Einar Rautjärvi

Valtiollinen kyber- ja hybridivaikuttaminen - case Venäjä

Tietotekniikan Kandidaatintutkielma

27. toukokuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Einar Rautjärvi

Yhteystiedot: einar.a.t.rautjarvi@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Valtiollinen kyber- ja hybridivaikuttaminen - case Venäjä

Title in English: cyber and hybrid influencing on a national level - Case Russia

Työ: Kandidaatintutkielma

Opintosuunta: Kaikki opintosuunnat

Sivumäärä: 23+0

Tiivistelmä: Tässä tutkielmassa kuvataan millaisia valtiollisia kyber- ja hybridivaikuttamisen keinoja on olemassa. Tutkielman tarkoituksena on kuvailla teknisellä tasolla kybertoimintaympäristössä tapahtuvaa vaikuttamista ja perehtyä hybridiuhkiin ja -sodankäyntiin ja siihen, miten hybridiuhkia pystytään torjua ja ehkäistä. Tutkielman lopussa tarkastellaan edellä mainittuja asioita reealimaailman esimerkein Venäjän suorittaman vaikuttamisen avulla.

Avainsanat: Kandidaatintutkielma, Kyberturvallisuus, Hybridiuhat, Venäjä

Abstract: This thesis' focus is to explain different methods of cyber and hybrid influencing on a national level. The purpose it to explain the technical aspects of influencing in a cyber environment and orientate on hybrid threats and warfare including prevention and defense against them. In conclusion this thesis will explore real world examples of these themes via influencing carried out by the Russian Federation.

Keywords: Bachelor's Thesis, Cyber security, Hybrid threats, Russia

Sisällys

1 Johdanto

Nykyisin on yhä yleisempää, että valtioille kriittisiä infrastruktuurin osia liitetään erilaisiin tietoteknisiin järjestelmiin sekä ratkaisuihin. Kyberturvallisuuden kannalta tämä tarkoittaa sitä, että mahdollisia iskujen kohteita on enemmän ja iskujen potentiaalinen kriittisyys sekä laajuus ovat suurempia kuin koskaan ennen. Tämä on johtanut siihen, että kyberiskut ja niihin tehtävät kineettiset vastatoimet ovat sumentaneet perinteistä käsitystä sodasta ja rauhasta (Bachmann ja Gunneriusson 2015). Usein hyökkäykset liitetään johonkin valtioon, vaikka taustalla olisi valtioon sitoutumaton järjestö tai yksittäinen henkilö, sillä jokainen järjestö tai yksittäinen henkilö toimii jostain maasta käsin ja sen tuomiovallan alla.

Hybridisodankäynnin tuomat hybridiuhat koetaan suurena turvallisuusuhkana (Simons, Danyk ja Maliarchuk 2020). Hybridiuhat sisältävät niin kybersodankäynnin kuin fyysiseen sodan käyntiin liittyviä asioita, kuten globaalin terrorismin, järjestäytyneen rikollisuuden, massatuhoaseiden lisääntymisen sekä asymmetriset konfliktiskenaariot (Bachmann ja Gunneriusson 2015).

Tämän kirjallisuuskatsauksen tavoite on selvittää millaisia kyber- ja hybridiuhkia on, millä tavoin niitä toteutetaan ja miten uhkia pystytään ehkäisemään ja torjumaan. Aihetta tarkastellaan konkreettisin esimerkein Venäjän avulla, joka on ollut yksi aktiivisimmista valtiosta hybriditoimintaympäristössä viimeisen 15 vuoden aikana.

Tutkielman toisessa luvussa keskitytään kybertoimintaympäristössä tapahtuvaan kybervaikuttamiseen ja avataan sen eri muotoja, joita ovat kyberhyökkäykset, kybervakoilu ja kyberterrorismi. Kyseisessä luvussa keskitytään kybertoimintaympäristössä tapahtuvaan vaikuttamiseen teknisellä tasolla.

Tutkielman kolmannessa luvussa liitetään edellisessä luvussa alustettu kybervaikuttaminen osaksi isompaa hybridivaikuttamisen kokonaisuutta. Luvussa käydään myös läpi millaisia hybridiuhkia valtioihin kohdistuu ja miten niitä pystytään torjumaan ja ehkäisemään.

Tutkielman neljännessä luvussa syvennytään edellisissä kappaleissa alustetuilla asioilla Venäjän toimintaan kyber- ja hybriditoimintaympäristössä. Toiminnasta annetaan myös kon-

kreettisia esimerkkejä Venäjän teettämistä erityyppisistä vaikuttamistoimista ja niiden motiiveista. Viimeisessä luvussa tutkielman pääkohat ja huomiot kootaan yhteen.

2 Kybervaikuttaminen

Tämän kirjallisuuskatsauksen kontekstissa valtiollisella kybervaikuttamisella tarkoitetaan, jonkun valtion tai jonkun yksilön suorittamaa kybervaikuttamista tietyn valtion intressien mukaisesti. Kybervaikuttaminen on lisääntynyt hyvin paljon tällä vuosituhannella teknologian lisääntyessä. Siihen on monia syitä, miksi valtiot käyttävät yhä enemmän kybervaikuttamista. Suurimpia kybervaikuttamisen etuja verrattaessa fyysiseen sodankäyntiin tai sotilaalliseen vaikuttamiseen ovat sen matalat kustannukset, iskujen vaikea jäljittäminen hyökkääjään ja sen tuoma voimasuhteiden muuttuminen. Voimasuhteiden muuttumisella tarkoitetaan sitä, että nykypäivänä pienet valtiot tai pienemmät järjestöt, kuten esimerkiksi terroristijärjestöt voivat saada paljon tuhoa aikaan suurempia valtiota vastaan. Kybersodankäynnillä tarkoitetaan sodankäyntiä, mikä tapahtuu kybertoimintaympäristössä. Se pitää sisällään niin ekonomiset vahingot, kuten pankkitilien sulkemisen, teknologiset ongelmat ja tärkeän datan varastamisen kuin maan puolustusjärjestelmien hakkeroinnin (Djaja 2020).

