UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Gregor Uranič

Internetna vojna v Estoniji: analiza in varnostne implikacije

Diplomsko delo

Ljubljana, 2010

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Gregor Uranič

Mentor: izr. prof. dr. Vladimir Prebilič
Somentor: doc. dr. Uroš Svete

Internetna vojna v Estoniji: analiza in varnostne implikacije

Diplomsko delo

Ljubljana, 2010

ZAHVALA

Zahvaljujem se mentorju izr. prof .dr. Vladimirju Prebiliču in somentorju doc. dr. Urošu Svetetu za nasvete in vso strokovno pomoč pri pisanju diplomskega dela.

Zahvaljujem se tudi moji družini in vsem drugim, ki ste me kakorkoli podpirali in vzpodbujali tekom študija.

INTERNETNA VOJNA V ESTONIJI: ANALIZA IN VARNOSTNE IMPLIKACIJE

Kaj bi se zgodilo, če bi internet jutri preprosto prenehal delovati ? Kako bi izgledal dan brez elektronske pošte, elektronskega bančništva, novic in socialnih omrežij. In kaj bi se zgodilo, če bi se ta dan raztegnil v teden, mesec? Majhen vpogled v takšno hipotetično prihodnost prikazuje ta diplomska naloga, ki govori o fenomenu informacijskega bojevanja, natančneje internetni vojni. Predmet analize so dogodki, ki smo jim bili priča v Estoniji maja 2007, ko so informacijski napadi ohromili temelje estonske vlade in gospodarstva. Kibernetski napadi so prizadeli tudi digitalne medije, elektronsko bančništvo, vladne komunikacije itd. Estonija velja za pionirko sodobne informacijske družbe, zato se naloga dotika tudi vplivov na širše varnostno okolje. Do neke meje je bila v Estoniji ogrožena nacionalna varnost – to odpira dodatna varnostna vprašanja. Kako se v takšni situaciji pravilno odzvati? Med drugim je Estonija tudi članica zveze NATO – ali se lahko Estonija sklicuje na 5. poglavje Washingtonske pogodbe? V iskanju teh odgovorov diplomska naloga ponuja tudi vpogled v aktualno kibernetsko-obrambno politiko zveze NATO.

Ključne besede: Internetna vojna, Estonija, kibernetski napadi, kibernetska politika, NATO.

THE INTERNET WAR IN ESTONIA: AN ANALYSIS AND SECURITY IMPLICATIONS

What would happen if the Internet simply stopped working one day? What would a day without an email, electronic banking, news and social networks look like? And what would happen if that day lasted a week or a month? Our thesis provides an insight into this hypothetical future. The diploma paper focuses on the phenomenon of Information warfare, particularly on the Internet war. The aim of the analysis is to present the events that we witnessed in Estonia in May 2007 when information attack paralyzed the foundation of Estonian government and the economy. Cyber attacks also caused damage to digital media, electronic banking, government communications, etc.. Estonia has the reputation of being the pioneer of modern information society, therefore the diploma paper discusses the mentioned issues in connection to wider security environment. To some extent, Estonia's national security was endangered and this fact can provoke additional security issues. How to act or respond properly when a situation of this kind occurs? Estonia is also a member of NATO – may a country such as Estonia rely on the Article 5 of the Treaty of Washington? In search of answers to this type of questions our thesis also provides an insight into the current cyber-defense policy of NATO.

Keywords: Internet war, Estonia, cyber attacks, cyber policy, NATO.

KAZALO

SEZNAM SLIK

SEZNAM KRATIC

DoS – *denial of service* – zavrnitev storitve

DDoS – *distributed denial-of service* – porazdeljena zavrnitev storitve

IKT – informacijsko-komunikacijska tehnologija

NATO – *North Atlantic Treaty Organisation*

CYBERWAR – kibernetska vojna

NETWAR – mrežna vojna

CCDCOE – *Cooperative Cyber Defence Centre of Excellence* – Center odličnosti za kibernetsko obrambo

CERT – *Computer Emergency Response Team* – Center za posredovanje pri omrežnih incidentih

BOTNET – prekrito omrežje

ICMP – *Internet Control Message Protocol*

PIAP – *Public Internet Access Point* – javno dostopna internetna točka

CDMA – *Cyber defence management authority* – Center za upravljanje kibernetske obrambe

RRT – *Rapid reaction team* – enote za hitro odzivanje

ATLAS – *Arbor Network Active Threat Level Analysis System*

NCIRC – *NATO Computer incident response capability*

FSB – ruska obveščevalna služba

FAPSI – ruska Zvezna agencija za vladne zveze in informacije

»Nemogoče je, da bi stari predsodki in sovražnosti še obstajale, ko pa je bil ustvarjen takšen inštrument, ki omogoča izmenjavo mnenj med vsemi narodi sveta. «

- Komentar na transatlantski telegrafski kabel, 1858.

1 UVOD

Danes živimo v svetu, ki močno presega tradicionalne dimenzije prostora. Življenje je vse bolj prepleteno z virtualno realnostjo in informacijskimi avtocestami. Govorimo o virtualnem prostoru, ki ima meje zabrisane, posameznik pa ni več omejen s fizično lokacijo, kar pomeni, da je internet že v osnovi globalen. Prostor, kjer težko definiramo meje, pa je že sam po sebi prvovrstno varnostno vprašanje, ki bo v prihodnosti še pridobivalo na pomenu.

Gospodarstva, države in družbe, nekatere bolj druge manj, funkcionirajo v odvisnosti do informacijsko-komunikacijske tehnologije. Razvoj informacijske tehnologije je po eni strani omogočil hitrejši način življenja in ga morda celo tudi poenostavil. Se je pa z uvedbo nove tehnologije in razvojem komunikacijskih sredstev pojavil tudi nov val ogrožanja družbe same.

Vse bolj se približujemo tako imenovani »e-družbi«. A vendarle se lahko za hip ustavimo in si zastavimo čisto preprosto vprašanje: Kaj bi se zgodilo, če bi internet jutri preprosto prenehal delovati in bi se prekinile vse informacijske poti? Kako bi izgledal dan brez elektronske pošte, elektronskega bančništva, novic, socialnih omrežij. In kaj bi se zgodilo, če bi se ta dan raztegnil v teden, mesec? Marsikomu se to zdi preprosto nemogoče, a vendarle. Majhen vpogled v takšno hipotetično prihodnost mi bo pokazala analiza, ki je predmet te diplomske naloge.

Maja 2007 je bila majhna baltska država Estonija, ki se rada ponaša z nazivom »E-stonija« in to vsekakor upravičeno, žrtev informacijskih napadov[1]. Država, za katero lahko rečemo, da je pionirka na marsikaterem področju, kar se tiče informacijske tehnologije, je na žalost odličen primer, kaj se lahko v prihodnosti zgodi vsakomur. Kibernetski napadi so ohromili digitalne medije, elektronsko bančništvo, vladne

[1] Uporabljajo se tudi têrmini virtualni napadi, digitalni napadi, kibernetski napadi.

komunikacije. Posledično so jo skupili tudi povsem običajni ljudje, saj brez svetovnega spleta tako rekoč ni več mogoče normalno živeti v enaindvajsetem stoletju.

Doslej je bilo že veliko primerov, ko je množičen napad hekerjev onemogočil mrežno poslovanje kakega podjetja, ustanove ali posameznika. V Estoniji pa lahko rečemo, da bi bila lahko na takšen način prvič ogrožena nacionalna varnost celotnega naroda. Tukaj se porajajo še druga varnostna vprašanja. Kako se v takšni situaciji pravilno odzvati? Estonija se je odzvala bolj ali manj uspešno z vsemi svojimi silami. Kako pa se je odzvala mednarodna skupnost? Med drugim je Estonija tudi članica zveze NATO – ali se lahko Estonija sklicuje na 5. poglavje Washingtonske pogodbe? Odgovore na ta vprašanja bom iskal skozi diplomsko nalogo.

Prvi del diplomske naloge bo metodološko-hipotetični okvir, kjer bom opredelil predmet, cilje preučevanja in postavil raziskovalni hipotezi. V drugem delu bom opredelil in definiral temeljne pojme ter koncepte, na katerih bo temeljila analiza. Tukaj bom razčlenil pojem informacijskega bojevanja in poskušal vanj umestiti pojem internetne vojne. V tretjem delu se bom posvetil analizi oz. študiji primera, sledila bo analiza širšega varnostnega okolja. Na koncu bom skušal verificirati hipotezi in podati sklep. V sklepnih mislih, kjer bom povzel ugotovljeno, bom skušal najti sintezo vsega napisanega – v kolikšni meri smo pripravljeni na kibernetsko prihodnost?

2 METODOLOŠKO – HIPOTETIČNI OKVIR

2.1 CILJ IN PREDMET

Cilj diplomske naloge je raziskati in opredeliti fenomen informacijskega bojevanja, natančneje internetne vojne. Predmet analize in raziskovanja bodo dogodki, ki smo jim bili priča v Estoniji leta 2007, ko so informacijski napadi ohromili temelje estonske vlade in gospodarstva. Preučil bom potek dogodkov, raziskal odziv Estonije in mednarodne skupnosti ter raziskal posledice. Estonija velja za pionirko sodobne informacijske družbe, zato me bo zanimal tudi vpliv na širše varnostno okolje.

2.2 HIPOTEZE

Na osnovi predpostavke, da globalizacija interneta in vse večja vpetost le-tega v družbo povečuje moč posameznika in v določeni meri zmanjšuje nadzor držav nad informacijsko-komunikacijsko tehnologijo postavljam naslednjo hipotezo:

> *H_1: Internetne vojne, kot smo ji bili priča v Estoniji, bodo v prihodnosti vse pogostejše.*

Tej hipotezi bo sledilo logično nadaljevanje z naslednjo hipotezo:

> *H_2: Razvoj kibernetske obrambne politike v zvezi NATO in članicah je skladen z naraščajočo grožnjo.*

V sklepnem delu naloge bom na podlagi raziskovanja in analize potrdil ali zavrnil zastavljeni hipotezi.

2.3 UPORABLJENA METODOLOGIJA

Pri izdelavi diplomskega dela, zasledovanju ciljev in verifikaciji hipotez bom uporabil več različnih metod družboslovnega raziskovanja. V prvi fazi bom za osvetlitev problematike in oblikovanje raziskovalnega vprašanja uporabil metodo zbiranja različnih virov in literature, relevantnih za problematiko, ki jo bom preučeval. Pri opredeljevanju temeljnih pojmov in konceptov bom analiziral in interpretiral primarne ter sekundarne vire. To bodo predvsem ustrezna akademska literatura in članki. Kot

osnovno metodo pri razlagi in opisovanju temeljnih pojmov in konceptov bom uporabil deskriptivno (opisno) metodo. Slednjo bom uporabil tudi v nadaljevanju, kjer bom natančneje opisal dogodke v Estoniji. Prav tako bom uporabil tudi metodo študije primera. Zaradi aktualnosti bodo prevladovali predvsem elektronski viri.

3 OPREDELITEV TEMELJNIH POJMOV

Opredelitev in podrobnejša razlaga temeljnih pojmov sta pomembno izhodišče za nadaljnje raziskovanje. Opredelil bom pojme, ki so neposredno povezani z raziskovalnim vprašanjem oziroma pripomorejo k razumevanju preučevane tematike.

