UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Sovič

Nato in njegovi mehanizmi za ohranjanje informacijske varnosti

Diplomsko delo

Ljubljana, 2012

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Sovič

Mentor: doc. dr. Uroš Svete

Nato in njegovi mehanizmi za ohranjanje informacijske varnosti

Diplomsko delo

Ljubljana, 2012

S tem diplomskim delom bi se rad zahvalil vsem bližnjim, ki so mi omogočili študij Obramboslovja in me podpirali pri izobraževanju in življenju v Ljubljani.

Zahvaljujem se tudi doc. dr. Urošu Svetetu, ki mi je predstavil varnostni aspekt informacijske dobe in mi nato kot mentor pomagal ter me usmerjal pri pisanju diplomskega dela.

Nato in njegovi mehanizmi za ohranjanje informacijske varnosti

Informacijska doba je z odvisnostjo od informacijsko-komunikacijske tehnologije poleg vseh ugodnosti prinesla tudi grožnje, katere lahko človeštvu povzročijo nepredstavljivo škodo. Digitalizacija je povezala razne družbene podsisteme v multimedijsko celoto, ki je sedaj osnova ključne informacijske infrastrukture. Države ne morejo zagotavljati ustrezne informacijske varnosti samostojno; tako kompleksnim asimetričnim grožnjam lahko konkurira le močan akter, ki ima na voljo ogromno mehanizmov in sredstev.
Zveza Nato, ki je zadolžena za skrb za mednarodno varnost in mir, želi vzpostaviti red tudi na področju informacijske varnosti. Izkušnje, študije primerov in zavedanje posledic, ki jih lahko prinese učinkovito izpeljan kibernetski napad, so znotraj zavezništva povzročili oblikovanje kibernetske politike. V okviru le-te so začeli razvijati zmogljivosti za odzivanje na računalniške incidente, s tem pa nadgrajevati in ustanavljati nove strukture in mehanizme. Razvoj Natovih mehanizmov je skladen nenehnemu razvoju informacijskih groženj, cilj pa je v zagotovitvi kibernetske obrambe, ki jih bo zmožna učinkovito preventivno zaznati in preprečiti.
V diplomski nalogi se bom osredotočil na razvoj Natovih zmogljivosti za zagotavljanje informacijske varnosti, potrdil ažurnost njegovih mehanizmov in s tem vodilno vlogo Nata pri krepitvi mednarodne informacijske varnosti.

Ključne besede: Nato, informacijska varnost, informacijske grožnje, informacijsko-komunikacijska tehnologija, zmogljivosti za odzivanje na računalniške incidente.

NATO and its mechanisms for maintaining information security

The information age, with its dependence on information and communication technologies not only brought us benefits, but also threats, which can cause unimaginable damage to the humanity. Digitization has brought together various social subsystems into one multimedia environment, which is now the basis of the critical information infrastructure. The states cannot provide adequate information security on their own. Such complex asymmetric threats can be dealt with only by a strong agent that has a lot of mechanisms and resources available for use.
NATO, which is responsible for the care for international security, wants to restore order in the area of information security. Experiences, case studies and awareness about the consequences, which could be caused by efficiently carried out cyber attacks, have resulted in the creation of Alliance cyber policy. The latter started the development of computer incident response capabilities, and with that they began to upgrade and establish new structures and mechanisms. The development of NATO's mechanisms is consistent with the continuous development of information threats, and the main objective is to provide cyber defense, which will be capable of effective preventive detection and prevention of designated threats.
In this thesis, I will focus on the development of NATO's capability to ensure information security, confirm the timeliness of its mechanisms and with it the leading role of NATO in strengthening international information security.

Keywords: NATO, information security, information threats, information and communication technology, computer incident response capability.

KAZALO

SEZNAM POGOSTEJE UPORABLJENIH KRATIC IN OKRAJŠAV

ang.	angleško
C4ISR	ang. Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (poveljevanje, nadzor, komunikacije, računalniki, obveščevalna dejavnost, nadzor in izvidništvo)
CCD CoE	ang. Cooperative Cyber Defence Centre of Excellence (Center odličnosti za sodelovanje pri kibernetski obrambi)
CDMA	Cyber Defence Management Authority (Urad za upravljanje kibernetske obrambe)
CERT	ang. Computer Emergency Response Teams (Odzivne skupine za računalniške nevarnosti)
CIAP	ang. Consolidated Information Assurance Picture (celovita slika informacijske zagotovitve)
CIS	ang. Computer information Systems (komunikacijski in informacijski sistemi)
DDoS	ang. Distributed Denial of Service (napad s porazdeljeno ohromitvijo storitve)
DoS	ang. Denial of Service (napad z ohromitvijo storitve)
DRA	ang. Dynamic Risk Assessment (dinamično zaznavanje tveganja)
ENISA	ang. European Network and Information Security Agency (Evropska agencija za varnost omrežij in informacij)
EU	Evropska unija
IDS	ang. Intrusion Detection Systems (sistemi za zaznavanje vdorov)
IKT	informacijsko-komunikacijska tehnologija
ipd.	in podobno
itd.	in tako dalje
NC3A	ang. NATO Consultation, Command and Control Agency (Agencija zveze Nato za posvetovanje, poveljevanje in nadzor)
NCIRC	ang. NATO Computer Incident Response Capability (Natove zmogljivosti za odzivanje na računalniške incidente)
NCIRC-FOC	ang. NATO Computer Incident Response Capability-Full Operational Capability (polna operativna sposobnost Natovih zmogljivosti za odzivanje na računalniške incidente)

NCIRC-IOC	ang. NATO Computer Incident Response Capability-Initial Operational Capability (začetna operativna sposobnost Natovih zmogljivosti za odzivanje na računalniške incidente)
NCSA	ang. NATO Communications and Information Agency (Natova agencija za komunikacijske in informacijske sisteme)
NEC	ang. Network Enabled Capability (zmogljivosti omrežnega delovanja)
npr.	na primer
RTO	ang. Research and Technology Organization (Organizacija za raziskave in tehnologijo)
t. i.	tako imenovani
tj.	to je
VA	ang. Vulnerability Assessment (ocena ranljivosti)
ZDA	Združene države Amerike

1 UVOD

Obstoj človeštva je v prvi meri odvisen od zagotovitve ustrezne varnosti, ta pa se že od nekdaj prepleta z razvojem družbe. Prehod iz industrijske dobe v informacijsko je naznanil dobo tehnologije in informacij. Le-ti sta olajšali opravljanje vsakodnevnih dejavnosti, pripomogli k hitrejšemu in lagodnejšemu načinu življenja, s sabo pa sta prinesli tudi negativne plati. Ljudje smo dandanes že skoraj popolnoma odvisni od tehnoloških produktov in storitev, poleg tega pa ima informacijsko-komunikacijska tehnologija marsikje dostop do osebnih podatkov posameznikov, pa tudi podatkov in informacij, ki so ključnega pomena za delovanje raznih organizacij in ne nazadnje tudi držav.

Pred informacijsko revolucijo smo poznali le tri dimenzije okolja, in sicer kopno, vodo ter zrak (kamor lahko štejemo tudi vesolje), nato pa je človek ustvaril še četrto, tj. virtualni oziroma kibernetski prostor. V njem ne šteje fizična premoč, temveč je poglavitnega pomena znanje, pomaga pa tudi napredna IKT. Z digitalizacijo podatkov in informacij se je zgodila še ena pomembna novost, in sicer združitev nekoč nepovezanih družbenih sistemov v eno entiteto, kar pomeni, da so se v enotnem multimedijskem okolju naenkrat znašli sektorji, ki skupaj tvorijo ključno infrastrukturo držav in organizacij. S tem se je pojavilo vprašanje, kako sploh lahko država, ki je po prepričanju realistične teorije glavni akter in zaščitnik, zagotovi varnost svojih državljanov. Jasno je, da tako kompleksnega prostora ne more popolnoma nadzorovati nihče. Obstaja pa možnost zagotavljanja določene stopnje informacijske varnosti in s tem tudi človekove varnosti, to pa lahko zagotovi le sodelovanje med močnimi akterji, ki so opremljeni z napredno IKT in sredstvi.

Zveza Nato ima kot najmočnejša mednarodna civilno-vojaška organizacija nalogo zagotavljanja mednarodnega miru in varnosti, z nastankom groženj ključni informacijski infrastrukturi zveze in posameznih članic, pa so svoje poslanstvo začeli opravljati tudi v kibernetskem prostoru. Nato se ne osredotoča le na vojaški aspekt; zaposleni se namreč zavedajo, da brez civilnih institucij vojaška sfera ne more delovati. Razvoj zmogljivosti za zagotavljanje primerne obrambe so v prvi vrsti usmerili k odpravi ranljivosti komunikacijskih in informacijskih sistemov, veliko truda pa vlagajo v izrazitejšo sodelovanje držav članic in ostalih partnerjev. Kot kaže, bodo morali akterji, ki so povezani z varovanjem ključne informacijske infrastrukture, sprejeti ponudbo k sodelovanju, ali pa se sami soočiti z novimi asimetričnimi grožnjami v kompleksnem okolju, kjer ni jasno določenih pravil, še manj pa struktur, ki bi lahko s kakršnimikoli sredstvi zagotavljale absolutno varnost.

Razvoj Natovih zmogljivosti za zagotavljanje kibernetske obrambe je vsota že znanih, preizkušenih in učinkovitih sredstev, mehanizmov, orodij in tehnik, nadgradnja le-teh in razvijanje novih. Širitev omenjenih zmogljivosti s pomočjo sodelovanja v druge obstoječe strukture bi lahko pripeljala do nekih univerzalnih standardov zagotavljanja informacijske varnosti, Nato pa še posebej poudarja potrebo po centralizaciji kibernetske obrambe, ki se bo izvedla znotraj Natove informacijske infrastrukture. S centralizacijo kasneje ciljajo tudi na države članice, ki so trenutno bolj ali manj prepuščene ravnanju v skladu z lastnimi interesi. Kako se bodo države znašle v obdobju, ko število informacijskih groženj narašča iz dneva v dan, je stvar njihove odločitve, Nato pa vsekakor ponuja trenutno najboljšo alternativo v okviru razvoja skupnih zmogljivosti.

2 METODOLOŠKI OKVIR

2.1 Opredelitev predmeta in cilja preučevanja

V diplomskem delu bom opredelil Natov pogled na informacijske grožnje in varnost, posvetil pa se bom tudi temeljnim mehanizmom in strukturam, ki skrbijo za ohranjanje le-te na ravni zavezništva, kot tudi med posameznimi članicami, kar posredno krepi informacijsko varnost celotne mednarodne skupnosti. Poleg naštetega bom zapisal tudi smernice razvoja na omenjenem področju, za lažjo predstavo pa dodal tudi nekaj primerov groženj zvezi Nato s področja informacijsko-komunikacijske tehnologije.

2.2 Hipotezi

Hipoteza 1: Natovi koncepti in mehanizmi informacijske varnosti so prilagojeni grožnjam, prav tako pa so primerno formalizirani znotraj Natove strukture.

Hipoteza 2: Nato je zaradi razvoja informacijsko-komunikacijske tehnologije razvil visoko funkcionalno kibernetsko obrambo, ki je kos grožnjam s področja informacijsko-komunikacijske tehnologije.

2.3 Metode

Pri pisanju diplomskega dela bom uporabil metodo zbiranja virov, analizo primarnih in sekundarnih virov, kjer se bom zaradi abstraktnosti teme posluževal predvsem internetnih virov. Prav tako bom uporablil deskriptivno in sintetično analitično metodo.

2.4 Definicije in temeljni pojmi

"**Informacijsko-komunikacijska tehnologija (IKT)** je sposobnost, znanje, spretnost oziroma tehnika, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti (zbiranje, obdelava, prikaz in prenos podatkov), dosežemo želene učinke" (Svete 2005, 16).

Informacijska infrastruktura je skupek komponent, ki so del IKT. To so računalniki, programska oprema, komponente, ki so namenjene telekomunikacijam, internet, sateliti itd. Lahko bi rekli, da gre za sistem povezanih računalnikov in omrežij, pa tudi informacijskih tokov, ki delujejo med napravami in/ali mrežami, izraz pa lahko uporabimo tudi za tisti del nacionalne ali globalne informacijske infrastrukture, ki je ključna za neprekinjeno delovanje ključnih informacijskih služb (Dunn in Wigert 2004, 363).

Informacijska varnost pomeni zaščito informacijskih sistemov pred nepooblaščenim dostopom do informacij ali pred nepooblaščeno modifikacijo le-teh ne glede na to ali so shranjene, v obdelavi ali v pošiljanju. Prav tako pomeni zaščito pooblaščenih uporabnikov pred napadi za ohromitev storitev (DoS) in pred oskrbo z informacijami za nepooblaščene uporabnike. Za dosego varnosti se koristijo ukrepi za zaznavo, dokumentacijo in odvrnitvijo omenjenih groženj (UNLV Office of Information Technology 2012).

"**Informacijsko bojevanje** pomeni zaščito, zlorabo, okvaro, uničenje ali onemogočanje informacij ali njihovih virov z namenom doseči prednost ali zmago nad nasprotnikom. Izraz se nanaša tudi na koordiniran, digitalen napad na vlado s strani druge vlade ali s strani velikih skupin civilistov" (Bernik in Prislan 2011, 264).

