Kapittel 3: Russiske tenestenektåtak (DDoS) som politisk verkemiddel i Estland og Georgia

Mass Soldal Lund

26. april 2007 braut det ut opptøyar i gatene i sentrum av Estlands hovudstad Tallinn. Det som hadde starta som ein fredeleg protest mot flyttinga av eit krigsmonument frå Sovjet-tida, utarta utover kvelden og natta til hærverk, vandalisering og kampar med politiet. I alt 1 300 personar blei arresterte, og rundt hundre personar vart skadde i opptøyane, for éin med døyeleg utgang. Kvelden etter – 27. april – flytta hærverket seg over til cyberdomenet, og web-sider som høyrde til estiske myndigheiter, vart utsett for såkalla tenestenektåtak. Dette var starten på ei tre veker lang kampanje av åtak mot internettenester i Estland. (Ottis, 2013, s. 121–122; Tikk et al., 2010, s. 15–16) Året etter vart Georgia utsett for liknande åtak. I morgontimane 8. august 2008 starta omfattande tenestenekt mot georgiske web-sider. Det er ingenting som tydar på at tidspunktet var tilfeldig; natt til 8. august hadde russiske styrker kryssa grensa til Georgia for å forsvare utbrytarrepublikken Sør-Ossetia mot georgiske forsøk på å få tilbake kontroll over utbrytarane. Cyberåtaka, som ramma det georgiske statsapparatet, media og bankvesenet, heldt fram parallelt med den militære konflikten, men dabba av etter at våpenkvile var inngått fem dagar seinare (Laaneots, 2014/2016, s. 60; Tikk et al., 2010, s. 69–70).

Tenestenekt er ein enkel og relativt primitiv form for maktutøving gjennom cyberdomenet. I eit distribuert tenestenektåtak (engelsk: Distributed Denial of Service; DDoS) er målet å overbelaste ein internettbasert ressurs eller teneste, til dømes ei web-side, for på den måten gjere ho utilgjengeleg for dei tiltenkte brukarane. I si enklaste form kan dette vere overdriven bruk av ei teneste, til dømes ved å generere så mange førespurnadar til ei web-side at tenaren ikkje er i stand til å respondere, men det finst òg tenestenektåtak som utnyttar svakheiter i internett-teknologien.[1] Ved å få mange deltakarar til å bruke ei programvare som sender førespurnadar til målet, eller ved hjelp av eit nettverk av kompromitterte datamaskiner – eit såkalla botnett – kan ein generere så stor datatrafikk at tenesta ikkje er i stand til å ta unna. Ordet *distribuert* siktar til at åtaket kjem frå mange ulike stadar på ein gong, noko som gjer det både vanskelegare å spore og vanskelegare å verne seg mot (Brooks et al., 2022, s. 44–46; Grindal 2022, s. 30–31).

Distribuerte tenestenektåtak oppstod på midten av 1990-talet som ei form for politisk protest. Dei fyrste åtaka var organisert av kunstnar- og aktivist-nettverka Strano Network og Electronic Distrubance Theater og retta seg mot franske og mexicanske web-sider, høvesvis i protest mot franske atomprøvesprengingar og til støtte for den mexicanske zapatisit-rørsla (Grindal, 2022, s. 32–39). Seinare har særleg hackarnettverket Anonymous vore forbunde med tenestenektåtak. Dei utførte ei

[1] Eit eksempel på eit meir avansert tenestenektåtak er såkalla SYN-flaum-åtak. Åtakaren vil initiere nettverkssesjonar mot tenaren, men avbryte før sesjonen er etablert og dimed tvinge tenaren til å nytte ressursar på å handtere eit stort tal avbrotne oppkoplingar.

Referanse: Lund, M. S. (2024). Russiske tenestenektåtak (DDoS) som politisk verkemiddel i Estland og Georgia. I V. R. Berrefjord & M. S. Lund (Red.), *Cybermakt – en tverrfaglig innføring* (s. 61–79). Universitetsforlaget.

rekkje profilerte og politisk motiverte kampanjar mellom 2008 og 2012, til dømes OpTunisia i 2011 der tunisiske myndigheiter vart utsett for tenestenektåtak og andre primitive formar for cyberåtak til støtte for den folkelege demokratirørsla i landet (Coleman, 2014, s. 143–165). Utover 2010-talet forsvann tenestenekt i stor grad som politisk protest og vart i større grad eit verkemiddel for utpressing utført av kriminelle organisasjonar ved hjelp av botnett. Men etter Russlands invasjon av Ukraina i starten av 2022 ser tenestenekt og andre formar for aktivistisk utnytting av cyberdomenet ut til å ha fått ein renessanse (Brooks et al., 2022, s. 44–50; Burgess, 2022b).

Dei to tenestenektkampanjane i Estland i 2007 og Georgia i 2008 har i ettertida fått ein spesiell status. I båe tilfella har Russland blitt peika på som aktøren bak åtaka, og dei vert ofte sett som cyberåtak utført av ein stat for å påverke ein annan stat. På den måten kan tenestenektåtak utgjere ei form for hard cybermakt. Samtidig, på grunn av innslaget av aktivistiske grupperingar, er det er ikkje naudsynleg så enkelt. Dette kapittelet vil sjå nærmare på dei to hendingane. Gjennomgangen vil leggje vekt på det politiske bakteppet for cyberåtaka, vil sjå på kva som var konsekvensane av åtaka, og vil stille spørsmålet om kva ein kan seie om kven som stod bak åtaka. Kapittelet vil deretter drøfte tenestenektåtaka som verkemiddel i konflikt, spesielt i lys av teoriar om informasjonskrigføring og politisk krigføring. Til slutt vil kapittelet sjå på likskapar og skilnadar med den russiske invasjonen av Ukraina i 2022, der tenestenektåtak (i volum og det å vere synleg) har blitt den dominerande forma for maktbruk i cyberdomenet.[2]

Estland 2007

Estland har ei lang og turbulent historie med Russland. Landet vart innlemma i det russiske keisardømet i 1720, men utkjempa i etterdønningane etter fyrste verdskrigen og den russiske revolusjonen i 1917 ein frigjeringskrig som leidde til sjølvstende i 1920. Sjølvstendet varte i berre 20 år, til Estland under andre verdskrigen fyrst vart okkupert av Sovjetunionen i 1940 og deretter av Tyskland i 1941. Mot slutten av krigen vart Estland igjen okkupert av sovjetiske styrkar i 1944 – og vart innlemma i Sovjetunionen som sovjetrepublikk. Frå midten av 1980-talet vaks kravet om sjølvstende. Ei folkerøysting våren 1991 viste 78 prosent fleirtal for å forlate Sovjetunionen, og i august same år fekk Estland igjen sjølvstende. Landet orienterte seg raskt mot Vesten. Ein ny demokratisk grunnlov etter vestleg modell vart vedteken i 1992, og Estland vart medlem av EU i 2003 og av NATO i 2004 (Bærug, 2021; Lurås & Seim, 2021).