3.1 KIBERNETSKI PROSTOR

Ameriško ministrstvo za obrambo definira kibernetski prostor kot globalni prostor znotraj informacijskega okolja, ki je sestavljen iz neodvisnih omrežij IT infrastrukture. Ta omrežja vključujejo internet, telekomunikacijska omrežja, računalniške sisteme in procesorje (Libicki 2009, 6).

Definicija je malce toga, manjka pa ji tudi pomembna sestavina – katera značilnost je tista, ki daje kibernetskemu prostoru unikaten značaj? Kuehl nadgradi zgornjo definicijo z naslednjo. Kibernetski prostor je operativni prostor, čigar značilni in unikatni značaj je uokvirjen z uporabo elektronike in elektromagnetne zmožnosti ustvarjati, shranjevati, spreminjati, izmenjavati in izkoriščati informacije preko sistemov temelječih na informacijsko-komunikacijski tehnologiji (IKT) in pripadajoči infrastrukturi (Kuehl 2009).

3.2 INFORMACIJSKO – KOMUNIKACIJSKA TEHNOLOGIJA (IKT)

Poglavitna sestavina kibernetskega prostora je torej informacijsko – komunikacijska tehnologija, ki je v zadnjem času postala zelo pomemben sestavni element sodobne informacijske družbe. Zelo preprosto jo lahko opredelimo kot kombinacijo informacijske tehnologije (IT) in druge podobne tehnologije, predvsem komunikacijske. Vendar za namene raziskovanja potrebujemo natančnejšo definicijo.

Začnimo z najširšo opredelitvijo informacijsko-komunikacijske tehnologije. Ta se nanaša na zbiranje, obdelavo in prikaz podatkov, prav tako pa vključuje tudi komunikacijski element, ki omogoča prenos podatkov (Alberts in Wilson v Svete 2005,

16). Izvor termina IKT sicer sega v 70. leta 20. stoletja (Bosh v Svete 2005, 16), bistveno pa je, da ne govorimo samo o tehnično-infrastrukturnem strojnem vidiku in napravah. Upoštevati je potrebno tudi vidik programske opreme, ki daje napravam uporabno vrednost in človeški dejavnik, ki programsko in strojno opremo tudi uporablja. IKT lahko torej opredelimo kot sposobnost, znanje, spretnost oziroma tehniko, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti, dosežemo želene učinke.

IKT lahko obravnavamo kot osnovo informacijske revolucije, ki je najbolj očitna v povečevanju zmogljivosti računalnikov, digitalizaciji podatkov in informacij ter v konvergenci nekoč ločenih družbenih podsistemov v novo entiteto produkcijskih, distribucijskih in aplikativnih aktivnosti. Digitalizacija informacijskih procesov je tako omogočila združitev računalnikov, telekomunikacij, televizije in interneta v enotno multimedijsko (komunikacijsko) okolje, prav tako pa povzročila širjenje IKT tehnologije (predvsem njenega informacijskega dela) v skoraj vse družbene sektorje in aktivnosti, od zdravstva do transporta in izobraževanja (Wilson v Svete 2005, 17).

Spletni slovar definira IKT kot tehnologijo, ki omogoča dostop do informacij preko telekomunikacij. Gre za podoben pojem kot informacijske tehnologije (IT), le da se primarno fokusira na komunikacijske tehnologije. Vključuje pa internet, brezžična omrežja, mobilne telefone in ostale komunikacijske medije (TechTerms.com 2009). V zadnjih desetletjih je IKT ljudem omogočil široko paleto novih komunikacijskih zmožnosti – v zadnjem času so v ospredju predvsem socialna omrežja.

IKT je torej, če uporabimo preprosto prispodobo, dežnik, ki pokriva vse tehnične in programske poti procesiranja in komuniciranja informacij. Najpogosteje ga uporabljamo za opisovanje digitalnih tehnologij, vključno z metodami komunikacij, kot tudi tehnikami shranjevanja in procesiranja informacij. IKT uporabnikom tudi omogoča participacijo v hitro se spreminjajočem svetu (IDI 2009).

Kar se tiče IKT – tehnologij, ima uporaba interneta zagotovo največje družbene implikacije (Svete 2005, 19). Računalniška omrežja so velik del sveta povezala v celoto – informacijsko družbo.

3.3 INFORMACIJSKA DRUŽBA

Informacijsko ali postindustrijsko družbo lahko opredelimo kot prihajajočo družbo, ki učinkovito in uspešno uporablja sodobne informacijske, komunikacijske in transportne tehnologije za ustvarjanje in nudenje cele vrste novih, informacijsko zasnovanih in podprtih proizvodov. Informacijska družba temelji na obvladovanju sodobnih tehnologij in kompleksnih procesov, za kar je potrebno znanje, ki ga je, zaradi hitrega tehnološkega razvoja, potrebno nenehno obnavljati. Zato lahko informacijsko družbo označimo kot učečo se družbo, v kateri mora biti proces učenja in pridobivanja novih znanj ter spoznanj neprekinjen in intenziven (Kovačič v Juvan 2006, 3). Kot sem že omenil je Estonija pionirka na marsikaterem področju, kar se tiče informacijske tehnologije. V nadaljevanju bomo videli, da so njeni načrti o informacijski družbi zelo ambiciozni. V to nas lahko prepriča že dejstvo, da so v ustavo zapisali dostop do interneta, kot osnovno človekovo pravico.

3.3.1 Varnostne razsežnosti informacijske družbe

Informacijska revolucija nas je torej pripeljala oziroma nas pelje v informacijsko družbo. To pa ima tudi pomembne varnostne implikacije. Obravnavanje varnosti v informacijski družbi se danes ne omejuje več le na vojaške vire ogrožanja, katerih cilj je predvsem država, vedno bolj se varnost obravnava kompleksno tako v smislu virov ogrožanja, referenčnih objektov, na katere se varnost nanaša, kot mehanizmov za njeno zagotavljanje. Pojmovanje varnosti se spreminja vzporedno z novimi viri ogrožanja, kot tudi novimi akterji zagotavljanja varnosti, saj predstavlja tehnološka odvisnost od splošno družbeno prisotne IKT v informacijskih družbah osnovo za razpravo o informacijskem bojevanju, po drugi strani pa naj bi njena razširjenost pomenila tako vir moči kot vir ranljivosti in s tem povezanih varnostnih izzivov, tveganj in groženj (Svete 2005, 17).

Za državo lahko rečemo, da je imela v zgodnjem obdobju informacijske revolucije prevladujočo vlogo na področju razvoja interneta. To se je danes spremenilo, saj države lahko le še ohlapno določajo pravila razvoja. Države se soočajo z izgubo moči in oblasti tako v odnosu do lastnih in tujih državljanov oz. posameznikov kot drugih držav in varnostnih akterjev. Na to varnostno zaznavo vplivata predvsem širjenje različnih tehnologij, ki povečujejo anonimnost posameznikov ter javno širjenje programske

opreme za kodiranje sporočil oziroma komuniciranja. Tovrstne tehnologije in programska oprema namreč spodkopavata uveljavljanje pravnega sistema oz. državne jurisdikcije ter obveščevalne sposobnosti držav ipd .(Svete 2005, 212).

Popolnoma se je spremenila zaznava prostora, časa in informacij. Uporaba IKT je povzročila razpadanje tradicionalnega gospodarskega, družbenega in političnega prostora ter glavne funkcije države. Informacijska družba tako postavlja pod vprašaj temelje moderne države – enačenje družbe z državo. Na mednarodnem trgu je država tako dobila konkurente v obliki nevladnih organizacij, multinacionalk in interesnih združenj (Svete 2005, 21-25). Vloga posameznika v informacijski družbi se je torej bistveno okrepila.

3.4 KIBERNETSKE GROŽNJE

Zelo preprosto lahko kibernetske grožnje razdelimo na štiri ravni: hekanje, organizirani kriminal, ideološki in politični ekstremizem ter državno sponzorirano kibernetsko agresijo (EU Cybersecurity 2009, 7).

V spektru kibernetskih groženj je vstopna točka hekanje. Ta obsega preprosto hekanje, kot je uporaba posebnih programov, ki so jih napisali drugi, pa do bolj sofisticiranega hekanja. O hekanju bomo več povedali v naslednjem poglavju. Druga raven je organiziran kriminal. Internet je postal, poleg vseh drugih aktivnosti, tudi življenjsko pomemben medij finančnih in intelektualnih transakcij. Kibernetski svet je tako postal zelo vabljiva tarča modernega kriminala[2]. Naslednja raven je ideološki in politični ekstremizem. Internet postaja za te skupine najpomembnejši prostor komunikacije in diskusij. Sem lahko uvrstimo tudi tako imenovani kibernetski terorizem. Pri državno sponzorirani kibernetski agresiji je ključno, da je na takšen ali drugačen način vpletena država. Zelo verjetno je, da bo ta raven groženj v prihodnosti postala del konfliktov med državami (EU Cybersecurity 2009, 8).

[2] Po nekaterih ocenah so različne spletne prevare leta 2007 v Veliki Britaniji povzročile 535 milijonov funtov izgube.

3.5 INFORMACIJSKO BOJEVANJE

Pri informacijskem bojevanju gre za izredno širok in kompleksen koncept. Mnogo avtorjev ga je poskušalo definirati, vendar nekega splošno sprejetega konsenza ni. Specifičnost informacijskega bojevanja se kaže skozi: a) okolje, kjer poteka informacijska vojna, ki ni fizično temveč kibernetsko, b) udeležence (vojaške, obveščevalne, teroristične, kriminalne organizacije in/ali posamezniki, c) katastrofalne posledice (ki lahko zahtevajo človeške žrtve ali pa tudi ne), č) nejasno razmejitev med vojaškim in civilnim delovanjem ter javnimi in zasebnimi interesi, d) neobstoj meje med fronto in zaledjem in e) nepredvidljivosti obsežnosti napadov in njihovih posledic (Arsić 2004, 24). Arsić pravi tudi, da lahko informacijsko bojevanje razvrstimo v tri osnovne kategorije: osebno (napadi na elektronsko zasebnost posameznika), korporacijsko (informacijske vojne po svetu , ki potekajo predvsem na ravni zbiranja in posredovanja dejanskih in lažnih podatkov) in globalno (globalni napadi nevidnega sovražnika, ki lahko napada cele države).

Nekateri avtorji se osredotočajo na značilnosti informacijskega bojevanje, drugi na sredstva in oblike bojevanja, tretji pa na to kakšni so njegovi nameni in cilji.

Eden od ciljev diplomske naloge je tudi poizkus umestitve internetne vojne v koncept informacijskega bojevanja, zato bom iskal definicije predvsem v tej smeri.

Začnimo z enim od prvih avtorjev, ki so raziskovali fenomen informacijskega bojevanja. Martin C. Libicki je že leta 1995 v knjigi *What is Information Warfare?* podrobno razčlenil informacijsko bojevanje. Zanj informacijsko bojevanje kot samostojna, ločena tehnika bojevanja ne obstaja. Tako informacijsko bojevanje loči med sedmimi različnimi oblikami, ki služijo širšemu konceptu informacijskega bojevanja. Sedem oblik informacijskega bojevanja – konflikti, ki vključujejo zaščito, manipulacijo, tajitev oz. prikrivanje resničnih informacij, razdeli med:

1. bojevanje na področju poveljevanja in nadziranja (ang. command and control warfare),
2. bojevanje na področju obveščevalne dejavnosti (ang. intelligence-based warfare),
3. elektronsko bojevanje (ang. electronic warfare),
4. psihološko bojevanje (ang. psychological warfare),

5. hekersko bojevanje (ang. hacker warfare),
6. ekonomsko informacijsko bojevanje (ang. economic information warfare) in
7. kibernetično bojevanje (ang. cyberwarfare) (Libicki 1995, 4).