Kibernetska obramba je aplikacija varnostnih enot, ki so namenjene varovanju in reakciji na kibernetske napade, usmerjene proti informacijski infrastrukturi. Zahteva zmogljivosti za pripravo, preprečitev, zaznavo, odgovor, obnovo in pridobivanje izkušenj iz napadov, ki lahko prizadenejo zaupnost, integriteto in dostopnost informacijskih ter podpornih servisov in sredstev (NATO C3 Agency 2011b).

3 INFORMACIJSKA VARNOST

3.1 Ključna informacijska infrastruktura

IKT je pomembna za razvoj obče razvojne strategije informacijsko razvitih držav, le-ta pa zajema vsa področja družbenega življenja, ključna za obstoj modernih držav. Pojavila se je nova oblika moči, ki jo imenujemo informacijska moč. Zaradi kompleksnosti in neomejenosti prostora presega omejitve in sredstva klasičnih oblik moči (npr. vojaških, političnih itd.), tako velikokrat ni več dovolj le grožnja s surovo, fizično silo, temveč se interesi uveljavljajo v kibernetskem prostoru, kjer fizični obstoj sredstev (npr. orožja), geografski prostor in čas nimajo pomena. Omenjeni dejavniki so pomembni le za sam dostop do omenjene virtualne dimenzije. Za zagotavljanje informacijske moči pa je potrebna informacijsko-komunikacijska tehnologija (IKT), ki s svojimi komponentami (računalniki, omrežja, telekomunikacije, programska oprema, internet, sateliti itd.) tvori t. i. informacijsko infrastrukturo. Le-ta predstavlja vejo ključne infrastrukture, ki vključuje vse sisteme in imetje, ki je ključno za državno varnost in ekonomsko ter socialno blaginjo. Informacijska infrastruktura se je močno razširila pod vplivom digitalizacije in s tem povezano širitvijo IKT v sodobnem okolju. Sam narastek uporabe IKT je viden povsod okoli nas – predstavlja namreč gonilno silo delovanja in razvoja, kar lahko vidimo pri uporabi v industriji, raznih institucijah in nasploh v večini struktur, ki služijo tako zasebnemu kot tudi javnemu sektorju držav. Brez IKT organizacije ne morejo biti konkurenčne drugim, saj je informatizacija olajšala vsakdanje opravke, predvsem pa skrajšala potreben čas za določena dela. Z uporabo IKT se je povečala tudi učinkovitost mehanizmov za zagotavljanje varnosti, po drugi strani pa je družba postala tudi ranljiva, saj je možno z raznimi metodami, tehnikami izkoristiti zanašanje ljudi na uporabo IKT (Abele-Wigert 2006, 55; Bernik in Prislan 2011; Dunn in Wigert 2004, 19–26; Svete 2007, 159–162).

3.2 Varnostne implikacije IKT in vloga držav

Teoretično gledano ima IKT posredne in neposredne varnostne implikacije.

- *Neposredne implikacije* se kažejo prek vplivanja na družbene konstrukte in oblikovanje dojemanja stvarnosti (gre za nekakšno manipulacijo) s pomočjo raznih telekomunikacijskih tehnik (elektronska pošta, spletni dnevniki, socialna omrežja, forumi, digitalizacija medijev itd.), pa tudi prek zlorab (uporaba raznih škodljivih tehnik), ki omogočajo posamezniku ali skupini ljudi, ki imajo potrebno znanje in namero, škodovati interesom posameznikov, skupin, držav ali drugih referenčnih

struktur varnosti. Prek raznih proizvodov in storitev namreč razkrivamo osebne podatke, saj zaupamo varnosti IKT, vendar ta lahko zataji (okvare, odpovedi, napake opreme) ali popusti pod tehnikami škodovanja (za namene računalniškega kriminala, kibernetskega terorizma ali informacijskega bojevanja), že najmanjša anomalija v informacijski infrastrukturi pa lahko kmalu preide na nivo državne ali celo mednarodne skupnosti.

- *Posredne implikacije* IKT pa predstavlja vpliv omenjene tehnologije na zbiranje, obdelavo in posredovanje podatkov, ki se kaže kot pozitivna nadgradnja in pomemben del družbene moči sodobne družbe (Svete 2007, 160).

Zaradi preteklih slabih izkušenj in želje po varni družbi, pa tudi zaščiti povezovalne vloge med različnimi sektorji in naraščajočega elektronskega gospodarstva, je trend zlasti med informacijsko razvitimi državami, da se poveča informacijska varnost, katere temelje predstavlja ključna informacijska infrastruktura. Države se varovanja lotevajo povsem različno, nekatere prepustijo delo zasebni sferi, nekatere uvajajo cenzuro, spet druge prepustijo delo samim zakonitostim trga. Svete deli pristop držav do zaščite ključne infrastrukture na 3 skupine, in sicer na:

- zaščito ključne infrastrukture (ZDA in Nemčija);
- vseobsežno zaščito infrastrukture v okviru totalne obrambe (Švica) in
- avtoritarno-centralistični pristop (Kitajska) (Svete 2007, 174).

Z večanjem števila uporabnikov in ponujenih storitev – pravzaprav gre za nenadzorovano širjenje – pa se veča tudi ranljivost. Težava je v tem, da se največ sredstev in časa posveča razvoju informacijskih sredstev in storitev, saj to prinaša denar, pozablja pa se na ustrezno zagotavljanje varnosti. Samo uvajanje novih ključnih delov infrastruktur ponavadi ni deležno potrebnih testov, saj proizvajalci in posredniki želijo prehiteti konkurenco na trgu. Produkti in storitve se nahajajo v zasebni in javni sferi, ki imata prepleteno informacijsko infrastrukturo, s tem pa je akterjem, ki se želijo okoristiti, vstop v njo veliko lažji kot bi bil v primeru bolj varovane in ločene opreme. Krivda leži tudi na strani države kot primarnega zaščitnika državljanov. Marsikje vodilni ne vlagajo v razvoj potrebnih struktur, kar je lahko posledica nerazumevanja IKT, ravnodušja, pomanjkanja politične volje itd., potrebno pa je poudariti, da se stvari obračajo na bolje, saj mednarodne organizacije težijo k določenim minimalnim standardom na področju informacijske varnosti in med temi organizacijami ima vodilno vlogo NATO (Abele-Wigert 2006, 56–60; Dunn in Wigert 2004; Svete 2007, 160–162, 174).

4 RAZVOJ NATOVIH MEHANIZMOV ZA ZAGOTAVLJANJE INFORMACIJSKE VARNOSTI

4.1 Razvoj Natovih zmogljivosti kot odgovor na grožnje

Uporaba informacijsko-komunikacijske tehnologije med splošno populacijo se je pojavila relativno pozno, le nekaj desetletij nazaj. S tem, ko je postala omenjena tehnologija dostopna vsem, se je povečala tudi nevarnost izkoriščanja le-te v namene škodovanja in zlorabe. Zveza Nato je po hladni vojni skladno s trendi razširila spekter svojega delovanja, torej zagotavljanja varnosti na več področij, med katerimi pa so od poznih devetdesetih let 20. stoletja med vodilnimi tudi grožnje s strani IKT tehnologije. Pred letom 1999 ni bilo potrebe po vlaganju v sredstva informacijskega bojevanja, saj sta bili informacijska varnost in kibernetska obramba le tema razprav nekaterih Natovih strokovnjakov, ki so videli potencial, ki ga tehnologija prihodnosti premore.

Prva resna grožnja se je pojavila leta 1999, in sicer v času kosovske krize, ko je bila Natova spletna stran neprestano tarča vdorov, prav tako pa so hekerji preprečili dostop do elektronske pošte za zunanje obiskovalce. Naslednji korak k razvoju mehanizmov, ki bi naj skrbeli za informacijsko varnost, pa je posledica terorističnega napada na World Trade Center 11. 9. 2001, saj je pokazal neločljivo odvisnost družbe od tehnologije, ki predstavlja ne le koristi, temveč tudi ranljivost (Thelier 2011).

Prelomna točka je bil napad na Estonijo leta 2007, ko so hekerji z napadi na uradne strani politikov, bank in informacijsko infrastrukturo popolnoma ohromili dejavnosti državljanov, ki so zahtevale uporabo IKT tehnologije. Sledile so ostre obsodbe estonske vlade, ki so zahtevale pomoč Nata pri identifikaciji krivca in povračilne ukrepe v okviru kolektivne obrambe (Thelier 2011).

V Natu so se najprej odločili za razvoj obrambnih mehanizmov za Natove CIS, kmalu pa so ugotovili, da varovanje le-teh ni dovolj, saj bi uspešen napad na države članice lahko kmalu prešel tudi na raven zavezništva. Zaradi hipoteze, da je neučinkovita in pomanjkljiva kibernetska obramba neke specifične države članice šibka točka varovanja ključne informacijske infrastrukture celotne zveze, so razvoj omenjenih zmogljivosti razširili tudi na omrežja držav članic. Težava je v nacionalnih interesih držav in zakonodajah, da bi pa varovanje ključne informacijske infrastrukture lahko doseglo vrh, je potrebno še naprej delati v smeri centralizacije kibernetske obrambe. Za uspeh sta nujna interes in sodelovanje držav članic.

Novi mehanizmi za zagotavljanje informacijske varnosti so se torej razvijali v skladu z grožnjami; formalno so jih z novimi politikami in strategijami oblikovali ter sprejemali na srečanjih Severnoatlantskega sveta, pa tudi raznih drugih srečanjih.

4.2 Srečanje Severnoatlantskega sveta v Pragi in Rigi

Nato je zaradi prej omenjenih groženj pomen novih t. i. asimetričnih groženj prvič obravnaval leta 2002 na srečanju v Pragi. Odziv na grožnje se je pokazal v pasivnih zaščitnih ukrepih, ki so bili namenjeni le reševanju obstoječih problemov in zahtevani s strani vojaškega dela organizacije. Na tem srečanju so z razvojem projekta imenovanega Natove zmogljivosti za odzivanje na računalniške incidente položili temelje za "Cyber Defence 1.0", ki se nekaj let kasneje uveljavi kot sistem kibernetske obrambe. Načrt, ki so ga sprejeli v Pragi, obsega 3 dele, in sicer:

1. ustanovitev NCIRC in vzpostavitev njegovega delovanja;
2. vizija nadgradnje NCIRC-IOC na NCIRC-FOC do konca leta 2012;
3. identifikacija potreb in sredstev, ki bodo odpravila ranljivosti sistema kibernetske obrambe, poleg naštetega pa so želeli identificirati reševanje problemov na ravni celotne zveze NATO, kamor spada tudi nova tehnologija, ki zagotavlja zmanjšanje tveganja na področju informacijske varnosti (Severnoatlantski svet 2002; Theiler 2011).

Štiri leta kasneje je potekalo srečanje Severnoatlantskega sveta v Rigi, kjer so informacijskemu bojevanju dali večjo vlogo. V zaključni deklaraciji so poudarili nujno potrebo po razvoju Natovih zmogljivosti omrežnega delovanja, ki bi zvišal nivo varnosti informacijskih sistemov, poleg tega pa bi zagotavljal zanesljiv, varen in ažuren pretok podatkov, informacij ter obveščevalnih podatkov. Ta nov koncept je v skladu z aktualnim razmišljanjem o zmanjševanju oboroženih sil (t. i. pametna obramba), saj bi omogočal Natu opravljanje večjega števila zahtevnejših nalog in misij z manjšimi enotami, vendar bi za učinkovitost morali povečati samo koherentnost akterjev (Kaiser 2008; Severnoatlantski svet 2006; Svete in Jankovič 2009, 141–144; Theiler 2011).

4.3 Srečanje Severnoatlantskega sveta v Bukarešti

Gre za prvo srečanje, ki je postavilo pomen informacijsko-komunikacijske tehnologije in s tem povezane informacijske varnosti na prvo mesto. Napad na estonsko informacijsko infrastrukturo leta 2007 in ostra reakcija estonske vlade, ki je zahtevala obravnavanje napada

po petem členu Severnoatlantske pogodbe, torej povračilo z uporabo sile ali drugih ukrepov v okviru kolektivne obrambe, je dala vodilnim v Natu vedeti, da je potrebno informacijske grožnje ustrezno formulirati. Do srečanja je za grožnje in napade na področje informacijske varnosti zadostoval četrti člen Severnoatlantske listine, ki je problem obravnaval kot predmet posvetovanja držav članic zveze Nato (Kaiser 2008; Laasme 2011; Severnoatlantska pogodba 1949).

Udeležencem na konferenci je bilo jasno, da je potreben nov koncept informacijske varnosti, ki ne bo zagotavljal le pasivne zaščite, temveč bo zmožen tudi preventivnega preprečevanja groženj in koncentriranega odgovora na le-te. S poudarkom na izkušnjah iz kibernetskega napada na Estonijo so se lotili oblikovanja novih smernic. V deklaraciji, ki so jo izdali po končani konferenci, so zapisali, da Nato vztraja pri krepitvi informacijskih sistemov, ki zagotavljajo kibernetsko varnost (Severnoatlantski svet 2008).