[2] Hovudkjeldene for skildring av hendingane i Estland er Ottis (2013), Tikk et al. (2010, s. 14–34) og Schmidt (2013). For hendingane i Georgia er hovudkjeldene Cohen og Hamilton (2013) og Laaneots (2014/2016) for den militære konflikten og Hagen (2013) og Tikk et al. (2010, s. 66–90) for cyberåtaka. *Store norske leksikon (snl.no)* er nytta for å kvalitetssikre historiske opplysingar. Hendingane i Ukraina er openbert av nyare dato, og det har difor vore naudsynt å i større grad nytte seg av rapportar frå medium og sikkerheitsselskap.

I 1947 vart ein krigsgrav og eit minnesmerke over den sovjetiske Raude arméens siger over Nazi-Tyskland etablert i sentrum av Estlands hovudstad Tallinn. Minnesmerket, kjent som Bronsesoldaten, vart av mange estarar oppfatta som eit symbol på den sovjetiske okkupasjonen. For delar av den store russiskspråklege minoriteten[3] var det derimot eit symbol for sigeren over og frigjeringa frå nazismen. Etter 1991 heldt minnesmerket fram som samlingspunkt for russiskspråklege estarar på merkedagar for andre verdskrigen, men vart utover 2000-talet i aukande grad også eit samlingspunkt for russisk nasjonalisme. Etter konfrontasjonar mellom russisktalande og konservative estarar i 2005 kom det forslag om å flytte Bronsesoldaten frå sentrum av Tallinn, og dette vart også ei av hovudsakene i det estiske parlamentsvalet på våren 2007. Forslaget vart fordømd av russiske myndigheiter (Ottis, 2013, s. 121–122; Schmidt, 2013, s. 174–176; Tikk et al., 2010, s. 15–16). Ein del av bakteppet er òg, som påpeika av Herzog (2011, s. 50–51), den sovjetiske «russifiseringspolitikken» med flytting av hundretusenvis av russarar til Estland, med ein påfølgjande marginalisering av russisktalande etter 1991.

Etter valsiger for den konservative koalisjonen i parlamentsvalet bestemte den estiske regjeringa at minnesmerket og krigsgravene skulle flyttast til ein militær gravplass i utkanten av Tallinn. 26. april vart området gjerda inn som førebuing til flyttinga av statuen og opning av gravene. Dette førte til protestar frå russisktalande estarar, som utover kvelden og natta utvikla seg til valdelege opptøyar. Som eit svar på opptøyane vart fjerninga framskynda, og Bronsesoldaten vart midlertidig plassert på ein hemmeleg plass alt på kvelden og natta 27. april (Ottis, 2013, s. 121–122; Schmidt, 2013, s. 174–176; Tikk et al., 2010, s. 15–16).

Tenestenektåtak

Rundt kl. 22 på kvelden 27. april 2007 – same kveld som Bronsesoldaten vart flytta – kom estiske internettenester under åtak. I laupet av dei to neste dagane vart web-sidene til regjeringa, statsministerens kontor, fleire departement, parlamentet og einskilde nyhendesider utsett for tenestenektåtak. 28. april var regjeringas internettsider nede samanhengande i åtte timar. I tillegg vart også statsministeren og andre leiande politikarar spamma med e-post, og e-posttenesten til det estiske parlamentet vart midlertidig stengt ned. Åtaka, som varte til 29. april, var teknisk relativt usofistikerte. Instruksjonar om korleis ein kunne nytte si eigen datamaskin og internettkopling til å delta i åtaka, vart posta på russiske internettforum og spreidd gjennom chatte-kanalar.[4] Det er difor ei implisitt antaking om at den fyrste fasen av åtaka vart utført av aktivistar, altså ei stor gruppe einskildpersonar som fylgde instruksjonar eller oppskrifter som sirkulerte på internett (Schmidt, 2013, s. 176–177; Tikk et al., 2010, s. 18–20).

[3] Ifølgje Lundbo (2021) var 29,6 % av Estlands befolkning russiskspråkleg i 2011.
[4] Gjerne omtala som IRC-kanalar etter Internet Relay Chat (IRC), det føretrekte chattesystemet mellom hackarar på den tida.

Den andre fasen av åtaket starta 30. april og varte til 18. mai. Gjennom desse to og ein halv vekene heldt åtak av same type som i fyrste fase fram. Samtidig kom det nye og kraftigare åtak. I fire bølgjer eller toppar – 4. mai, 9.–11. mai, 15. mai og 18. mai – vart web-sidene til estiske myndigheiter, finansinstitusjonar og nyhendemedium utsett for tenestenektåtak utført ved hjelp av botnett. På det meste var internettrafikken mot estiske myndigheiter 400 gonger høgare enn normalen. Av dei mest synlege konsekvensane hadde nettbankane til to av dei største bankane i Estland nedetid: Hansapank i 1,5–2 timar på 9. og 10. mai, og SEB Eesti Ühispank i 1,5 time på 15. mai. Den andre fasen skilte seg òg ut ved at også delar av internettinfrastrukturen var under åtak. Dette skjedde på to måtar som båe har potensial til å hindre internettkommunikasjon. Estiske namnetenarar vart utsett for gjentekne åtak, og namnetenesten (DNS) vart slått ut i kortare periodar i delar av landet.[5] Det var òg forsøk på å slå ut sårbare ruterar,[6] noko som råka visse system som var avhengige av nettverkstilkobling, slik som minibankar og kortterminalar (Greenberg, 2019, s. 82–85; Ottis, 2013, s. 123–124; Schmidt, 2013, s. 181–183, 189; Tikk et al., 2010, s. 18–22).