Osredotočimo se le na hekersko in kibernetično bojevanje, ki se zdita preučevani tematiki najbližja. Hekersko bojevanje samo po sebi navadno ni nevarno, kajti pravi hekerji želijo opozoriti le na ranljivost sistemov in vdorov v sisteme ne izkoriščajo. Hekerske napade delimo na nenamerne (niso pomembni kot instrument informacijskega bojevanja, čeprav imajo lahko hude posledice) in namerne, v katerih se hekerji postavijo na eno stran v konfliktu in poskušajo: onemogočiti delovanje nasprotnikovih spletnih strani ali samo spremeniti njihovo vsebino, ukrasti in prodati informacije, zlorabiti informacijske sisteme, izvajati programske napake znotraj informacijskih sistemov idr. (to politično delovanje hekerjev imenujemo tudi hektivizem) (Svete v Dovč 2005, 15).

Kibernetsko bojevanje je oblika informacijskega bojevanja, ki poteka na internetu. Cilji bojevanja so tako civilni kot vojaški, med najbolj znanimi sredstvi kibernetskega bojevanja pa so virusi, logične bombe, trojanski konji in vohunska programska oprema (ang. spyware). Pri kibernetskem bojevanju gre za izkoriščanje računalnikov in omrežij za napadanje nasprotnika, glavni cilj pa je povzročanje kinetičnih posledic v fizičnem okolju. Libicki razume kibernetsko bojevanje predvsem kot futuristični scenarij (Svete in Pinterič 2008, 137) .

Arquilla in Ronfeldt se izogibata pojma informacijsko bojevanje, zato raje govorita o kibernetskem – »Cyberwar« in omrežnem bojevanju – »Netwar«. Kibernetsko bojevanje se po njunem nanaša na vojaško sfero, kjer je govora predvsem o konfliktih visoke intenzivnosti in konfliktih srednje intenzivnosti. Omrežno bojevanje pa obsega socialno, politično, vojaško in ekonomsko obliko konflikta, kjer govorimo predvsem o konfliktih nizke intenzivnosti, operacijah drugačnih od vojne (OOTW – operations other than war) in drugih, predvsem nevojaških, oblikah konflikta in kriminala (Arquilla in Ronfeldt v Dovč 2005, 8).

Informacijsko bojevanje se nanaša na napadanje in motenje računalnikov, ki upravljajo borze, energetska omrežja, nadzor zračnega prometa, telekomunikacije in obrambne sisteme. Tradicionalni virusi, trojanski konji in zavrnitev storitve (DoS) so del arzenala, ki se uporablja pri tem bojevanju. Informacijsko bojevanje je vse pogosteje prva napadalna poteza pred fizičnim napadom (PCMag.com 2010).

Zanimiv pa je predvsem pristop Johna Ryana, ki predlaga pojem i-vojna (I-war). I-vojna se razlikuje od prej omenjenega kibernetskega ali informacijskega bojevanja. Ta dva se namreč med drugim nanašata na občutljive zmogljivosti vojaške in kritične infrastrukture ter na zveze na bojišču in satelitske obveščevalne informacije. I-vojna pa se nanaša na napade prek interneta, katerih cilj je uporabniška internetna infrastruktura, kot so spletne strani, ki zagotavljajo dostop do spletnih storitev. Izkorišča povsod prisotno in slabo zavarovano infrastrukturo. Nanaša se na napade, izvedene preko interneta, katerih cilj je uporabniška internetna infrastruktura, kot so spletne strani, ki zagotavljajo dostop do spletnih storitev. Medtem ko se za kibernetsko in informacijsko bojevanje lahko odločijo države, i-vojno lahko sprožijo posamezniki, korporacije in skupnosti. Moč te oblike bojevanja bo vse večja s tem, ko bodo gospodarstva, vlade in skupnosti odpravljala tako imenovano »digitalno ločnico«. Tisti, ki največ uporabljajo internet, bodo vse bolj ranljivi za napade i-vojne, ki izkoriščajo uporabniško infrastrukturo. I-vojna se bo širila hitro, sprožil jo bo lahko vsakdo, ki ima internetni priključek in ki zna slediti poenostavljenim spletnim navodilom (Ryan 2007).

Po pregledu različnih pristopov k definiranju informacijskega bojevanja lahko rečemo, da bodo za analizo, ki bo sledila v naslednjih poglavjih, prišli v poštev predvsem zadnji koncepti. Tradicionalne definicije se bolj ali manj osredotočajo na vojaške zmogljivosti. Arquilla in Ronfeldt sicer omenjata tudi omrežno bojevanje ali »Netwar«, ki zajema nevojaške oblike konflikta. Kot pravita, »Netwar« označuje pojavljajočo se obliko konflikta (in kriminala) na družbeni ravni, obsega merila krajše vojne, v kateri protagonisti uporabljajo in so odvisni od mrežne oblike organizacije, doktrine, strategije in komunikacije (Arquilla in Ronfeldt v Dovč 2005, 9).

Vendar pa lahko rečemo, da je najprimernejši koncept za analizo, kot bomo videli v nadaljevanju, koncept t.i. i-vojne, ki ga predvideva Ryan. Pojem internetne vojne v kontekstu te diplomske naloge lahko torej najbolje definiram z definicijo i-vojne.

4 ANALIZA NA PRIMERU ESTONIJE

4.1 E-STONIJA

Preprosto internetno bančništvo, plačevanje parkiranja prek sporočil SMS, zastonj brezžični internet skorajda povsod – to je E-stonija. Govorimo o državi, kjer je internet od februarja leta 2000 zagotovljen z ustavo kot osnovna pravica državljanov. Državljani lahko brezplačno dostopajo do interneta preko 729 javnih dostopnih točk (PIAP). Do leta 2015 pa naj bi imel vsak državljan 1,3-milijonske Estonije širokopasovni dostop do interneta. Dogovor, ki sta ga dosegla ministrstvo za gospodarske zadeve in komunikacije ter združenje estonskih IT in telekomunikacijskih podjetij, obljublja prelevitev celotne države v eno samo veliko širokopasovno internetno vročo točko s pomočjo projekta, poimenovanega EstWin (Dnevnik.si 2009). Ta namerava zagotoviti možnost dostopa do internetne povezave s hitrostjo najmanj 100 Mbit/s po vsej državi, in sicer s pomočjo skoraj 7.000 kilometrov optičnih kablov in 1.400 brezžičnih vročih vstopnih točk, torej območij z možnostjo dostopa do javnega brezžičnega omrežja. Estonci so še posebej ponosni na dejstvo, da je bil v Estoniji razvit popularni Skype (Roman 2008, 6).

Estonija je na področju informacijskih inovacij daleč pred evropskim povprečjem. In to ne po naključju, saj se je, zahvaljujoč hitri prilagoditvi na moderne tehnologije ter pripravljenosti na eksperimentiranje z novimi rešitvami, uspešno predstavila svetu kot hitro razvijajoča se informacijska država in ta status tudi suvereno ohranja. Ne nazadnje to potrjuje tudi s trenutno kandidaturo za sedež nove agencije EU za področje informacijskih tehnologij (IT), ki naj bi začela delovati leta 2012 (Dnevnik.si 2010). V Estoniji sicer že deluje tudi NATO Center odličnosti za kibernetsko obrambo (CCDCOE).

4.1.1 E-vlada in e-uprava

Projekt E-vlade se je v Estoniji začel z gradnjo funkcionalne IKT-infrastrukture. Ta vsebuje zavarovan informacijski sistem, poimenovan X-Road, ki prestavlja hrbtenico delovanja. Sistem omogoča, da se vsak uporabnik lahko poveže z vladnimi bazami podatkov. V X-Road je povezanih več podsistemov: portal državljanov, socialno zavarovanje, register prebivalstva, zdravstveno zavarovanje ter davki in carina.

Uporabniki lahko skupaj dostopajo do 54 različnih baz podatkov in uporabljajo 349 različnih storitev (Kalvet 2007, 12). Že leta 2000 so uvedli e-cabinet, informacijski sistem, s pomočjo katerega ministri v estonski vladi kar prek uporabe interneta pripravijo gradiva, dopišejo pripombe in predloge, pa tudi glasujejo. Tudi zato se je estonske družbe prijel naziv e-družba, njene rešitve pa veljajo za zgled stroškovno ugodnejše in bolj učinkovite vlade.

Pomemben del celotnega informacijskega sistema je t. i. kartica ID, ki omogoča posamezniku vstop v e-državo. Gre za osebno kartico PIN, ki vsebuje šifriran čip in je postala osnova za marsikatero javno storitev. Poleg tega, da jo uporabljajo kot identifikacijski dokument po celi EU, jo lahko uporabljajo tudi za javni prevoz, e-volitve in tudi kot digitalni podpis. Odkar so jo leta 2002 dali v uporabo, so jo uporabili že več kot 6,5-milijonkrat za digitalni podpis, danes jo poseduje skoraj 90 odstotkov populacije, redno pa jo uporablja okrog 10 odstotkov Estoncev. Zadnja variacija na to temo, je kartica ID združena s kartico SIM, ki jo uporabljajo tudi v prenosnih telefonih. To pomeni, da se lahko na primer v banki ali doma digitalno podpišete s svojim mobilnim telefonom (Roman 2008, 8). To je še posebej prikladno, ker za to ne potrebuješ čitalca kartice ID.

4.1.2 E-volitve

Oktobra 2005 so prvi izvedli lokalne volitve tudi preko spleta. Storitev je uporabilo skoraj 2 odstotka volivcev. Marca 2007 so izvedeli tudi prve parlamentarne volitve, kjer je elektronsko glasovalo že 5,4 odstotkov volivcev. Leta 2009, ko so potekale volitve v Evropski parlament, je možnost elektronskega glasovanja uporabilo že 15 odstotkov volivcev (Kalvet 2007, 13). Za elektronsko glasovanje so državljani potrebovali le računalnik in osebne kartice ID, ki so omogočile oddajo digitalno podpisanih volilnih lističev. Elektronsko glasovanje sicer poteka le predčasno (4–6 dni pred volitvami), volivec pa lahko svoj glas neštetokrat spremeni – kot veljaven šteje zadnji oddani glas. Volilna komisija rezultate razglasi na volilni dan.

4.1.3 E-storitve

Preko 98 odstotkov vseh bančnih transakcij v Estoniji izvedejo elektronsko. Še bolj impresiven je podatek, da je bilo v letu 2009 več kot 90 odstotkov davčnih napovedi oddanih elektronsko. Z januarjem 2010 je začel delovati sistem digitalnih zdravniških receptov – vsi predpisani recepti se hranijo v bazi, do katere lahko dostopa uporabnik

sam ali na primer farmacevt v lekarni. Prav tako lahko vsak, seveda z uporabo osebne kartice ID, dostopa do lastne zdravniške kartoteke. Na področju šolstva lahko starši in otroci aktivno sodelujejo, preko komunikacijskega okolja eSchool. Spremljajo lahko ocene, predavane snovi in domače naloge (Kalvet 2008, 14) .

Estonci lahko na takšen način uporabljajo okrog 349, bolj ali manj uporabnih, različnih storitev. Velike zasluge za vsa našteta dejstva ima pragmatična informacijska politika in pogumna implementacija novih e-rešitev v njihov javni sektor.

