УДК: 355.02(430) ; 343.533::004(430)

УЛОГА ЦИВИЛНОГ И ВОЈНОГ ОБАВЕШТАЈНО-БЕЗБЕДНОСНОГ СЕКТОРА СР НЕМАЧКЕ У СПРОВОЂЕЊУ СТРАТЕГИЈЕ САЈБЕР БЕЗБЕДНОСТИ

Милан Миљковић
Министарство одбране Републике Србије

Стратегија сајбер безбедности Немачке, у навођењу и малициозних активности у сајбер простору, говори и о сајбер шпијунажи, појашњавајући да сајбер шпијунажа представља сајбер напад који је усмерен према тајности ИТ система и који је извела обавештајна служба. Такође, стратегија оцењује да су сајбер напади, када је Немачка у питању, реализовани како из Немачке тако и са територије страних држава, чиме имплицитно указују на могуће ангажовање и страних обавештајних служби у тим нападима. На државном нивоу, целокупну сајбер политику Немачке координише Национални савет за сајбер безбедност, као орган Владе Немачке (The National Cybersecurity Council), у чији састав је ушло и неколико припадника Бундесвера. Од државних агенција, водећу улогу у области сајбер безбедности Немачке има Федерална канцеларија за информациону безбедност (Bundesamt für Sicherheit in der Informationstechnik – BSI), која је део Министарства унутрашњих послова, и која је водећи ауторитет у области сајбер безбедности. У оквиру BSI, главну оперативну улогу у обезбеђивању сајбер безбедности има новоформирани Национални центар за одбрану сајбер простора. У центру су од средине 2011. године деташирани и ангажовани припадници Савезне службе за заштиту устава (BfV), Савезног завода за заштиту народа и помоћ при катастрофама (BBK), Савезне криминалистичке службе, Савезне полиције, Савезне царине, Савезне обавештајне службе (BND) и оружаних снага Немачке (Бундесвера). Одговорност ОС Немачке за сајбер безбедност лимитирано је на заштиту ИТ система који се налазе у употреби у Бундесверу. Са друге стране, Стратегијска команда за извиђање (Kommando Strategische Aufklärung – KSA), која је је интегрални део војнообавештајних органа ОС Немачке, од 2006. године поседује капацитете за извођење сајбер напада и сајбер шпијунирање, груписаних унутар посебног Одељења за информационе и компјутерско мрежне операције (Abteilung Informations und Computernetzwerkoperationen).

Кључне речи: *Немачка, стратегија, сајбер безбедност, сајбер шпијунажа, поверљивост података*

Увод

Стратегија сајбер безбедности Немачке[1] дефинише *сајбер простор* као виртуални простор свих информационо-телекомуникационих (ИТ) система повезаних на нивоу база података на глобалном нивоу. У стратегији се истиче да је интернет, као универзална и јавно приступачна мрежа, основни предуслов постојања сајбер простора, која може даље да се шири и дограђује са додатним умреженим базама података. Наводи се да ИТ системи у изолованом виртуелном простору нису део сајбер простора. У навођењу и малициозних активности у сајбер простору, у односу на циљеве тих активности, немачка стратегија говори о:

– сајбер нападу,
– сајбер шпијунажи и
– сајбер саботажи.

Појашњава се, такође, да је *сајбер напад* ИТ напад у сајбер простору, усмерен директно према једном или неколико ИТ система ради уништења тих система и ИТ безбедности. Иначе, циљ напада може да буде уништење ИТ безбедности, тајности, интегритета или доступности података[2] у ИТ систему, појединачно или комбинација појединих циљева. *Сајбер шпијунажа* представља сајбер напад који је усмерен према тајности ИТ система и који је извела страна обавештајна служба. *Сајбер саботажа* представља сајбер напад усмерен према интегритету и доступности ИТ система.

Основне смернице Стратегије сајбер безбедности Немачке

Доступност сајбер простора, интегритет, аутентичност и поверљивост података у сајбер простору постало је за Немачку витално питање у 21. веку. Обезбеђивање сајбер безбедности због тога је постало централни изазов за државу, економско пословање и друштво, како на националном, тако и на међународном плану.

Оцењују да су, када је Немачка у питању, сајбер напади реализовани како из Немачке тако и са територије страних држава, чиме имплицитно указују на могуће ангажовање и страних обавештајних служби у тим нападима. Немачка стратегија даље наводи да криминалци, терористи и шпијуни користе сајбер простор као простор за своје активности и да се при томе не заустављају на „државним границама".

Иако се Стратегија сајбер безбедности, како се наводи, тежишно фокусира на цивилни приступ и мере које примењују цивилне институције, треба напоменути да су оне ипак комплементарне са мерама које спроводи Бундесвер да би заштитио способности ОС Немачке и мере базиране на мандату Бундесвера да обезбеди „сајбер безбедност Немачке", као саставни елеменат целокупне државне превентивне стратегије безбедности.