Både estiske og internasjonale IKT-sikkerheitsmiljø klarte å føresjå dei kommande åtaka i den fyrste fasen ved å følgje med på russiske hackar-forum. I tillegg hadde myndigheitene høgt medvit om IKT-sikkerheit etter å ha gjennomført elektronisk val (røysting over internett) som ein del av parlamentsvalet to månadar tidlegare. Alt 28. april vart cyberåtaka erklært som ei nasjonal krise. Det vart raskt sett ned ei responsgruppe leia av det estiske nasjonale datasikkerheitssenteret CERT-EE og med representantar frå ulike departement, forsvaret og etterretningsmiljøa.[7] Det kom også raskt på plass eit ad hoc-samarbeid med estiske internettleverandørar, teleoperatørar og bankar som delte informasjon og hjelpte til med handteringa. Internasjonalt fekk CERT-EE støtte frå systerorganisasjonane i Tyskland (CERTBund), Slovakia (SI-CERT) og spesielt Finland (CERT-FI). Denne konstellasjonen freista å motverka åtaka ved å oppskalere kapasiteten i nettverk og tenarar, og ved filtrering av nettverkstrafikken. Datatrafikken var likevel for stor til at det var mogleg å stå i mot, og løysinga vart til slutt å stenge all internettrafikk frå utlandet (Greenberg, 2019, s. 82–85; Schmidt, 2013, s. 178–181, 183–186, 189; Tikk et al., 2010, s. 24).

Konsekvensar

Det finst ulike vurderingar av storleiken på konsekvensane av åtaka mot Estland. Tikk et al. (2010, s. 24–25) legg vekt på at Estland alt i 2007 hadde kome langt i å digitalisere innbyggjaranes kommunikasjon med myndigheitene. Når statlege internettportalar og e-posttenarar var under åtak, vart såleis innbyggjaranes moglegheit til å kommunisere med myndigheitene avgrensa. Til dømes var

[5] Domain Name System (DNS) er ei teneste for omsetjing av web-adresser til internettadresser som vert nytta når ein vil kople seg mot ein web-tenar for å vitje ei web-side. Dette systemet er bygd opp av eit hierarki av såkalla namnetenarar.
[6] Ruterar er sentrale komponentar som dirigerer trafikken i eit datanettverk.
[7] CERT er ei forkorting for Computer Emergency Response Team og er ei nemning for ein dedikert organisasjon eller gruppe personar med ansvar for å forhindre, detektere og handtere cybersikkerheitshendingar på lokalt eller sentralt nivå (Ruefle et al., 2014).

det i periodar ikkje mogleg å rapportere skatt. Som nemnt førte åtak på nettbankane til to av Estlands store bankar til at mange estarar i periodar på 1,5–2 timar var avskore frå banktenester. Tikk et al. (2010, s. 25) konkluderer med at åtaka «may have had undesirable effects for parts of the population that went beyond mere inconvenience and also caused material damange or loss». Konklusjonane til Schmidt (2011, s. 182, 186–187, 190–191) er at Estland vart usett for eit relativt moderat tenestenektåtak; dei økonomiske konsekvensane var små og stort sett relatert til hendingshandteringa, og åtaka «had only a relatively mild direct impact on Estonian society». Men han konkluderer òg med at den estiske responsen (som skildra over) var medverkande til at konsekvensane ikkje var større.

Tikk et al. (2010, s. 25) peikar også på ein annan type konsekvens av åtaka. Det at åtaka råka myndigheitenes informasjonskanalar på internett, samt estiske medium, kan ha svekka moglegheitene til å formidle det estiske synet på konflikten rundt flyttinga av Bronsesoldaten til internasjonale medium og opinion. Frå eit slikt utgangspunkt går Valieriano og Maness (2015, s. 148) så langt som å antyde at den største skaden av åtaka var sjølvforskyldt av estarane når dei internasjonale internettkoplingane vart stengte.

Det estiske samfunnet kom seg gjennom prøvingane, og ein kan argumentere for at for Estlands del var dei viktigaste konsekvensane politiske. Åtaka og den påfølgjande ordkrigen bidrog til å forsure forholdet mellom Estland og Russland, og landet vart dytta ytterlegare bort frå Russland og nærare dei vestleg allierte. Åtaka bidrog også til å konsolidere det estiske forsvaret mot cyberåtak, og til at Estland i etterdønningane bygde seg opp som eit føregangsland for cybersikkerheit. Hendingane i den nye NATO-medlemmen gjorde også at cyberforsvar vart sett på agendaen i NATO (Richards, 2014, s. 35; Schmidt, 2013, s. 190–193). Dei folkerettslege sidene ved åtaka er handsame av Lein, Moe og Bjørvik i kapittel 10 i denne boka.

Kven stod bak?

Estiske myndigheitspersonar var raskt ute med å skulde russiske myndigheiter for åtaka, medan dei på sin side har nekta å ha hatt noko med åtaka å gjere (Schmidt, 2011, s. 188). Mellom desse to ytterpunkta finst det ulike vurderingar av i kva grad russiske myndigheiter må ha vore involverte. Opphavet til åtaka og samanfall i tid med opptøyane i Tallinn synest å etterlata liten tvil om at dei var politisk motiverte og direkte relaterte til flytting av Bronsesoldaten. I den fyrste fasen var åtaka organisert gjennom russiske hackarforum og chatte-kanalar, og utført av aktivistar. I den andre fasen var åtaka utført ved hjelp av botnett og var tilsynelatande betre koordinert enn i den fyrste fasen (Tikk et al., 2010, s. 23–24). Botnetta var styrte av kriminelle organisasjonar, som må ha stilt dei til disposisjon med eller utan vederlag. Valeriano et al. (2019, s. 126) tek det for gjeve at «the Kremlin was involved in the second wave», der argumentet synest å vere at «the incidents needed the organization of many skilled operatives, working on coordination and with a clear motive» (Valeriano

& Maness, 2015, s. 147). Dei trekk i tillegg fram nære relasjonar mellom russiske hemmelege tenester og kriminelle nettverk, og spesielt organisasjonen Russian Business Network (RBN) som var ein av «botnett-tilbydarane» som vart mistenkt å ha bidrege i åtaka (Greenberg, 2019, s. 83; Valeriano et al., 2019, s. 112, 115–117). På den andre sida kan ein ikkje slutte beinveges frå observasjonen at åtaka må ha hatt organisering, finansiering og motivasjon, til at «the actions were directed by the state», slik Valeriano og Maness (2015, s. 147) formulerer det. Korkje Ottis (2013, s. 127) eller Schmidt (2011, s. 188–191) finn det bevist at «Kreml stod bak». Derimot finst det klare indikasjonar på at Kreml lét åtaka skje, og dermed gav eit stillteiande samtykke. Russiske myndigheiter gav heller ingen politisk eller teknisk bistand til å stoppe åtaka, og dei avslo i etterkant å assistere etterforsking og å utlevere personar i Russland som estiske myndigheiter meiner var involverte i åtaka. Det at Russlands president Vladimir Putin – i ein tale 9. mai, på ei minnemarkering for andre verdskrigen – fordømte flyttinga av Bronsesoldaten medan tenestenektåtaka framleis gjekk føre seg, har blitt tolka som ei indirekte velsigning (Ottis 2013, s. 126–129; Schmidt, 2013, s. 189–190).