4.2 OSVETLITEV POLITIČNE SITUACIJE

Napadi na estonsko informacijsko infrastrukturo, katere bom preučeval v naslednjem poglavju, so bili posledica kompleksne politične in zgodovinske situacije. Tukaj mislim predvsem na odnose z Rusijo, ki je imela zelo močan vpliv na estonsko zgodovino. Ta odnos še danes predstavlja zelo občutljivo vprašanje. Naj najprej navedem nekaj zgodovinskih dejstev.

4.2.1 Zgodovinski pregled

Sovjetska zveza je Estonijo prvič zasedla že poleti 1940, v skladu s sporazumom med Stalinom in Hitlerjem, ki je bil podpisan slabo leto pred tem. Najprej se je zgodila vojaška zasedba, nato imenovanje marionetne vlade, ki je potem sama zaprosila za priključitev k Sovjetski zvezi, in nazadnje uslišanje te »prošnje«. Pri tem je zelo nesrečno vlogo odigrala tudi tedanja estonska politična elita: v grozljivem položaju, v katerem se je znašla dežela po izbruhu druge svetovne vojne, je domnevala, da bo sovjetska protekcija manjše zlo od nacistične okupacije. Zato je najprej dovolila postavitev sovjetskih vojaških oporišč na estonskem ozemlju, nato pa brez odpora sprejela sovjetske okupacijske sile, upajoč na najboljše. A stvari so se hitro obrnile. V prvem letu okupacije so Sovjeti aretirali vso politično in gospodarsko elito, okoli 8.000 ljudi; 2.000 od njih so takoj usmrtili, okoli 3.000 jih je izginilo v sibirskih taboriščih. Nemško manjšino so sporazumno z nacisti deportirali v Reich. A najhuje je šele prihajalo. Ob nemškem napadu na Sovjetsko zvezo je bilo v Sibirijo deportiranih okoli 40.000 Estoncev, od tega jih je vsaj polovica do konca vojne umrla. Razumljivo je, da so mnogi Estonci nemško vojsko pozdravili kot osvoboditelje. A Hitler estonske samostojnosti ni obnovil, saj je imel z Estonci enake načrte kot s slovanskimi narodi – v

treh letih nacistične okupacije je bilo ubitih okoli 12.000 Estoncev, od tega 3.500 Judov. Šele v drugi polovici leta 1943 so Nemci začeli mobilizirati Estonce za boj proti Sovjetom. Jeseni 1944 so Sovjeti ponovno zasedli baltske države in začela se je druga okupacija, ki je bila še hujša od prve. Okoli 80.000 Estoncev je emigriralo na Zahod, večinoma v ZDA, najmanj 40.000 pa jih je bilo deportiranih v Sibirijo, kjer jih je do Stalinove smrti vsaj 12.000 umrlo. Vse to se je zgodilo v deželi, ki je leta 1939 štela nekaj nad milijon prebivalcev. Zahodne države niso nikoli priznale sovjetske aneksije baltskih držav. Ne le po estonski ustavi, temveč tudi po mednarodnem pravu je edino pravilno poimenovanje za obdobje med 1944 in 1990 – sovjetska okupacija. V obdobju med 1945 in 1951 je v Estoniji delovalo partizansko gibanje proti sovjetski okupaciji: to je bil – poleg nekaj sporadičnih skupin v zahodni Ukrajini v istih letih – edini primer oboroženega ljudskega odpora proti Stalinovemu sistemu v celotni Evropi. Junaško poglavje evropske zgodovine, je izven Estonije povsem pozabljeno. Koliko ljudi je umrlo v teh spopadih, ni znano: ocene so zelo različne in se gibljejo od 8.000 pa vse do 25.000 padlih (Lisjak 2007).

Sledilo je dolgo obdobje sovjetske okupacije, ki je globoko predrugačilo estonsko družbo. Od poldrugega milijona ljudi, kolikor jih ima danes Estonija, jih je kar pol milijona priseljencev iz drugih dežel Sovjetske zveze. Osamosvojitev baltskih držav se je zgodila v velikem gibanju, v velikem patosu novega. V tem osamosvojitvenem gibanju baltski Rusi niso množično sodelovali, a mu niso bili sovražni. Obstajala je možnost, da bi jih nekako vključili v gradnjo nove države. Toda Estonci so vztrajali pri obnovitvi nekdanje samostojnosti. Državljanstvo so podelili samo potomcem državljanov izpred 1940. Šli so celo v to skrajnost, da so ob osamosvojitvi najprej ponovno obudili staro ustavo iz leta 1937 in jo šele nato nadomestili z novo. Na tisoče prebivalcev Estonije je tako postalo tujcev v svoji deželi, čeprav so bili mnogi pripadniki druge ali celo tretje generacije. To je pustilo globoke rane v estonski družbi in od tod izvirajo razlogi za nemire spomladi 2007 (Lisjak 2007).

4.2.2 Demonstracije in nemiri

Gre torej za problematični model sobivanja med estonsko večino in rusko manjšino. Dogodki, ki so se zvrstili v letu 2007, so pokazali, da je ta v zelo slabem stanju. Celotna zgodba pa je dosegla vrhunec z odstranitvijo bronastega spomenika (glej prilogo A), ki so ga Rusi v obdobju, ko je bila Estonija povsem pod taktirko Moskve, v Talinu

postavili neznanemu sovjetskemu vojaku kot spomin na obdobje druge svetovne vojne. Ni presenetljivo, da se je ves gnev osredotočil na odstranitev spomenika sovjetskemu vojaku. Predstavljal je simbol ruske prisotnosti v Estoniji in njihove zmage nad nacizmom. Demonstracije je bilo tako za pričakovati, demonstrirali pa so izključno pripadniki t. i. ruske manjšine.

Na trgu v središču Talina, kjer je stal spomenik sovjetskemu vojaku, se je 26. aprila zbralo kakih 1.000 ljudi, ki so mirno protestirali proti vladnim načrtom, da spomenik premaknejo na manj ugledno lokacijo, na mestu, kjer je stal, pa opravijo izkopavanja, da bi ugotovili, če so bile pod spomenikom morda pokopane žrtve druge svetovne vojne. Skupina mladih je nato skušala prebiti policijski kordon in izbruhnili so izgredi. Policija je protestnike razgnala s pomočjo vodnih topov, pendrekov ter svetlobnih in zvočnih granat. V neredih je umrl 20-letnik, 43 ljudi je bilo ranjenih. Po najhujšem nasilju v Estoniji, odkar je država leta 1991 razglasila neodvisnost od Moskve, so policisti pridržali več kot 300 ljudi. Izgredi so se v estonski prestolnici nadaljevali še naslednji dan. Spomenik so oblasti prestavile na neznano lokacijo, kot so sporočili, zato, da bi v prihodnje preprečili podobne kršitve javnega reda. Kasneje pa so ga postavili na vojaško pokopališče na obrobje mesta. Rusija se je na odstranitev spomenika seveda odzvala ostro, parlament v Moskvi pa je pozval celo k sankcijam in prekinitvi diplomatskih odnosov z Estonijo. Estonski predsednik pa je medtem Rusijo obtožil, da v državo vnaša razdor. Evropska komisija je v odzivu poudarila, da obžaluje smrt protestnika in nasilje, ki je ob tem izbruhnilo (Delo.si 2007).

Za to diplomsko nalogo pa je pomembno tisto, kar je sledilo. 26. aprila, ko so v središču Talina izbruhnili nemiri, so se začeli tudi »nemiri« v virtualnem svetu. Začeli so se virtualni napadi na estonsko informacijsko-komunikacijsko infrastrukturo, ki so trajali dobre tri tedne.

4.3 VIRTUALNI NAPADI

Virtualni napadi na Estonijo so bili izvedeni zelo koordinirano, zato so povzročili precejšni kaos. Napadi so bili tako intenzivni, da so morali do določenih spletnih strani blokirati dostop iz tujine. Spletne strani, ki imajo običajno 1.000 obiskovalcev na dan, so jih imele kar naenkrat 2.000 na sekundo. Napadi so bili osredotočeni predvsem na

spletne strani parlamenta in ministrstva, političnih strank, večjih pomembnih organizacij, bank in komunikacijske infrastrukture. Podatki spletne strani ATLAS[3], ki trdi, da lahko spremlja 80 odstotkov svetovnega internetnega prometa, kažejo, da je bilo v treh tednih izvršenih 128 edinstvenih DoS napadov na naslove IP znotraj Estonije. Večina je bila t. i. poplav ICMP[4] PING, ki so ciljali na celoten estonski sistem in ne zgolj na določene strežnike. Estoniji so prišli na pomoč tudi številni tuji strokovnjaki iz zveze NATO, EU, Izraela in ZDA (Evron 2008). V nadaljevanju bom podrobneje raziskal tipe napadov in orodja, ki so bili uporabljeni v napadih.

4.3.1 Orodja in tipi napadov

Napadi na estonsko omrežno infrastrukturo so bili večinoma tipa DoS ter DDoS in so obsegali od preprostih oblik PING poplav do bolj sofisticiranih botnet napadov.

Napad DoS[5] ali slovensko zavrnitev storitve je zlonamerna dejavnost na medmrežju, ki ne poskuša razbiti varnostne zaščite ciljnega strežnika ampak doseči, da je povezava do le-tega strežnika popolnoma prenatrpana, kar rezultira v neuporabnosti servisov, ki jih nudi strežnik različnim obiskovalcem medmrežja in kar posledično pomeni tudi izgubo prihodka za ponudnika storitev napadenega strežnika. Pri napadu DoS napadalec medse in med napadeni strežnik vnese en sloj računalnikov, ki služijo kot sužnji za napad. Računalnike sužnje pridobi napadalec tako, da preizkuša računalnike na medmrežju, če imajo nameščen kakšen ranljiv servis ali aplikacijo, nanje vdre in namesti t. i. rootkit, ki mu omogoča oddaljeno upravljanje računalnika brez, da bi administrator računalnika sužnja to sploh zaznal. Tako si napadalec pridobi možnost zakritja, saj ima popolno kontrolo nad računalnikom sužnjem in prav tako tudi nad vsemi sledmi, ki so zapisane na računalniku sužnju. Dejanski napad izvajajo računalniki sužnji, napadalec pa ostane neizsledljiv v ozadju. Napadi DoS so v bistvu enako nevarni kot napadi, ki vključujejo vdore v sistem, vendar se tega dejstva lastniki medmrežnih strežnikov še ne zavedajo in zato je tudi preventivna dejavnost v tej smeri skoraj zanemarljiva (Krulec 2004).

1. Napad prekoračitve vmesnika

Največji delež pripada prav temu načinu. Na omrežni naslov se pošlje več podatkov, kot so programerji predvidevali, da bi ga lahko kdo poslal. Najbolj zaležejo e-mail

[3] Arbor Network Active Threat Level Analysis System
[4] Protokol ICMP se uporablja za pošiljanje nadzornih sporočil in sporočil stanja internet omrežja. Pakete ICMP razlikujemo po tipu sporočila, ki ga nosijo, to je lahko zahteva, odgovor na zahtevo, statusna informacija in vrsta napake.
[5] ang. Denial of Service

sporočila, katerih ime priložene datoteke dosega 256 znakov in prekomerni ICMP paketi. Slednji so znani tudi kot »ping of death«.

2. Napad »SYN«

Pri vzpostavljanju seje med TCP odjemalcem in strežnikom, se opravlja veliko dela. V ta namen obstaja zelo majhen vmesnik za sporočila. Ko prispe prvo sporočilo z omogočeno SYN zastavico, strežnik ustvari nov vmesnik za sporočila za točno to povezavo in čaka na naslednja nek določen čas. Cilj napadalca je, da odpre čimveč povezav in tako povzroči strežniku poplavo odprtih vmesnikov.