[1] Cyber Security Strategy for Germany, Министарство унутрашњих послова Немачке, фебруар 2011, страна 14.

[2] Тајност је начин поступања са податком који обезбеђује да током обраде и чувања није постао доступан неовлашћеним лицима, односно није неовлашћено обрађиван.

У Стратегији се наводи да критичне инфраструктуре чине организационе и физичке структуре и средства од виталне важности за немачко друштво и економију, тако да њихово прекидање и деградирање може довести до недостатка њиховог напајања, значајног ремећења друштвене сигурности или других драматичних последица.[3]

Критичне инфраструктуре могу бити изложене спектру претњи које се могу, условно, сврстати у следеће групе:

– елементарне непогоде (екстремни временски услови, пожари, потреси, епидемије, пандемије, космички догађаји и сл.);

– технички пропусти/људске грешке (системски пропусти, немар, организациони пропусти и сл.);

– тероризам, криминал, рат.

Да би заједничка акција била успешна, неопходне су стратегијске смернице битне за заштиту критичних инфраструктура, а које се тичу свих релевантних ризика. На бази смерница могуће је утврдити потциљеве, који ће бити специфицирани и имплементирани кроз програме, планове или концепте. Тако у ИТ сегменту такав план већ постоји у облику Националног плана за заштиту информационих инфраструктура (National Plan for Information Infrastructure Protection – NPSI).

Конзистентна имплементација циљева реализује се у форми кружног циклуса управљања ризицима у критичним инфраструктурама: превенција – имплементација – вежбе – одговор – анализа – евалуација (Prevention – Implementation, Exercises – Response – Analysis – Evaluation).

У Стратегији се захтева заједничко ангажовање и имплементација Стратегије на федералном и локалном нивоу, у складу са областима одговорности.

Цивилне и војне безбедносне институције Немачке за сајбер безбедност и извођење сајбер операција

У основи, када анализирамо активности безбедносног сектора Немачке у области сајбер безбедности, делимо их на три дела:

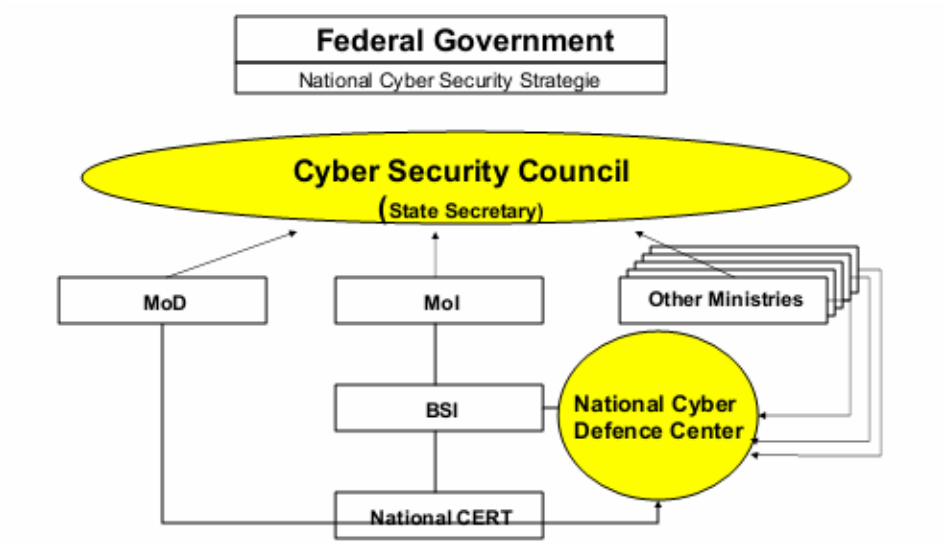
1) цивилни сектор, који је обично одговоран за заштиту критичне инфраструктуре,

2) обавештајни сектор, који је одговоран за анализу комуникација и протока података (Signals Intelligence SigInt) и

3) и војни сектор. Најчешће, офанзивне сајбер способности су у надлежности војног сектора, што се закључује на основу расположивих званичних и незваничних извора. Иначе, немачке војне јединице и обавештајне агенције имају сајбер компоненте.

На државном нивоу, целокупну сајбер политику координише Национални савет за сајбер безбедност, као орган Владе Немачке (The National Cybersecurity Council), у чији састав је ушло и неколико припадника Бундесвера.

[3] National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Ministry of Interior, Federal Republic of Germany, Berlin, 17th June, 2009, p. 4.