Georgia 2008

Georgia vart innlemma i Det russiske keisardømet i 1801, men braut ut i 1918 i etterdønningane etter den russiske revolusjonen. I 1921 vart Georgia invadert av den Raude arméen og deretter innlemma i Sovjetunionen som sovjetrepublikk. Som Estland erklærte Georgia sjølvstende i 1991, men har hatt ei meir turbulent reise etter Sovjetunionens fall (Bærug et al., 2022; Filseth & Thordarson, 2021; Laaneots, 2014/2016, s. 9–19).

I 1991 hadde Georgia tre etnisk baserte autonome regionar som no søkte sjølvstende: Adsjaria, Abkhasia og Sør-Ossetia (sjå kart i Figur 1). Etter ein turbulent periode oppnådde utbrytarane uavhengigheit frå det georgiske styresmaktene i Tbilisi i laupet av 1990-talet. Ingen av dei tre utbrytarrepublikkane vart internasjonalt anerkjent, men sjølvstende var garantert av Russland. For Abkhasia og Sør-Ossetia tok dette form av fredsavtalar framforhandla av Russland og som innebar utplassering av russiske fredsbevarande styrkar under det russiskdominerte Samveldet av uavhengige statar (SUS) som Georgia hadde gått med i etter Sovjetunionens fall. Russland gav militær og politisk støtte til utbrytarane og starta i 2002 ein kampanje med å dele ut russisk statsborgarskap til innbyggjarane i utbrytarrepublikkane (Cohen & Hamilton, 2013, s. 51; Laaneots, 2014/2016, s. 9–24).

Figur 1: Georgia og utbrytarrepublikkar[8]

Spenninga mellom Georgia og Russland auka utover 2000-talet. Etter den såkalla Roserevolusjonen i 2003 vart den vestlegorienterte Mikhail Saakasjvili vald til president. Det nye styret under Saakasjvili førte ein aktiv samlingspolitikk og ønskte medlemskap i NATO, medan Russland utstasjonerte militære styrker i både Abkhasia og Sør-Ossetia. Hausten 2007 trakk Russland uventa styrkane sine frå Sør-Ossetia og stod igjen berre med ein mindre fredsbevarande styrke under SUS. Samtidig sendte dei fleire styrkar til Abkhasia. Forholdet mellom Russland og Georgia vart forverra av at NATO-toppmøtet i april 2008 stadfesta at Georgia var kandidat for medlemskap (Cohen & Hamilton, 2013, s. 49, 60; Laaneots, 2014/2016, s. 18–37).

Russland gjennomførte i juli 2008 ei større militærøving – Kavkaz 2008 – mot grensa til Sør-Ossetia. Samtidig starta ei bølgje av nesten daglege åtak og provokasjonar frå sør-ossetiske styrkar mot georgiske landsbyar, politi og fredsbevarande styrkar i Sør-Ossetia. 8. august gjekk georgiske styrkar inn i Sør-Ossetia for å sikre georgiske landsbyar og opna også artillerield mot den sør-ossetiske hovudstaden Tskhinvali. Det uttalte målet var å vinne att kontroll med regionen. Russland hadde framleis styrkar frå Kavkaz 2008 på nordsida av grensa og svarte beinveges med å invadere Sør-Ossetia. Berre få timar seinare var russiske styrker på veg gjennom den strategiske viktige Roki-tunnelen – den einaste grenseovergangen mellom Russland og Sør-Ossetia, som delar grense i fjella i Store Kaukasus (Cohen & Hamilton, 2013, s. 60–63; Laaneots, 2014/2016, s. 32–37).

Dette var starten på ein fem dagar lang væpna konflikt. Dei georgiske styrkane var betre utstyrt og trena, men vart raskt slått tilbake av ein numerisk overlegen russisk motstandar. Den georgiske

[8] Adaptert frå *Georgia location map*, av NordNordWest, 2009, Wikimedia Commons (https://commons.wikimedia.org/wiki/File:Georgia_location_map.svg). CC BY-SA 3.0.

militære leiarskapen var uerfaren og hadde store utfordringar på det operasjonelle nivået. Den politiske leiarskapen blanda seg inn i kommandokjeda, og georgiarane hadde ikkje ein ordentleg utarbeidd operasjonsplan då dei gjekk inn i Sør-Ossetia. På grunn av ekstensiv russisk jamming av georgiaranes kommunikasjonssystem braut den georgiske kommandokjeda i praksis saman, og den georgiske militære leiinga var ikkje i stand til å koordinere bakkestyrkane så lenge stridigheitene varte (Cohen & Hamilton, 2013, s. 62–77; Laaneots, 2014/2016, s. 50–78).

12. august hadde Russland kontroll over Sør-Ossetia og hadde oppretta ei sikkerheitssone rundt utbrytarrepublikken. Parallelt hadde georgiske militære styrkar og politi som hadde hatt kontroll over delar av den andre utbrytarrepublikken Abkhasia, blitt omringa og overgjeve seg. Russiske styrkar tok seg frå Abkhasia til den georgiske hamnebyen Poti ved Svartehavskysten og øydelagde den georgiske marineflåten som låg til hamn der. På kvelden 12. august aksepterte den georgiske presidenten Saakasjvili eit russisk forslag til våpenkvile (Cohen & Hamilton, 2013, s. 62–77; Laaneots, 2014/2016, s. 50–78).

Tenestenektåtak

Omtrent på same tid som russiske styrkar invaderte Sør-Ossetia, starta ei bølgje av åtak mot georgiske web-sider. Som i Estland var åtaka ein kombinasjon av tenestenektåtak utført av aktivistar og tenestenektåtak utført ved hjelp av botnett. Dei patriotiske hackarane som tok del i åtaket, fekk instruksjonar, verktøy og lister over mål gjennom russiskspråklege web-sider som StopGeorgia.ru, StopGeorgia.info og xaker.ru (hacker). Til skilnad frå Estland var det aktive botnett med frå starten, og analysar tyder på at i alt seks ulike botnett vart nytta i åtaka (Hagen, 2013, s. 196–203; Tikk et al., 2010, s. 69–71).