3. Napad razpršitve

Ta način izkorišča slabost nekaterih usmerjevalnikov, ki paketov določene velikosti ne zmorejo poslati v celoti, temveč jih razdrobijo v manjše paketke. Pri čemer se paketki, ko so enkrat dostavljeni spet združijo v celoto, glede na priložene »odmike« od prvega paketa. Napadalec vnese napačno vrednost odmika enemu izmed kapljic prvotnega paketa ter tako običajno povzroči, da se prejemnik paketkov sesuje. Prejemnik namreč velikokrat nima izdelanega načrta, kako ravnati v taki situaciji.

4. »Smurf« napad - poplava paketov ICMP

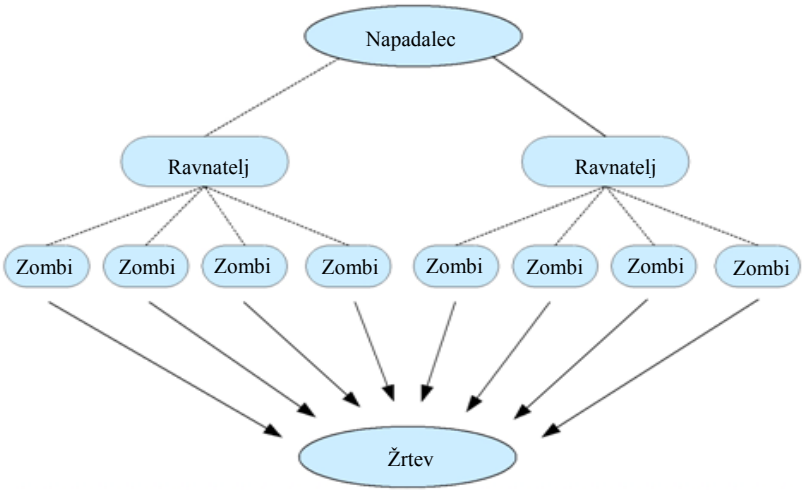
Napadalec pošlje IP ping[6] sporočilo. Ta ping paketek vsebuje tudi podatek, da naj se sam dostavi še na preostale gostitelje znotraj lokalne mreže. Seveda se dostavi z lažno navedenim mestom, od koder je IP paketek v originalu prispel. Tako se iz vseh teh številnih gostiteljev, ki so paketek obravnavali, vrača odgovor na nek nedolžen računalnik.

5. Porazdeljeni DoS napadi (DDoS)

Proti DoS napadu se je mogoče boriti z blokiranjem prometa iz zlonamernega strežnika, zato se za oviranje delovanja računalniških sistemov pogosteje uporablja DDoS[7] napad . Gre za podoben napad, ki pa simultano poteka iz večjega števila računalnikov, zaradi česar se ga je težje ubraniti. DDoS napad med napadalcem in računalnikom sužnjem vnese še en dodatni sloj in sicer računalnik ravnatelj. Računalniki ravnatelji se pridobijo z vdorom v sistem in namestitvijo ti. rootkita. S pomočjo teh računalnikov napadalec ročno ali avtomatsko vdira v računalnike »zombije« na katere namesti rootkit in sistem za sprejemanje ukazov od računalnikov ravnateljev.

[6] Gre za osnoven program za preverjanje nastavitev in kontrole na TCP/IP mreži, uporablja pa se tudi za odpravljanje težav povezljivosti, ponovne dostopnosti in razpoznavanja imen.
[7] ang. Distributed Denial of Service.

Slika 4.1: Shematski prikaz DDoS napada



Vir: Hribar (2006).

Pri napadu, računalniki ravnatelji sporočijo računalnikom »zombijem« kateri ciljni strežnik naj napadejo. S tem dodatnim slojem je zasledovalcem oteženo iskanje računalnikov ravnateljev preko računalnikov sužnjev in šele, ko odkrijejo računalnike ravnatelje, lahko iščejo dejanskega napadalca (Hribar 2006, 32).

Takšna prikrita omrežja imenujemo botneti [8]. Upravljavec takšnega omrežja ima skozi nadzorni center botneta na svojih strežnikih nad okuženimi računalniki ali tako imenovanimi zombiji popoln nadzor, uporabljajo pa jih lahko za prej omenjene DDoS napade, okuževanje in vdore na spletne strani, vrivanje SQL stavkov, krajo osebnih podatkov, izsiljevanja, pošiljanje neželenih in ribarskih sporočil ter vse ostale nevarne dejavnosti. Svoja botnet omrežja preko spletnih forumov ponujajo celo v najem. Dejstvo je, da botneti postajajo vse večja težava. Zaenkrat je boj proti upravljavcem takšnih omrežij mogoč le s sodelovanjem strokovnjakov s področja informacijske varnosti, ponudniki internetnih storitev in predstavniki zakona (SI Splet 2009). Eno od bolj odmevnih takšnih prekritih omrežij v zadnjem času, je bil botnet Mariposa, ki je vseboval skoraj 13 milijonov okuženih računalnikov (Pandalabs 2010). Eden od ustvarjalcev tega botneta je bil tudi 23-letni Mariborčan.

[8] *botnet* - izraz izvira iz besed 'robot' ter 'network'.

Po podatkih spletne strani ATLAS je bilo v napadih na estonsko omrežno infrastrukturo udeleženih več takšnih botnet omrežij, ki so bila razpršena po celem svetu (Davis 2007).

4.3.2 Analiza napadov

Vse skupaj se je začelo le nekaj ur po tistem, ko so na ulicah izbruhnili nemiri. Konstantin Goloskov, član prokremeljskega političnega gibanja »Nashi« iz Moldavije, naj bi organiziral prvi val napadov (DDoS) na estonske internetne ponudnike in vladne strani. Vstopni internetni promet v Estonijo se je kar naenkrat zelo povečal (glej prilogo B). Sočasno so bila na ruskih blogih in forumih objavljena navodila, kako izvesti napade ICMP. Kasneje so ta navodila zbrali skupaj in jih objavili na spletnem naslovu (priloga C).

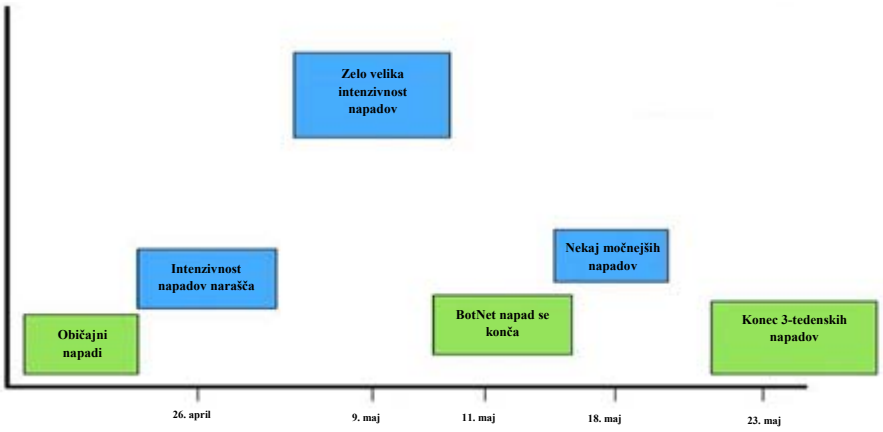
Drugi val napadov se je začel 30. aprila, ko so uporabniki portala Livejournal objavili seznam naslovov elektronske pošte (glej sliko 4.2) estonskih poslancev, ki so glasovali za odstranitev bronastega vojščaka in poziv, da seznam čim bolj razširijo po medmrežju. Sledilo je nešteto elektronskih sporočil, s ciničnim voščilom za dan zmage, ki ga v Rusiji v tem času praznujejo.

Slika 4.2: Naslovi elektronske pošte estonskih poslancev

Vir: Estonia cyber attacks (2007).

Rezultat je bil naslednji: parlamentarni strežnik je bil preobremenjen in nedostopen naslednja dva dneva. Hekerji so tudi vdrli na spletno stran Reformne stranke in objavili ponarejeno pisno opravičilo estonskega premierja za odstranitev bronastega kipa.

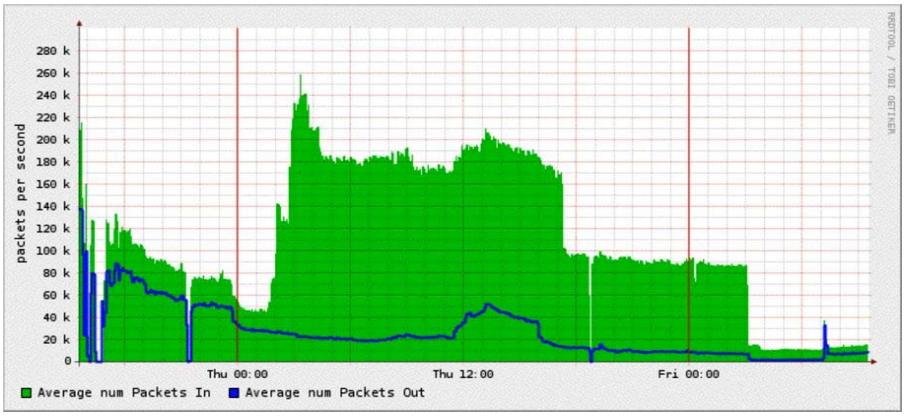
Slika 4.3: Časovnica napadov



Vir: Estonia cyber attacks (2007).

Napadi so dosegli vrh v obdobju med 3. in 9. majem. Napade je podkrepil govor ruskega predsednika Vladimirja Putina, ki se je na dan zmage na nacizmom zelo kritično opredelil do Estonije. V noči iz 8. na 9. maj se je začel zelo močan napad. Običajni podatkovni promet ob tej uri predstavlja približno 20.000 paketov na sekundo. Kar naenkrat pa je poskočil na 4 milijone podatkovnih paketov na sekundo in za 200-krat povečal obremenitev. Okrog milijon računalnikov po celem svetu je naenkrat poslalo zahtevke na estonske spletne strani. Kasneje so analize pokazale, da so bili to računalniki iz ZDA, Kanade, Brazilije in celo Vietnama (The Economist 2007). Do jutra se je promet umiril, čez dan pa je estonsko omrežje ponovno udarilo 58 napadov DDoS. Dve največji estonski banki sta morali za več ur prekiniti vse transakcije. Banka Hansabank je imela v nekaj dneh skoraj milijon dolarjev izgube. Močan napad DDoS se je nadaljeval do 11. maja, ko naj bi se po nekaterih podatkih iztekel »najem« botneta. Slika 4.4 prikazuje internetni promet na ta dan.

Slika 4.4: Internetni promet 11.5.2007



Vir: Estonia cyber attacks (2007).

Estonske spletne strani so bile napadene še z drugimi orodji, med drugimi tudi z vrivanjem SQL[9] stavkov (Traynor 2007). Napadalci vrivanje SQL izkoriščajo za krajo zaupnih podatkov, manipulacijo podatkov (tudi v obliki razobličenja spletne strani) ter kompromitiranje sistema. Nekatere spletne strani v Estoniji so bile razobličene (slika 4.5)

Slika 4.5: Razobličena spletna stran

Vir: Estonia cyber attacks (2007).

