Iida Lehto

POLIITTISESTI MOTIVOITUNUT KYBERVAKOILU JA TIEDUSTELUTOIMINTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Lehto, Iida
Poliittisesti motivoitunut kybervakoilu ja tiedustelutoiminta
Jyväskylä: Jyväskylän yliopisto, 2020, 37 s.
tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Räisänen, Jaana

Tässä kandidaatintutkielmassa pohditaan poliittisesti motivoitunutta kybervakoilua, sekä sitä, kuinka se ilmenee modernissa tietoyhteiskunnassa. Tämän lisäksi tutkimuskohteena on valtiollinen tiedustelutoiminta, jonka avulla pyritään parantamaan valtion operatiivista tilannetietoisuutta vieraan valtion toimintaa kohtaan. Tutkielmassa määritellään myös Suomen turvallisuuspolitiikan kannalta oleellisia näkymiä kybervakoilun ja -tiedustelun kokonaisuudesta. Kybervakoilulla tarkoitetaan yleisesti ottaen laittomin keinoin hankittua tiedonkeruuta kybertilassa, joka tässä kontekstissa ymmärretään poliittisesti motivoituneena. Kybertiedustelu taas kuvaa niitä keinoja, joilla valtio hankkii tiedustelutietoa uhkana pidetystä tahosta, kuten toisesta valtiosta. Kybervakoilu sekä tiedustelutoiminta muodostavat monitahoisen kokonaisuuden, johon limittyy useita kyber- ja reaalimaailman ilmiöitä, kuten APT-hyökkäyksiä, informaatio-operaatioita sekä poliittista liikehdintää. Suomen turvallisuuspolitiikan kannalta kybervakoilu nähdään kohonneena uhkana.

Asiasanat: kybervakoilu, kybertiedustelu, kyberoperaatiot, turvallisuuspolitiikka

ABSTRACT

Lehto, Iida
Politically motivated cyber espionage and intelligence activities
Jyväskylä: University of Jyväskylä, 2020, 37 pp.
Information Systems Science, Bachelor's Thesis
Supervisor(s): Räisänen, Jaana

This Bachelor's thesis examines politically motivated espionage and the way it manifests itself in the modern information society. In addition to this, the subject of the study is to examine government intelligence activities, which are aimed at improving the operative and situational awareness of foreign countries' actions. Furthermore, this study defines the essential views on the field of cyber espionage and intelligence in the context of Finnish security policy. Cyber espionage describes the illegal actions by which an entity collects information in the cyber space, which in this context is viewed as politically motivated action. Cyber intelligence, on the other hand, describes the methods by which a state obtains intelligence from a party considered to be a threat, such as another state. Cyber espionage, and intelligence form a complex entity that envelop several cyber and real-world phenomena, such as APT attacks, information operations, and political movement. From the point of view of Finnish security policy, cyber espionage is seen as an increased threat.

Keywords: cyber espionage, cyber intelligence, cyber operations, security policy

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kybervakoilun ja valtiollisen tiedustelun tutkimus on kasvattanut merkitystään viime vuosina, sillä kybertoimintaympäristön hyödyntämisestä vakoiluoperaatioissa on tullut kustannustehokkaampaa, ovelampaa sekä huomaamattomampaa teknologisten harppausten seurauksena (Lohse, Meriniemi, Honkanen, 2019, s. 34). Kyberpuolustuksen keskeisenä ongelmana onkin viime vuosina nähty vakoiluhaittaohjelmien monimutkaistuminen sekä hyökkääjien alati paremmat operatiiviset kyvyt ja mahdollisuudet (Limnéll, 2014).

Poliittinen kybervakoilu on valtioidenvälistä toimintaa, jossa toiseen valtioon pyritään saamaan informaatioyliote keräämällä tiedustelutietoa laittomin keinoin (Harknett & Smeets, 2020). Valtiollinen tiedustelutoiminta pyrkii määrittelemään sekä torjumaan niitä uhkia, jota kohdistuu valtiolliseen turvallisuuteen (Bigelow, 2019). Enenevässä määrin kybermaailman tapahtumat ja uhkakuvat vaikuttavat kansalliseen kokonaisturvallisuuden käsitykseen (Suojelupoliisi, 2018). Kybervakoilun sekä tiedustelutoiminnan tutkimus on tässä suhteessa erityisen tärkeää, sillä uhkien torjuminen nähdään osittain asymmetrisenä (Toveri & Pelttari, 2020). Epätasapainon ratkaisemiseksi on löydettävä yhtäältä uusia keinoja sekä toimintamalleja uhkien torjuntaan, kuin myös kehitettävä kansainvälistä yhteistyötä osaamisen yhdistämiseksi (Weissbrodt, 2013; Lledo-Ferrer & Dietrich, 2020).