Mål for åtaka var web-sidene til georgiske myndigheiter, georgiske nyhendesider og nyhendeportalar, og dessutan Georgias største bank. I tillegg til tenestenekt vart georgiske web-sider utsett for såkalla «website defacement». Det er eit todelt åtak der ein fyrst skannar ei web-side for sårbarheiter, for deretter å utnytte eventuelle sårbarheiter til å få kontroll over sida og endre innhaldet i ho. På den måten vart web-sidene til den georgiske presidenten, nasjonalbanken og utanriksdepartementet endra til ein kollasj av bilete som samanlikna Saakasjvili med Hitler (Hagen, 2013, s. 197–198; Tikk et al., 2010, s. 71).

Det største volumet av åtak varte i fire dagar fram til 12. august. Dei åtaka som var utført av botnett, slutta samtidig som våpenkvila vart inngått, medan åtak utført av aktivistiske hackarar heldt fram til 28. august. Det har òg blitt registrert eit tenestenektåtak som 19. juli, med andre ord to og ei halv veke før den væpna konflikten, tok ned web-sidene til den georgiske presidenten i 24 timar (Greenberg, 2019, s. 91–92; Hagen, 2013, s. 197; Tikk et al., 2010, s. 69–71).

Georgia hadde ikkje noko nasjonalt datasikkerheitssenter eller nokon annan statleg funksjon som kunne koordinere eit forsvar mot cyberåtaka. Organisasjonen som til vanleg hadde ansvar for datasikkerheita til Georgias høgre utdanningsinstitusjonar, vart difor oppgradert til nasjonalt datasikkerheitssenter – CERT Georgia. Dei fekk ansvar for handteringa og fekk støtte får CERT-ane i Polen, Frankrike og spesielt Estland (Hagen, 2013, s. 199; Tikk et al., 2010, s. 76).

Den georgiske internettinfrastrukturen gjorde forsvaret vanskeleg. Georgia hadde på det tidspunktet ikkje eit eige Internet exchange point (IXP), og alle internettkoplingar i landet var derfor avhengige av infrastruktur i naboland som Tyrkia, Armenia og Russland.[9] Det var difor ikkje mogleg å få kontroll over den nasjonale internettinfrastrukturen på den måten estarane hadde gjort i 2007. Dei forsøkte fyrst å filtrere ut nettverkstrafikk frå russiske internettadresser, men dette viste seg lite effektivt sidan åtakarane flytta seg til tenarar i andre land som Tyrkia og Ukraina. Det einaste mottiltaket dei stod igjen med, var difor å migrere dei råka internettsidene til utanlandske tenarar: Presidentens web-side vart overført til ein bloggeteneste hjå Google, utanriksdepartementets sider vart flytta til tenarane til eit selskap i Atlanta, USA, og forsvarsdepartementets sider til ein tenar i Estland. I tillegg tilbaud den polske presidenten å publisere pressemeldingar frå georgiske myndigheiter på ein del av web-sida si (Hagen, 2013, s. 199–200; Tikk et al., 2010, s. 77).

Konsekvensar

Metodane, omfanget og måla for åtaka mot georgiske web-sider kan samanliknast med dei Estland opplevde i 2007, men konsekvensane var ulike. Georgia hadde i 2008 ein svakare internettinfrastruktur enn Estland og var dårlegare rusta til å forsvare seg mot åtaka. Dette gjorde at konsekvensane i Georgia på ein måte var større enn i Estland. Myndigheitene var nøydde å flytte web-sidene sine til utanlandske web-tenarar, og to av dei viktigaste internettleverandørane i Georgia klarte over fleire dagar ikkje levere tenester på grunn av at nettverka deira var overbelasta av datatrafikken. 9. august beordra den georgiske nasjonalbanken stopp i alle elektroniske banktenester med bakgrunn i åtak mot nasjonalbanken og Georgias største bank. Dette førte til at elektroniske betalingstenester var ute av funksjon i ti dagar, og at georgiske bankar mista kontakt med bankar i utlandet. I praksis var Georgia i periodar utan fungerande internettenester, og det elektroniske betalingssystemet var paralysert (Hagen, 2013, s. 198; Tikk et al., 2010, s. 77–78).

Samtidig var Georgia i 2008 eit mykje mindre digitalisert land enn Estland, med langt færre internettbrukarar og mindre digital kommunikasjon mellom myndigheiter og befolkning. For innbyggjarane var difor konsekvensane av åtaka mindre enn dei var for innbyggjarane i Estland. At det elektroniske betalingssystemet vart slått ut, kan seiast å delvis vere sjølvforskyldt på grunn av ein

[9] Eit Internet exchange point (IXP) er eit punkt der ulike internettleverandørar koplar seg saman og utvekslar datatrafikk. For nasjonal kontroll med internettrafikken vil ein vere heilt avhengig av å ha nasjonale IXP-ar.

overreaksjon frå nasjonalbanken. Det er lite som tydar på at cyberåtaka hadde nokon påverknad på den militære konflikten, og ein kan argumentere for at konsekvensane av cyberåtaka relativt sett var små eller ubetydelege samanlikna med invasjonen. Konsekvensane av cyberåtaka vert såleis overskygde av det militære nederlaget, og det er også vanskeleg å isolere og vurdere dei direkte kostnadane av cyberåtaka. Det har difor blitt argumentert for at den største konsekvensen av tenestenektåtaka var at georgiske myndigheiter mista ein informasjonskanal og dimed fekk svekka evna til å kommunisere med utanomverda (Cohen & Hamilton, 2013, s. 77–78; Greenberg, 2019, s. 95; Tikk et al., 2010, s. 77–78).

Kven stod bak?