Od prve konference (Praga 2002), ki je obravnavala informacijske grožnje, so tam začet projekt NCIRC želeli pripeljati do polne operativnosti, omenjen mehanizem pa je tudi izpolnil pričakovanja in postal osnova za novo politiko kibernetske obrambe ("Politika Nata za kibernetsko obrambo"). Omenjena politika teži k zaščiti ključnih informacijskih sistemov zveze Nato in njenih posameznih članic, poudarja pa tudi potrebo po interakciji na področju IKT. Politika posebej intenzivno poudarja spoštovanje obveznosti, kot so na primer razvijanje lastnih zmogljivosti in delitev izkušenj, ki bi omogočale vzpostavitev celovite kibernetske obrambe in izvajanje protiukrepov v obliki odgovora na prošnje ogroženih držav članic (Hughes 2009; Theiler 2011).

Politika je sestavljena iz treh stebrov, to so:

- subsidiarnost (pomoč Nata je mogoča le kot odgovor na izrecno prošnjo ogrožene države članice);
- nepodvajanje (Nato in države članice se morajo izogibati nepotrebnemu podvajanju zmogljivosti ali struktur na ravni zveze ali posameznih držav);
- varnost (za sodelovanje je potrebno zaupanje in upoštevanje občutljivosti nujnih informacij) (Theiler 2011).

Na srečanju so uvedli tudi dva nova pomembne mehanizma, ki skrbita za ohranjanje informacijske varnosti, to sta Urad za upravljanje kibernetske obrambe in Center odličnosti za sodelovanje pri kibernetski obrambi.

4.4 Srečanje Severnoatlantskega sveta v Lizboni

Srečanje je potekalo novembra 2010, kjer so se udeleženci posvetili razvoju obstoječih in potencialnih groženj, med katerimi po stopnji nevarnosti najbolj izstopajo grožnje s področja informacijske tehnologije – natančneje možnost kibernetskih napadov, ki so zaradi olajšane uporabe in naprednejšega poznavanja IKT vse lažje izvedljivi. Odločili so se, da dotedanja politika kibernetske obrambe ni zadostna in potrebuje prenovo, v okviru katere so se lotili posodobitve obstoječih struktur (izpostaviti velja vlogo Natovih zmogljivosti za odzivanje na računalniške incidente), napredek pa so naredili tudi v samem pojmovanju informacijske varnosti, saj so grožnje na omenjenem področju opredelili kot možne aktivatorje za uporabo petega člena Severnoatlantske listine. Nov strateški koncept, sama nadgradnja kibernetske politike in akcijski načrt za njeno uresničevanje pa so definirali potrebne jasne smernice, kako naj se obstoječe strukture in mehanizmi razvijajo v prihodnje. Zelo pomembna je bila tudi odločitev, da se od takrat dalje kibernetska obramba vedno izvaja kot samostojna točka Natovega delovnega načrta, kar je pripomoglo k večji učinkovitosti samega razvoja zagotavljanja informacijske varnosti (Abrial 2011; Nato C3 Agency 2011b; Noshiravani 2011, 2–6; Severnoatlantski svet 2010; Theiler 2011).

Načrti za prihodnost so bili torej v nadgradnji politike kibernetske obrambe, ki je delovala v smeri zagotavljanja polne operativne zmogljivosti delovanja NCIRC, ki so zmožne odvrniti grožnje in braniti informacijsko infrastrukturo Nata oziroma natančneje zaznati, preprečiti, se braniti in obnoviti pred kibernetskimi napadi. Nova politika je tudi predvidevala združitev Natovih struktur pod centralizirano kibernetsko obrambo in ozaveščanje držav članic o samih grožnjah informacijski infrastrukturi kot tudi pripravljenosti na izvajanje protiukrepov. Pohvale je bila deležna odločitev s konference iz Rige, in sicer razvoj NEC, ki so v preteklih šestih letih že prinesle napredek in želene rezultate, same na omrežju temelječe operacije pa so v veliki meri nadomestile klasične vojaške in nevojaške operacije (Abrial 2011; NATO C3 Agency 2011b; Severnoatlantski svet 2010; Theiler 2011).

Niso pa govorili le o posodobitvah, temveč so se lotili tudi pristopov, s katerimi se informacijska obramba zagotavlja. Ker gre za zelo širok spekter dejavnosti, ki zahteva delovanje mnogih mehanizmov, struktur in ostalih akterjev, informacijska obramba ne bi smela biti odvisna le od nekaterih posameznih držav, ki so pripravljene namenjati sredstva (predvsem ZDA). Za učinkovito informacijsko varnost bi morale skrbeti vse države članice, ki bi naj poskrbele vsaj za primerno zaščito svojih sistemov IKT, saj bi vdor v enega izmed njih lahko posledično pomenil grožnjo celotni zvezi Nato. Sodelovanje ni potrebno samo

znotraj zveze, temveč tudi z drugimi akterji, kot so na primer Evropska unija, mednarodne nevladne organizacije ipd. Subjekti, ki so zmožni in pripravljeni zagotavljati informacijsko varnost, bi se morali povezati in delovanje razširiti prek mednarodne skupnosti, s čimer bi se povečala enotnost ukrepanja in zmanjšala ogroženost. Jasno je bilo, da je potrebno delati v smeri interakcije znotraj in zunaj zveze.

Poleg sodelovanja je pomembna tudi legitimnost sredstev za zagotavljanje informacijske varnosti, ki bi jo naj dosegli s civilnim vodstvom znotraj raznih struktur in agencij v državah članicah. Pomembno je, da ljudje vidijo, da se IKT ne uporablja zgolj v vojaške namene. Še ena zelo pomembna točka je postopno uvajanje legalne podlage za izvajanje kibernetske obrambe, le-ta pa bi lahko povzročala veliko preglavic (Abrial 2011; Noshiravani 2011, 6–8; Theiler 2011).

5 OBSTOJEČE NATOVE STRUKTURE IN MEHANIZMI NA PODROČJU ZAGOTAVLJANJA KIBERNETSKE OBRAMBE

5.1 Natove zmogljivosti za odzivanje na računalniške incidente

Projekt z imenom Natove zmogljivosti za odzivanje na računalniške incidente so torej ustanovili na prvem srečanju Severnoatlantskega sveta v Pragi in obsega vse dejavnosti ter ukrepe, ki izvajajo kibernetsko obrambo in višajo nivo varnosti Natove ključne informacijske infrastrukture. V skladu z načrti bi moral projekt to leto (2012) doseči predvideno stopnjo polne operativne sposobnosti, vendar trenutno še deluje na stopnji začetne operativne sposobnosti delovanja. Vodilni poudarjajo, da je težko definirati, kdaj bo cilj dosežen, če sploh, saj se grožnje informacijski varnosti ves čas razvijajo, dopolnjujejo in kontinuirano naraščajo, temu tempu pa morata slediti tudi tehnologija in znanje zaposlenih v Natu, ki so zadolženi za varovanje informacijske infrastrukture. Na srečanju Severnoatlantskega sveta v Lizboni leta 2010 so v skladu z novim strateškim konceptom sicer napovedali in formalizirali nadgradnjo iz NCIRC-IOC v NCIRC-FOC do konca leta 2012, vendar se bo projekt glede na zadnja poročila Natovih poveljujočih zavlekel v začetek leta 2013. Junija 2011 so obrambni ministri znotraj Nata v skladu z novim strateškim konceptom uradno sprejeli novo politiko na področju kibernetske obrambe, ki je bila že predstavljena na srečanju v Lizboni. S tem so naredili odločilni korak do polne operativne sposobnosti NCIRC, pa tudi dokončne uveljavitve politike na področju informacijske varnosti z vsemi predvidenimi novostmi in usmeritvami. Tako so končno realizirali vsa predhodna dogovarjanja (NATO C3 Agency 2011b; Seffers 2011a).

Agencija zveze Nato za posvetovanje, poveljevanje in nadzor je s tem dobila zeleno luč in razpisala ponudbo za podjetja, ki želijo sodelovati pri nadgradnji Natove informacijske infrastrukture. Med prijavljenimi podjetji so se odločali na podlagi naslednjih kriterijev: tehnična ponudba (60 %) in cena (40 %), pri čemer so tehnični del še dodatno razčlenili (NATO C3 Agency 2011c). Zmagalo je zasebno podjetje Finmeccanica prek hčerinskih podjetij SELEX Elsag in VEGA skupaj s partnerjem Northrup Grumman, ki je aktiven pri raznih drugih projektih, pomembnih za zagotavljanje informacijske varnosti (npr. sodelovanje z ameriškimi univerzami, projekt globalna informacijska mreža itd.). Marca 2012 so podpisali pogodbo in se s tem zavezali, da bodo razvili, testirali in namestili nove zmogljivosti kibernetske obrambe, prav tako pa nudili vzdrževanje in podporo za obdobje petih let. Sam projekt je vreden okoli 58 milijonov evrov in predstavlja rezultat pripadnosti držav članic Nata skupnemu cilju, ki se kaže v razvoju učinkovitih zmogljivosti za zaznavo, preprečitev, obrambo in obnovo v primeru kibernetskega napada na ključno informacijsko infrastrukturo zveze. (CircleID 2012; Defence Professionals 2012; Northrop Grumman Company; Seffers 2011a).

Testna oprema je letos že dala želene rezultate in s tem optimistične napovedi za nadaljnji razvoj (GlobeNewswire 2012).

5.2 Novosti v okviru nadgradnje v NCIRC-FOC

Polna operativna sposobnost zajema mnoge nove pristope, tehnike in orodja. Že na Posvetu o varnosti informacijske tehnologije in komunikacije (SSTIC2010) so omenili razvoj dveh novih projektov, in sicer celovite slike informacijske zagotovitve in dinamičnega zaznavanja tveganja. Projekta predstavljata močno nadgradnjo kibernetske obrambe. Nato je do konference že imel mnogo mehanizmov, ki so zagotavljali varnost – med njimi je potrebno omeniti sisteme za zaznavanje vdorov, orodja za oceno ranljivosti, protivirusne programe in sisteme za upravljanje varnostnih informacij ter dogodkov. Vendar pa je manjkal sistem, ki bi bil zmožen strniti želene prefiltrirane podatke in bi hkrati omogočal tudi vizualni prikaz dogajanja. Težava je bila tudi v tem, da uporabljana orodja niso bila vedno kompatibilna, včasih pa tudi niso zmogla filtrirati ogromne količine podatkov, ki so jih pridobili v omrežjih nameščeni senzorji (Decalarge 2010).

CIAP predstavlja želeno rešitev, saj bi s pomočjo skupnega podatkovnega modela, kateri bi zahteval uporabo določenih standardov, prefiltriral podatke, ki bi jih nato shranili ali distribuirali. Omogočil bi tudi razne možnosti vizualnega nadzora zbranih podatkov in hkrati

pregled nad omrežjem ter geografsko lokacijo dogajanja. Vse skupaj bi poenostavilo in izboljšalo pregled nad dogajanjem v Natovem kibernetskem prostoru. Izboljšala se bo tudi distribucija podatkov, saj bo CIAP omogočala prenos podatkov tistim, ki jih potrebujejo in ko jih potrebujejo. Uporabljale ga bodo lahko vse pooblaščene osebe zaposlene v Natu, kasneje pa tudi iz držav članic oziroma partnerjev. Poleg tega bodo zmožni izvoziti podatke v želeni obliki (kot informacije na papirju, PPT predstavitev, v tabelah itd.). CIAP se bo razvila na podlagi že obstoječega omrežja misije v Afganistanu, ki pa deluje le na minimalnih zahtevah (Decalarge 2010; Seffers 2011a).

Ne smemo pozabiti, da informacijske varnosti ne zagotavlja le tehnologija, temveč z njo upravlja človek, in prav ta velikokrat odpove, če mu primanjkuje znanja, izkušenj ali pa stori kakšno napako. Če na primer spregleda grožnjo in ne sproži alarma, lahko s tem ogrozi dejavnosti celotnega omrežja. Za ta namen želijo vzpostaviti delovanje DRA, ki bi nenehno opravljal ocenjevanje tveganja in avtomatsko določil vpliv na varnostno stanje sistema ter omrežja. V času simpozija je že deloval prototip, ki je prej omenjene dejavnosti opravljal z avtomatiziranim orodjem, ki je z grafikoni napadov določil, katere ranljivosti sistema glede na njegovo zgradbo lahko napadalci dejansko izkoristijo. Potem je na podlagi analize določil tveganja za sredstva, storitve in misije Nata ter jih razvrstil po vrstnem redu glede na nujnost in predlagal tudi primerne protiukrepe (Decalarge 2010).

Prej omenjena projekta pa nista edini pričakovani izboljšavi, saj so se odločili, da bodo v več korakih postopoma okrepili obrambne mehanizme informacijske varnosti. Primarni cilj je uvedba centralizacije kibernetske obrambe struktur Nata, ki bi dodatno okrepila že obstoječo. Prvi korak je nadgradnja Tehničnega centra Natovih zmogljivosti za odzivanje na računalniške incidente (NCIRC-TC), ki je lociran v Belgiji. V skladu z njo bodo uvedli sistem za podporo odločanju, ki bo izluščil bistvo velike količine podatkov in hkrati pomagal pri soočanju z incidenti. Uvedli bodo tudi referenčni sistem, ki bo osebju centra omogočal testiranje nove obrambne programske opreme ali pa preučevanje že obstoječe škodljive (Seffers 2011a).