2.1 Kybervakoilu

Kybervakoilulla tarkoitetaan samaa kuin klassisella vakoilun termillä, mutta erona on se, että kybervakoilu tapahtuu kybertoimintaympäristössä. Motiivi kuitenkin molemmissa on sama eli yrittää suorittaa tiedonkeruuta toisesta osapuolesta salassa heidän tietämättä. Kuitenkaan teidonkeruu ei ole aina laitonta, sillä yksi kybervakoilun muoto on OSINT (engl. Open Source Intellegent) eli avointen lähteiden tiedustelu, jossa informaatiota etsitään avoimista lähteistä (Hribar, Podbregar ja Ivanuša 2014). Avoimia lähteitä voivat olla esimerkiksi sosiaalisen median kanavat tai yritysten nettisivuilta löytyvä informaatio, joka on julkisesti kaikille näkyvillä. OSINT:in lisäksi vakoilua voidaan myös suorittaa kyberhyökkäysten omaistesti, kuten tietojen kalastelulla tai haittaohjelmilla.

Kybervakoilun suorittamiseen on olemassa paljon erilaisia työkaluja ja bottiverkkojen (engl. Botnet) avulla niitä pystytään käyttämään laajamittaisesti. Bottiverkosta puhuttaessa tarkoitetaan hyökkääjän haltuun saamia verkkolaiteitta. Bottiverkkojen yhdessä toimivia työkaluja ovat esimerkiksi keylogger, trojalaiset, adware ja informaation varastamiseen tarkoitetut

ohjelmat. Suuri osa käyttöjärjestelmistä ja verkkolaitteista on edellä mainittujen työkalujen riskin piirissä, kuten Microsoft Windows, Linux, MacOS, mobiililaitteet ja erilaiset IoT (Internet of Things) laitteet. (Zsolt ja Tamas 2020)

Haittahojelma VPNFilter:illä, joka käyttäytyy bottiverkon tavoin. Heinäkuussa 2018 tutkijat arvioivat VPNFilter:in vaikuttaneen 500 000 verkkolaitteeseen. Aluksi se iski verkkolaitteisiin, jotka oli Ukrainassa, mutta lopulta se levisi ainakin 54 eri maahan. VPNFilter pystyy varastamaan informaatiota, kaappaamaan ja estämään verkkoliikenettä, monitoroimaan SCADA protokollaa (Supervisory Control and Data Acqusition) ja tekemään haavoittuneista reitittimistä toimimattomia. (Zsolt ja Tamas 2020)

2.2 Kyberhyökkäykset

Kyberhyökkäyksiä voidaan toteuttaa hyvin monin eri keinoin. Se miten kyberhyökkäys toteutetaan riippuu pitkälti siitä, mitä hyökkääjät haluavat saavuttaa hyökkäyksellään ja millaiseen järjestelmään isku kohdistetaan. Yleisesti ottaen kyberhyökkäykset pystytään jakamaan verkossa tehtäviin ja fyysisesti järjestelmässä tehtäviin. Iskujen tavoitteena on tuhota, varastaa tai muuntaa jo olemassa olevaa dataa (Biju, Gopal ja Prakash 2019). Yleisimpiä kyberhyökkäysten muotoja ovat palvelunestohyökkäykset DoS (engl. Denial-of-service) ja DDoS (engl. Distributed denial-of-service), tietojen kalastelu (engl. Phishing), haittaohjelmat (engl. Malware) sekä BEC-huijaus (engl. Business Email Compromise) (Timofeyev ja Dremova 2022).

DoS ja DDoS hyökkäyksissä tarkoitus on estää järjestelmän oikeanlainen toiminta, lähettämällä siihen niin paljon kutsuja, että kutsujen määrä ylittää järjestelmän kapasiteetin (Timofeyev ja Dremova 2022). DoS ja DDoS hyökkäysten ero on se, että DoS hyökkäyksessä yksi järjestelmä lähettää kutsuja toiseen järjestelmään, kun taas DDoS hyökkäyksessä, monta järjestelmää suorittaa DoS iskuja yhteen järjestelmään (Zargar, Joshi ja Tipper 2013). Tällä tavoin hyökkääjät voivat estää ihmisten pääsyn halaumiinsa järjestelmiin. DDoS hyökkäyksillä on mahdollisuus saada paljon tuhoa aikaan esimerkiksi fyysisen hyökkäyksen alkaessa, DDoS hyökkäyksillä voidaan evätä siviileiltä mahdollisuus saada informaatiota tapahtumista sekä estää pääsy tarpeellisten palveluiden käyttöön.

Tietojen kalastelua voidaan suorittaa monella eri tavalla, joista yleisimpä ovat linkkien, sähköpostien ja nettisivujen avulla tapahtuvat. Kalastelun tarkoituksena on saada henkilökohtaisia tietoja joko käyttäjästä itsestään tai tunnuksia järjestelmiin (Ripa, Islam ja Arifuzzaman 2021).

Haittaohjelmat ovat ohjelmia, joiden tarkoituksena on korruptoida dataa, varastaa informaatiota, häiritä järjestelmän toimivuutta tai saada järjestelmä hyökkääjien hallintaan (Engel, Joshua ja Engel 2020). Uhka haittaohjelmista kasvaa jatkuvasti ja vuonna 2017 löydettiin 3.5 miljoonaa uutta haittaohjelmaa pelkästään android puhelimiin liittyen (Engel, Joshua ja Engel 2020). Yleisimmät haittaohjelmat ovat kiristysohjelmia (engl. ranmsomware), tietokone madot (engl. computer worms) ja trojalaiset (engl. trojan horses). Yksi tunnetuimmista kiristyshaittaohjelmista on WannaCry, jonka tutkijat löysivät ensimmäisen kerran vuonna 2017.