Som i Estland tyder ting på at det var russiske hackarar og kriminelle organisasjonar som Russian Business Network som stod bak dataåtaka i Georgia. Det har i etterkant vore umogleg å bevise at russiske myndigheiter var involvert, men åtaka utført med botnett fall tidsmessig saman med den militære konflikten, noko som kan vere eit teikn på koordinering med dei konvensjonelle, militære åtaka. Ifølgje Greenberg (2019, s. 93–94) er det også eksempel på at cyberåtak og militære åtak fall saman i geografi, til dømes vart offisielle web-sider og lokalmedium i den georgiske byen Gori råka av cyberåtak berre kort tid før russiske luftstyrker starta bombetokt mot byen. Eit anna argument for god planlegging og organisering av åtaka er tilsynelatande god koordinering mellom dei seks ulike botnetta som tok del (Hagen, 2013, s. 200–203; Tikk et al., 2010, s. 74–76). Deibert et al. (2012, s. 13–15) peikar derimot på at ressursane som vart nytta i cyberåtaka, vart observert både før og etter den militære konflikten, og at sjølv om intensiteten i cyberåtaka var størst medan det var kampar på bakken, var timinga mellom cyberåtaka og dei konvensjonelle åtaka mindre presis enn det mange kommentatorar vil ha det til. Den russiske militære operasjonen var prega av dårleg koordinering og kommunikasjon på tvers av dei ulike forsvarsgreinene (Cohen & Hamilton, s. 71). Sjølv om russiske myndigheiter kan ha koordinert (delar av) cyberåtaka, synest det difor å vere liten grunn til å tru at den operasjonelle militære leiinga hadde tett koordinering med ulike nettverk av frittståande hackarar og kriminelle organisasjonar.

Tenestenekt som politisk verkemiddel

Åtaka mot Estland har blitt omtala som «Cyber war I» og liknande nemningar, altså som historias fyrste tilfelle av cyberkrigføring. Estiske myndigheiter har sjølv i stor grad bidrege til å fremje dette synet (Blank, 2017, s. 85–87; Greenberg, 2019, s. 88; Ruus, 2008; Schmidt, 2023, s. 188). Cyberåtaka mot Georgia har blitt omtala som «the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains» (Brooks et al., 2022, s. 48; Hollis, 2011, s. 2; Greenberg, 2019, s. 95). Sjølv om det i Estland i utgangpunktet var ein intern konflikt, medan Georgia var i ein militær konflikt med Russland, er det store likskapar mellom dei to

hendingane; i båe tilfella kan åtaka sjåast som usofistikert vandalisme med relativt moderate (materielle og økonomiske) konsekvensar. Det politiske bakteppet var det same for dei to hendingane; båe kan sjåast i lys av russisk strev etter å framleis ha innverknad på sin gamle interessesfære i det tidlegare Sovjetunionen, og å motverke vestleg påverknad.

I båe tilfella gjekk det føre seg ein strategisk kamp om sanninga. For hendingane i Estland kan dette illustrerast med den russiske presidentens tale 9. mai der han – medan cyberåtaka gjekk føre seg – fordømte «[t]hose who attempt today to belittle this invaluable experience and defile the monuments to the heroes of this war [andre verdskrigen]» for å «insulting their own people and spreading enmity and new distrust between countries and peoples» (Putin, 2007). I Georgia gjennomførte Russland ein større informasjonsoperasjon som eit ledd i kampanjen med å ta kontroll over Sør-Ossetia. Det russiske narrativet var at Georgia var aggressoren, og at Russland måtte gripe inn for beskytte eiga befolkning og fredsbevarande styrkar i Sør-Ossetia. For å styrke dette narrativet fløyg dei inn 50 russiske journalistar til den sør-ossetiske hovudstaden i dagane før dei militære kampane braut ut, og den russiske generalstaben heldt pressebrifar etter amerikansk modell frå Irak og Afghanistan. Det vart også levert overdrivne rapportar om eit georgisk regissert folkemord i Sør-Ossetia (Cohen & Hamilton, 2013, s. 77–80, 83–85). Laaneots (2014/2016, s. 66) skildrar at georgiske tenestegjerande og familiane deira vart utsett for påverknad gjennom meldingar og oppringingar på mobiltelefonane deira, og set det i samanheng med at dei viktigaste mobiloperatørane i Georgia var russiske.

Blank (2017, s. 81–85) og Lilly og Charvitch (2020, s. 133–139) viser korleis informasjonskrigføring har blitt ein integrert del av russiske myndigheiters syn på konflikt. Russland ser informasjonskrigføring som ein pågåande kamp om herredøme i informasjonsdomenet som kan ta ulike formar. Cyberoperasjonar gjev dominans i informasjonssfæren ved hjelp av tekniske metodar for å manipulere informasjonssystem, medan påverknadsoperasjonar gjev dominans ved hjelp av psykologiske metodar for å manipulere ein opinion. Kveberg og Alme skriv i kapittel 7 om russiske påverknadsoperasjonar, men Sæther i kapittel 9 gjev eit eksempel på korleis Russland i 2014 freista fremje narrativ gjennom nettaviser i Ukraina.

Det kan argumenterast for at cyberåtaka i Estland og Georgia er tidlege eksempel på den tekniske forma for russisk informasjonskrigføring (Blank, 2017, s. 85–90; Cohen & Hamilton, 2023, 83–84; Deibert et al., 2012; Richards, 2015, s. 34–35). Både i Estland og i Georgia var myndigheitene og media mål for cyberåtaka, noko som svekka estiske og georgiske myndigheiters evne til å formidle sine versjonar av hendingane både internt og internasjonalt. Cyberåtaka kan difor sjåast som informasjonsoperasjonar som skulle bidra til at den russiske framstillinga av hendingane skulle dominere nyhendebiletet. Ein interessant kontekst for dette blir gjeve av Cohen og Hamilton (2013, s. 79–80): I 2008 vart internett ein viktig informasjonskanal for mange russarar nettopp på grunn av

den einsidige russiske pressedekninga av hendingane i Georgia. For å dominere informasjonsdomenet var det ikkje lenger tilstrekkeleg å dominere massemedia.

I båe hendingane har russiske myndigheiter blitt skulda for å stå bak, men attribusjonen er ikkje eintydig. Det synast klart at åtaka vart utførte av ein kombinasjon av politisk motiverte aktivistar oppmuntra av russiske hackarforum, og botnett leigde eller stilt til rådvelde av russiske kriminelle organisasjonar som Russian Business Network. Er det mogleg å seie noko meir enn å skråsikkert slå fast at Kreml må ha stått bak, slik som til dømes Blank (2017), Valeriano og Maness (2015, s. 147) og Valeriano et al. (2019, s. 126) gjer? I ei vidare analyse av hendingane vil Galeottis (2019) modell for russisk politisk krigføring vere nyttig. Han nyttar termen som eit alternativ til hybrid krigføring og legg i det ein russisk «campaign to influence and subvert the West, using everything from aggressive intelligence operations to cultural manipulation» (s. 12). Innanfor dette spekteret finn vi også informasjonskrigføring (Galeotti, 2019, s. 34–36). Dette gjev støtte til å sjå cyberåtaka i Estland og Georgia som ledd i informasjonskrigføring, men meir interessant er Galeottis analyse av korleis den politiske krigen mot Vesten vert ført.