V drugem koraku bodo v omrežja dodali celo zbirko senzorjev, ki so namenjeni poznavanju razmer omrežja z dodanimi sistemi za zaznavanje vdorov in omrežnimi forenzičnimi orodji. Najprej jih bodo namestili le v Natova omrežja, v okviru pričakovanega večnacionalnega sodelovanja pri razvoju kibernetske obrambe pa predvidevajo tudi razpršitev le-teh v nacionalna omrežja. Za takšno dejanje je trenutno veliko ovir, od suverenosti držav, zakonodaje itd., pa tudi v premajhnem številu organizacij in zaposlenih, da bi zmogli

zagotavljati tako obširen nadzor. Agencija zveze Nato za posvetovanje, poveljevanje in nadzor razvija primeren sistem, da bodo senzorje lahko namestili le na ključne točke omrežja, ne pa na vse strežnike. Po namestitvi se bodo soočili s še večjo količino podatkov in temu primerno bodo morali razviti tudi orodja, ki bodo uspešno prefiltrirala le-te (Hale 2011; Seffers 2011a).

Tretji korak bo vzpostavitev prej omenjenih projektov CIAP in DRA.

Četrti korak predstavlja vzpostavitev zmogljivosti za oceno groženj za Natov oddelek za varnostne izzive na sedežu zveze v Bruslju, peti korak pa bo izgradnja replike Tehničnega centra, ki bo v pripravljenosti in možna za takojšnjo uporabo, če se bo kaj zalomilo v delovanju prvotnega centra (Seffers 2011a).

Nadgradnja zmogljivosti naj ne bi prinesla nobenih sredstev za ofenzivno delovanje, temveč le izboljšala obrambne ukrepe, ki bi v okviru aktivne obrambe omogočali napadalno akcijo na napadalca le takrat, ko bi bil ta znotraj Natovih omrežij. Obstoj ofenzivnih informacijskih sredstev sicer lahko obstaja, vendar le v okviru posameznih držav in se ne sme uporabljati za namene Nata kot tudi ne deliti z ostalimi članicami zveze (Seffers 2011a; Sheldon 2011).

5.2.1 Natove skupine za hitro odzivanje

Del nadgradnje zmogljivosti na polno operativno sposobnost predstavlja tudi nadgradnja Natovih skupin za hitro odzivanje. Te skupine bodo polno operativne do konca leta 2012 oziroma začetka leta 2013, gre pa za ekipe strokovnjakov na področju informacijske varnosti, ki bodo zmožne nuditi takojšno strokovno in dobro organizirano pomoč ogroženi državi članici oziroma partnerjem, ki bodo zaprosili zanjo. Predvsem bodo na voljo tistim državam, ki same nimajo dovolj sredstev za vzpostavitev samostojne obrambe. Jedro ekipe bo trajno tvorilo šest usposobljenih strokovnjakov, ki bodo izurjeni za koordinacijo in izvršitev misij, sodelovali pa bodo tudi z lokalnimi ali Natovimi strokovnjaki na specifičnih področjih. Samo število vseh udeleženih in tip nalog bosta odvisna od zahtev misije. Ekipe bodo opremljene z IKT, natančneje s satelitskimi telefoni, kriptografsko opremo, opremo za digitalno obdelavo, digitalno forenzično analizo, omrežno varnost itd. Strokovnjaki bodo izurjeni v vseh procedurah Nata kot tudi v uporabi te napredne opreme, sodelovati pa bodo morali na raznih vajah kot je npr. Cyber Coalition, ki je že pripomogla z novimi izkušnjami. Ekipe bodo na voljo ves čas (NATO 2012).

Države članice bodo v primeru napada lahko zaprosile za pomoč, prošnjo bo odobraval Upravljalni odbor za kibernetsko obrambo, medtem ko bo prošnje držav nečlanic odobraval Severnoatlantski svet.

5.3 Iskanje in odprava ranljivosti

Oceno ranljivosti Natove kibernetske obrambe v praksi je leta 2011 prevzela nova skupina strokovnjakov, ki so jo poimenovali "Cyber Red Team". Naloge sile so ocenitev celotne učinkovitosti varnostnih ukrepov in procesov, ki so namenjeni Natovi kibernetski obrambi, prikaz posledic kibernetskega napada na informacijsko infrastrukturo ter večanje sposobnosti Natovih sredstev, da bi bile sposobne delovati v škodljivem informacijskem okolju. Z zaigranimi napadi poiščejo ranljivosti obrambe in potem sodelujejo na področju sprejemanja odločitev, ne vpletajo pa se v tehnične podrobnosti. Za izvedbo akcij uporabljajo realistične scenarije, do informacij poskušajo priti npr. prek komponent IKT določene Natove strukture ali pa tudi s prevaro. Težava teh igranih napadov je lahko v t. i. stranski škodi, saj je v tako kompleksnem okolju težko predvideti posledice, ki bi jih pustile simulacije, poleg vsega pa tudi v legitimnosti, saj je potrebno ljudi prepričati, da gre za razvoj obrambnih zmogljivosti in ne ofenzivnih. Edino ofenzivno sredstvo, ki bi ga pod določenimi kriteriji lahko uporabili, je izvedba DoS napada (Dillow 2011; Sheldon 2011).

5.4 Skupen projekt držav članic

Pritisk s strani ZDA je v Natu oblikoval nove smernice razvoja, ki bodo zagotovile dovolj napredno informacijsko infrastrukturo držav članic za interoperabilnost z napredno ameriško IKT. Prilagoditi se je bilo potrebno že za vzpostavitev globalne informacijske mreže (GIG), ki omogoča dostop do skupnih podatkov in komunikacij tako na terenu kot tudi v bazah. V okviru nove politike so se lotili tudi večnacionalne pobude za razvoj zmogljivosti kibernetske obrambe, ki od držav članic zahteva ustvarjanje in nadgrajevanje zmogljivosti z ozirom na nadaljnjo možnost sodelovanja z ostalimi, torej s ciljem interoperabilnega delovanja. Cilj projekta je združljivost informacijskih sistemov držav članic, kar bi omogočilo posamezni ogroženi članici, da je v primeru nevarnosti informacijski infrastrukturi lahko deležna pomoči s strani zveze Nato. Opravili so analizo zmogljivosti posameznih držav in izpostavili tri temeljna področja, ključna za učinkovitost zagotavljanja informacijske varnosti:

- prvo področje zajema zmogljivosti delitve ključnih informacij, v okviru katerih bi povečali varnost in hitrost delitve le-teh med državnimi CERT in NCIRC. Potrebno bo razviti novo večnacionalno informacijsko infrastrukturo, uvesti testirane komponente

in izuriti osebje, ki bo sodelovalo. Pomagale bodo izkušnje iz vaje Cyber Coalition in delovanja RTO, pomembna pa bosta meddržavna koordinacija in veljavnost zmogljivosti.

- Drugo področje predstavljajo zmogljivosti za zaznavanje kibernetskih razmer. Države članice že uporabljajo določena orodja (IDS, senzorje, orodja za VA …) v lastnih omrežjih, ki se upravljajo individualno in ročno s strani državnih ekspertov. Cilj je v uvedbi že omenjene CIAP, ki bo na voljo vsem pooblaščenim osebam in organizacijam.
- Tretje področje pa bo pokrilo dogajanje v informacijski infrastrukturi držav članic, in sicer z uvedbo raznih večnamenskih senzorjev in korelacijske infrastrukture (Jordan in Hallingstad 2011; Libicki 2007, 125–166).

Sodelovanje v projektu ne pomeni, da bodo morale države delovati v Natovih kibernetskih operacijah, temveč le to, da razvijejo lastne zmogljivosti za zagotavljanje informacijske varnosti, ki bodo skladne z zmogljivostmi ostalih članic (NATO 2011; NATO C3 Agency 2011a).

Trenutno stanje držav članic je povsem raznoliko, nekatere v kibernetske zmogljivosti vlagajo zelo veliko (npr. ZDA), spet drugih pa ta dimenzija ne zanima. Slednje so relativno lahka tarča potencialnih napadov, saj brez minimalno razvite IKT, ki bi bila namenjena kibernetski obrambi in kompatibilna s tehnologijo tistih držav, ki že imajo svoje obrambne mehanizme, ne morejo dobiti ustrezne pomoči s strani le-teh (NATO C3 Agency 2011a).

NC3A je že pripravila osnutek potrebne dokumentacije o C4ISR, ki teži k enotnosti, vendar so naleteli na ovire s področja državnih zakonodaj. Zakonom je potrebno prilagoditi imena in pojme (npr. ali uporabljati izraz "kibernetsko bojevanje" ali "kibernetske operacije"), koncepte, pa tudi norme z vidika funkcionalnosti informacijskih sredstev, saj ne smejo obiti legalnega sistema nobene posamezne članice, ki želi sodelovati. Dokumentacija bo opredelila področje delovanja kibernetske obrambe, vzpostavila skupen sistem, identificirala mejnike interoperabilnosti in dala podlago za večnacionalni razvoj skupnih zmogljivosti, poleg tega pa bo hierarhično razčlenila zmogljivosti kibernetske obrambe. To pomeni, da bo omogočila holističen pristop k razvoju. Holističen pristop v tem primeru pomeni pregled nad razvojem posameznih sklopov zmogljivosti v državah (rezultat bo v sistematičnem vodenju evidence, kje se kaj razvija), to pa bo jasno izoblikovalo potrebe za nove cilje. Prvi korak je razvoj opreme za zaznavo škodljivih aktivnosti, odpravo/odvrnitev/ublažitev napada, okrevanje po kibernetskem napadu in dinamično zaznavo groženj, škode ter napada, pa tudi uveljavitev

oddelka, ki bo skrbel za kibernetsko obrambo in pravočasno sprejemanje odločitev. Določeni ukrepi v nekaterih državah seveda že obstajajo, v skladu z dokumentacijo pa morajo države prilagoditi obseg ukrepov in jih poenotiti, kar pomeni, da morajo biti na tisti stopnji učinkovitosti, ki bo definirana v dokumentaciji. Skupen projekt je del aktualnega koncepta, imenovanega "pametna obramba", ki želi z zmanjšanjem sredstev in enot povečati učinkovitost obrambnih mehanizmov, v tem primeru na področju informacijske varnosti (NATO 2011; NATO C3 Agency 2011a; NATO C3 Agency 2011b).

Vodilni sili projekta sta Zavezniško poveljstvo za transformacijo (ACT) in Agencija zveze Nato za posvetovanje, poveljevanje in nadzor. Na delovnem seminarju slednje so septembra 2011 napovedali, da bi uspešno izpeljan projekt državam prihranil 15–20 % sredstev, ki bi jih sicer namenile za razvoj lastnih informacijskih zmogljivosti. Skupen razvoj zmogljivosti ima tudi dolgoročne učinke, ne bodo se pojavile potrebe posameznih držav po lastnih investicijah, olajšana in cenejša pa bosta tudi oskrba in vzdrževanje. Cilj je sodelovanje vseh držav članic, kar bi dalo projektu tako podporo kot tudi olajšalo sam razvoj skupne tehnologije. Države se bodo lahko odločile za razvoj tistih zmogljivosti, ki jih posebej zanimajo, celoten projekt ne bo državam nalagal nobenih denarnih omejitev. (NATO C3 Agency 2011a). Pomisleke držav kot vedno povzroča izbira vodstva. Rado se namreč zgodi, da pobudo prevzame tista država, ki največ prispeva – tudi v tem primeru so to ZDA, evropske velesile pa želijo svoj delež vodenja.

Vodilni poudarjajo, da projekt za sodelujoče države ne pomeni, da bodo morale posredovati vse informacije; glavna prednost je predvsem v varnosti in hitrosti posredovanja informacij. Strokovnjaki že nekaj časa sicer skrbijo za standardizacijo programske opreme med državami članicami, le-te sodelujejo tudi pri koordiniranih raziskavah v okviru RTO, ki pa sicer nima pooblastil za razvoj zmogljivosti (NATO C3 Agency 2011a; Seffers 2011a).

V okviru projekta se pričakuje skupen trud držav članic na področju raziskav, načrtovanja in tehničnega razvoja, testiranja ter eksperimentov, preverjanja, načrtovanja dobave in nato še same dobave. Končna interoperabilnost bo na koncu podprta s pravno podlago in/ali overitvijo. Potreben je razvoj mehanizma, ki bo nadziral in usmerjal razvoj zmogljivosti na državni ter mednarodni ravni, moral bo razumeti in ugoditi potrebam držav ter predvsem paziti, da bo razvoj ves čas v korak z grožnjami, torej da ne bodo zaostajali in izpostavljali sistema celotnega zavezništva (Jordan in Hallingstad 2011).

Celoten projekt se poleg pravne podlage in dokumentacije sooča tudi z drugimi problemi. Ker gre za tako kompleksno in neoprijemljivo okolje, strokovnjaki ne morejo izračunati točnih

zahtev, ki bi zagotovile ustrezno obrambo. Od sodelujočih držav se pričakuje, da same zagotovijo ustrezno informacijsko varnost lastne ključne infrastrukture (energetika, transport, gospodarstvo …), Nato bo pri tem nudil le minimalno pomoč (Hale 2011).