Потпуна одговорност за заштиту критичних информационих инфраструктура Немачке је на Министарству унутрашњих послова (BMI),[4] заједно са неколико његових потчињених агенција, као што је Федерална служба за информациону безбедност (BSI), Федерална служба за заштиту цивила и помоћ у несрећама (BBK), Федерална агенција криминалистичке полиције (BKA) и Федерална полиција (BPOL). За координацију између наведених агенција, у Министарству унутрашњих послова формирана је, 2002. године, посебна јединица за заштиту критичних инфраструктура (AG KRITIS). Развој стратегија и других активности се координирају са другим федералним министарствима (министарством одбране, правде, иностраних послова, економије и технологије и других релевантних агенција.[5]

Од наведених агенција, водећу улогу има наведена Федерална канцеларија за информациону безбедност (Bundesamt für Sicherheit in der Informationstechnik – BSI), која је, као што је наведено, део Министарства унутрашњих послова, и која је водећи ауторитет у области сајбер безбедности.[6] BSI је „одговоран за осигуравање чврсте, функционалне електронске комуникације између јавне администрације, грађана и предузећа“, посебно заштиту дигиталне димензије „кључне јавне инфраструктуре“. (електропривреде, железнице, авио превоза и итд.).

Немачки Федерални ЦЕРТ тим,[7] (CERT-Bund) део је 12. одељења BSI[8] и представља централни contact point за решавање компјутерских и мрежних безбедносних проблема за федералне институције.

[4] *Одбрана од претњи у сајбер простору*, др Дејан Вулетић, Београд, 2011, Институт за стратегијска истраживања, Београд.

[5] Idem, p. 169.

[6] Ibid.; *Cyber Security Strategy for Germany , German Federal Ministry of the Interior*, 2011, pp. 8–10.

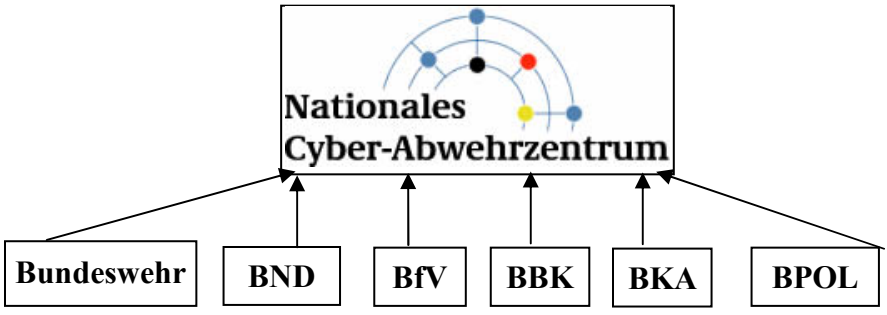
[7] Computer Emergency Response Team – CERT, је опште прихваћен назив за експертску групу која се бави компјутерским инцидентима.

Bundesamt
für Sicherheit in der
Informationstechnik

У оквиру BSI главну оперативну улогу у обезбеђивању сајбер безбедности има новоформирани Национални центар за одбрану сајбер простора,[9] који је добио задатак да у случају сајбер напада анализира ситуацију и препоручује решења.

Оснивање посебног центра образложено је чињеницама да „криминални, терористички и обавештајни актери користе сајбер простор за своје деловање, при чему иза напада на сајбер простор могу бити и војне операције". Немачки извори указују на то да је протеклих година порастао број шпијунских сајбер напада на компјутере немачке Владе, а тадашњи министар одбране Томас де Мезијер тада је изјавио да Немачкој треба национални сајбер одбрамбени центар који ће надгледати и осигуравати безбедност интернета.

У центру су, од средине 2011. године, деташирани и ангажовани припадници Савезне службе за заштиту устава (BfV), Савезног завода за заштиту народа и помоћ при катастрофама (BBK), Савезне криминалистичке службе, Савезне полиције, Савезне царине, Савезне обавештајне службе (BND) и оружаних снага Немачке (Бундесвера).[10]



[8] Види://www.bsi.bund.de/cln_183/ContentBSI/EN/TheBSI/Functions/Department1/department1.html

[9] http://www.rtv.rs/sr_lat/evropa/nemacka-osniva-centar-za-odbranu-sajber-prostora_240400.html

[10] http://www.24sata.rs/vesti/svet/vest/nemacka-dobila-centar-za-odbranu-od-sajber-napada/5025.phtml

Задатак Центра је „прикупљање“ или „фузија“ информација о претњама виртуалној безбедности које дају полиција и обавештајне службе на државној нивоу и нивоу савезних покрајина. Од тих информација Центар саставља генералне процене о виртуалној безбедности, укључујући препоруке полицији, обавештајним и осталим државним агенцијама за примену противмера. Национални центар за одбрану сајбер простора или, како га другачије зову „центар за интернетски криминал“ на неки је начин немачки интернетски обавештајни центар – иако сам по себи није обавештајна служба.