WannaCry:n on arvioitu iskeneen 150 eri maahan ja saastuttaneen yli 300 000 järjestelmää (Akbanov, Vassilakis ja Logothetis 2019). Sen aikaansaama laaja tuho johtui sen uniikista tavasta levitä, minkä mahdollisti siinä oleva tietokonemato komponentti. WannaCry käytti tartuttamisvaiheessa MS17-010 EternalBlue haavoittuvuutta ja takaporttina DoublePulsar:ia (Akbanov, Vassilakis ja Logothetis 2019).

2.3 Kyberterrorismi

Teknologian kehittyessä ja lisääntyessä yhteiskunnissa, myös verkon välityksellä tapahtuva rikollinen toiminta, kuten kyberterrorismi on lisääntynyt sen seurauksena. Kyberterrorismin määritelmä on hyvin laaja ja vaihteleva, mutta yleisesti sillä tarkoitetaan verkon avulla tapahtuvaa terroristista toimintaa. Verkon tarjoama yhteisöllisyys, anonymiteetti ja halpuus ovat syitä, miksi verkon käyttö on lisääntynyt äärijärjestöjen keskuudessa (Palasinski ja Bowman-Grieve 2017). Terroristiärjestöt ovat jo pitkään käyttäneet verkkoa hyväkseen propagandan levittämiseen ja rekrytointiin ja nykyään verkkoa käytetään vieläkin laajemmin laajemmin hyväksi, kuten rahoituksessa ja iskujen suunnittelussa sekä toteutuksessa (Palasinski ja Bowman-Grieve 2017).

Kyberterrorismin avulla voidaan saada paljon tuhoa aikaan, sillä tärkeitä infrastruktuureita

on liitetty jollain tasolla osaksi teknologisia ratkaisuita. Esimerkiksi isku Ukrainan sähköverkkoon vuonna 2015 (Baezner 2018) osoittaa, kuinka keskeisiä ja suuria infrastruktuurin osia on mahdollista kaataa kyberhyökkäyksin. Näin suureen infrastruktuurin osaan onnistunut pitkäaikainen hyökkäys voi lamaannuttaa pahimmassa tapauksessa koko valtion toimivuuden siksi aikaa. Yhteiskunnan lamaantuminen voi pahimmassa tapauksessa johtaa myös kuolonuhreihin, jos esimerkiksi terveydenhuollon toimivuus saadaan pysäytettyä.

Kriittisten infrastruktuurien lisäksi myös liikennöinti on enemmän riippuvainen teknologiasta kuin koskaan ennen ja niihin kohdistuvien hyökkäyksien seuraukset voivat olla vakavia. Esimerkiksi vuonna 2010 Yhdysvaltojen hallinnon teettämän tutkimuksen mukaan FAA:n (Federal Aviation Administration) tietokone järjestelmät ovat haavoittuvaisia kyberhyökkäyksille, sillä laitteistoa ei ole päivitetty riittävälle tasolle hakkeroinnin torjumiseksi (Abeyratne 2011). On myös raportoitu FAA:n väittäneen, että esimerkiksi Boeing Dreamliner 787-mallin lentokoneen keskustietokonejärjestelmä saattaa olla haavoittuvainen ja sen hakkeroinnilla voi olla katastrofaaliset seuraukset (Abeyratne 2011). Lentokoneen keskusjärjestelmän hakkerointi voisi johtaa potentiaalisesti moniin satoihin kuolonuhreihin, jollei jopa tuhansiin hakkeroidun lentokoneen iskiessä asutetulle alueelle.

2.4 Valtiosidonnaisuus

Usein kyberiskuista puhuttaessa iskut liitetään tiettyyn valtioon tai tiettyyn lähtömaahan, vaikka takana olisi vain yksittäinen valtion kansalainen. Näin kävi esimerkiksi vuoden 2001 tapahtumissa, joissa joukko etelä-korealaisia yliopisto-opiskelijoita kohdisti hyökkäyksen Japanin opetusministeriön nettisivuille (Gandhi ym. 2011). Motiivi hyökkäykselle oli se, että opiskelijoiden mielestä Japanin armeijan aggressioita ei käsitelty julkaistuissa historian kirjoissa (Gandhi ym. 2011). Vaikka hyökkäyksen takana oli ryhmä opiskelijoita, iskusta puhuttaessa käytetään termejä "etelä-korealaislähtöinen hyökkäys"ja "etelä-korealainen hakkeriryhmä".

On vaikeaa tietää varmasti, mitkä järjestöt ja yksilöt, jotka suorittavat kyberhyökkäyksiä, ovat tietyn valtion kustantamia toimijoita. Kyseiset tiedot ovat valtion toimesta salattua informaatiota, mutta silti kyseiset toimijat tekevät toimensa tietyn alueen toimivallan alla. Näi-

den syiden takia hakkerijärjestöt, jotka tekevät hyökkäyksiä valtion intressien mukaisesti, usein liitetään kyseiseen valtioon.

3 Hybridivaikuttaminen

Nykypäivänä yksi suurimmista uhista valtioiden turvallisuudelle on hybridivaikuttaminen ja sen tuomat hybridiuhat. Hybridivaikuttamisen seurauksena perinteinen ajattelutapa rauhan ja sodan välillä on muuttunut ja rajat niiden välillä ovat sumentuneet. Valtiollisella tasolla tämä tarkoittaa sitä, että hybridivaikuttamisessa on suuri harmaa alue, jota osa valtioista käyttää radikaalisti hyväkseen. Tässä luvussa käsitellään hybridivaikuttamisen osa-alueita tarkastelemalla hybridiuhkia, hybridisodankäyntiä sekä lopuksi hybridiuhkien torjuntaa.