Uporabniki estonskih mobilnih omrežij pa so dobivali ponarejena SMS sporočila, ki naj bi jih pošiljala estonska vlada. Veliko vlogo pri teh napadih pa so odigrali tudi t.i. skriptarji[10] – gre za osebe, ki nimajo pretiranega računalniškega znanja, pač pa za vdore uporabljajo javno dostopna vdiralska orodja, ki so jih razvili drugi in podrobno sledijo navodilom.

Močnejši napadi so se končali do 18. maja. Vsi trije napadi skupaj so močno vplivali na infrastrukturo vseh estonskih omrežij – poškodovali so nekaj usmerjevalnikov, spremenjene so bile nekatere usmerjevalne tabele, preobremenjeni so bili strežniki DNS itd. Posledica tega je bila popolna neoperativnost parlamenta, skoraj vseh ministrstev, političnih strank, treh največjih medijskih hiš, dveh največjih bank, estonskega Telekoma (Nazario 2008). Skupaj so pri podjetju ATLAS našteli 128 unikatnih napadov DDOS (115 poplav ICMP, 4 napadi TCP SYN in 9 drugih napadov). Napadi so bili izvedeni na zelo različnih prenosnih povezavah, od manj kot 10 pa vse do 95 Mbit/s. Tri

[9] ang. SQL injection
[10] ang. Script kiddies

četrtine napadov ni trajalo več kot eno uro, 5,5 odstotkov pa jih bilo daljših od 10 ur (Svete in Pintarič 2008, 160).

Prebivalci Estonije so bili ob napadih presenečeni. Velik odstotek ni mogel opraviti nikakršnih transakcij – te so vse vezane na internet. Se pravi nekaj časa ni bilo možno opraviti na primer preprostih brezgotovinskih nakupov v trgovini ali na bencinski postaji. Nekaj časa je bila država dejansko paralizirana.

4.3.3 Obramba

Estonski obrambni minister Jaak Aaviksoo je takoj ob začetku napadov na pomoč poklical vodjo estonskega CERT-a. Ustanovili so krizno skupino v sodelovanju z profesionalnimi strokovnjaki IT iz vlade in gospodarstva. Po nekaj urah, ko so ugotovili razsežnosti napada, so zaprosili za pomoč zvezo NATO, ki je poslala na pomoč dva vodilna strokovnjaka s področja informacijskega bojevanja (The Economist 2007). Napadi so bili vsak dan bolj sofisticirani in so zlahka obšli filtre, ki so jih le nekaj ur pred tem napisali v Estoniji. Estonska skupina CERT je po standardni proceduri poskušala ugotoviti tri stvari: kje so viri napadov, katere tarče so trenutno na udaru in kje so glavni strežniki omrežij botnet (Evron 2007).

Prvi odziv Estoncev je bil sicer dokaj preprost, ampak drag – prekinili so vse dostope v njihovo omrežje iz tujine. To je zaustavilo 99 odstotkov zlonamernega prometa in dalo skupini CERT nekaj časa za razvoj obrambne strategije. Razvili so tudi napredne filtre, ki so uspeli začasno omejiti mednarodni promet. Nato so organizirali varni forum, na katerem so zbirali nasvete za obrambo vseh relevantnih strokovnjakov IT daleč naokoli. Poleg tega je omogočal estonski vladi aktualne informacije o napadih in varno komunikacijo s tujimi CERT-i ter drugimi varnostnimi skupnostmi (Evron 2007).

Pomembnejši korak za zaustavitev napadov je bila identifikacija in nato blokada botneta na korenskem strežniku. Za to so morali ugotoviti izvor prekritega omrežja. Za pomoč so tako zaprosili ponudnike internetnih storitev (ISP) po celem svetu, ki so postopoma blokirali posamezne okužene računalnike, ki so bili vključeni v botnet. Na takšen način so postopoma omejili grožnjo, napadalci pa bi morali za ponoven učinkovit napad uporabiti drug botnet, kar bi bilo dolgotrajno in drago. Sodelovanje estonskega CERT-a

z drugimi iz Nemčije, Finske in Slovenije se izkazalo za zelo učinkovito, saj so napadi po skupni akciji zelo hitro zamrli.

V retrospektivi Estonija ni bila kos množičnemu informacijskemu napadu. Ta je razkril nekatere strukturne ranljivosti in pokazal, kako pomemben je obstoj učinkovitega CERT-a. Prav tako pomembno je dojemanje interneta kot kritične infrastrukture, ki postaja enako strateško pomemben kot na primer elektrika ali voda (Davis 2007) .

Po tem ko so napadi zamrli, se je pojavilo vprašanje, kdo je pravzaprav stal za napadi. Strokovnjaki so si skupni v dveh stvareh – napad je bil zelo sofisticirane narave in zelo natančno usmerjen na ključno estonsko infrastrukturo. Estonski politiki so sicer zelo vehementno povezovali napade s Kremljem, a se je izkazalo, da so bili naslovi IP, ki so jih izsledili v Kremelj, zgolj okuženi računalniki, ki so sodelovali v botnetu kot milijoni drugih. Kakorkoli, napadi so bili neobičajni, ne toliko zaradi masovnega prometa, temveč zaradi zelo dobro koordiniranih napadov. Ostaja nejasno, kdo bi zapravil kar precejšnja finančna sredstva samo za izkaz nezadovoljstva ob odstranitvi bronastega vojščaka. Nekateri namigujejo, da za napadom stojijo vplivne ruske strukture, ki imajo povezave s FSB in FAPSI. Po nekaterih podatkih naj bi obveščevalne agencije po svetu konstantno preizkušale vladna omrežja in iskale slabosti, ki jih nato uporabljajo pri razvoju novih metod zbiranja informacij (McAfee Inc 2007). Mogoče je bil estonski primer prvi poizkus, kako onesposobiti celotno vladno infrastrukturo in je ruska oblast le raziskovala, kakšne bodo posledice. Ne nazadnje ne obstaja nobena veljavna zakonodaja, še posebej na mednarodni ravni, ki bi krila te napade. Kasnejše raziskave so pokazale, da vpletenost Kremlja ni verjetna in da je šlo bolj za »naključno« vojsko posameznikov, ki so povzročili kibernetske nemire.

Kakorkoli, Estonci so našli in dokazali estonskemu študentu Dmitriju Galushkevichu, da je v znak protesta iz svojega računalnika s pomočjo botneta sprožil napade DoS na Estonijo iz računalnikov po celem svetu. 20- letni Rus je tako postal prva oseba, ki je bila obsojena zaradi virtualnih napadov na Estonijo. Oglobljen je bil za 17,500 kron (£830), ker je blokiral dostop do spletne strani stranke estonskega premierja (BBC 2008). Drugačna pa je zgodba prej omenjenega Goloskova, saj so njegova dejanja po moldavskih zakonih popolnoma legalna, NATO in EU pa tam nimata pristojnosti. Seveda pa ga čaka drugačna zgodba, če se bo kdaj pojavil v kakšni državi članici.

5 NATO IN KIBERNETSKA POLITIKA

Čeprav je zveza NATO vedno skrbela za varnost lastnih informacijsko-komunikacijskih sistemov, neke širše razprave o kibernetski politiki ni bilo. Sredi leta 2002 je Severnoatlantski svet sprejel Kibernetsko-obrambni program (Cyber defence program). Ta je predvidel povečanje zmogljivosti za obrambo sistemov zavezništva pred kibernetski napadi. Kot del programa je bil ustanovljen NCIRC[11], ki bo popolne zmogljivosti dosegel leta 2012 (NATO 2010).

Pravi zagon je kibernetska politika doživela leta 2007 ob virtualnih napadih na državo članico – Estonijo. Iz perspektive zveze NATO je bil informacijski napad na Estonijo eden od zgodovinskih dogodkov v evoluciji zavezništva. Prvič se je zgodilo, da je država članica formalno zaprosila za pomoč pri obrambi pred digitalnimi napadi. Estonija je pomoč tudi dobila, na pomoč sta prišla dva vrhunska strokovnjaka IT, ki pa nista pomembno spremenila poteka dogodkov. Bolj pomembno je bila pritegnitev politične pozornosti. Na vrhu zveze NATO leta 2008 v Bukarešti je tako prvič prišlo do resne debate o odnosu zavezništva do kibernetske varnosti in revizije dogodkov v Estoniji (Hughes 2009).

V preteklosti je bila primarna skrb zavezništva fokusirana na varovanje lastnih komunikacijskih sistemov, sedaj pa se je ta, ob napadu na javne servise v Estoniji, preusmerila na države članice. To je pomenilo, da mora zveza razviti mehanizme za pomoč posameznim članicam, če v primeru napada zanjo zaprosijo. Rezultat vrha v Bukarešti je bila tako obveza, da bo zavezništvo okrepilo prizadevanja pri razvoju kibernetske obrambne politike.

Približno leto po Bukarešti je prišlo do pomembnih premikov tako na operativni ravni kot tudi strateški. V Bruslju je bil ustanovljen nov center za upravljanje kibernetske obrambe CDMA[12]. Namen centra je centralizacija operativne kibernetske obrambe zavezništva, glavna naloga pa koordinacija obramb članic v primeru virtualnih napadov. V centru so zbrani politični in vojaški predstavniki ter operativno-tehnično osebje s področja kibernetske varnosti. Pričakuje se, da se bo CDMA v prihodnjih letih razvil v

[11] NATO Computer incident response capability
[12] ang. Cyber defence management authority

t. i. vojno sobo s konkretnimi taktičnimi obrambami. Podrobneje pa bodo morali še izpopolniti sodelovanje le-tega z NCIRC. Pomembno je to, da sedaj države članice vedo, kako v primeru virtualnih napadov ukrepati in kam se obrniti (Hughes 2009).

Druga pomembna pridobitev, sicer bolj na strateški ravni, je Center odličnosti[13] za kibernetsko obrambo CCDCOE[14]. Center domuje v Talinu, kajti Estonija je uspešno iztržila status napadene žrtve. Formalno je bil ustanovljen maja 2008, popolno akreditacijo pri zvezi NATO pa si je pridobil oktobra. Trenutno pri projektu sodelujejo in ga tudi sponzorirajo naslednje države: Estonija, Litva, Latvija, Nemčija, Madžarska, Italija, Slovaška in Španija. Zaposlenih je okrog 30 strokovnjakov iz vseh sodelujočih držav. Če gre pri centru CDMA v Bruslju predvsem za telo koordinacijske narave, gre pri centru odličnosti za dolgoročni razvoj kibernetsko-obrambne politike in strategije. CCDCOE je takoj začel z raziskovanjem, kako lahko zavezništvo okrepi svoje kibernetsko-obrambne kapacitete. Med drugim, kot je razvidno iz uradne spletne strani, center organizira vrsto dogodkov, delavnic in konferenc, s katerimi zbira mnenja in nasvete širokega spektra udeležencev (Hughes 2009).

Zelo pomembno vlogo pri izvajanju kibernetske politike v zvezi NATO imajo nacionalni CERT-i. Čeprav trenutno po svetu deluje okrog 250 takšnih ekip, nekatere države članice na nacionalni ravni nimajo popolnoma razvitih. V zavezništvu velja za splošno sprejeto smernico, ki sicer ni formalna, da države članice ustanavljajo CERT-e. Ne nazadnje takšno infrastrukturo potrebuje Center za upravljanje kibernetske obrambe (CDMA) v Bruslju, če želi biti efektiven.