Иначе, када се говори о цивилним институцијама Немачке, одговорне за сајбер безбедност, поготово о обавештајном сектору,[11] важно је напоменути основне историјске податке о Федералној канцеларији за информациону безбедност (BSI). Као што је наведено, BSI је владина агенција одговорна за компјутерску и комуникациону безбедност за Немачке владине органе од 1991. године. Претходник BSI било је криптографско одељење немачке спољне обавештајне службе BND. Са порастом употребе интернета и са окончањем хладног рата нарасла је потреба за агенцијом која ће бити одговорна за нове техничке изазове. У оквиру Немачке спољне обавештајне службе BND, централна јединица одговорна за информациону безбедност формирана је још 1989. године под називом Zentralstelle ZSI, које је касније издвојена и прерасла у BSI 1991. године. Нови амандман закона који је донет 2009. године (BSI-Act BSIG von 2009) знатно је појачао централне надлежности BSI за информациону безбедност на државном нивоу, посебно у одељку пет (section 5) амандмана, где је добио надлежност и за комуникацију владиних органа.[12]

Важне надлежности и пројекти BSI су:[13]

• члан је Владине радне групе за критичну инфраструктуру (AK KRITIS);[14]

• обезбеђује комуникациону безбедност за органе Владе Немачке, обезбеђујући криптоване мобилне телефоне, одржава информациону мрежу Берлин–Бон (IVBB) и информациону мрежу за федералну администрацију (IVBV) коју BSI контролише, скенира и штити од вируса (malware) још од 2009. године;[15]

• обезбеђује документациону заштиту (document protection) у оквиру безбедносних процедура које се спроводе у владиним органима;

• штити комуникацију према НАТО (NATO communication) применом криптоване технологије, посебно Elcrodat 6.2;

• обезбеђује архитектуру Secure Inter-Network Architecture (SINA) која обезбеђује безбедну комуникацију преко „обичног“ интернета;

• ради на пројектима комуникационе безбедности (Comsec), као што су заштита зграда од зрачења компјутера (shielding of buildings);

---

[11] У оквиру обавештајног сектора Немачке, Федерална канцеларија за заштиту устава (Bundesamt für Verfassungsschutz – BfV), као и Landesämter fürVerfassungsschutz – LfV на федералном нивоу, унутрашња је обавештајна агенција, док је војна контраобавештајна агенција (Militärischer Abschirmdienst – MAD) одговорна за контраобавештајну заштиту ОС Немачке. Спољна обавештајна агенција Bundesnachrichtendienst BND одговорна је за све спољне обавештајне активности. У том смислу, BSI може да подржава у техничком смислу све обавештајне агенције под одређеним условима.

[12] Act to Strengthen the Security of Federal Information Technology dated 14 August 2009.

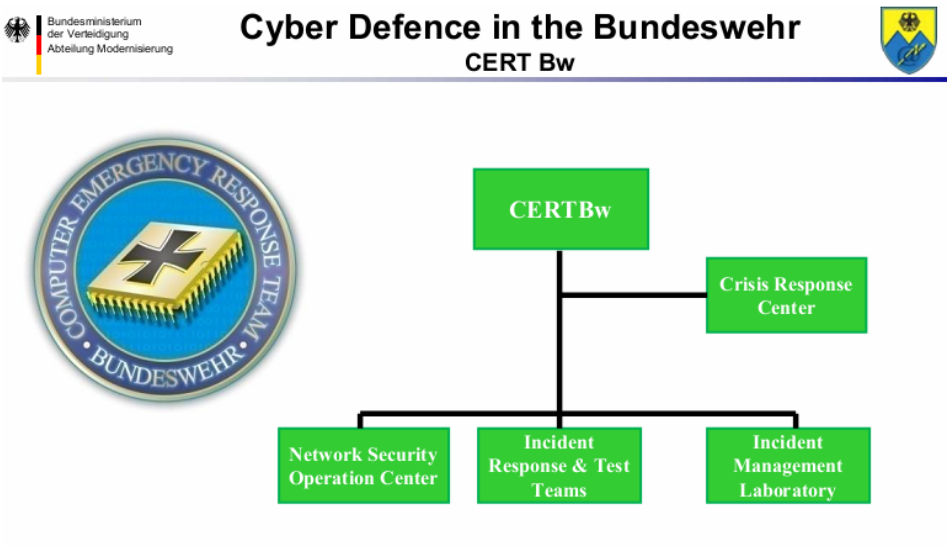
[13] Према Annual reports of the BSI 2005, 2006–2007 и 2008–2009.

[14] Као део Националног плана за заштиту информационе инфраструктуре (NPSI) BMI и BSI наложено им је 2005 да припреме имплементације плана за критичне инфраструктуре (German Umsetzungsplan KRITIS).

[15] Steinmann 2010, p.10.