Sodelovanje pa ni pomembno le znotraj Nata, temveč tudi zunaj njega. Največ truda se je doslej vložilo v koordinacijo z EU, v prihodnosti pa se želi Nato osredotočiti tudi na bolj oddaljene celine, predvsem na Azijo in Afriko. Rasmussen je julija 2012 povedal, da je zadovoljen z urjenjem, izobraževanjem in vajami držav partneric, vendar je potrebno uvesti bolj strukturiran pristop, ki bo partnerjem omogočal sodelovanje pri razvoju zmogljivosti in oblikovanju prioritet. Partnerji ne smejo gledati le na razvoj naprednega orožja (izpostavil je predvsem brezpilotna vozila in letala), temveč predvsem obrambnih informacijskih ukrepov. Nato ima okoli 100 kibernetskih napadov na dan, zato je investiranje v kibernetsko obrambo ključnega pomena. Da bi lahko zagotovili mednarodno informacijsko varnost, pa je vsekakor potrebno sodelovati z velikimi državami, kot sta Kitajska in Rusija, posebej pomembno pa je tudi usklajevanje z njunimi politikami. Omenjeni državi imata možnost veta pri sprejemanju odločitev Varnostnega sveta Združenih narodov, kar pomeni, da lahko omogočita ali onemogočita vse pomembne napore zveze Nato (Pellerin 2012).

Iskanje partnerjev je zelo pomembno tudi znotraj sektorja industrije, ki se ukvarja z IKT. Nato ima za svoje strukture sklenjene pogodbe z raznimi zasebnimi in javnimi podjetji. K partnerstvu ponavadi pristopijo, če so izbrani na raznih razpisih. Takšno sodelovanje pa ni edina želja Nata, ki podjetja poziva, naj zvišajo kriterije varnosti pri produktih in storitvah, ki jih dajo na trg.

5.4.1 Sodelovanje z Evropsko unijo

Večina članic Nata je hkrati članica Evropske unije, zato je potrebno raziskati povezavo med omenjenima mednarodnima organizacijama. Poglobitev odnosov in strateško partnerstvo sta organizaciji sklenili na Srečanju Severnoatlantskega sveta v Lizboni 2010. Kot novo področje sodelovanja so izpostavili informacijsko varnost, nadaljnje smernice pa bi naj določili po raznih posameznih posvetih znotraj organizacij (NATO 2011b). Pobudo za izvajanje potrebnih ukrepov so kmalu prevzeli Američani, ki so prek raznih sestankov začeli pritiskati na pospešitev sicer dolgotrajnega procesa (Garamone 2011a; Garamone 2011b).

Agencija, ki je od leta 2005 namenjena krepitvi informacijske varnosti EU, se imenuje ENISA. S svojim delovanjem nudi strukturam in državam članicam strokovno pomoč pri zagotavljanju informacijske varnosti, organizira razne vaje in delavnice na omenjenem

področju, tako kot Nato se osredotoča na preventivno izvajanje ukrepov na nacionalnih ravneh članic, torej prek CERT. Le-te so nastale v okviru skupnih naporov obeh organizacij (ENISA 2012).

Skupaj z Natovim CCD CoE in Zvezo nemške industrije računalništva v oblaku je leta 2011 organizirala dvodnevno delavnico, ki se je osredotočila na merjenje, zaznavo, sledenje in obrambo pred omrežjem robotskih računalnikov (CCD CoE 2011).

ENISA je junija 2012 organizirala prvo mednarodno konferenco, katere temi sta bili sodelovanje v kibernetski krizi in kibernetske vaje. Sedemnajst strokovnjakov iz raznih organizacij (med katerimi je bil zastopan tudi Nato) je v štirih tematskih sklopih predstavilo svoj pogled na določeno temo. Le-te so se nanašale na sodobne kibernetske krize in potrebne vaje, kjer so opredelili praktične aktivnosti predstavljenih struktur, predstavili so tudi študije primerov in izkušnje, ki so jih že pridobili, ter tehnično opremo in orodja. Zaključili so z odprto debato o prihodnosti kibernetskih vaj, kjer so poudarili potrebo po mednarodni koordinaciji (ENISA 2012).

EU ima tudi ostale mehanizme, ki skrbijo za varovanje informacijske infrastrukture organizacije in njenih članic, posebej odmevna pa je pobuda, ki jo je že leta 2010 omenila Evropska komisija, marca 2012 pa se je na podlagi analize razmer zopet osredotočila nanjo. Januarja 2013 želijo ustanoviti evropski center za kibernetski kriminal, ki bi deloval kot del Europola. Gre torej za mehanizem, ki se bo lotil zadev, kot so otroška pornografija, kraja identitet ipd., poraja pa se vprašanje, kako se lahko njegovo delovanje preplete z Natovimi mehanizmi (Evropska komisija 2012).

Kljub temu da ima Nato trenutno glavno vlogo pri varovanju nacionalnih CIS, se znotraj zveze zavedajo, da je samostojni nadzor brez pomoči ostalih večjih akterjev nemogoče izvajati. Vodilni Nata in EU so zato izpostavili potrebo po interakciji na 4 informacijskih področjih, in sicer na področju urjenja in izobraževanja, izmenjave informacij, varovanja nacionalnih CIS in usklajevanja postopkov kriznega menedžmenta. V primeru večje nesreče bi uskladitev med zvezama pripomogla k hitrejši in učinkovitejši reakciji. Če do krepitve sodelovanja pri zagotavljanju informacijske varnosti ne bo prišlo, se zna zgoditi, da bi ob večji grožnji ključni informacijski infrastrukturi specifične države mehanizmi obrambe popolnoma odpovedali, posledice pa bi lahko občutila celotna mednarodna skupnost (Hale 2012).

5.5 Vodilne strukture Nata pri razvoju zmogljivosti

Ključne strukture na področju zagotavljanja kibernetske obrambe so:

- Center odličnosti za sodelovanje pri kibernetski obrambi (CCD CoE);
- Urad za upravljanje kibernetske obrambe (CDMA);
- Agencija zveze Nato za posvetovanje, poveljevanje in nadzor (NC3A);
- Natova agencija za komunikacijske in informacijske sisteme (NCSA);
- Organizacija za raziskave in tehnologijo (RTO);
- Odzivne skupine za računalniške nevarnosti (CERT).

5.5.1 Center odličnosti za sodelovanje pri kibernetski obrambi

Napad na Estonijo je sprožil potrebo po mehanizmu, ki bo skrbel za razvoj Natove kibernetske obrambe in tehnologije, ki bo zagotavljala informacijsko varnost na strateški ravni. V okviru le-tega je potrebno sestaviti učinkovito dolgoročno doktrino in strategijo. Ustanovitev Centra odličnosti za sodelovanje pri kibernetski obrambi (v nadaljevanju Center) je bila namenjena prevzemu omenjenih nalog, poleg njih pa Center zagotavlja tudi mnoge druge izboljšave na področju politike Nata, razvoju konceptov in višanja standardov varovanja podatkov ter informacij. Ustanovili so ga na podlagi izkušenj in predlogov akterjev iz zasebnega ter javnega sektorja, s katerimi v okviru raznih projektov sodelujejo še danes. Center ima po Pariškem protokolu status mednarodne vojaške organizacije, kar pomeni da ne spada pod poveljevalno strukturo Nata. Z delovanjem je začel oktobra 2008, in sicer s podporo ustanovnih članic Estonije, Litve, Latvije, Španije, Italije, Nemčije in Slovaške, ki so ga simbolično locirale v Talinu, glavnem mestu Estonije. Članstvo je mogoče za vse države članice zveze Nato, sodelujejo pa lahko tudi nečlanice, univerze, razni inštituti in podjetja kot sodelujoči udeleženci. Za vstop ali sodelovanje je potrebno soglasje Usmerjevalnega odbora Centra, ki ga sestavljajo predstavniki že sodelujočih držav (CCD CoE; Hughes 2009; Laasme 2011).

Center danes predstavlja eno izmed najbolj naprednih raziskovalnih središč, ki poleg že omenjenih nalog skrbi za interakcijo, večanje zmogljivosti in varno izmenjavo informacij znotraj zveze med državami članicami in tudi z drugimi akterji, ki delujejo kot partnerji na področju zagotavljanja informacijske varnosti. Z raznimi produkti in storitvami, ki se letno prilagajajo Programu dela, odobrenemu s strani Poveljstva vrhovnega zavezniškega poveljnika za preoblikovanje, Center izboljšuje aktivnosti Natovega na omrežju temelječega delovanja, analizira in dopolnjuje legalno podlago zagotavljanja informacijske varnosti,

organizira ter sodeluje pa tudi pri raznih eksperimentih in vajah (CCD CoE; Hughes 2009; Laasme 2011).

Organizacija vaj, konferenc, usposabljanj ipd. zahteva visoko stopnjo interaktivnosti med državami članicami in tudi partnerji. Center ponuja razna izobraževanja tako na tehničnem in operativnem področju kot tudi na področju prava. Najbolj odmevna vaja za prikaz dejanskega stanja učinkovitosti kibernetske obrambe Nata je imenovana "Cyber Coalition", ki se je prvič izvedla leta 2009, sedaj pa jo izvršujejo vsako leto. Zadnja se je izvedla decembra 2011, in sicer z namenom testiranja obrambnih postopkov zveze, ki se naenkrat znajde pod množico kibernetskih napadov na informacijsko infrastrukturo Nata in posameznih držav članic. Center zasnuje vajo, pripravi scenarij in ga nato prek raznih usposobljenih akterjev tudi izvrši, s tem pa se pokažejo zmogljivosti in tudi pomanjkljivosti delovanja Natovih obrambnih mehanizmov. Z vajo se izboljšuje tudi praktični del koordinacije ter interakcije sodelujočih. Sodelovanje na tej vaji je neobvezno, kljub temu pa se število udeleženih držav povečuje. Na zadnji vaji iz leta 2011 je sodelovalo kar 23 držav članic in 6 držav partneric (skupaj okoli 100 strokovnjakov, ki so se zbrali na sedežu v Vrhovnega poveljstva zavezniških sil v Evropi v Bruslju), Evropska unija pa je prevzela vlogo opazovalca. Poleg omenjene vaje organizirajo tudi konference, ki obravnavajo aktualno dogajanje s področja informacijskega bojevanja in varnosti, delavnice, tehnične tečaje, kjer dvakrat letno usposabljajo strokovnjake, ki znotraj centra skrbijo za omrežno varnost, elektronske tečaje ozaveščenosti za vse uporabnike Natovega omrežja, razne tečaje, ki se navezujejo na kibernetske grožnje, seminarje, ki so namenjeni civilnemu in vojaškemu osebju, ki delujejo na področju prava, na raznih vajah pa so sodelovali tudi z estonskimi in švedskimi institucijami ter obrambnimi silami z namenom prikaza zmogljivosti sodelujočih pred grožnjami informacijski varnosti (CCD CoE; Hughes 2009).

Pomembna je tudi dejavnost strokovnjakov Centra na teoretičnem področju. Znotraj NCIRC se pod pokroviteljstvom CCD CoE vsakih 6 mesecev srečajo delegati vojaške in civilne sfere držav članic Nata na delavnicah in izmenjajo znanja ter izkušnje, posebej pa se posvetijo trem področjem, to so:

- tehnična strokovna znanja, standardni operacijski postopki za analizo določenih računalniških incidentov in sistemov za zaznavanje ter preprečevanje vdorov,
- digitalna forenzika in organi pregona,
- vaje kibernetske obrambe (ENISA 2009; NCIRC).

Zaposleni izdajajo razne članke, poročila in knjige, ki zajemajo politične, pravne ter tehnične detajle in težave v zvezi z zagotavljanjem informacijske varnosti, pripravljajo pa tudi težko pričakovani priročnik z naslovom Manual on International Law Applicable to Cyber Warfare oziroma "The Talinn Manual", ki bi naj izšel spomladi 2013 pri založbi univerze Cambridge.

Priročnik bo definiral informacijsko bojevanje z vidika nacionalnega prava, pa tudi mednarodnega prava oboroženih spopadov in mednarodnega humanitarnega prava, pripomogel pa bo tudi k unifikaciji definicij posameznih pojmov, ki so sedaj deležni različnih razlag s strani posameznih subjektov, ki se teoretično ukvarjajo z dogajanjem na informacijskem področju. Do sedaj veljavne pogodbe in konvencije niso primerno interpretirane za uporabo v kibernetskem prostoru. Poleg interpretacije bo tudi določil odgovornosti držav na omenjenem področju, kako sta definirani njihova suverenost in nevtralnost, torej vse aspekte, ki so potrebni za umestitev kibernetskega bojevanja v pravni okvir. V prvi vrsti bo namenjen vladnim pravnim svetovalcem ministrstev, oboroženih sil in obveščevalnih agencij, akademikom prava, varnostnim študijam, svetovalcem obrambne industrije, pravnim firmam itd. Torej vsem akterjem, ki so povezani z IKT in aplikacijo le-te v obrambni sferi (CCD CoE).