3.1 Hybridiuhat

Hybridiuhkien ja -sodankäynnin konsepti tuli ensimmäisen kerran tutuksi vuonna 2006. Tällöin libanonilainen järjestö Hizbollah sai konkreettisia tuloksia Israelin puolustusvoimia (IDF) vastaan Toisessa Libanonin sodassa. Sen hetkinen määritelmänä hybridille oli se, että valtiosta riippumattomat toimijat tekivät asioita, jotka oltiin ennen liitetty vain valtiollisiin toimijoihin, asioiden vaikeuden takia. (Bachmann ja Gunneriusson 2015)

Nykypäivän määritelmä hybridistä ja hybridiuhista on muuttunut paljon vuodesta 2006. Tämän hetkinen määritelmä hybridiuhille on hyvin laaja. Nykyään hybridiuhkiin luetaan edellisessä luvussa mainittujen kybertoimintaympäristöön liittyvien uhkien lisäksi myös fyysiseen sodankäyntiin ja yhteiskunnallisiin asiohin liittyviä uhkia (Bachmann ja Gunneriusson 2015). Näitä asioita ovat esimerkiksi armeijajoukkojen strateginen liikehdintä, taloudellinen painostus sekä disinformaation jakaminen (Wijnja 2022). Näkyvimmät hybridiuhat valtioiden kansalaisille ovat sosiaalisen median manipulointi, valeuutiset sekä disinformaatio (Wijnja 2022). On olemassa myös valtioita, joiden suuri osa puolustusstrategiasta koostuu hybridiuhkien luomisesta, kuten ydinaseita omaavan Pohjois-Korean puolustusstrategia.

3.2 Hybridisodankäynti

Hybridisodan määritelmä ei ole yksiselitteinen. Yleensä sillä tarkoitetaan sodankäyntiä, joka on yhdistelmä perinteisestä käsityksestä sodankäynnistä ja kybertoimintaympäristössä ta-

pahtuvasta vaikuttamisesta. Hybridisodankäynti ei ole käsitteenä uusi, mutta ajan kuluessa hybridisodankäynnin paradigma on muuttunut. Myöskään oikeaa suhdetta kybervaikuttamisen ja fyysisen sodankäynnin kesken ei ole löydetty ja valtioiden käyttämä suhde elää kokoajan. (Simons, Danyk ja Maliarchuk 2020)

Hybriditaktiikoiden käyttäminen ei ole ilmiönä uusi, sillä niitä ollaan käytetty aikojen saatossa paljon. Nämä taktiikat pitävät sisällään esimerkiksi propagandan levittämisen, harhaanjohtamista ja muita ei armeijaan liittyviä taktiikoita (Wijnja 2022). Nykypäivän tiedonleviämisen nopeus, jonka sosiaalinen media tarjoaa, on muuttanut taktiikoiden merkityksen täysin (Wijnja 2022). Sosiaalinen media tarjoaa valtiolle helpon, nopean ja halvan tavan suorittaa hybriditaktiikoita.

Hybridisodankäynnissä on myös ongelmakohtia, kuten tarkan määritelmän puutteellisuus (Simons, Danyk ja Maliarchuk 2020). Toinen ongelma on se miten vähän laillisia asetuksia tällä hetkellä on hybridisodankäyntiä kohtaan, sillä esimerkiksi hybridisodankäyntiä kohtaan ei ole sovittu universaaleja lakeja, toisin kuin traditionaaliselle sodankäynnille on (Simons, Danyk ja Maliarchuk 2020). Erityisesti puolustavalle osapuolelle määrittelyn ja kriteerien puutteellisuus tuo ongelmia, sillä ne vaikeuttavat reagointia.

Edellä mainitut seikat aiheuttavat vaikeita ristiriitoja. Usein voi olla vaikea rajata voidaanko hyökkäys laskea sotatoimeksi vai ei, kuten esimerkiksi Yhdysvallat sai syyn kohdistaa voimakeinoja ja sotatoimia Japaniin Pearl Harborin iskujen jälkeen, mutta hybridisodankäynnissä hyökkäyksiin reagointi ei ole niin yksinkertaista (Almäng 2019). Lakien puuttelliisuuden takia hyökkäysten tulkinta voi muuttua pikemminkin poliittiseksi asiaksi kuin oikeusasiaksi (Almäng 2019). On helppo ymmärtää, että toinen konfliktin osapuolista voi helposti pystyä hyödyntämään harmaata aluetta omien tarkoitusperiensä edistämiseen.

3.3 Hybridiuhkien torjunta

Eri maiden käyttämissä hybridiuhkien torjuntastrategioissa on eroja, vaikka samoja piirteitä on huomattavissa. Eroihin vaikuttavat esimerkiksi maiden erilainen halukkuustaso käyttää armeijajoukkoja ja maiden mahdollinen kuuluminen erilaisiin liittoihin, kuten NATO ja Euroopan Unioni. Useiden tutkijoiden ja päättäjien mukaan hybridiuhkien torjunta voidaan

jakaa neljään osaan: turvallisuuteen järjestäytyminen, hybridiuhkien havaitseminen, hybridiuhkien estäminen ja hybridiuhkiin vastaaminen (Wijnja 2022).