Војне сајбер јединице Немачке

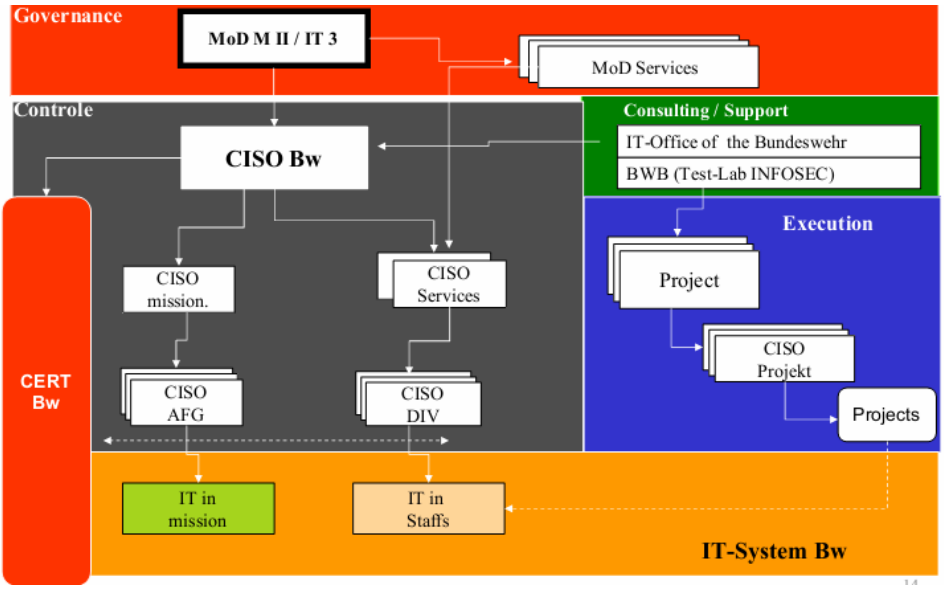
Одговорност ОС Немачке за сајбер безбедност лимитирано је на заштиту ИТ система који се налазе у употреби у Бундесверу. Према подацима, од 1992. године у Бундесверу су формиране организационе целине одговорне за безбедност ИТ система у ОС Немачке. Од 2002. године формиран је и функционише ЦЕРТ Бундесвера (CERTBw) који у свом саставу има Центар за кризни одговор, Оперативни центар за безбедност мрежних система, Тим за тестирање и одговоре за инциденте и Лабораторију за инциденте.



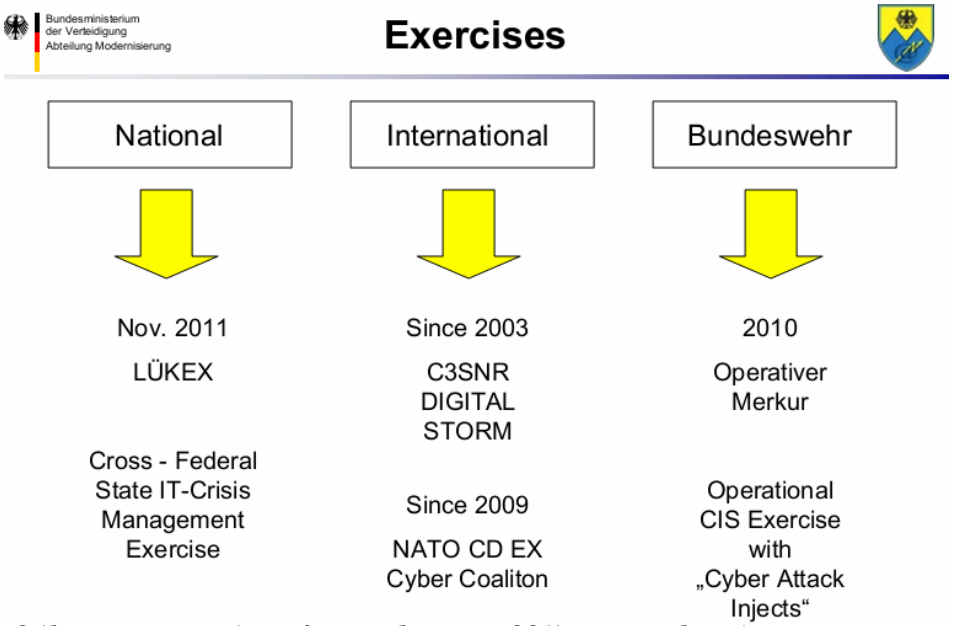
Структура ЦЕРТ Бундесвера (CERTBw)

Од 2003. године ОС Немачке изводе сајбер вежбе са одговарајућим саставима ОС САД, ОС Велике Британије, ОС Француске и ОС Италије, а од 2009. године учествују у НАТО сајбер вежбама.