Tässä tutkielmassa pohditaan poliittisesti motivoitunutta kybervakoilua sekä sen toiminnan muotoja. Kybervakoilun toimijoita sekä heidän toimintamallejaan arvioidaan kriittisesti kirjallisuuteen perustuen. Tutkielma keskittyy täten myös rajaamaan keskeisimmät motiivit vakoilun taustalla, sekä määrittämään ne tahot, jotka vakoiluoperaatioita suorittavat. Tämän lisäksi tarkastellaan valtioiden omaa tiedustelutoimintaa, jonka tarkoituksena on kokonaisvaltaisen uhkakuvan laatiminen sekä hybridiuhkiin vastaaminen valtiollisella tasolla. Lisäksi tutkimuksessa pohditaan Suomen valtiollista tiedustelutoimintaa sekä suojautumista kybervakoilulta. Tämän lisäksi pohditaan globaalin yhteistyön implikaatioita sekä kybervakoilun lainsäädännöllistä asemaa kansainvälisen lainsäädännön puitteissa.

Tutkimuskysymykset ovat seuraavanlaisia:

- Mitä on poliittisesti motivoitunut kybervakoilu ja kuinka se ilmenee?
- Kuinka tiedusteluviranomaiset harjoittavat toimintaansa vakoilun estämiseksi ja havaitsemiseksi?
- Millainen on kybervakoilun sekä tiedustelun toimintaympäristö Suomessa?

Tämä kandidaatintutkielma on toteutettu kuvailevana kirjallisuuskatsauksena, jonka muoto on narratiivinen (Salminen, 2011). Tämän kirjallisuuskatsauksen muodon on tarkoitus tuottaa looginen sekä akateeminen, mutta samalla helppolukuinen kokonaisuus. Lähdeainestoa on haettu pääasiallisesti AND-OR-hakulauserakenteita käyttäen Jyväskylän yliopiston JYKDOK-tietokannasta, sekä Scopuksesta ja Google Scholarista. JYKDOK:ia on käytetty sekä hakemaan yksittäisiä artikkeleja tietyillä hakusanoilla että pääsemään käsiksi englanninkielisiin tietokantoihin, esimerkiksi Taylor & Francis Groupiin.

Hakutuloksia haettiin ensisijaisesti englanniksi, jolloin käytettiin hakusanoina pääasiassa kolmea termiä, jotka olivat: ”cyber espionage”, ”cyber reconnaissance” ja ”cyber intelligence”. Tämän lisäksi hakutermeinä käytettiin suomenkieliselle aineistolle termejä ”kybervakoilu” ja ”kybertiedustelu”. Haku toteutettiin usein käytännössä siten, että yhtenevät englanninkieliset termit sijoitettiin AND-lausekkeen sisään ja sanan suomenkieliset vastineet sijoitettiin OR-lausekkeen sisään. Käytännössä hakulauseke saattoi siis olla esimerkiksi tällainen: (”cyber espionage” AND ”cyber reconnaissance”) OR (”kybervakoilu” AND ”kybertiedustelu”).

Materiaali koostuu pääasiassa tieteellisistä artikkeleista sekä konferenssijulkaisuista, mutta myös tiedekirjoista sekä luotettavaksi todennetuista sähköisistä lähteistä, kuten Valtioneuvoston julkaisuista. Lähteiden luotettavuutta on pyritty arvioimaan artikkeli- ja konferenssilähteiden puolesta etenkin Julkaisufoorumin julkaisukanavahaun tuottamien luokitusten perusteella. Tutkielmaa rakentaessa on pyritty käyttämään mahdollisimman paljon 1–3:n luokituksen saaneita lähteitä. Verkkoaineistoa, kuten erilaisia raportteja, on pyritty arvioimaan niiden lähdeorganisaation tai -sivuston luotettavuuden arvioinnilla. Tutkielmaan on otettu mukaan luotettavien tahojen, kuten valtiollisten toimijoiden sekä tunnettujen järjestöjen, tuottamia julkaisuja. Tämän lisäksi on arvioitu lähteiden saamaa viittausten määrää, jota on peilattu esimerkiksi julkaisuvuoteen sekä aiheen tunnettavuuteen. Tässä tutkielmassa on suosittu etenkin sellaisia tekstejä, jotka lähdeviittaustensa määrän perusteella voidaan arvioida luotettaviksi.