Turvallisuuteen järjestäytyminen on suositelluin tapa parantaa valtion turvallisuutta hybridiuhkia vastaan. Tämä tarkoittaa sitä, että lähestymistapa hybridiuhkien estämiseen on koko kansan tekemän työn tulos. Hybridiuhkien suhteen valtio ei ole riippuvainen vain poliisista sekä armeijasta, sillä suurin osa työkaluista hybridiuhilta puolustautumiseen löytyy yksityisistä yrityksistä sekä erilaisista järjestöistä. Kyseisiä työkaluja ovat esimerkiksi lait, jotka säätelee hallinnolliset elimet ja yksityiset yritykset, jotka tekevät kyberturvallisuuden alalla töitä valtiolle. Näin ollen myös yksityisillä yrityksillä sekä järjestöillä, jotka tekevät töitä kriittisen infrastruktuurin ympärillä, on vastuu infrastruktuurin suojelemiseen. (Wijnja 2022)

Hybridiuhkien havannointi on tärkeä osa puolustusstrategiaa. Niiden havainnointi vaatii jaettua tietoisuutta tietoisuutta eri instituutioiden välillä, mikä pohjautuu luotettaviin analyyseihin ja tiedustelutietoihin. Olisi myös tärkeää, että maat tekisivät haavoittuvuuksien kartoittamista, joka auttaisi ymmärtämään maahan liittyviä potentiaalisia iskujen kohteita. Kuitenkin uhkien monitorointi nousee tärkeimpään asemaan havainnoinnissa, sillä hybridi uhkia on haastavaa ennustaa. (Wijnja 2022)

Hybridiuhkien estämisessä on tärkeää, että pystytään lisäämään maan ja kansan sietokykyä kestää painetta ja palautua kriiseistä, jotka ovat hybridiuhkien tuomaa. Sietokyvyn lisääminen on kauan aikaa vievä lähestymistapa ja prosessi ja se vaatii pohjakseen vahvan ja adaptiivisen infrastruktuurin. (Wijnja 2022)

Se, miten hybridihyökkäyksiin vastataan, on paljon hyökkäyksen konteksista riippuvainen. Ennen hyökkäykseen vastaamista on otettava huomioon sen kokonaisvaltainen vaikutus ja kaikki hyökkäykseen liittyvät asiahaarat. Valtioiden välinen linja hyökkäyksiä vastaan voi vaihdella hyvin paljon. Vaikuttavia asianhaaroja ovat esimerkiksi valtion halukkuus käyttää armeijaa ja kyberjoukkoja. (Wijnja 2022)

Valtiotasolla hybridiuhkien torjuntaan panostaminen on suhteellisen uusi asia joillekin valtiolle. Siihen milloin valtion teettämä panostus on alkanut riippuu paljon valtion geologisesta sijainnista ja poliittisten jännitteiden määrästä. NATO:n tasolla hybridiuhkien torjunta on

kauan ollut jokseenkin puutteellista ja suoraa linjausta miten iskuihin vastataan ei ole tehty. Latvia pitää vuoden 2014 Ukrainan tapahtumia todisteena siitä, että NATO ei haluaisi eikä pystyisi puolustamaan Balkanin aluetta Venäjän hybridihyökkäykseltä (Bachmann ja Gunneriusson 2015). NATO:n viidenteen artiklaan ollaan tehty muutosehdotus, jonka avulla jäsenmaat saisivat muista jäsenmaista turvaa myös hybridiuhkia vastaan (Bachmann ja Gunneriusson 2015).

4 Case Venäjä

Venäjä on yksi maailman vaikutusvaltaisimmista maista, mitä tulee globaaliin politiikkaan. Monet maat mukaan lukien EU:n valtiot ja Yhdysvallat ovat riippuvaisia Venäjän vienti-tuotteista, kuten öljystä ja maakaasusta. Useilla mailla on Venäjän kanssa suuria projekteja, jotka ovat vaatineet mittavia investointeja Venäjälle. Venäjä, kuten monet muutkin suurvallat, on käyttänyt paljon resursseja kyber- ja hybriditoimintaympäristöön. Venäjän tiedetään omaavan ydinaseita ja niiden käytöllä uhkailu kuuluu osaksi Venäjän hybridivaikuttamisen strategiaa. Myös armeijajoukkojen strateginen liikuttelu Venäjän raja-alueella voidaan laskea hybridiuhkien luomiseksi, sillä joukkojen liikutelulla saadaan aikaan uhkakuva mahdollisesta hyökkäyksestä. Venäjällä on suuri määrä niin suoraan valtiosidonnaisia kuin valtiositoutumattomia järjestöjä ja organisaatioita, jotka suorittavat tiedustelua ja kyberhyökkäyksiä muihin maihin.

Tässä luvussa käsitellään Venäjän organisoitumista kyber- ja hybriditoimintaympärisössä, millaisia erityylisiä hyökkäyksiä Venäjä on suorittanut ja mitkä ovat olleet kyseisten hyökkäyksien motiivit. Luvun tarkoitus on saada kuva siitä, millaista toimintaa Venäjä on tehnyt hybriditoimintaympäristössä.

4.1 Venäjän tiedustelu ja kybervoimat

Venäjässä toimii ainakin kolme merkittävää toimijaa tiedustelun ja kyberturvallisuuden alalla. Näitä ovat sotilastiedustelu GRU, turvallisuusvirasto FSB ja ulkomaantiedustelu SVR (Riehle 2020). Näiden kolmen lisäksi Venäjällä on myös muita toimijoita, jotka voidaan rinnastaa kyberkyvyiksi, kuten esimerkiksi "Pietarin trollitehdas"Internet Research Agency (McCombie, Uhlmann ja Morrison 2020) ja hakkeriryhmä APT28 sekä sen yhdeksi alahaaraksi epäilty Sandworm (Baezner 2018).

Internet Research Agency tutkimusten mukaan teetti monia tuhansia botti-käyttäjiä Yhdysvaltojen 2016 presidenttien vaalien aikaan (McCombie, Uhlmann ja Morrison 2020). Nämä bottikäyttäjät jakoivat ja tykkäsivät sosiaalisissa medioissa levinneitä propagandajulkaisuja (McCombie, Uhlmann ja Morrison 2020).