Mednarodno sodelovanje je zaradi transnacionalne narave kibernetske obrambe zelo pomembno. Vrh v Bukarešti je prinesel koncept Globalnega partnerstva. Govori o tem, da ni potrebno samo sodelovanje med državami članicami, temveč z vsemi regijami po svetu. Virtualni napadi so danes globalni in veliko le-teh prihaja tudi na primer s Kitajske. NATO pa vzdržuje tudi delovne stike z globalnimi družbami informacijske tehnologije, kot so Microsoft, Google, IBM ipd.

[13] Centri odličnosti so rezultat transformacije zveze NATO in prilagajanja na nove varnostne izzive. Odprti so za sodelovanje vseh držav članic, glavni namen pa je izboljšanje sodelovanja, razvoj doktrin itd.
[14] ang. Cooperative Cyber Defence Centre of Excellence

Aprila 2009 je bil vrh zveze NATO postavljen v Strasbourg/Kehl. Države članice so se dogovorile za pospešitev uvajanja kibernetsko-obrambne politike in čimprejšnjo uvajanje le-te v prakso ter še tesnejše sodelovanje zavezništva s partnerskimi državami. Izpostavili so tudi zahtevo po čimprejšnji zakonodaji, ki po pokrivala področje kibernetskih napadov (Hughes 2009).

Pred kratkim so predstavniki zveze NATO potrdili dejavnosti v razvoju Rapid-reaction timov (RRT), ki bodo na voljo državam članicam za obrambo pred kibernetskimi napadi. V letu 2007 in 2008 je NATO v Estonijo in kasneje Gruzijo poslal ekipe ad hoc, ki so zasledovale virtualne napade, enote RRT pa bodo na klic in v stalni pripravljenosti. Država članica bo morala za takojšnje posredovanje izraziti politično zahtevo zavezništvu. Zgodba bo malce drugačna za države nečlanice, saj bo moral posredovanje odobriti Severnoatlantski svet. Polno operativnost bodo enote RRT dosegle do leta 2012, sestavljene pa bodo iz kombinacije osebja zveze NATO in strokovnjakov iz držav članic. Enote bodo, v primeru da bodo poklicane na pomoč, delovale pod direktnim vodstvom napadene nacije (NATO Annual Report 2009).

6 ZAKLJUČEK

Globalizacija je naredila svet precej manjši, kot je nekdaj bil. Posamezniki, organizacije in vlade so vse bolj prepleteni in povezani, ne glede na to, kaj počnejo. Grožnje, ki se rojevajo na drugem koncu sveta, so lahko že naslednji trenutek pred našimi vrati. Poskusimo torej verificirati zastavljeno hipotezo, ki se glasi takole: *Internetne vojne, kot smo ji bili priča v Estoniji, bodo v prihodnosti vse pogostejše.* Verifikacija hipoteze je kompleksna in večplastna, zato pojdimo po vrsti. Nesporno dejstvo je, da brez informacijsko-komunikacijske tehnologije ni mogoče opravljati vsakodnevnih opravil. Kot navaja Ryan, imajo t. i. internetne vojne pet pomembnih značilnosti, ki bi lahko v prihodnosti revolucionarno spremenile konflikt: možnost razširitve obsega ofenzivnih dejanj, geografski doseg, prikritost, enostavno širjenje in učinek na cilje, ki so e-pripravljeni[15] (Ryan 2007).

Napadalec je v primeru internetne vojne opremljen s poceni in močno tehnologijo, ki pa ne zahteva nekega posebnega usposabljanja. Zato se lahko obseg ofenzivnih dejanj hitro razširi v neslutene razsežnosti. Praktično vsak posameznik, ki ima osnovno računalniško znanje in seveda dostop do interneta, lahko sodeluje v takšnih akcijah. To se je pokazalo tudi v Estoniji, kjer so veliko škode naredili skriptarji, se pravi amaterji, ki so sledili dokaj preprostim navodilom po forumih in blogih. Virtualni napadi nimajo praktično nobenih geografskih omejitev – Estonijo so napadali računalniki iz Brazilije in celo Vietnama. Škodo lahko povzročajo od koderkoli in to brez omembe vrednih finančnih sredstev. Ta so pomembna samo v primeru bolj sofisticiranih kibernetskih napadov, kot je na primer najem omrežja botnet. Ta pa omogočajo še eno pomembno lastnost internetnih vojn – je zelo prekrita, storilce pa je praktično nemogoče odkriti. Četudi bi do računalnika, ki nadzoruje botnet, prišli, bi pregon lahko oviralo dejstvo, da se računalnik nahaja na področju druge sodne pristojnosti. Lahko pa bi bil ta računalnik na anonimnem javnem mestu. Tudi v Estoniji do konkretnih odgovorov niso prišli. Uradno krivdo nosi 20-letni študent, čeprav je jasno, da sam napadov takšnih razsežnosti ni mogel organizirati. Problem je v tem primeru predstavljala Rusija, ne glede na to kakšna je bila njena vloga v konfliktu, ki za preiskavo ni pokazala niti najmanjšega interesa in tako onemogočila kakršnokoli nadaljnjo raziskavo. Napadalci

[15] Pojem označuje vpetost interneta v družbo, razvitost informacijske infrastrukture, uporabo virtualnih orodij pri državljanih in potrošnikih.

so pri virtualnih napadih tudi zelo inovativni in fleksibilni. To zelo dobro ponazarjajo napadi zavrnitve storitve (DoS). Princip napada je v osnovi zelo preprost, pa vendarle se je zelo težko obraniti.

Dejstvo je, da se bo učinek virtualnih napadov povečeval z vse večjo vpetostjo interneta v vsakdanje življenje. Vse več storitev lahko državljani že opravljamo prek informacijskih poti. Ne nazadnje sem to prikazal v enem od prejšnjih poglavij, kjer sem raziskoval Estonijo in tudi Slovenija se na lestvicah e-pripravljenosti uvršča dokaj visoko. Paradoks je torej ta, da bodo v prihodnosti najbolj na udaru tehnološko in informacijsko najbolj razvite države. Na podlagi vseh zgoraj naštetih dejstev potrjujem hipotezo, da bodo internetne vojne, kot smo ji bili priča v Estoniji, v prihodnosti vse pogostejše.

Ta ugotovitev nas vodi do verifikacije naslednje hipoteze: *Razvoj kibernetske obrambne politike v zvezi NATO in članicah je skladen z naraščajočo grožnjo.* Po vseh naštetih dejstvih, je potrebno redifinirati kibernetsko politiko. Kako to uspeva zvezi NATO?

Brez dvoma je kibernetska politika dobila pospešek z dogodki v Estoniji. NATO se je k sreči zavedel, da živimo v multipolarnem omrežnem svetu in to tudi po svoje izkoristil v procesu lastne transformacije. Poleg tega se je v zavezništvu spremenil koncept dojemanja informacijskih groženj. Do sedaj je bila primarna skrb zavezništva fokusirana na varovanje lastnih komunikacijskih sistemov, sedaj pa se je ta, ob napadu na javne servise v Estoniji, preusmerila na države članice.

Prvi rezultati pospešene kibernetsko-obrambne politike se tako že kažejo. Postavljena sta bila dva temelja. Z ustanovitvijo Centra za upravljanje kibernetske obrambe v Bruslju (CDMA) in enotami RRT v razvoju so se zgodili pomembni operativni koraki. Na doktrinarno-strateški ravni pa pomembno novost predstavlja Center odličnosti za kibernetsko obrambo (CCDCOE).

Hipotezo lahko, na podlagi zgoraj navedenih dejstev, tudi v tem primeru potrdim. Predvsem s konkretnimi spremembami na operativnimi ravni je zveza NATO pokazala zobe resnim kibernetskim grožnjam. Kako ostri pa so ti zobje, bo pokazala prihodnost.

Kljub napredku na področju kibernetsko – obrambne politike, je potrebno opozoriti na dve stvari. Ryan opozarja, da morajo biti temelj sodelovanja držav članic nacionalni

CERT-i. Izmenjava informacij na mednarodni ravni lahko omogoči zgodnje opozarjanje o sumljivih dejavnostih in profiliranje možnih napadov. Nekatere vlade so že naredile prve poteze, da se zaščitijo pred grožnjami internetne dobe, in so ustanovile nacionalne ekipe. Estonska ekipa CERT je bila ustanovljena leta 2006, mnoge vlade pa morajo to šele storiti.

Posebno vprašanje v domeni kibernetskih napadov je tudi vloga mednarodne zakonodaje. Zaenkrat je edini relevantni dokument Konvencija o kibernetski kriminaliteti, ki je bil sprejet pod okriljem Sveta Evrope. Gre za pomembno vprašanje, saj NATO težko legitimno deluje na področju brez pravih pravnih okvirov. Postavlja se vprašanje, kako danes razumeti kredo zavezništva – napad na enega je napad na vse. Na to vprašanje ni jasnega odgovora. Leta 1949, ko so to zapisali, se ni še nikomur sanjalo o kibernetskih napadih, zato bo moral predvsem NATO dati poziv za čimprejšnjo definicijo kibernetskih napadov in sprejetje ustrezne mednarodne zakonodaje. Ker mednarodnega dogovora, ki bi vseboval sprejete pravne predpise, po vsej verjetnosti še nekaj časa ne bo, mora NATO pristopiti k problemu kot k neposredni grožnji ter si prizadevati za vzpostavitev čim boljšega praktičnega obrambnega sodelovanja.

Naj zaključim z vprašanjem, s katerim sem začel to nalogo. Kako smo torej pripravljeni na kibernetsko prihodnost? Konkreten odgovor na to vprašanje je težko podati. Jasno pa je po mojem mnenju nekaj: internet so bo v prihodnosti prepletel z družbo v nove razsežnosti; t. i. internet 3.0 pa bo zato zahteval konkretno in predvsem usklajeno varnostno politiko.

7 LITERATURA

1. Arsić, Stanislav. 2004. Informacijsko vojskovanje – nevidni sovražnik. *Revija Obramba* 36 (12): 23–25.
2. BBC. 2008. *Estonia fines man for 'cyber war'.* Dostopno prek: http://news.bbc.co.uk/2/hi/technology/7208511.stm (24. september 2010).
3. Davis, Jashua. 2007. Hackers take down the most wired country in Europe. *Wired magazine*. Dostopno prek: http://www.wired.com/politics/security/magazine/15-09/ff_estonia (21. september 2010).
4. Delo.si. 2007. *Ruski hekerski napadi na estonske spletne strani?* Dostopno prek: http://www.delo.si/clanek/41831 (19. september).
5. Dnevnik.si. 2009. *Estonija upa na sedež nove agencije EU za področje informacijskih tehnologij.* Dostopno prek: http://www.dnevnik.si/novice/eu/1042364834 (17. september 2010).
6. --- 2010. *Estonija je predstavila načrt za zagotovitev širokopasovnega dostopa do interneta.* Dostopno prek: http://narocanje.dnevnik.si/novice/znanost/1042262330 (17. september 2010).
7. Dovč, Danica. 2005. *Uporaba oblik informacijskega bojevanja v sodobnem terorizmu: Primer teroristične organizacije PKK.* Diplomsko delo. Ljubljana: Fakulteta za družbene vede. Dostopno tudi prek: http://dk.fdv.uni-lj.si/dela/Dovc-Danica.PDF (3. september 2010).
8. Estonia Cyber Attacks. 2007. *Estonia Cyber Attacks.* Dostopno prek: www.africaasia.net/.../Estonia_cyber_attacks_2007_latest.ppt (29. september 2010).
9. EU Cybersecurity. 2009. *Cyber security and politically, socially and religiously motivated cyber attacks.* Directorate - general for external policies of the union. Dostopno prek: http://www.chathamhouse.org.uk/files/13346_0209_eu_cybersecurity.pdf (29. september 2010).
10. Evron, Gadi. 2008. *Battling Botnets and Online Mobs: Estonia's Defence Efforts during Internet War.* Dostopno prek: http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf (8. september 2010).
11. Hribar, Gašper. 2006. *Hekerska orodja.* Diplomsko delo. Ljubljana: Center za pošto, ekonomijo in telekomunikacije. Dostopno prek:

http://www.scpet.net/vss/at/diplome/Hribar%20Gasper_tk.pdf (12. september 2010).