I analysen til Galeotti (2019, s. 59–66) har ikkje den politiske krigen nokon «masterplan» der Kreml eller den russiske presidenten trekk i alle trådane. Presidenten og hans administrasjon sender signal om generelle strategiske målsettingar, men baserer seg i stor grad på lokale initiativ nedetter i systemet for verkemiddel som kan bidra til å nå dei strategisk måla, kombinert med ein tradisjon for utnytting av frontar, folkelege rørsler, næringsliv og kriminelle nettverk. Det er med andre ord eit system av sjølvmotiverte personar og organisasjonar i eller utanfor statsapparatet som handlar utifrå eit ønskje om å oppfylle presidentens generelle strategi (og, får vi tru, ei von om løn for strevet). Denne forma for desentralisert verkemiddelbruk, med stor grad av «outsourcing», gjev ein fridom i systemet som både fremjar kreativitet og sikrar nektbarheit (deniability) for toppen. Men det gjer også at toppen har mindre kontroll over verkemidla i bruk, og at resultatet vert mindre effektivt enn om verkemiddelbruken var under direkte kontroll.

I Galeottis analyse er det med andre ord ikkje nokon motsetnad mellom cyberåtak utført av aktivistar og kriminelle og russisk politisk krigføring. I Estland hadde både dei som protesterte i gatene og dei som protesterte på internett, politisk støtte frå Moskva. I Georgia er det openbert at cyberåtaka var ei støtte til den militære innsatsen. På same måte som at russisk påverknad frå massemedia eller agentar kan ha bidrege til å piske opp stemninga i gatene i Tallinn, kan russiske agentar kan ha piska opp stemninga på russiske internettforum og laga avtalar med kriminelle organisasjonar som har botnett til leige. Uavhengig av graden av oppmuntring eller direkte deltaking frå delar av det russiske statsapparatet (om det er initiert, koordinert eller berre akseptert av russiske myndigheiter) er det konsistent med den desentraliserte forma for verkemiddelbruk som Galeotti skildrar. Deibert et al.

(2012, s. 16–18), Hagen (2013, s. 203–204) og Schmidt (2013, s. 191–192) har i sine analysar av hendingane i Estland og Georgia kome til liknande konklusjonar.

Konklusjon: Ukraina 2022

24. februar 2022 gjekk Russland til invasjon av Ukraina. I kjølvatnet av invasjonen vart tenestenekt og andre formar for aktivistiske cyberåtak igjen eit politisk verkemiddel. Invasjonen viste også utvikling i bruken av cybermakt i konfliktar; i krigens fyrste fase vart Ukraina utsett for ein kampanje med destruktive og langt meir avanserte cyberåtak enn Georgia i 2008. Men etter at Russland måtte gje opp målet om ein rask siger over Ukraina og krigen gjekk over i ein meir statisk fase med russisk okkupasjon av dei austlegaste delane av Ukraina, var det tenestenekt og andre formar for primitive cyberåtak som «website defacement» som dominerte. Med hundrevis av åtak i månadslange kampanjar hadde dei eit omfang og ei varigheit som langt overgjekk åtaka i 2007 og 2008 (Bateman, 2022, s. 9–16; Burgess, 2022a, 2022b; Insikt Group, 2023, s. 15–16; Schroeder & Dack, 2023, s. 6–9).

Bak desse tenestenektåtaka stod ei lang rekkje pro-russiske hackargrupperingar; ulike oversikter viser opp mot 70 ulike grupper, med namn som for eksempel XakNet, Killnet, NoName 057, FromRussiaWithLove og Anonymous Russia. Tenestenektåtaka vart ikkje retta berre mot mål i Ukraina, men også mot ei rekkje av Ukrainas støttespelarar, inkludert Noreg. Mange av hackargruppene har truleg oppstått spontant. Samtidig skjedde det ei konsolidering av gruppene gjennom det fyrste året etter invasjonen der Killnet stod fram som leiande, og andre grupper slutta seg til Killnet som undergrupper. Det kom etter kvart også indikasjonar på at det var kontakt mellom Killnet og russiske hemmelege tenester (Burgess, 2022a, 2022b; Insikt Group, 2023, s. 17–18; Mandiant Intelligence, 2023).

Ukraina organiserte eigne tenestenektkampanjar mot Russland. Ukrainas minister for digital transformasjon Mykhailo Federov tok etter invasjonen initiativ til oppretting av det dei kallar den ukrainske IT-hæren for å rekruttere aktivistar til å utføre cyberåtak på vegne av Ukraina etter same lest som andre aktivistiske grupperingar. Ukrainske myndigheiter heldt ein armlengd avstand, men det er grunn til å tru at dei var involvert i bakgrunnen. Eit gjenoppstått Anonymous og ei gruppe med namnet Belarusian Cyber Partisan gjennomførte også tenestenektåtak og andre primitive cyberåtak til støtte for Ukraina. IT-hæren og Anonymous gjekk mot russiske mål, medan Belarusian Cyber Partisans rettar åtaka sine mot mål i Belarus (Burgess, 2022a; 2022b; Insikt Group, 2023, s. 16–17; Soestano, 2022).

Den store skilnaden mellom Estland og Georgia i 2007 og 2008 til Ukraina i 2022–23 var omfanget av åtak, grupperingar og mål. Åtaka var også langt meir internasjonale – korkje gruppene, deltakarane eller måla er avgrensa til Ukraina og Russland. Ein tredje skilnad ser ut til å vere at sjølv om myndigheiter og media var sentrale mål for tenestenektåtaka i 2022–23, har dei hatt mindre å seie for evna til offentleg kommunikasjon. I Ukraina var truleg fysisk øydelegging og anneksjon av

internettinfrastruktur og påverknadsoperasjonar gjennom tradisjonelle og sosiale medium større trugsmål mot myndigheitenes evne til å kommunisere (Bergengruen, 2023; Schroeder & Dack, 2023, s. 6–12). Trass skilnadane var det også kontinuitet. Russland nytta kriminelle og aktivistar som proxy og lét kriminelle organisasjonar og aktivistgrupperingar gjere cyberåtak på vegne av seg. Ukraina skil seg frå Russland ved at dei opent tok initiativ til og organiserte IT-hæren, men det igjen illustrerer at det ikkje er nokon motsetnad mellom eit statleg initiativ og utnytting av aktivistar.