Strokovnjaki znotraj Centra opozarjajo na neprilagojenost globalnih politik in strategij mednarodnih akterjev, ki ne sledijo napredni tehnologiji, ta pa se razvija zelo hitro. Predlagajo nove pristope, ki bi ponudili tako ofenzivne kot defenzivne ukrepe oziroma taktike. Za razliko od otipljivega okolja, kjer se napad velikokrat izkaže za najboljšo obrambo, je v virtualnem svetu zaenkrat lažje pripraviti dobre defenzivne ukrepe, ki zaradi učinkovitosti marsikoga odvrnejo od napada. Ofenzivni ukrepi, kot je na primer preventivno sledenje dinamičnim IP naslovom, bi vzeli preveč časa in so tudi težko izvedljivi. Eden izmed nujnih pogojev za večjo uspešnost pri zagotavljanju informacijske varnosti je interakcija med civilnimi in vojaškimi strokovnjaki, saj je IKT v večini primerov lahko uporabljena za namene ene ali druge sfere, poleg tega pa samostojno delovanje vojaške sfere ne more prilagajati kolektivne obrambe hitro se razvijajočim informacijskim grožnjam. Dejstvo je, da je ravno civilni sektor najbolj ogrožen, ker tarče nimajo dovolj dobrega varovanja, pa tudi same posledice napada so bolj efektivne (vpliv na javnost, propaganda, manipulacija ipd.). Civilni sektor je največkrat tarča t. i. kibernetskega kriminala in/ali vohunstva, ki narašča in je tudi vse lažje izvedljiv s pomočjo napredne programske opreme (Laasme 2011; Svete 2007).

5.5.2 Urad za upravljanje kibernetske obrambe

Natov center za NCIRC v Bruslju je osrednji mehanizem, ki skrbi za informacijsko varnost celotne zveze, začetek delovanja Urada za upravljanje kibernetske obrambe pa predstavlja prvi korak k centralizaciji kibernetske obrambe in zmogljivosti informacijske infrastrukture na operativni ravni zveze Nato. Primarna naloga je izvedba koordiniranega odgovora (protiukrepov) držav članic na grožnjo s področja informacijske sfere, izvrši pa se lahko le v primeru, da ogrožena država članica sama prosi za pomoč. CDMA je nastal kot odgovor na razmere iz Estonije leta 2007, torej kot nekakšen center, ki skrbi za pomoč v sili, v času delovanja pa se je razvil v glavno posvetovalno telo na področju informacijske varnosti za Severnoatlantski svet. Nasvete nudi tudi državam članicam, ki potrebujejo pomoč pri obrambi, razvoju in interpretaciji zahtev zveze (Hughes 2009).

CDMA vodi Upravni odbor za kibernetsko obrambo, ki ga tvorijo vodilne osebe iz političnega, vojaškega, operativnega in tehničnega področja, ki se ukvarjajo z informacijsko varnostjo. V uradu bi naj imeli najnaprednejšo tehnologijo, ki lahko natančno opredeli in locira razne grožnje, prav tako pa nudi visoko varovano deljenje in prenos ključnih informacij prek IKT. Natančni podatki o sami opremi zaradi varovanja podatkov niso na voljo javnosti. Napoved za CDMA je, da se bo v kratkem obdobju razvil v "vojno sobo" (v obliki že obstoječih, ki so namenjene koordinaciji misij in operacij), ki bo skrbela za centralizirano upravljanje kibernetske obrambe in izvajanje potrebnih protiukrepov za države članice, ki bodo želele sodelovati (Computer Weekly 2008; European Parliament 2010; Hughes 2009).

5.5.3 Agencija zveze Nato za posvetovanje, poveljevanje in nadzor

Agencija je v okviru reform julija 2012 prišla pod upravljanje Natove komunikacijske in informacijske agencije (NCIA). NC3A je pravna oseba Nata in je zadolžena za izvajanje aktivnosti v okviru zmogljivosti za C4ISR. Aktivna je pri razvoju kibernetskih zmogljivosti, kjer je skozi leta delovanja pridobila glavno izvršilno vlogo. Zaposleni razumejo tehnične zahteve, saj gre za skupino znanstvenikov, ki niso vezani na podjetja ali nacionalne omejitve in lahko nudijo neodvisno strokovno podporo ter širijo nove ideje. Nepristranskost agencije je tudi lastnost, ki je zaželena za nadzornika večnacionalnih podatkovnih baz, pripomorejo pa tudi pogodbe z raznimi državami članicami. Agencija izvaja tudi razne razpise na področju informacijske infrastrukture in podpore (Jordan in Hallingstad 2011; NATO C3 Agency 2011b).

5.5.4 Natova agencija za komunikacijske in informacijske sisteme

NCSA predstavlja tehnično podporo informacijski infrastrukturi Nata, hkrati pa nenehno varuje občutljive podatke pred grožnjami. Agencija nudi tudi strokovne tehnične storitve zvezi Nato in državam članicam, skrbi za vse pomembne strukture ter mehanizme, prisotna pa je tudi na raznih vajah, konferencah ali operacijah, kjer zagotavlja podporo ter nemoteno in varno delovanje komunikacijskih ter informacijskih sistemov. Primarna naloga je torej skrb za neovirano in zaščiteno delovanje Natove IKT. Strokovno podporo nudi vsem ključnim Natovim štabom, deluje pa tudi drugod po Evropi, pa tudi zunaj nje, in sicer kot podpora za posebne centre, ki so locirani v Aziji in Severni Ameriki. (NCSA Connecting NATO).

Temeljne dejavnosti NCSA so naslednje:

- vzdrževanje, oskrba, nadzor in upravljanje centralnih komponent Natovih omrežij, ki so namenjene kontinuiranemu in nemotenemu delovanju;
- nudenje strateških in političnih nasvetov vodilnim na področju CIS;
- varovanje ključnih podatkov in informacij;
- zagotavljanje varnih in klasičnih telekomunikacijskih konferenc za Natove štabe;
- zagotavljanje kompatibilnosti in delovanja nove strojne ter programske opreme s področja CIS;
- nudenje nasvetov, pomoči s tehničnega vidika itd. (NCSA Connecting NATO).

5.5.5 Organizacija za raziskave in tehnologijo

Organizacija je ena izmed največjih mednarodnih znanstvenih struktur, ki se je julija 2012 v okviru Natovih rekonstrukcij združila z Natovim podvodnim raziskovalnim centrom in preimenovala v Organizacijo za znanost in tehnologijo. Namenjena je večnacionalnemu znanstvenemu sodelovanju in izmenjavi tehničnih podatkov znotraj Nata ter med partnerji. Z njo sodeluje 26 držav članic in 38 partneric. Okoli 3000 strokovnjakov skrbi za razvoj obrambne tehnologije (NATO Science and Technology Organization).

5.5.6 Odzivne skupine za računalniške nevarnosti

Mehanizem so razvili v ZDA, in sicer že leta 1988 na univerzi Carnegie Mellon kot odgovor na škodljive programe, viruse in črve, ki so se širili po omrežju. Raziskovalci univerze so prišli do spoznanja, da se že najmanjše motnje ali grožnje informacijski infrastrukturi lahko prelevijo v krizo na nivoju državne ali celo mednarodne varnosti. Učinkovita rešitev se jim je zdela ustanovitev skupin strokovnjakov, ki bi preventivno nadzorovali nemoten potek IKT, v

primeru anomalij pa bi bile zmožne neposredno in v najkrajšem možnem reakcijskem času posredovati in vzpostaviti normalno stanje (Bernik in Prislan 2011; CERT).

Odzivne skupine delujejo na nacionalni ravni in imajo predvsem preventivno nalogo. Njihovo delovanje je pogojeno z razumevanjem, da je za poznavanje varnostnih problemov in rešitev zanje potrebno poznati tudi okvare ter tehnike zlorab, izkušnje pa morajo pridobiti z analizo težav, vdorov in ranljivosti programske opreme. Poznavanje lastnega okolja in tuja poročila/opozorila jim omogočajo pravočasne ukrepe ter ozaveščanje ostalih akterjev omrežja. Če bo Natov projekt medsebojnega sodelovanja uspel, bo olajšano sodelovanje z mehanizmi in strukturami drugih mednarodnih akterjev, s tem bodo pravočasno pridobili več informacij, v primeru groženj pa bodo lažje izvajali potrebne protiukrepe (Dunn in Wigert 2004, 349, 362).

Do terorističnega napada na ZDA leta 2001 CERT niso imele vidne vloge, po njem pa se je pojavila potreba po krepitvi informacijske varnosti; dobili so argumente za zagotavljanje potrebnih sredstev in s tem so se kmalu pojavile težnje ZDA in drugih močnih (evropskih) držav, da se vzpostavijo mehanizmi, ki bodo zagotavljali ažurnost informacijske varnosti. Jasno je bilo, da je potrebno ameriško prakso razširiti po drugih državah, da se zagotovi vsaj minimalna zaščita na državnih ravneh. To je še posebej pomembno za države članice Nata, saj bi vdor v omrežje specifične članice lahko pomenil vdor v informacijsko infrastrukturo celotne zveze. Cilj Nata je, da se CERT vzpostavi v vsaki državi članici in zagotavlja ustrezno delovanje informacijske infrastrukture na državni ravni, prav tako pa mora sodelovati z Uradom za upravljanje kibernetske obrambe. Ta jim že sedaj nudi ustrezne obveščevalne podatke in postopke, s katerimi se zagotavlja ažurnost CERT, posledično pa se veča učinkovitost (CERT; Hughes 2009).

Države članice Nata imajo na državnih nivojih več struktur zagotavljanja informacijske varnosti, med katerimi so tudi Odzivne skupine za računalniške incidente. V ZDA imajo 2 veliki skupini, in sicer pod poveljstvom Ministrstva za domovinsko varnost (US-CERT) in drugo, ki je oblikovana kot temeljni center v okviru univerze Carnegie Mellon (CERT/CC). Evropske države bolj ali manj ločujejo državne CERT in politiko. Nacionalne ekipe delujejo v okviru univerz ali večjih dobro opremljenih podjetij, ki svoje storitve ter produkte usmerjajo v IKT in informacijsko varnost. V Sloveniji imamo Slovenski center za posredovanje pri omrežnih incidentih, ki je del podjetja Arnes (Hughes 2009; SI-CERT 2012).

6 GROŽNJE NATU IN ODZIV NA NJIH

Znotraj držav članic se dnevno soočajo z grožnjami, občasno se pojavijo tudi odmevne grožnje ključnim infrastrukturam, kot je bil npr. napad na Estonijo leta 2007, redko pa se govori o napadih na Natovo informacijsko infrastrukturo, torej na njihova notranja omrežja in komponente. Iz Nata neradi dajejo sporočila za javnost o napadih, pravzaprav se o tej temi govori zelo malo. Zaposleni se zavedajo, da bi informacije o uspešnem napadu lahko izdale informacije o potencialnih ranljivostih Natove ključne informacijske infrastrukture.

SPIEGEL Online je konec aprila na podlagi pogovora z generalpodpolkovnikom Herrmannom aprila 2012 izdal članek, v katerem so razjasnili nekatere varovane informacije s področja Natove informacijske varnosti in groženj, s katerimi se zveza srečuje. Po njihovih podatkih se pojavlja vedno več groženj Natovim strukturam, dnevno okoli 30 omembe vrednih napadov na njihova omrežja ali posamezne računalnike. Ponavadi napadalci izberejo vohunsko programsko opremo (t. i. spyware), ki jo (naključnemu) zaposlenemu pošljejo prek elektronske pošte. Napade bi naj večinoma izvajale obveščevalne službe Kitajske in Rusije, seveda pa je to neuraden podatek. Odgovor na grožnje so znotraj Nata pripravili z oblikovanjem posebne enote s stodvajsetimi zaposlenimi strokovnjaki s področja informacijske varnosti, ki ves čas varujejo občutljive podatke in informacije. Enoto sem že omenil, gre za NCSA. Strokovnjaki so opazili večanje števila napadov, pa tudi izboljšanje kvalitete le-teh. Največkrat se še vedno pojavijo elektronska sporočila, ki so produkt prepleta obveščevalne dejavnosti in hekerskega delovanja, vsebinsko pa niso dovršena, torej imajo bolj splošno orientirano sporočilo, kot so npr. reklamna sporočila, vabila, nagradne igre ipd. Večjo težavo predstavljajo nova, bolj dovršena elektronska sporočila, ki so usmerjena v prejemnika. Napadalec se predhodno pripravi in preuči določenega zaposlenega, nato pa na podlagi raziskave sestavi sporočilo, ki bi naj pritegnilo prejemnika. Napadalca zanima osebno življenje tarče, tako lahko nato vzbudi njegovo zanimanje in ga pripravi do tega, da odpre priponko, ki običajno vsebuje trojanskega konja. Omenjeni virus se po zagonu samodejno namesti in začne prenašati podatke na napadalčev strežnik. Za takšne napade imajo po mnenju strokovnjakov dovolj mehanizmov, ki premorejo ustrezna orodja za izvajanje obrambe, ranljivost je predvsem v ravnanju ljudi. Le-te se da z prepričljivo prevaro velikokrat pripraviti, da podležejo namenu napadalcev in s tem ogrozijo Natovo ključno infrastrukturo. Znotraj zveze so pripravljeni tudi na takšne spodrsljaje, razna orodja (npr. IDS, VA itd.) hitro opozorijo, če so Natovi CIS ogroženi (Gebauer 2012).