12. Hughes, Rex. *NATO and Cyber Defence.* Cyber security project. Dostopno prek: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (27. september 2010).
13. IDI. 2009. *Measuring the Information Society - The ICT Development Index.* International Telecommunication Union. Dostopno prek: http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf (27. september 2010).
14. Juvan, Evridika. 2006. *Analiza kazalcev prehoda Evropske unije v informacijsko družbo.* Magistrsko delo. Ljubljana: Ekonomska fakulteta.
15. Kuehl, Dan. 2009. *From Cyberspace to Cyberpower.* Information Resources Management College/National Defense University. Dostopno prek: www.carlisle.army.mil/.../Cyber%20Chapter%20Kuehl%20Final.doc (27. september 2010).
16. Krulec, Rok. 2004. *Mrežni napadi onemogočitve servisov.* Dostopno prek: http://rok.fpp.edu/projects/dos_attacks/Mrezni%20napadi%20onemogocitve%20servisov%20-%20Denial%20Of%20Service%20attacks.html (11. september 2010).
17. Kalvet, Tarmo. 2007. *The Estonian Information Society Developments Since the1990s.* Praxis Center for Policy studies. Tallinn. Dostopno prek: http://www.ittk.hu/netis/doc/textbook/Estonian_country_report_final_est.pdf (17. september 2010).
18. Lisjak, Luka. 2007. *Primer Estonija ali zgrešeni model sobivanja.* Dextera et anima. Dostopno prek: http://dextersweblog.blogspot.com/2007/04/primer-estonija-ali-zgreeni-model.html (18. september 2010).
19. Libicki, Martin.1995. *What is Information Warfare?*. Washington D.C.: Institute for National Strategic Studies.
20. --- 2009. *Cyberdeterrence and cyberwar.* Rand Corporation. Dostopno prek: http://www.rand.org/pubs/monographs/2009/RAND_77.pdf (29. september 2010).
21. McAfee Inc. 2007. *Virtual criminology report. Cybercrime: the next wave.* Santa Clara. Dostopno prek: http://www.mcafee.com/us/research/criminology_report/default.html (22. september 2010).
22. NATO. 2010. *Defending against cyber attacks.* Dostopno prek: http://www.nato.int/cps/en/natolive/topics_49193.htm (22. september 2010).

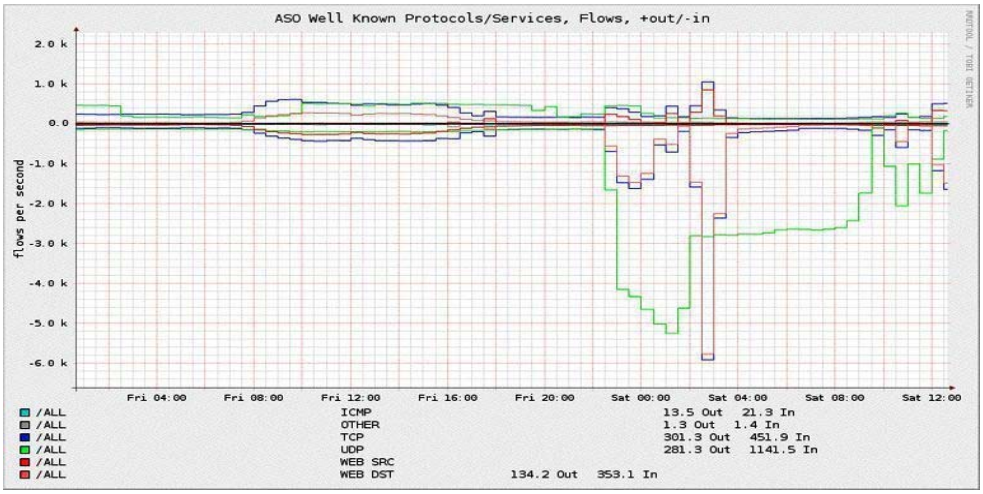
23. NATO Annual Report. 2009. *NATO and Cyber Defence.* Annual Session in Warsaw: Committee Reports. Dostopno prek: http://www.nato-pa.int/default.asp?SHORTCUT=1782 (29. september 2010).
24. Nazario, Jose. 2007. *Estonian DDoS Attacks – A summary to date*. Aarbor Networks. Dostopno prek: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ (24. september 2010).
25. Pandalabs. 2010. *Mariposa botnet*. Dostopno prek: http://pandalabs.pandasecurity.com/mariposa-botnet/ (15. september 2010).
26. PCMag.si. 2010. *Information warfare.* Dostopno prek: http://www.pcmag.com/encyclopedia_term/0,2542,t=information+warfare (27. september 2010).
27. Roman, Steve. 2008. *E-stonia.* American chamber of commerce. Dostopno prek: http://www.amcham.ee/failid/AmCham_EA_Fall_2008_content.pdf (15. september 2010).
28. Ryan, Johnny. 2007. "I-vojna": Nova grožnja, njena pripravnost – in naša vse večja ranljivost. *Revija NATO.* Dostopno prek: http://www.nato.int/docu/review/2007/issue4/slovene/analysis2.html (29 . september 2010).
29. SI Splet. 2009. *Omrežja okuženih računalnikov.* Dostopno prek: http://www.eset.si/news/pdf9/december_2009/SI_SPLETOmrezja_okuzenih_racunalnikov.pdf (13. september 2010).
30. Svete, Uroš. 2002. *Vloga in pomen informacijske tehnologije v sodobnem asimetričnem vojskovanju*. Magistrsko delo. Ljubljana: Fakulteta za družbene vede.
31. --- 2005. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
32. --- in Uroš Pinterič. 2008. *E-država: upravno-varnostni vidiki.* Nova Gorica: Fakulteta za uporabne družbene študije.
33. TechTerms.com. 2009. *ICT.* The tech term computer dictionary. Dostopno prek: http://www.techterms.com/definition/ict (27. september 2010).
34. Traynor, Ian. 2007. *Russia accused of unleashing cyberwar to disable Estonia.* Guardian magazine. Dostopno prek: http://www.guardian.co.uk/world/2007/may/17/top3.russia (25. september 2010).
35. The Economist. 2007. *A cyber-riot Estonia and Russia.* Dostopno prek: http://www.economist.com/node/9163598 (21. september 2010).

8 PRILOGE

Priloga A: Bronasti kip neznanega vojščaka

Vir: The Economist (2007).

Priloga B: Primerjava vstopnega (negativne vrednosti) in izstopnega internetnega prometa (pozitivne vrednosti) na dan 27.4.2007



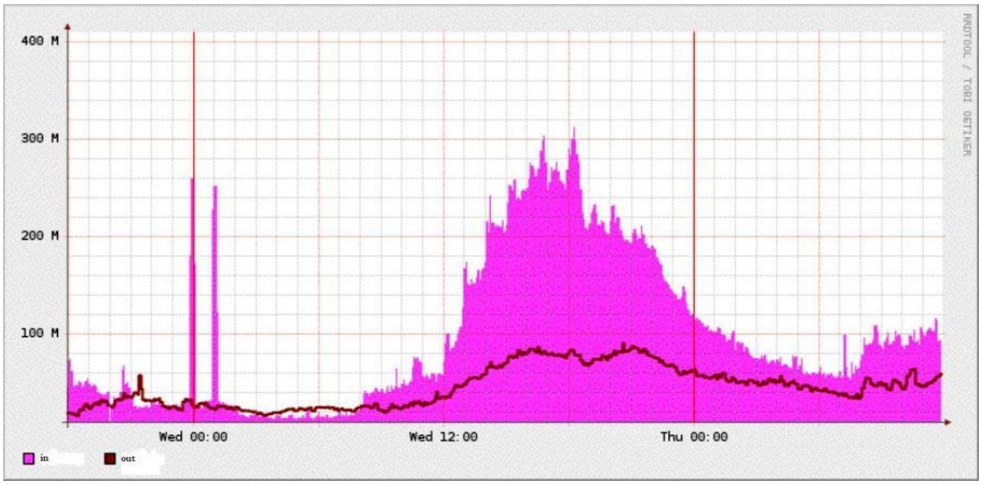
Vir: Estonia cyber attacks (2007).

Priloga C: Navodila za napad ICMP poplav, objavljena na spletni strani http://fipip.ru/raznoe/pingi.bat

```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.56.245
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.133.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.online.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.106.96.21
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.1
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.99
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uu.net
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 137.39.1.3
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% sunic.sunet.se
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 192.36.125.2
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% muheleja.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.132
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.12
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% smtp.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.4
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ptah.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.aso.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.96.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.76
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% mail.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.kul.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.envir.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.mil.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.ema.edu.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.ehi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.ebs.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% est.ttu.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.infoatlas.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.zzz.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.er.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.estonica.org
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.insidebaltics.com
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.n-m.ru
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.balticmarkets.com
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.export.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% www.investinestonia.com
GOTO PING
```

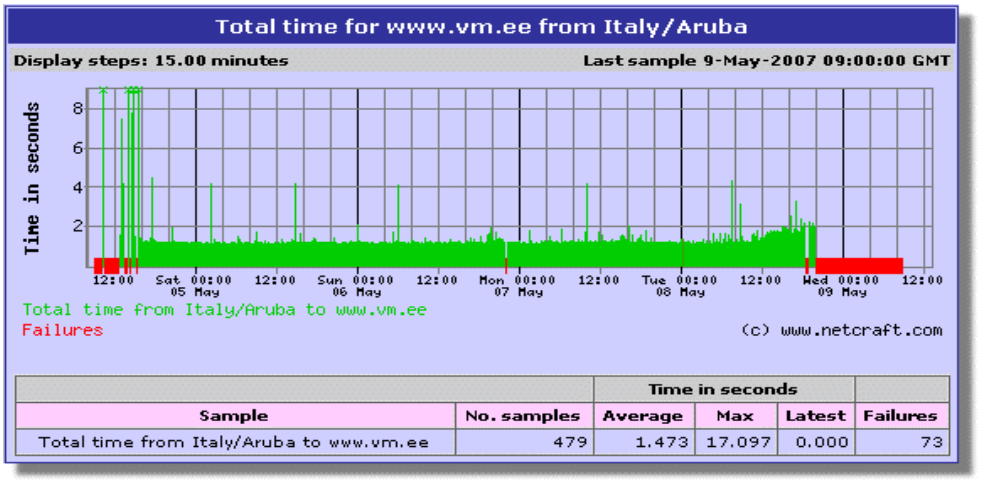
Vir: Estonia cyber attacks (2007).

Priloga Č: Internetni promet 2. maja 2007



Vir: Estonia cyber attacks (2007).

Priloga D: Dostop do estonskih spletnih strani iz Italije (časovna komponenta) na dan 9. maja. Rdeča barva prikazuje nedostopnost spletne strani zaradi botnet napada



		Time in seconds			
Sample	No. samples	Average	Max	Latest	Failures
Total time from Italy/Aruba to www.vm.ee	479	1.473	17.097	0.000	73

Vir: Estonia cyber attacks (2007).