У међувремену интензивирана је сарадња са војним и цивилним институцијама (универзитетима и научним установама) ради јачања сајбер капацитета Бундесвера. Од маја 2008. године Немачка спонзорише рад НАТО сајбер Центра у Талину у Естонији (Cooperative Cyber Defence Centre of Excellence in Tallinn).



Распоред подтимова ЦЕРТ Бундесвера (CERTBw) у ОС Немачке



Сајбер националне, међународне и вежбе у оквиру ОС Немачке; вежбе у којима су учествовали састави Бундесвера одговорни за сајбер безбедност

Улога обавештајних јединица Бундесвера у сајбер операцијама

У војном сектору Војнообавештајни центар Бундесвера (Zentrum für Nachrichtenw esen in der Bundeswehr – ZnBW) већ неколико година представљао је обавештајни центар ОС Немачке, али је касније подељен између спољне обавештајне службе BND и нове обавештајне службе ОС Немачке за спољно деловање, Стратегијске команде за извиђање (Kommando Strategische Aufklärung – KSA), која је основана 2002.[16] и која има главну улогу у војним обавештајним активностима од 2008. године.

Стратегијска команда за извиђање је интегрални део војнообавештајних органа ОС Немачке. Она има значајне обавештајно-извиђачке капацитете, који могу да буду глобално ангажовани, на великим удаљеностима, као и директно у областима ангажовања мировних контингената ОС Немачке. Због тога Стратегијска команда за извиђање (KSA) значајно учествује у процесу процењивања ситуације, као и процесу планирања, припреме и извођења операција јединица ОС Немачке у земљи и иностранству. Она својим информацијама подржава државно руководство Немачке у процесу доношења одлука за спровођење важних међународних акција Немачке. Стратегијска команда налази се под административном контролом Здружене команде за подршку, а под техничком контролом Федералног министарства одбране.

Симбол Стратегијске команде за извиђање

Стратегијска команда за извиђање спроводи специјалне задатке са своја четири специјализована одељења: Одељења за операције (Ops/G3), Одељења за концепцију и развој, Одељења за аналитику и подршку операцијама, Одељења за извиђање из свемира, као и елементима за криптоанализу и контролу система. Са сателитским радаром високе резолуције SAR Lupe (Synthetic Aperture Radar), Бундесвер од краја 2007. године, када је систем достигао пуне оперативне способности, по први пут поседује капацитете за спровођење сликовне обавештајно-извиђачке делатности (IMINT) на глобалном нивоу.

[16] Eberbach 2002.

Ради извршења наменских задатака, Стратегијска команда за извиђање има у свом саставу две SIGINT команде (SIGINT команда 92 је укинута). Свака SIGINT команда има у свом саставу, у начелу, један стационарни COMINT батаљон и један мобилни батаљон за (EW) електронско ратовање.

–  SIGINT Команда 91 (Фленсбург)

–  Комуникацијско- обавештајна секција (COMINT) 911 (Bramstedt)

–  Батаљон за електронско ратовање (EW) 912 (Nienburg/Weser)

–  SIGINT Команда 93 (Daun)

–  Батаљон за електронско ратовање (EW) *931 (ehem. FmAufklAbschn 931, davor FmAufklRgt 940)* (Daun)

–  Батаљон за електронско ратовање (EW) *922* (Donauwörth)

–  Батаљон за електронско ратовање (EW) *932* (Frankenberg/Eder)

–  Школа за стратешко извиђање (Flensburg-Mürwik)

–  Центар за техничку анализу сигнала (Hof)

Одељење за информације и мрежно-компјутерске операције

Стратегијска команда за извиђање има у свом саставу и Центар за SIGINT техничку анализу, као и Школу за стратегијско извиђање. Са таквом концентрацијом снага и средстава, ова команда је способна да припреми податке за доношење адекватних политичких и војних одлука, посебно за могуће ангажовање оружаних снага у кризним регионима. Такође, ова централизована структура обезбеђује блиско међусобно увезивање извиђачких компоненти у свемиру, стационарних и мобилних компоненти за сигнални обавештајни рад. Оно што посебно треба напоменути јесте да Стратегијска команда за извиђање од 2007. године поседује капацитете за извођење информационих (Info Ops), односно компјутерских мрежних операција (Computer Network Operations – CNO).

У 2010. години имала је око 6.300 војних лица и око 700 цивилних лица, из сва три вида оружаних снага,[17] и одговорна је за електронско ратовање (Elektronische

[17] Bischoff 2009.

Kampfführung EloKa). Такође, у њеној надлежности су и нови војни сателити Synthe tic Aperture Radar (SAR-Lupe)[18] и комуникациони сателити COMSATBW 1 and 2.