Javnosti so najbolj vidni vdori na spletno stran Nata. Ta je tarča raznih aktivistov, posebej vztrajni so politični. Prvo javno soočenje z grožnjo so doživeli med kampanjo v Srbiji leta 1999. Takrat je bila Natova spletna stran ves čas ovirana, velikokrat so jo napadalci onemogočili z DDoS napadi. Srbski hekerji so poleg tega pošiljali prek 2000 elektronskih sporočil na dan, s čimer so preobremenili strežnik, pošiljali pa so tudi manjše viruse, ki so jih Natova orodja takoj zasledila in onemogočila. Napadi so prinesli zmago hekerjev na področju propagande, saj v Bruslju niso mogli objavljati svojih uradnih sporočil (BBC News 1999). Hekerji so spomladi 2011, ko se je začela kampanja v Libiji, vdrli na Natovo osnovno spletno stran in označili pripadnike zavezništva za morilce. Znotraj Nata so brez težav takoj vzpostavili nemoteno delovanje strani. Napad na spletno stran se je zgodil tudi pred kratkim, natančneje marca 2012, ko so jo napadli z DDoS in kratkoročno onemogočili dostop do nje. Stran ni delovala eno uro, po vnovični vzpostavitvi pa je naslednjo jutro bila spet kratkoročno onemogočena. Napad je bil del povračilnih ukrepov, saj so ameriške oblasti priprle nekatere aktiviste, ki so protestirali proti Natovi konferenci v Čikagu (Gebauer 2012; Ragan 2012).

Bolj resnih groženj so se lotili Anonymous, ki so se povezali z udarno LulzSec skupino, ki je kriva za vdore v Sony, omrežje Playstation, Infragard, PBS, strežnike ameriškega senata, spletno stran agencije CIA in ostalih odmevnih organizacij. Začeli so s t. i. Anti Security oz. AntiSec operacijami. Julija 2011 so vdrli na strežnike Nata in odtujili okoli 1 gigabit podatkov, nato pa objavili 3 dokumente v PDF obliki (Mick 2011). Zaposleni niso izsledili napadalcev, prav tako niso ugotovili, katere podatke so ukradli, podali so le izjavo, v kateri so pozvali napadalce, naj ne objavijo ukradenega materiala, ker bi to ogrozilo življenja ljudi (Lawson 2012).

Odmevna je bila tudi objava osebnih podatkov zaposlenih britanskega vojaškega osebja in Natovih zaposlenih. V začetku leta 2012 so objavili 242 osebnih elektronskih naslovov, gesel, informacij, ki so jih posredovali spletni strani Stralfor. Napadalcev niso izsledili, oškodovanci so lahko le spremenili svoje osebne podatke (Pilkington in Norton-Tayler 2012).

Posebej priljubljena tehnika je postala uporaba družbenih omrežij, kjer lahko širiš propagando ali pa se tudi pretvarjaš, da si nekdo drug, torej izvršiš neke vrste krajo identitete. Gre za novo obliko naprednih in obstojnih groženj, katere tarča je bil marca 2012 vrhovni poveljnik zavezniških sil za Evropo, admiral James Stavridis. Ni šlo le za nedolžno šalo, temveč bi naj bili v ozadju kitajski vohuni, ki so z lažnim profilom na Facebook omrežju želeli pridobiti admiralove osebne podatke. Pod pretvezo, da gre za Stavridisa, so prek Facebook omrežja

navezali stike z njegovimi prijatelji, znanci, sodelavci in družino. Omenjenim osebam so pošiljali namenska osebna sporočila, odgovor nanje pa bi razkril določene osebne podatke (Hopkins 2012).

Z grožnjami se srečujejo tudi na misijah. Računalniški črv (t. i. Conficker), ki je napadal operacijske sisteme Windows, je leta 2008 okužil tudi Natove računalnike, ki so bili del omrežja misije v Afganistanu. Omrežje so pred tem vzpostavili s pomočjo NC3A. Šlo je za okužbo s starejšo verzijo črva, ki so ga orodja za preprečevanje groženj hitro zaznala. Podporno osebje je izoliralo okužene komponente, ostali del omrežja pa dodatno zavarovalo. Virus se je že nekaj časa širil po celem svetu, zato so zaposleni že vedeli, kako se odzvati in celoten sistem je nemoteno deloval po slabih petih urah dela (Seffers 2011b).

Poleg groženj, ki so prišle v javnost, pa obstajajo še tiste, za katere se zaradi interesa po tajnosti nikoli ne izve. Veliko se špekulira o obveščevalnih dejavnostih usmerjenih v Nato. Podatkovne baze zavezništva so tarča mnogih akterjev, ki imajo različne cilje. Lahko gre za vohunjenje, ko želijo pridobiti informacije, ki bi jim olajšale pogajalsko pozicijo (npr. v primeru razpisov, pogodb ipd.), obstajajo pa tudi bolj škodljive namere (npr. iskanje lukenj v obrambi, gesla za dostop do omrežij, tajni podatki o misijah itd.).

Podatki o uspešnih kibernetskih napadih torej pridejo v javnost le v primeru, ko tako želi napadalec, ali pa je grožnja tako velika, da so znotraj Nata prisiljeni obvestiti javnost. Iz zavezništva večkrat poročajo o uspešnem delovanju obrambnih mehanizmov, neuradno pa tudi pricurljajo podatki o občasni neuspešnosti, npr. ko so zaposleni več dni brez dostopa do omrežja. Natovi mehanizmi zaenkrat še vseeno uspešno kljubujejo grožnjam, vendar se poraja vprašanje, kako bodo odreagirali, če bo koordiniran napad izvedla večja skupina profesionalcev z napredno IKT, ki bo imela namen kraje informacij ali celo uničenja Natove informacijske infrastrukture.

7 ZAKLJUČEK

V prvi hipotezi sem zapisal, da so Natovi koncepti in mehanizmi informacijske varnosti prilagojeni grožnjam, prav tako pa so primerno formalizirani znotraj Natove strukture. Hipotezo lahko potrdim le delno.

Če se najprej osredotočim na prvi del stavka, torej da so koncepti in mehanizmi zavezništva prilagojeni grožnjam, opažam, da je razvoj le-teh resnično v skladu z grožnjami in ga lahko potrdim. Kljub novim grožnjam, se večinoma pojavljajo nadgradnje že znanih, seveda pa občasno prihaja tudi do izjem, ki presenetijo ves svet (tak primer je bil Conficker), ko obstoječe strukture in mehanizmi občasno tudi zatajijo, saj jih tvorita človek in tehnologija, ki imata svoje pomanjkljivosti. NCIRC se ves čas dopolnjujejo, pomembno vlogo igrajo pridobljene izkušnje soočanja z grožnjami. Študije primerov so izhodišče za teoretično opredelitev nadaljnjih smernic razvoja, ko pa se pojavi dovolj argumentov (ponavadi so ti odvisni od posledic, ki jih je neka grožnja že pustila na informacijsko infrastrukturo tarč, ki niso nujno del Natovega omrežja) se najdejo sredstva in interes po razvoju mehanizmov, ki delujejo v praksi. Po napadu na Estonijo se je interes zelo povečal, dokončno pa so izdelali strategijo kibernetske obrambe na srečanju Severnoatlantskega sveta v Lizboni in od takrat dalje se zelo veliko vlaga v krepitev mehanizmov in struktur. Z NCIRC-FOC se na nekaterih informacijskih področjih prvič pričakuje celo prednost pred napadalci.

Problematična pa je formalizacija konceptov in mehanizmov. Ta del moram ovreči, saj so do sedaj različne Natove strukture imele na voljo lastne pristope k varovanju informacijske infrastrukture, kar pa se je v končni fazi izkazalo za neučinkovito. Poleg tega so se tudi pojavljali zelo neusklajeni dokumenti v zvezi z informacijsko obrambo, in sicer ne le med raznimi agencij in ostalimi organizacijami, temveč tudi znotraj le-teh. Projekt NCIRC–FOC med drugim zahteva centralizacijo kibernetske obrambe, pa tudi primerno pravno podlago, ki bo prav tako usklajena z zakonodajami držav članic. Polna operativnost bi naj bila dosežena šele v začetku leta 2013, spomladi tega leta pa bo predvidoma izšel tudi priročnik, ki ga pišejo strokovnjaki CCD CoE (naslov bo Talinn Manual). V njem bodo poleg pravne ureditve informacijskih aktivnosti zapisane definicije (ključnih) pojmov in konceptov s področja informacijske varnosti. Do sedaj je imelo kar nekaj Natovih struktur različne razlage tudi za najbolj osnovne izraze (npr. kaj je informacijska varnost), priročnik pa bo med drugim imel tudi vlogo terminološkega slovarja, ki ga bodo morali spoštovati znotraj Nata, zagotovo pa bo imel vpliv tudi na ostale mednarodne organizacije in strokovnjake, ki jih zanima

informacijska dimenzija. Formalizacija bo torej predvidoma dosežena, ko se bosta uveljavila NCIRC-FOC in Talinn Manual, to pa bo predvidoma v prvi polovici leta 2013.

Drugo hipotezo, ki pravi, da je Nato zaradi razvoja informacijsko-komunikacijske tehnologije razvil visoko funkcionalno kibernetsko obrambo, ki je kos grožnjam s področja informacijsko-komunikacijske tehnologije moram ovreči.

Nato je razvil učinkovito kibernetsko obrambo, vendar le-ta ni visoko funkcionalna, dokler je v domeni različnih struktur in s tem neenotna. Do te stopnje bo prišla šele z dokončno uveljavitvijo NCIRC-FOC, katerim pa bo potrebno dodati tudi aktivno sodelovanje držav članic in partnerjev. Centralizacija obrambe bo s pomočjo novosti kot je CIAP omogočila celovit nadzor, nadgrajena in nova orodja pa bolj avtomatiziran odgovor na grožnje.

Če vse države članice ne bodo spoštovale zahtev za zagotovitev določenih informacijskih zmogljivosti, bodo s tem vsi napori Nata odveč. Te države bodo vedno predstavljale ranljivost celotne zveze in najlažji dostop do skupnih podatkovnih omrežij. Nato bo moral kmalu določiti sankcije za članice, ki ne bodo hotele slediti smernicam razvoja, ali pa bo kljub vloženim sredstvom in trudu še vedno imel vidne ranljivosti.

Znotraj zavezništva imajo že sedaj, torej pred NCIRC-FOC, dobro usposobljene strokovnjake, ki hitro obnovijo in spravijo v delujoče stanje ogrožene/napadene tarče, pa tudi orodja, ki predčasno zaznajo grožnje v obliki škodljive programske opreme, črvov in enostavnih trojanskih konjev. Imajo torej dobre razvite mehanizme, ki se soočajo z že nastalimi težavami (v prihodnje tudi Natove odzivne skupine), manjkajo pa jim boljše preventivne aktivnosti. Težave se namreč pojavijo, ko je ravnanje z grožnjami odvisno od človeškega faktorja, ali ko se soočijo s hekerji, ki premorejo malo več kot povprečno poznavanje kibernetskega prostora.

Za rešitev prve težave že nekaj časa izobražujejo zaposlene prek raznih vaj, delavnic, delovanja Cyber Red Team ipd., kjer jim prikažejo možne scenarije in večkrat uporabljene metode napadov. Ozaveščenost pred informacijskimi grožnjami je največ, kar jih lahko naučijo, sama previdnost in skeptičnost pri ravnanju z elektronskimi sporočili, neznanimi spletnimi stranmi in orodji, pa je v domeni posameznih zaposlenih. Prva ranljivost je torej odvisna od vsakega posameznika, Nato jim namreč nudi dovolj strokovnih izobraževanj. Orodja z avtomatskim delovanjem (npr. DRA) bodo delno izključila človeške zmote, vendar ne bodo smela povsem izključiti ljudi, saj se da vsako programsko in strojno opremo prelisičiti.

Zaskrbljujoča je predvsem druga težava, saj še vedno kljub vsem novostim niso našli dovolj učinkovitega sredstva, ki bi zaznalo kompleksnejšo kibernetsko grožnjo in pravočasno reagiralo. Res je, da se napadov na Nato ne lotevajo hekerji, ki nimajo dovolj dobre opreme in premorejo le površno poznavanje ofenzivnih tehnik, vendar bi se v tako pomembni organizaciji morala zagotoviti večja informacijska varnost. Napadalci imajo večinoma močne interese, pa naj gre za aktiviste ali pa za obveščevalne organizacije. Zanimivo bo spremljati, ali bo polna operativnost NCIRC resnično izboljšala zaščito ključne informacijske infrastrukture in skupaj s prenovljeno zakonodajo morda zaradi strahu pred kaznijo celo odvrnila potencialne napadalce. Zaenkrat je dobro, da dovolj sredstev za resnejši kibernetski napad premorejo le države, ki si zaradi mednarodne ureditve ne upajo poseči po njem, vendar obstaja grožnja, posebej s strani držav, ki veliko vlagajo v IKT (npr. Kitajska) in jih tudi večkrat okrivijo raznih hekerskih aktivnosti.