APT28 hakkeriryhmä on toiminut aktiivisesti ainakin vuodesta 2007 lähtien. APT28 on tutkimusten valossa liitetty vahvasti Venäjään, sillä suurin osa ryhmän kommunikaatiosta tapahtuu venäjän kielellä ja haittaohjelmien käännösajat vastasivat Moskovan aikavyöhykkeen työaikoja. Hakkeriryhmä on liitetty moniin kybervakoilu operaatioihin, kuten operaatio RussianDoll ja operaatio Fancy Bear. Ryhmän intressit ovat Kaukasuksen alue, Itä-Euroopan hallinnot ja armeijat, NATO ja muut Euroopan turvallisuusorganisaatiot. (Zsolt ja Tamas 2020)

Monet tutkijat, tietoturvayhtiöt ja kyberasiantuntijat ovat yhdistäneet APT28 hakkeriryhmän alahaaran, Sandwormin, moniin Ukrainassa vuoden 2016 jälkeen tehtyihin iskuihin. Yhdistetyt iskut pitävät sisällään NotPetya:n, BadRabbit:in, CrashOverride:n ja VPNFilter:in (Baezner 2018).

4.2 Hyökkäykset

Venäjän valtio on vuosien varrella liitetty moniin eri kyberiskuihin. Usein iskut keskittyvät erityisesti maihin, jotka ovat kuuluneet entiseen Neuvostoliittoon alueeseen, kuten esimerkiksi hyökkäykset, jotka kohdistuivat Viroon vuonna 2007 (Alenius 2013), Georgiaan vuonna 2008 (Deibert, Rohozinski ja Crete-Nishihata 2012) ja Ukrainaan vuoden 2014 jälkeen (Simons, Danyk ja Maliarchuk 2020). Vuoden 2014 Ukrainan venäjämielisen hallinnon kaatumisen ja Krimin niemimaan miehityksen jälkeen iskujen kohteeksi on joutunut usein viimeisempänä mainittu Ukraina. Pelkästään vuoden 2016 jälkeen Ukraina on joutunut monen Venäjän aiheuttaman haittaohjelma iskun kohteeksi. Voisi sanoa, että Ukrainasta on tullut Venäjän testiympäristö itse kehitetyille viruksille sekä kyberhyökkäyksille.

4.2.1 Hyökkäykset Viroon vuonna 2007

Venäjän valtion teettämät poliittiset kyberiskut alkoivat vuonna 2007 Virosta. Hyökkäykset alkoivat sen jälkeen, kun Viro päätti poistaa neuvostoliittoajalta säilyneen pronssipatsaan pois Tallinnasta. Viron tapahtumia voidaan pitää hybridimäisenä hyökkäyksenä, sillä kyberhyökkäysten lisäksi Venäjä myös rahoitti Venäjämielisiä mellakoitsijoita Virossa tapahtuneissa mellakoissa (Alenius 2013).

Kyberhyökkäykset olivat suurimmalta osaa DDoS hyökkäyksiä, joiden kohteena oli Viron valtiolliset verkkosivustot. Hyökkäysten aikana venäjänkielisillä foorumeilla jaettiin ohjeita ja tietoja siitä, miten Viroa pystytään vahingoittamaan erilaisilla kyberhyökkäyksillä kuten esimerkiksi palvelunestohyökkäyksillä (Schmidt 2012). Viron sen hetkinen oikeusministeri Rein Lang julkisti, että tutkimukset mukaan hyökkääjien IP osoiteista paljastui, että hyökkäykset tulivat Venäjältä ja jotkut Moskovassa sijaitsevat Venäjän valtiolliset instituutiot olivat mukana hyökkäyksissä (Alenius 2013).

4.2.2 2016 presidentinvaalit Yhdysvalloissa

Vuoden 2016 pidettyjen Yhdysvaltojen presidentin vaalien jälkeen on ollut paljon puhetta, että Venäjä on yrittänyt vaikuttaa vaalien lopputulokseen. Venäjän epäiltiin sekaantuneen vaaleihin monella tavalla, kuten sosiaalisessa mediassa bottien kautta tapahtuneella vaikuttamisella.

Vuonna 2018 Yhdysvaltojen oikeuslaitos syytti 13 Venäjän kansalaista vaaleihin sekaantumisesta (Linvill ym. 2019). Syytteen mukaan venäläisen oligarkin Jevgeni Prigožin omistama Internet Resesearch Agency aloitti operaationsa vuonna 2014, jonka päämääränä oli kylvää eripuraa Yhdysvaltojen poliittiseen järjestelmään (Linvill ym. 2019). Syytteessä myös viitattiin todisteisiin, joiden mukaan IRA oli luonut monia kuvitteellisia järjestöjä, joiden agendat ja intressit olivat usein toisiaan vastaan. Järjestöjä olivat esimerkiksi Blue Lives Matter (Poliiseja tukeva) ja Black Culture (Vähemmistöjä tukeva ja poliisiväkivaltaan puuttuva) sekä Trumpia tukeva ja Bernie Sandersia tukeva (McCombie, Uhlmann ja Morrison 2020). Järjestöjä luotiin, jotta samoja mielipiteiden omaavat ihmiset saataisiin yhdistettyä ja sitä kautta olisi helpompi vaikuttaa samanmielisten ihmisten mielipiteisiin.

4.2.3 Ukrainan konflikti vuoden 2014 jälkeen

Vuonna 2014 Ukrainassa tapahtui vallankumous, jonka seurauksena sen hetkinen venäjämyönteinen presidentti Viktor Janukovytš erotettiin. Samana vuonna Venäjä miehitti Krimin niemimaan ja vallankumouksen jälkeen Ukrainaan on kohdistunut paljon kyberiskuja, joiden kohteena ovat olleet Ukrainan valtiollisen infrastruktuurin eri osat. Kyberiskuja ovat ol-

leet esimerkiksi CrashOverride (kiristysohjelma), NotPetya (tietokone mato), BadRabbit (kiristysohjelma), VPNFilter (haittaohjelma) ja Python/TeleBot (trojalainen) (Baezner 2018). Yleinen konsensus tutkijoiden ja kyberasiantuntijoiden mukaan on, että todisteiden valossa Venäjä on ollut iskujen takana.