Tutkielman ensimmäinen luku koostuu lyhyestä historiakappaleesta, sekä kybervakoilun ja -tiedustelun käsitteidenmäärittelystä. Ensimmäinen luku nivoo yhteen kybervakoilun sekä kybertiedustelun merkityksen globalisoituneessa maailmassa. Toisessa sisältöluvussa tarkastellaan tarkemmin kybervakoilua poliittisena ilmiönä, jonka pohjalta määritellään poliittisesti motivoituneiden kyberhyökkäyksen vaiheet. Tämän lisäksi tarkastellaan poliittiseen kybervakoiluun käytettäviä APT-hyökkäyksiä sekä valtioiden konkreettista toimintaa ky-

bervakoilussa. Lopuksi tarkastellaan Suomen tilannetta kybervakoilun saralla. Neljäs luku keskittyy kybertiedusteluun sekä kybervakoilulta suojautumiseen. Tässä luvussa käsitellään eri tiedustelutoiminnan lajeja, sekä tarkastellaan älykästä tiedustelua ja hämäystä potentiaalisina kybervakoilun torjuntamenetelminä. Lopuksi arvioidaan tiedustelupoliittista lainsäädäntöä sekä mahdollisuuksia kansainväliselle yhteistyölle. Tutkielman yhteenvetokappale nivoo käsitellyt asiat sekä johtopäätökset lopuksi yhteen.

2 HISTORIALLINEN KONTEKSTI JA KESKEINEN KÄSITTEISTÖ

Kyberympäristön ja digitaalisen maailman kehitys on muuttanut maailmaa perustavanlaatuisesti ja saanut aikaan suuria teknologisia harppauksia. Samalla kehitys on kuitenkin mahdollistanut entistä kehittyneempien kybervakoilu ja -vaikutusoperaatioiden ilmaantumisen. (Lohse, Meriniemi & Honkanen, 2019, s. 34.) Tässä tutkielmassa kybervakoilua ja -tiedustelua käsitellään toisiaan vastakkaisina ilmiöinä. Näkemyseroja tiedustelun ja vakoilun määritelmistä on löydettävissä laajalti turvallisuuspoliittisessa keskustelussa, sillä joissain tapauksissa ne voidaan ymmärtää myös lähestulkoon synonyymeina (esim. Jansson & Sihvonen 2018; Lehto & Limnéll 2017b). Tutkimuskohteen selkeyttämiseksi tässä tutkielmassa pyritään kuitenkin kuvaamaan tiedustelua tietyn valtion laillisten tiedusteluviranomaisten toiminnan kautta. Vakoilutoimintaa kuvataan sen lainvastaisuuden näkökulmasta toimintana, joka ilmenee etenkin valtiollisella tasolla laittomien keinojen käyttämisenä tiedonkeruussa kybertilassa.

Hyökkäykselliset kyberoperaatiot kuvastavat erilaisia toimia, joita kybermaailmassa voidaan tehdä toista kybertoimijaa vastaan. Tässä tutkielmassa vastakkainasettelu fokusoidaan etenkin valtioidenvälisiin kyberoperaatioihin. Hyökkäykselliset kyberoperaatiot eivät kuitenkaan ilmaannu tyhjästä, vaan niitä edeltää usein vakoilu- ja tiedusteluoperaatioita (Moran, 2010). Tässä tutkielmassa puhutaan kybervakoilusta ja -tiedustelusta, jotka tapahtuvat ”kybertilassa” tai ”kybermaailmassa”. Kybertilalla tarkoitetaan yleisesti globaalille tietoyhteiskunnalle ominaista informaatioinfrastruktuuria, jonka kehikossa tietokoneiden muodostama ulottuvuus toimii (Harknett & Smeets, 2020).

Tässä luvussa esitellään vakoilun ja valtiollisen tiedustelun historiallista kontekstia reflektoiden sitä modernin sodankäynnin tapahtumiin. Tämän lisäksi otetaan tarkasteluun kybervakoilun ja -tiedustelun käsitteet, sekä pohditaan niiden merkitystä globaalin politiikan ympäristöön. Tämän luvun tarkoituksena on johdatella lukija tutkielman aihepiiriin avaamalla tutkimuskysymyksissä käsiteltyjä aiheita laajassa mittakaavassa.