Kot kaže, leži odgovor na nove grožnje informacijski varnosti v dokončni uveljavitvi NCIRC-FOC, vendar tudi to ne bo dovolj. Nato bo moral še naprej ves čas slediti aktualnim grožnjam, ki se pojavljajo skladno z novostmi, pa naj gre družbena omrežja, programsko in strojno opremo ali prenos določenih dejavnosti na informacijsko-komunikacijsko tehnologijo. Kibernetski prostor ponuja še veliko neraziskanih možnosti, ki bodo morale Natu, organizaciji namenjeni svetovnemu miru in varnosti, predstavljati izziv in vodilne pripraviti, da jih raziščejo pred akterji, ki bi jih lahko zlorabili. Šele s tem lahko vnaprej zavarujejo ključno informacijsko infrastrukturo in dosežejo želeni cilj, da bodo svoje zmogljivosti resnično razvili do polne operativne sposobnosti.

8 LITERATURA

1. Abele-Wigert, Isabelle. 2006. *Challenges Governments Face in the Field of Critical Information Infrastructure Protection (CIIP): Stakeholders and Perspectives*. Dostopno prek: http://cms02-s1.ethz.ch/silva/ETH/css_test/pdfs/CIIP-HB-2006-2-55-68.pdf (7. avgust 2012).
2. Abrial, Stephane. 2011. NATO Builds Its Cyberdefenses. *The New York Times*, 27. februar. Dostopno prek: http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=3 (16. april 2012).
3. *BBC News*. 1999. Kosovo info warfare spreads, 1. april. Dostopno prek: http://news.bbc.co.uk/2/hi/science/nature/308788.stm (22. avgust 2012).
4. Bernik, Igor in Kaja Prislan. 2011. *Informacijsko bojevanje: premik tradicionalnih metod vojskovanja in bojevanja v kibernetični prostor*. Dostopno prek: http://www.fvv.uni-mb.si/dv2011/zbornik/informacijska_varnost/Bernik-Prislan.pdf (7. avgust 2012).
5. *CCD CoE*. Dostopno prek: http://www.ccdcoe.org/ (15. avgust 2012).
6. --- 2011. *Botnet Workshop with ENISA*. Dostopno prek: http://www.ccdcoe.org/222.html (22. avgust 2012).
7. *CERT*. Dostopno prek: http://www.cert.org/cert/ (19. avgust 2012).
8. CircleID. 2012. *NATO Announces 58 Milion Euro Investment in Cyber Defence*, 12. marec. Dostopno prek: http://www.circleid.com/posts/nato_announces_58_million_euro_investment_in_cyber_defence/ (13. avgust 2012).
9. Computer Weekly. 2008. *Cyber Defence Managment Authority in Brussels*, 4. april. Dostopno prek: http://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels (16. avgust 2012).
10. Decalage. 2010. *SSTIC10 – Visualization and Dynamic Risk Assessment for Cyber Defence*. Dostopno prek: http://www.decalage.info/en/sstic10 (15. avgust 2012).
11. Defence Professionals. 2012. *NATO Signs Largest Contract to Date for Cyber Defence*, 9.marec. Dostopno prek: http://www.defpro.com/news/details/33224/?SID=7186f181c883085d2466e302af94920e (13. avgust 2012).
12. Dillow, Clay. 2011. Red Team GO! It's NATO's Turn to Build a Cyber Defence Force. *Popular Science*, 6. september. Dostopno prek: http://www.popsci.com/technology/article/2011-06/red-team-go-now-its-natos-turn-build-cyber-defense-force (20. avgust 2012).

13. Dunn, Myriam in Isabelle Wigert. 2004. *International CIIP Handbook 2004 – An Inventory and Analysis of Protection Policies in Fourteen Countries*. Dostopno prek: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=452 (7. avgust 2012).
14. ENISA. 2009. *NCIRC*. Dostopno prek: http://www.enisa.europa.eu/activities/cert/background/inv/initiatives-outside-europe/ncirc (15. avgust 2012).
15. --- 2012. *First International Conference on Cyber Crisis Cooperation: Cyber Exercises*, 11. julij. Dostopno prek: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercise-stocktaking/cyber-exercise-conference/report (22. avgust 2012).
16. European Parliament. 2010. *Defending against cyber attacks*. Dostopno prek: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/sede/dv/sede251010audnatocyberattacks_/sede251010audnatocyberattacks_en.pdf (16. avgust 2012).
17. Evropska komisija. 2012. *EU ustanavlja center za boj proti kibernetski kriminaliteti in zaščito e-potrošnikov*, 28. marec. Dostopno prek: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=1&language=SL&guiLanguage=en (22. avgust 2012).
18. Garamone, Jim. 2011a. Lynn Arrives in Brussels for Cybersecurity Talks. *American Forces Press Service*, 23. januar. Dostopno prek: http://www.globalsecurity.org/security/library/news/2011/01/sec-110123-afps01.htm (22. avgust 2012).
19. --- 2011b. Lynn Assesss NATO's Cybersecurity Progress. *American Forces Press Service*, 25. januar. Dostopno prek: http://www.globalsecurity.org/security/library/news/2011/01/sec-110125-afps03.htm (22. avgust 2012).
20. Gebauer, Matthias. NATO Faced with Rising Flood of Cyberattacks. *SPIEGEL Online*, 26. april. Dostopno prek: http://www.spiegel.de/international/world/nato-concerned-about-increasing-numbers-of-cyberattacks-a-829908.html (22. avgust 2012).
21. GlobeNewswire. 2012. *Finmeccanica Cyber Solution Team Completes First Tests for NATO Cyber Defence Security*, 12. julij. Dostopno prek: http://www.globenewswire.com/newsroom/news.html?d=262046 (13. avgust 2012).
22. Hale, Julian. 2011. NATO Boosts Sensors, Analysis to Protect Networks. *Defense News*, 14. junij. Dostopno prek: http://www.defensenews.com/article/20110614/DEFSECT04/106140310/NATO-Boosts-Sensors-Analysis-Protect-Networks (15. avgust 2012).

23. --- 2012. NATO Official Highlight Area for EU-NATO Cyber Cooperation. *Defense News*, 31. maj. Dostopno prek: http://www.defensenews.com/article/20120531/DEFREG01/305310005/NATO-Official-Highlights-Areas-EU-NATO-Cyber-Cooperation (22. avgust 2012).
24. Hopkins, Nick. 2012. China suspected of Facebook attack on Nato's supreme allied commander. *The Observer*, 11. marec. Dostopno prek: http://www.guardian.co.uk/world/2012/mar/11/china-spies-facebook-attack-nato (23. avgust 2012).
25. Hughes, Rex B. 2009. *Nato and Cyber Defence: Mission Accomplished?* Dostopno prek: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (8. avgust 2012).
26. Jordan, Frederic in Geir Hallingstad. 2011. Towards Multinational Capability Development in Cyber Defence. *Information & Security: An International Journal* 27: 81–89. Dostopno prek: http://infosec.procon.bg/v27/27.09_Jordan.pdf (16. avgust 2012).
27. Kaiser, Ryan. 2008. Estonia: NATO's Cyber Warrior. *Center for European Policy Analysis*, 1. maj. Dostopno prek: http://www.cepa.org/ced/view.aspx?record_id=34 (9. avgust 2012).
28. Lawson, Sean. 2012. *NATO & Cyber Conlict*. Dostopno prek: http://basicint.org/sites/default/files/lawson-nato__cyber_conflict.pdf (22. avgust 2012).
29. Laasme, Häly. 2011. Estonia: Cyber Window into the future of NATO. *Joint Force Quarterly* 63 (4/4): 58–63.
30. Libicki, Martin C. 2007. *Conquest in cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.
31. Mick, Jason. 2011. Anonymous Hacks NATO, HackersDeface Anonymous Site. *Daily Tech*, 21. julij. Dostopno prek: http://www.dailytech.com/Anonymous+Hacks+NATO+Hackers+Deface+Anonymous+Site/article22225.htm (22. avgust 2012).
32. NATO. 2011a. *NATO boosts cyber defence investments, launches multinational effort*, 22. september. Dostopno prek: http://www.nato.int/cps/ en/natolive/news_78418.htm
33. --- 2011b. *NATO-EU: a strategic partnership*, 15. november. Dostopno prek: http://www.nato.int/cps/en/natolive/topics_49217.htm (16. avgust 2012).
34. --- 2012. *NATO Rapid Reaction Team to fight cyber attack*, 13. marec. Dostopno prek: http://www.nato.int/cps/en/natolive/news_85161.htm (19. avgust 2012).

35. *NATO Science and Technology Organization*. Dostopno prek: http://www.sto.nato.int/ (17. avgust 2012).
36. NATO C3 Agency. 2011a. *2nd Workshop on Multinational in Cyber Defence Capability Development (MN CD 2)*. Dostopno prek: https://www.eiseverywhere.com/ehome/25957/39795/?& (20. avgust 2012).
37. --- 2011b. *Multinational Cyber Defence Capability Development Initiative*, januar. Dostopno prek: http://www.ncia.nato.int/Opportunities/Documents/6-MN-CyberDefence-02.pdf (12. avgust 2012).
38. --- 2011c. *Notification of Intent: NCIRC-FOC*. Dostopno prek: http://www.fsi.no/sfiles/91/15/2/file/13212-ncirc-foc-final.pdf (13. avgust 2012).
39. *NCIRC*. Dostopno prek: http://www.ncirc.nato.int/index.htm (16. avgust 2012).
40. *NCSA Connecting NATO*. Dostopno prek: http://www.ncsa.nato.int/index.html (16. avgust 2012).
41. *Northrop Grumman Company*. Dostopno prek: http://www.northropgrumman.com/index.html (13. avgust 2012).
42. Noshiravani, Reyhaneh. 2011. NATO and Cyber Security: Building on the Strategic Concept. *Chatham House*, 20. maj. Dostopno prek: http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/200511nato.pdf (10. avgust 2012).
43. Pellerin, Cheryl. 2012. NATO to Strenghten Ability to Act with Global Partners. *American Forces Press Service*, 5. julij. Dostopno prek: http://www.globalsecurity.org/military/library/news/2012/07/mil-120705-afps04.htm (23. avgust 2012).
44. Pilkington Ed in Richard Norton-Tayler. 2012. Hackers expose defence and intelligence officials in US and UK. *The Guardian*, 8. januar. Dostopno prek: http://www.guardian.co.uk/technology/2012/jan/08/hackers-expose-defence-intelligence-officials (23. avgust 2012).
45. Ragan, Steve. 2012. Chicago Police and NATOWebsites Hit by DDoS Attacks. *Security Week*, 21. maj. Dostopno prek: http://www.securityweek.com/chicago-police-and-nato-websites-hit-ddos-attacks (22. avgust 2012).
46. Research and Technology Organization. 2008. *Improving Common Security Risk Analysis – Chapter 7*. Dostopno prek: http://ftp.rta.nato.int/public//PubFullText/RTO/TR/RTO-TR-IST-049///TR-IST-049-07.pdf (14. avgust 2012).

47. Seffers, George I. 2011a. Nato to Strenghten Cybersecurity. *SIGNAL Online*, avgust. Dostopno prek: http://www.afcea.org/signal/articles/templates/ Signal_Article_Template.asp?articleid=2686&zoneid=326 (12. avgust 2012).
48. --- 2011b. Conficker Worms Its Way Into Afgan Mission Network. *SIGNAL Online*, 27. april. Dostopno prek: http://www.afcea.org/signal/articles/templates/ Signal_Article_Template.asp?articleid=2606&zoneid=313 (22. avgust 2012).
49. Severnoatlantski svet. 2002. *Prague Summit Declaration*. Dostopno prek: http://www.nato.int/docu/pr/2002/p02-127e.htm (8. avgust 2012).
50. --- 2006. *Riga Summit Declaration*. Dostopno prek: http://www.nato.int/ docu/pr/2006/p06-150e.htm (8. avgust 2012).
51. --- 2008. *Bucharest Summit Declaration*. Dostopno prek: http://www.nato.int/ cps/en/natolive/official_texts_8443.htm (8. avgust 2012).
52. --- 2010. *Lisbon Summit Declaration*. Dostopno prek: http://www.nato.int/ cps/en/natolive/official_texts_68828.htm?mode=pressrelease (9. avgust 2012).
53. *Severnoatlantska pogodba*. 1949. Dostopno prek: http://nato.gov.si/slo/dokumenti/ severnoatlantska-pogodba/ (8. avgust 2012).
54. Sheldon, John B. 2011. *NATO and Cyber Defence: Hanging together or Hanging Separately?* Dostopno prek: http://www.unidir.ch/pdf/conferences/sheldon_ cyber_24aug11.pdf (12. avgust 2012).
55. *SI-CERT*. 2012. Dostopno prek: http://www.cert.si/ (19. avgust 2012).
56. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: FDV.
57. --- 2007. Zaščita informacijske infrastrukture v precepu državne varnostne politike. V *Elektronsko upravljanje in poslovanje v službi uporabnika*, ur. Uroš Pinterič in Uroš Svete, 159–176. Ljubljana: Fakulteta za družbene vede.
58. --- in Zoran Jankovič. 2009. Izkušnje Republike Slovenije pri uvajanju zmogljivosti omrežnega delovanja. *Bilten Slovenske vojske 2009* (11) 3*: 135–158*.
59. Theiler, Olaf. 2011. *New Threats: the cyber-dimension*. Dostopno prek: http://www.nato.int/docu/review/2011/11-september/Cyber-hreads/EN/ index.htm (7. avgust 2012).
60. UNLV Office of Information Technology. 2012. *Definition of Information Security*. Dostopno prek: https://oit.unlv.edu/network-and-security/definition-information-security (19. avgust 2012).