У ИТ сектору Бундесвер ради на изради модерне и безбедне ИТ (Herkules), коју заједно израђују Siemens и IBM под називом BWI IT. Нема података да је изградња Herkules платформе завршена.[19] Сматра се да је од 2008. године Команда преузела значајне обавезе Војнообавештајног центра Бундесвера и да представља централну целину у војнообавештајној организацији Бундесвера.

Од 2007. године KSA има јединицу за компјутерске мрежне операције (computer network operation – CNO)[20] која је, такође, одговорна за извођење сајбер операција.

Како се наводи, сајбер јединице формиране су у ОС Немачке због тога што су њене обавештајне службе 2007. године регистровале и пријавиле масовне сајбер нападе из Кине 2007. године. Тада су кинески хакери напали компјутерске системе неколико министарстава и Владе, покушавајући да открију поверљиве информације.

Први јавни подаци о припремама ОС Немачке за сајбер операције појавили су се 2009. Тада је обелодањено да је немачка војска у то време припремала око 76 својих припадника, који су рачунарима увежбавали методе инфилтрације, шпијунирања и манипулисања, као и разарања компјутерских мрежа.[21] Са друге стране, према подацима објављеним у немачкој штампи, током јуна 2012. године, формирање „хакерске јединице“ Бундесвера тече још од 2006. године.[22]

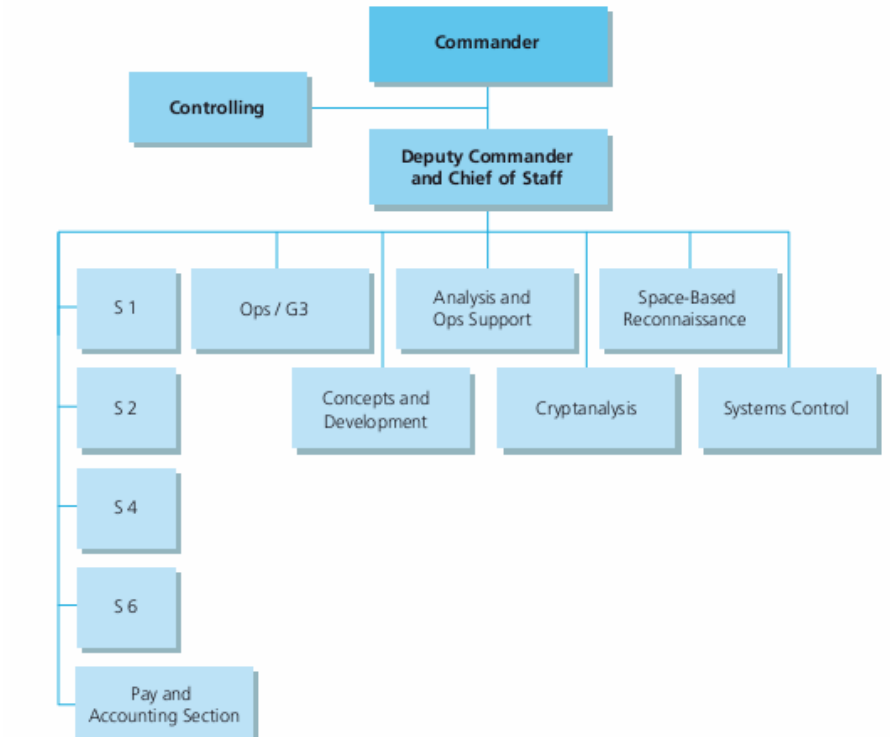
[18] Bischoff 2009. Acc. to Bischoff, SAR Lupe је такође део Немачко-Француске сарадње у домену сателитског извиђања. Заједно са француским сателитом Helios II он је основа European satellite reconnaissance cooperation ESGA..

[19] Scheidges 2010a, p. 2–3.

[20] Bischoff 2009.

[21] http://www.pressonline.rs/sr/vesti/globus/story/59380/NEMA%C4%8CKA SE+SPREMA+ZA+SAJBER+RAT.html.

[22] Bundesver se sprema za sajber-napade, Тањуг, 05. јун 2012, наводи из немачког дневника „Financial Times Deutsćland“.



Организацијско-формацијска структура Стратегијске команде за извиђање (KSA) из 2007. године

Припадници Бундесвера су се тада обучавали у касарнама Tomburg-a у месту Rheinbach, близу Бона. Ради се, у ствари, о Одељењу за информационе и компјутерско- мрежне операције (Abteilung Informations und Computernetzwerkoperationen) у саставу Команде Бундесвера за стратегијско извиђање (Kommando Strategische Aufklärung KSA) под командом бригадног генерала ваздухопловних снага генерала Фридриха Вилхелма Кризела. Према доступним подацима, ова јединица се већ тада припремала, како за дефанзивне, тако и за офанзивне задатке, где спада и сајбер шпијунирање.[23]

Командант, генерал Kriesel је почетком 2009. године изјавио да је његова јединица извела успешне компјутерске акције, као и операције електронског извиђања у Авганистану.[24] Нешто касније је обелоданио да ће његова сајбер јединица бити оперативно способна 2010. године, када ће од ње бити затражено да у пракси демонстрира своје оперативне способности кроз симулирани напад на стварну мету, што се назива пенетрациони тест.