Vuonna 2014 Venäjä hyökkäsi Krimin niemimaalle miehittäen sen ja liittäen sen itseensä. Miehityksen aikana lukuisat Ukrainan valtiolliset internet sivut DDoS hyökkäyksien joutuivat uhreiksi ja Ukrainan tietoverkkoon hyökättiin Snake nimisellä haittaohjelmalla (Kateryнchuk 2019). Myös koko Krimin niemimaan alueen kommunikaatioverkot katkaistiin ja alue eristettiin siten hetkellisesti muusta maailmasta (Kateryнchuk 2019). Niemimaan miehityksen jälkeen Ukrainaan on kohdistunut monia kyberiskuja, joista yksi tunnetuimpia on NotPetya.

Vuonna 2017 maailmanlaajuinen kyberhyökkäys alkoi tietokonemato NotPetyalla, joka vaikutti kiristysohjelmalta (Baezner 2018). NotPetya iski ensimmäisenä päivänä yli 2000 organisaatioon ja 75 prosenttia haittaohjelman kohteista oli Ukrainassa, jossa uhreiksi joutuivat ministeröitä, poliisi, pankkeja, teleoperaattoreita, Kiovan metro ja Borysplin kansainvälinen lentokenttä. (Kateryнchuk 2019). Osa NotPetyan koodista oli peräisin jo aiemmin löydetystä kiristysohjelma Petyasta ja osa NotPetyan ominaisuuksista oli peräisin WannaCry kiristysohjelmasta. NotPetyan ominaisuus, joka erotti sen muista kiristysohjelmista oli se, että se kryptasi datan siten, että sitä oli mahdotonta palauttaa (Baezner 2018). NotPetyan takana epäillään olleen hakkeriryhmä Sandworm.

4.3 Hyökkäysten motiivit

Hyökkäysten taustalla voi olla usein monia eri motiiveeja, joista kaikkia yksityiskohtia ei välttämättä aina saada selville. Yhdysvaltojen syyttäjän ja hallituksen mukaan Venäjän motiivi presidentinvaalien lopputulokseen vaikuttamisella oli Venäjän halu horjuttaa ja kylvää eripuraa Yhdysvaltojen poliittista järjestelmää kohtaan (Linvill ym. 2019).

Entisiin Neuvostoliittoon kuuluneisiin maihin kohdistuneet iskut ovat usein tapahtuneet sen jälkeen, kun ne ovat alkaneet länsimaalaistumaan. Viroon kohdistuneet kyberiskut tehtiin, kun Viro päätti poistaa neuvostoliittoajoista muistuttavia patsaita vuonna 2007 (Alenius

2013). Ukrainaan kyberiskut ajoittuvat suurelta osin sen ajanjakson jälkeen, kun Ukrainan venäjämielinen hallinto kaatui vuonna 2014.

Tästä voidaan päätellä, että hyökkäysten motiivit entisiin Neuvostoliiton alueisiin ovat jollain tasolla geopoliittisia. Venäjä on osoittanut iskuilla ja uhittelulla halunsa pitää kyseiset maat heidän etupiirissään ja vähentää maiden halua liittyä esimerkiksi EU:hun tai NATO:on.

5 Yhteenveto

Voidaan todeta, että niin hybridi- kuin kybervaikuttamisen tapoja on monia ja toteutustavat mukautuvat tarpeiden ja haluttujen tulosten mukaan. Suurin syy miksi monet maat päättävät käyttää kybervaikuttamisen keinoja johtuu siitä, että sitä on vaikeaa jäljittää takaisin tekijään ja se on paljon halvempaa kuin klassinen sodankäynti. Myös hybridi- ja kybervaikuttamisen mukanaan tuomat voimasuhteiden muutokset ovat vaikeuttaneet monien maiden toiminta-strategioita ja lisänneet halua panostaa niihin toimintaympäristöihin.

Varsinkin 2000-luvulla kyberympäristössä tapahtuvat hyökkäykset ja vakoilu ovat lisääntyneet huomattavasti. Myös hybridiuhat ovat kasvaneet merkittävästi. Kaikki suurvallat ovat panostaneet kyberympäristössä tapahtuvaan toimintaan huomattavasti, minkä voi huomata siitä, miten moniin hybridi- ja kyberiskuihin maailman vaikutusvaltaisimpia valtioita kuten Yhdysvallat, Kiina ja Venäjä on liitetty. Tiedot valtioiden kybertoimintaympäristössä operoivista toimijoista ovat salaisia ja on vaikea tietää, mitkä hakkeriryhmät ovat valtioiden rahoittamia ja mitkä ovat valtioonsitoutumattomia toimijoita. Tietojen luottamuksellisuuden takia on vaikeaa löytää luotettavaa tietoa toimijoista ja kaikista heidän suorittamista operaatioistaan.

Suurvaltana Venäjällä on paljon resursseja ja myös halua panostaa huomattavia määriä resursseja kyber- ja hybriditoimintaympäristöön. Venäjään on liitetty moniin kyberiskuihin ja Venäjä myös käyttää hyväkseen hybridiuhkien luomista. Venäjän on ydinasevaltio, joka on liikuttanut armeijajoukkojaan strategisesti maansa sisällä luoden uhkakuvia hyökkäyksestä. Kaikilla valtioilla onkin syytä panostaa kyber- ja hybridiuhkien torjuntaan ja rakentaa infrastruktuurinsa siten, että se kestää mahdollisten iskujen aiheuttaman rasituksen.

