013" (*Strategische Führungsübung 2013 – SFU 13*). У једној такој ситуацији сачувати способност за ефикасно деловање захтева изванредну оспособљеност, посебно у домену обавештајних служби.

Процена изазова са становишта Војске

Развој нашег друштва, посебно растуће дигитално умрежавање у готово свим областима довело је до тога да смо постали јако зависни од нормалног функционисања постојеће инфраструктуре. Посебно критичне инфраструктуре, као што су нпр. системи за снабдевање водом, струјом или телекомуникације, добиле су на значају, јер нарушавање начина њиховог рада не може се дозволити (нпр. ометање дигиталних процеса помоћу сајбер напада). Такве сметње директно се одражавају на све области друштва, као и на друге критичне инфраструктуре.

И сама Војска је једна од критичних инфраструктура наше земље и зависи од нормалног функционисања других критичних инфраструктура, при чему се свакодневно конфронтира са сајбер претњама.



Графикон бр. 4 – Процена проблема из визуре војске

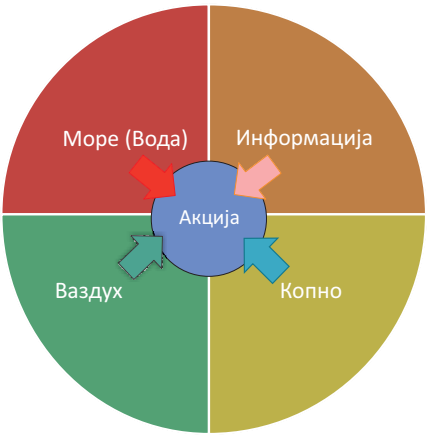
Сходно уставној улози Војске, пред њу се постављају следећа кључна питања (погледати графикон 4):

– како Војска треба да се штити и одбрани од сајбер претњи,

– како Војска треба да организује сарадњу са другим актерима од којих зависи реализација њених сопствених задатака,

– шта Војска генерално мора да учини за успешну заштиту критичних инфраструктура земље, односно у чему се састоји њен помоћни (солидарни) допринос.

Иако сва ова питања почињу префиксом „сајбер", у одговору на њих мора се обратити пуна пажња на друге димензије.



Графикон бр. 5 – Свеобухватни приступ са оперативним димензијама

Као што графикон 5 показује, свака акција је збир више истовремено дејствујућих вектора у операционим димензијама: копно, ваздух, море/вода и информација. Али, како пракса наше војске увек и изнова показује, координирано ангажовање више димензија (нпр. ваздух и копно, тзв. JOINT) и даље је неопходно унапређивати. И са димензијом „информација" која укључује домен „САЈБЕР" то ће бити (већ у мирнодопско време) још комплексније, на крају крајева, због преклапања ових области између војног и цивилног окружења. Дакле, за Војску то значи интегрисање сајбер простора у њене (свако)дневне активности и обуку.

Консеквенце по војску

За војску је најважније да обезбеди способност сопственог ангажовања и слободу деловања у свако време и у свим ситуацијама; да буде у стању да препозна сајбер претње, од њих се штити и одбрани.Да би се то постигло треба имплементирати и овладати следећим процесима:

РУКОВОЂЕЊЕ: у свако време и непрекидно војска треба да буде у ситуацији да на свим задацима свог развоја и употребе обезбеди и ангажује неопходне партнере и што је могуће боље сараднике у области сајбер одбране,

АНТИЦИПАЦИЈА: у свако доба војска треба да располаже неопходним знањима за осигурање процеса доношења одлука; да буде у оквирима дугорочних и средњорочних планских и наредних развојних активности или у карткорочним догађањима у оквиру једне операције или кризног менаџмента,

ПРЕВЕНЦИЈА: треба је спроводити у свим могућим сегментима (технички, организациони, људски итд.) који кроз сајбер претњом условљене ризике ограничавају ефикасност употребе војске. Војска мора у свако доба да спроводи превенцију, а у случају напада да је поново што пре успостави. То треба да функционише и у једном јако нарушеном амбијенту, чак и у сајбер простору који више не функционише.

РЕАКЦИЈА: у случају једног сајбер догађаја војска треба да га тачно и правовремено лоцира, разуме, а онда правилно делује, како у техничкој, тако и у нетехничкој области, нпр. кроз правне контакте или дипломатску сарадњу.

Да би ова четири оперативна процеса оптимално функционисала потребни су јасни политички и правни оквири, сигурне и отпорне (resiliente)[7] инфраструктуре, као и стабилно партнерство, како у Швајцарској, тако и у иностранству.

Дакле, то су стратегијски принципи које је одобрио Генералштаб који јасно показују правац деловања. На већ постојећим способностима и процесима биће предузети наредни кораци у развијању компетенција, с циљем да се достигне стање да се унутар војске може развијати, на будућност оријентисани „Еко систем сајбер одбране" („Öko-System Cyber-Defense").

Улога војске у националном решењу

Од војске као стратегијске резерве земље очекује се, на пример, у једној тешкој кризи, а такође и у сајбер кризи, да да пун допринос како би држава могла задржати контролу или у случају њеног губитка, да је што пре успостави посебно над критичном инфраструктуром, снабдевањем и безбедности уопште.