Distribuerte tenestenektåtak har opphavet sitt i politisk protest og eksisterer framleis som det. Det er difor ikkje overraskande at statar vil søkje å utnytte aksjonsforma for politisk krigføring. Som vi har sett, er sikker attribusjon utfordrande, og tenestenektåtak vert eit verkemiddel som kan nyttast utan stor risiko for eskalering. Tenestenektåtak er ei form for destruktive cyberåtak, men med relativt avgrensa konsekvensar. Dei «nektar» bruk av internettenester, men som regel forbigåande og utan å gjere skade på den underliggjande internettinfrastrukturen.

Tenestenektåtak blir ofte oppfatta meir som forstyrrande enn øydeleggande, men er på trass av det eit «hardt» verkemiddel. Måla for tenestenektåtak er i hovudsak web-sider, som alt i 2007 var viktige informasjons- og kommunikasjonskanalar, men som i dag har blitt essensielle for informasjonsflyten i samfunnet. Medan påverknadsoperasjonar søkjer å påverke ved å manipulere innhaldet i informasjonsstraumen, står tenestenektåtak fram som ei form for hard maktbruk der målet er å nekte motstandarens bruk av informasjonskanalen.

Referansar

Bergengruen, V. (2023, 22. februar). Inside the Kremlin's Year of Ukraine Propaganda. *Time*. https://time.com/6257372/russia-ukraine-war-disinformation/

Brooks, R. R., Yu, L., Ozcelik, I., Oakley, J. & Tusing, N. (2022). Distributed Denial of Service (DDoS): A History. *IEEE Annals of the History of Computing, 44*(2), 44–54.

Burgess, M. (2022a, 11. juli). Russian 'Hacktivists' Are Causing Trouble Far Beyond Ukraine. *Wired*. https://www.wired.co.uk/article/russia-hacking-xaknet-killnet

Burgess, M. (2022b, 27. desember). Hacktivism Is Back and Messier Than Ever. *Wired*. https://www.wired.com/story/hacktivism-russia-ukraine-ddos/

Bærug, J. R. (2021, 24. juni). Estlands samtidshistorie. I *Store norske leksikon*. https://snl.no/.versionview/1439749

Bærug, J. R., Filseth, G., Thordarson, F. (2022, 5. januar). Georgias historie. I *Store norske leksikon* på snl.no. https://snl.no/.versionview/1544373

Coleman, G. (2014). *Hacker, Hoaxer, Whilstleblower, Spy. The Many Faces of Anonymous*. Verso.

Cohen, A. & Hamilton, R. E. (2013). The Russian Military and the Georgian War: Lessons and Implications. *Current Politics and Economics of Russia, Eastern and Central Europe, 28*(1), 43–114.

Deibert, R. J., Rohozinski, R. & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, *43*(1), 3–24.

Galeotti, M. (2019). *Russian Political War. Moving Beyond the Hybrid.* Routledge.

Greenberg, A. (2019). *Sandworm. A New Area of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Grindal, K. (2022). Artist Collectives as the Origins of DDoS the Strano Network and Electronic Disturbance Theater. *IEEE Annals of the History of Computing*, *44*(3), 30–42.

Filseth, G. & Thordarson, F. (2021, 21. mars). Georgias samtidshistorie. I *Store norske leksikon*. https://snl.no/.versionview/1386244

Hagen, A. (2013). The Russan-Georgian War 2008. I J. Healey (red.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (s. 194–204). Cyber Conflict Studies Association.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security, 4*(2), 49–60.

Hollis, D. (2011, 6. januar). Cyberwar Case Study: Georgia 2008. *Small Wars Journal*. https://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008

Insikt Group. (2023). *Russia's War Against Ukraine Disrupts the Cybercriminal Ecosystem* (CTA-RU-2023-0223). Recorded Future. https://go.recordedfuture.com/hubfs/reports/cta-2023-0223.pdf

Laaneots, A. (2016). *The Russian-Georgian War of 2008: Causes and Implications* (ENDC occasional papers 4/2016, K. Salum, overs.). Estonian National Defence College. (Opphaveleg utgjeven 2014.)

Lilly, B. & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. I T. Jančárková, L. Lindström, M. Signoretti, I. Tolga & G. Visky (red.), *2020 12th International Conference on Cyber Conflict* (s. 129–155). NATO CCDCOE Publications. https://www.ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf

Lundbo, S. (2021, 14. januar). Estlands befolkning. I *Store norske leksikon*. https://snl.no/.versionview/1347853

Lurås, G. & Seim, J. (2021, 27. oktober). Estlands historie. I *Store norske leksikon*. https://snl.no/.versionview/1491331

Mandiant Intelligence. (2023, 10. august). Hacktivists Collaborate with GRU-sponsored APT28. *Mandiant*. https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

Ottis, R. (2013). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. I M. Warren (red.), *Case Studies in Information Warfare and Security* (s. 119–131). Academic Conferences and Publishing International.

Putin, V. (2007, 8. mai). *Speech at the Military Parade Celebrating the 62nd Anniversary of Victory in the Great Patriotic War*. President of Russia. http://en.kremlin.ru/events/president/transcripts/24238

Richards, J. (2014). *Cyber-War. The Anatomy of the Global Security Threat.* Palgrave Macmillan.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M. & Perl, S. J. (2014). Computer Security Incident Response Teams Development and Evolution. *IEEE Security & Privacy, 12*(5), 16–26

Ruus, K. (2008). Cyber War I: Estonia Attacked from Russia. *European Affairs, 9*(1–2).

Schmidt, A. (2013). The Estonian Cyberattacks. I J. Healey (red.), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (s. 174–193), Cyber Conflict Studies Association.

Schroeder, E. & Dack, S. (2023). *A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment*. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/

Soesanto, S. (2022). *The IT Army of Ukraine. Structure, Tasking, and Eco-System* (Cyberdefense report). Center for Security Studies (CSS), ETH Zürich.

Tikk, E., Kaska, K. & Vihul, L. (2010). *International Cyber Incidents. Legal Considerations*. CCD COE.

Valeriano, B., Jensen, B. & Maness, R. C. (2019). Cyber Strategy. *The Evolving Character of Power and Coercion*. Oxford University Press.

Valeriano, B. & Maness, R. C. (2015). *Cyber War versus Cyber Realities. Cyber Conflict in the International System.* Oxford University Press.