[23] John Goetz, Marcel Rosenbach and Alexander Szandar, „National defense in cyberspace“, Der Spiegel, 11 February 2009.

[24] Исто.

Према немачким изворима[25] припадници јединице користе исте методе као и припадници криминалних група. Врши се тајно убацивање малициозних програма у компјутерске системе противника, преко e-mail порука, спољних медија као што су CD-ROM дискови или „привлачењем“ противника да приступи припремљеном интернет сајту. Инфицирани компјутер тада може да „даунлоудује“ додатне малициозне софтвере, као што је *letter recorder,* који чита сваку кључну команду (keystroke) на компјутеру, који може да сними сваку e-mail поруку, интернет адресу или пасворд. Тај програм тајно, без знања власника компјутера, шаље прикупљене податке другом компјутеру. Обука посебног дела јединице која је намењена за офанзивне задатке сложенија је и, углавном, обухвата две врсте напада –„denial of service“ или „botnet attacks“, заснованих на сценарију који су били примењени у Естонији и Грузији.

Закључак

Немачка припада земљама које су међу првима иницирале операцију сајбер шпијунаже још средином 1980. године. Пројекат сајбер шпијунаже тада је развила обавештајна служба БНД (Bundes Nacrichten Dienst – BND), као заједнички напор централе БНД и одељења за оперативни рад и сигнални обавештајни рад (human and signals intelligence). Овако формирана јединица успела је да оствари продор у компјутерске мреже међународне финансијске организације SWIFT (Society for Worldwide Interbank Financial Telecommunications), која је поседовала податке о већини интернационалних банкарских трансфера. Данашња глобална мрежна повезаност је много напреднија од глобалне мрежне безбедности, што хакери и обавештајне службе могу лако да искористе за обавештајну делатност у сајбер простору.

Актуелна Стратегија сајбер безбедности Немачке наводи да сајбер шпијунажа представља сајбер напад који је усмерен према тајности ИТ система, а који је извела страна обавештајна служба. Сајбер шпијунажа је управо врста сајбер напада који је, пре свега, усмерен на „тајност“ информација и података у противничкој мрежи. Савремена обавештајна делатност тежи да искористи све предности које пружа масовна употреба компјутерске технологије и интернета за обављање обавештајних активности. Сматра се да нема озбиљне обавештајне службе у свету која није заинтересована за овај начин сајбер обавештајног истраживања, поготово због економичности овакве активности у односу на друге начине прикупљања поверљивих података. У том смислу, мало се зна о унапређењу и софистикацији капацитета развијених држава за вођење сајбер шпијунаже, као што је Немачка, која може да се сматра за лидера у овој области, поред САД, Велике Британије и Израела. На основу ставова изнетих у Стратегији сајбер безбедности Немачке, као и капацитета цивилних и војних обавештајно-безбедносних служби, може се рећи да Немачка „иде крупним корацима“ ка даљем јачању својих јединица за извођење операција сајбер шпијунаже.

[25] Исто.

Литература

1. *Cyber Security Strategy for Germany*, German Federal Ministry of the Interior, 2011.

2. *National Strategy for Critical Infrastructure Protection* (CIP Strategy), Federal Ministry of Interior, Federal Republic of Germany, Berlin, 17th June, 2009.

3. Вулетић, Д.: *Одбрана од претњи у сајбер простору*, Институт за стратегијска истраживања Министарства одбране, Београд, 2011.

4. Goetz, J., Rosenbach, M. & Szandar, A.: „National defense in cyberspace“, *Der Spiegel*, 11 February 2009.

5. http.www.bsi.bund.de/cln_183/ContentBSI/EN/TheBSI/Functions/Department1/department1.html.

6. http:www.rtv.rs/sr_lat/evropa/nemacka-osniva-centar-za-odbranu-sajber-prostora_240400.html.

7. http://www.24sata.rs/vesti/svet/vest/nemacka-dobila-centar-za-odbranu-od-sajber-napada/5025.phtml.

8. *Act to Strengthen the Security of Federal Information Technology,* 14th August 2009.

9. Refer to Annual reports of the BSI 2005, 2006–2007 and 2008–2009.

10. „Бундесвер се спрема за сајбер-нападе“, Тањуг, 5. јун 2012., наводи из немачког дневника *Financial Times Deutsćland*.

11. http://www.pressonline.rs/sr/vesti/globus/story/59380/NEMA%C4%8CKASE+SPREMA+ZA+SAJBER+RAT.html.