Тај „допринос" војске садржи се у одлуци Савезне владе од 15. 5. 2013. године као нови супсидијарни (помоћни) сајбер допринос. Тачни задаци биће предмет имплементације Националне стратегије сајбер одбране и следећег безбедносно-политичког извештаја, који би морао да садржи следеће:

– осигурање на кризе отпорних комуникација од интереса за Савез, кантоне и општине и изабране критичне инфраструктуре,

– подршку изабраним критичним инфраструктурама и партнерима из јавне безбедности за повећање њихове отпорности,

– пружање различитих врста помоћи за поновно успостављање функционалности критичних инфраструктура,

– заштита (логичка, физичка, семантичка и електромагнетна) посебно осетљивих објеката,

– допринос анализи и одбрани од претњи у сајбер домену.

[7] „Resilienz" (еластичност) означава способност једног система/организације против ометања (поред осталог и напада). Они морају бити отпорни и у случају, на пример, једног инцидента и да, што је могуће брже, успоставе пређашњу функцију на задовољавајућем нивоу.

Буде ли војска морала овакве задатке да реализује и у овој форми, поред дефинисања за то неопходних додатних средстава, морају се донети одговарајући планови, мере предострожности и увежбати алгоритми. Већ поменуте војне мреже требало би да буду посебно важан фактор успеха.

Изазови димензионирања

Ако се узме вероватноћа настанка могућих ризика као критеријум у прављењу приоритета и димензионирању мера, тада ће и изабрани правац деловања бити исправан. Свакако, у случају сајбер одбране није могуће узимати у обзир само оне ризике чија вероватноћа наступа је већа, јер управо најопаснији ризици и не указују на могућност да ће се и десити. Гледано из безбедносно-политичког угла, данас се готово без сумње прихвата оцена да оружани сукоб у Европи, у догледно време, није вероватан. Учестале или дуготрајније сметње на критичним инфраструктурама зато су много вероватније, а на основу наше енормне зависности могу водити ка катастрофалним последицама не само у друштвеном, привредном него и у политичко-безбедносном домену. Према уставу, компетентност за давање одговора на те ризике спада у надлежност Швајцарске Конфедерације.

Али, ако се ради о томе да се дефинишу тачни задаци за заштиту и одбрану Швајцарске од сајбер претњи и за то одреде потребна средства, за све инволвиране стране постављају се, поред осталих, и следећа кључна питања:

– којим и коликим компетенцијама располаже нападач,

– шта се мора одбранити,

– колико објеката би могло бити истовремено нападнуто,

– којим максималним интензитетом се заиста мора рачунати и шта би могло из те кризе да произиђе (консеквенце), и

– током којег периода (трајање)?

Одговори на ова питања су изузетно важни, али прецизан „попис" адекватних мера, с обзиром на природу ове проблематике, једва да се могу и замислити.

Као последице тога и даље ће нас пратити следећа питања:

– да ли је за планирање и имплементирање наших средстава увек оправдан амбицијски ниво примерен претњама,

– дозвољавају ли средства националног решења будући интензитет и комплексност за превенцију, а у случају догађаја адекватно и флексибилно деловање,

– јесу ли наши сценарији реални и колико би заиста била примерена наша средства у сузбијању таквих догађаја,

– да ли наше друштво довољно добро прати развој информационо-комуникационих средстава и пратеће дигитално умрежавање свих области друштвеног живота, и

– како то све изгледа с обзиром на актуелну енергетску зависност.

Посебан изазов лежи у домену регрутације персонала, јер се постојећи актери крећу у једном простору у којем се данас такмичи недовољан број специјалиста и талената, а то ће сигурно још потрајати. Све земље доживљавају исто. Дакле, не дозволимо себи да будемо заслепљени медијским саопштењима према којима из-

весне земље могу у веома кратком року ангажовати хиљаде висококвалификованих експерата. Додуше, постоји један јасан тренд који више не можемо занемаривати, али се при томе релативност не сме изгубити из вида.

Ако гледамо даље у будућност навиру нова питања, на пример: који значај има аутоматизација (роботи), а коју појединац; како ћемо сузбити растућу индустријализацију сајбер криминала; које ће последице на средства, образовање, правила итд. имати будући конфликти, код којих ће сајбер оружје са великом вероватноћом имати централну улогу?

Перспектива

Од почетка индустријске револуције захваћени смо информационом револуцијом, која више од 20 година битно утиче и мења наше друштво, природу конфликата и ратова. Индикатори јасно показују да су сајбер претње апсолутна реалност. Субјективно прецењивање или потцењивање овог облика претње, као и спектакуларни извештаји медија (нпр. случај Сноуден) више нам одмажу него помажу.

Наведеним изазовима не можемо се ефикасно супротставити малобројним и слабо координираним мерама. Оне захтевају дугорочно, стратегијско, безбедносно релевантно размишљање и деловање, насупрот партикуларним интересима појединаца, организација и индустрије.

Армија наставља да развија своје методе и средства за савладавање сајбер претњи. У оквиру спровођења Националне стратегије сајбер одбране и наредних безбедносноплитичких развојних корака, она треба посебно да прецизира своју помоћну улогу. Ми смо већ на том путу.