2.1 Historiallinen konteksti

Tiedustelulla on historiallisesti ollut suuri rooli valtiollisten intressien ajamisessa. Tiedustelutietoa on käytetty sotapoliittisena keinona läpi maailmanhistorian, sillä sen avulla voidaan kääntää valta-asetelmia vaivihkaa ja konfliktia heti herättämättä (Jansson & Sihvonen, 2018). 1900-luvun ensimmäisellä vuosikymmenillä Iso-Britanniaan perustettiin kotimaan tiedustelusta vastaava MI5 ja ulkomaan tiedusteluun keskittyvä MI6, jotka seilasivat tiedustelupolitiikan aallonharjalla luoden perustan monelle muulle kansalliselle tiedustelupalvelulle, kuten Yhdysvaltain CIA:lle, eli Central Intelligence Agencylle (Carlisle, 2005, s. 21). Toisen maailmansodan aikana tiedustelusta muovautui sodan ”neljäs ulottuvuus”, jonka seurauksena modernin tiedustelunpolitiikan kehitys sai alkunsa (Farago, 2012). Esimerkiksi Normandian maihinnousua on kuvattu maailmanhistorian onnistuneimmaksi harhautusoperaatioksi, sillä liittoutuneiden tiedusteluviranomaiset onnistuivat uskottelemaan, että hyökkäys tulisi tapahtumaan Normandian sijaan Pas de Calaisissa. Tämä harhautus sai saksalaisjoukot kohdistamaan miehityksensä taktisella hetkellä väärään paikkaan. (Carlisle, 2005, s. 21.) Toisen maailmansodan jälkeen valtiollinen tiedustelutoiminta vakiinnutti roolinsa maailmanpoliittisessa toiminnassa. Sodan vauhdittama teknologinen kehitys puski uusia muotoja myös tiedusteluoperaatioiden käytössä. (Denécé, 2013.)

Suomen tiedustelutoimintaa ja sen näkyvyyttä toisen maailmansodan jälkeen taas kuvaa hyvin Stella Polaris-operaatio. Jatkosodan päätyttyä vuonna 1944 Suomessa pelättiin Neuvostoliiton sotilaallisia jatkotoimia ja mahdollista Suomen miehittämistä. Suomen siihen aikaan nuori tiedustelupalvelu haluttiin suojata, jonka vuoksi kehitettiin operaatio siirtää Suomen tiedusteluosaston henkilöstöä ja arkistoja Ruotsiin. (Aid, 2002.)

Kylmän sodan aikana poliittinen idän ja lännen vastakkainasettelu oli varsin selkeä. Tällöin suurpiirteittäin katseltuna tiedustelu- ja vakoilutoiminnalla pyrittiin luomaan tilannekuvaa varsin tulenarassa poliittisessa ympäristössä. Tämä toisaalta johti myös molemminpuoliseen epäluottamukseen idän ja lännen suhteiden kireimpinä aikoina. (Carlisle, 2005, s. 22–25.) Neuvostoliiton romahdus vuonna 1991, sekä 2000-luvun vaihteessa tapahtunut terrorismin roolin merkittävä kasvu globaalissa turvallisuusympäristössä, johtivat tiedustelupolitiikassa painopisteiden uudelleenmäärittelyyn. Yhdysvaltain valtiota kohtaan toteutetut terrori-iskut vuonna 2001 ja niitä seurannut sota terrorismia vastaan antoivat uudenlaisen suunnan tiedusteluoperaatioille (Rudner, 2004). Terrorisminvastainen lainsäädäntö onkin itsessään edistänyt tiedustelupolitiikan kehitystä, sillä se on taannut tiedusteluviranomaisille laajemman kirjon työkaluja terrorismin ja sitä kautta myös esimerkiksi vakoilurikosten tutkimiseen (Gellman, 2002).

Neuvostoliiton johtaman itäblokin luhistumisella sekä vanhojen valtasuhteiden uudelleenasettelulla oli ainakin hetkellisesti rauhoittava vaikutus idän ja lännen jännitteisiin. Terrorismin vaikutuksesta itä ja länsi kokivat saaneensa

yhteisen vihollisen, jonka vuoksi kylmän sodan aikaiset jännitteet saivat väistyä. (Ohra-aho, 2020.) Idän ja lännen hetkellistä aseveljeyttä ja kumppanuutta kuvaa esimerkiksi se, että vuonna 2002 Venäjän ja Pohjois-Atlantin liiton Naton välille perustettiin yhteisiä uhkia vastustava kumppanuusvaltuusto, The NATO-Russia-council (Nato Public Diplomacy Division, 2013). Lämpimämpiä suhteita kuvastaa myös se, että Nato ei kohdistanut aktiivista sotilastiedustelua Venäjään viiteentoista vuoteen (Ohra-aho, 2020).