Lähteet

Abeyratne, R. 2011. “Cyber terrorism and aviation—national and international responses”. *Journal of Transportation Security* 4 (1): 337–349. https://doi.org/https://doi-org.ezproxy.jyu.fi/10.1007/s12198-011-0074-3.

Akbanov, Maxat, Vassilios G. Vassilakis ja Michael D. Logothetis. 2019. “Ransomware detection and mitigation using software-defined networking: The case of WannaCry”. *Computers Electrical Engineering* 76:111–121. ISSN: 0045-7906. https://doi.org/https://doi.org/10.1016/j.compeleceng.2019.03.012.

Alenius, K. 2013. “Victory in Exceptional War: The Estonian Main Narrative of Cyber Attacks in 2007”. Teoksessa *The Fog of Cyber Defence,* toimittanut J. Rantapelkonen ja M. Salminen, 78–87. Tampere: Juves Print oy.

Almäng, Jan. 2019. “War, vagueness and hybrid war”. *Defence Studies* 19 (2): 189–204. https://doi.org/10.1080/14702436.2019.1597631.

Bachmann, S., ja H. Gunneriusson. 2015. “Hybrid wars: The 21st-century’s new threats to global peace and security”. *Scientia Militaria, South African Journal of Military Studies* 42:77–98.

Baezner, M. 2018. “Addendum to Cyber and Information warfare in the Ukrainian conflict”. Teoksessa *Center for Security Studies (CSS),* 32–54. ETH Zürich.

Biju, J., N. Gopal ja A. Prakash. 2019. “IRJET - Cyber Attacks and Its Different Types”. *International Research Journal of Engineering and Technology (IRJET)* 3:4849–4852.

Deibert, Ronald J., Rafal Rohozinski ja Masashi Crete-Nishihata. 2012. “Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war”. *Security Dialogue* 43 (1): 3–24. https://doi.org/10.1177/0967010611431079.

Djaja, A. 2020. “The Rise of Cyber Warfare”. *Jurnal Kajian Peradaban Islam* 3:19–21.

Engel, V. J. L., E. Joshua ja M. M. Engel. 2020. “Detection of Cyber Malware Attack Based on Network Traffic Features Using Neural Network”. *Khazanah informatika* 6 (1): 26–32. https://doi.org/10.23917/khif.v6i1.8869.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu ja Phillip Laplante. 2011. “Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political”. *IEEE Technology and Society Magazine* 30 (1): 28–38. https://doi.org/10.1109/MTS.2011.940293.

Hribar, Gašper, Iztok Podbregar ja Teodora Ivanuša. 2014. “OSINT: A “Grey Zone”?” *International Journal of Intelligence and CounterIntelligence* 27 (3): 529–549. https://doi.org/10.1080/08850607.2014.900295.

Katerynchuk, P. 2019. “Challenges for ukraine’s cyber security: National dimensions”. *Eastern Review* 8:137–147. ISSN: 0045-7906. https://doi.org/http://dx.doi.org/10.18778/1427-9657.08.05.

Linvill, Darren L., Brandon C. Boatwright, Will J. Grant ja Patrick L. Warren. 2019. ““THE RUSSIANS ARE HACKING MY BRAIN!” investigating Russia’s internet research agency twitter tactics during the 2016 United States presidential campaign”. *Computers in Human Behavior* 99:292–300. ISSN: 0747-5632. https://doi.org/https://doi.org/10.1016/j.chb.2019.05.027.

McCombie, S., A. Uhlmann ja S. Morrison. 2020. “The US 2016 presidential election Russia’s troll farms”. *Intelligence and National Security* 35:95–114.

Palasinski, M., ja L. Bowman-Grieve. 2017. “Tackling Cyber-Terrorism: Balancing Surveillance with Counter-Communication.” *ProQuest Central; SciTech Premium Collection; Social Science Premium Collection,* 30 (2): 556–568.

Riehle, Kevin P. 2020. “Russia’s intelligence illegals program: an enduring asset”. *Intelligence and National Security* 35 (3): 385–402. https://doi.org/10.1080/02684527.2020.1719460.

Ripa, Sadia Parvin, Fahmida Islam ja Mohammad Arifuzzaman. 2021. “The Emergence Threat of Phishing Attack and The Detection Techniques Using Machine Learning Models”. Teoksessa *2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI),* 1–6. https://doi.org/10.1109/ACMI53878.2021.9528204.

Schmidt, Andreas. 2012. “At the boundaries of peer production: The organization of Internet security production in the cases of Estonia 2007 and Conficker”. *Telecommunications Policy* 36 (6): 451–461. ISSN: 0308-5961. https://doi.org/https://doi.org/10.1016/j.telpol.2012.02.001.

Simons, G., Y. Danyk ja T. Maliarchuk. 2020. “Hybrid war and cyber-attacks: creating legal and operational dilemmas”. *Global Change, Peace Security* 32:337–342. https://doi.org/10.1080/14781158.2020.1732899.

Timofeyev, Yuriy, ja Oksana Dremova. 2022. “Insurers’ responses to cyber crime: Evidence from Russia”. *International Journal of Law, Crime and Justice* 68.

Wijnja, Kim. 2022. “Countering hybrid threats: does strategic culture matter?” *Defence Studies* 22 (1): 16–34. https://doi.org/10.1080/14702436.2021.1945452.

Zargar, Saman Taghavi, James Joshi ja David Tipper. 2013. “A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks”. *IEEE Communications Surveys Tutorials* 15 (4): 2046–2069. https://doi.org/10.1109/SURV.2013.031413.00127.

Zsolt, Bederna, ja Szadeczky Tamas. 2020. “Cyber Espionage through Botnets”. *Security Journal* 33 (1): 43–62. https://doi.org/https://doi.org/10.1057/s41284-019-00194-6.