Tilanne muuttui kuitenkin Ukrainan kriisin puhjettua vuonna 2014, kun Venäjä valtasi Krimin niemimaan ja aloitti sotatoiminnan Itä-Ukrainassa. Ohra-ahon (2020) mukaan kohtalaisen rauhallisen yhteiselon jälkeen Venäjän toimet Ukrainassa tulivat länsimaille yllätyksenä. Painopiste heilahti täten takaisin valtiolliseen tiedusteluun ja geopoliittiset suhteet kiristyivät. Lännessä tiedustelun kentällä kohdistettiin operaatioita nyt entistä selkeämmin etenkin Venäjään, Kiinaan ja Pohjois-Koreaan.

2.2 Kybertiedustelun määritelmä

Kybertiedustelun tavoitteena on salaisen tiedon hankkiminen. Valtioiden välistä tiedonhankintaa kohdistetaan laaja-alaisesti yksittäisiin ihmisiin, hallituksiin ja poliittisiin vastustajiin. Tiedustelu ei kuitenkaan tapahdu tyhjiössä, vaan sille tulisi olla poliittisesti, sotilaallisesti sekä laillisesti tarkoin määritetyt päämäärät. (Lohse & Viitanen, 2019, s. 29–36.) Bigelow:n (2019) mukaan valtion tiedustelutoimintaa tulisi harjoittaa jatkuvasti, jotta ulkoiset uhkakuvat voitaisiin määritellä mahdollisimman tarkasti. Hänen mukaansa rutiininomainen tiedustelu lisää valtion valmiutta toteutumattomiin, mutta ehkä tulevaisuudessa häämöttäviin kyberhyökkäyksiin ja takaa paremman puolustuskyvyn.

Tiedustelulla pyritään luomaan tietynlaista tilannetietoisuutta vastustajan aikeisiin, sekä mahdollisesti maalittamaan omia tavoitteita tulevista kyberoperaatioista (Lehto & Limnéll, 2017b). Tiedustelu on tässä tutkielmassa mielletty puolustukselliseksi kyberoperaatioksi. Tiedustelusta voidaan käyttää myös nimitystä ”vastatiedustelu” kuvaamaan sen puolustuksellista luonnetta. Tällöin sanapari kuvaamaan vakoilua ja tiedustelua on kuitenkin yleensä tiedustelu ja vastatiedustelu (esim. Carlisle, 2005; Lehto & Limnéll, 2017a). Tiedustelutoimintaa ohjaavat ennen kaikkea kansalliset tavoitteet ja uhkakuvat. Tiedustelua ja vakoilua ympäröivässä keskustelussa tulee kuitenkin ottaa huomioon, että vastakkainasettelu käsitteiden välillä on usein vääristynyttä. (Pun, 2017.) Tiedustelua perustellaan yleensä kansallisen turvallisuuden suojelemisen näkökulmasta ja vastustajien luomien uhkakuvien ymmärtämisellä. Yleisesti ottaen tiedustelussa käytetty keinovalikoima toista valtiota kohtaan voidaan kuitenkin nähdä kohdistettuna vakoiluna. Käytännössä siis valtion kritisoidessa toisten valtioiden vakoilutoimintaa, toteuttavat he usein sitä myös itse omassa tiedustelutoiminnassaan. (Pun, 2017.)

Kansainvälisen lainsäädännön puute vie valtiollisen tiedustelutoiminnan siis auttamatta toimimaan toisaalta laillisuuden ja toisaalta laittomuuden väli-

maastossa. Globaalin maailman verkottuneisuuden ja laajojen turvallisuusuhkien vuoksi kybertiedustelu nähdään kuitenkin välttämättömänä toimena poliittisella kentällä toimimiselle ja kansallisen turvallisuuden suojaamiselle. (Gunneriusson & Ottis, 2013.)

2.3 Kybervakoilun määritelmä

Enisan (2020) raportti kuvaa kybervakoilua toiminnaksi, jossa tietokoneen ja tietoverkkojen avulla pyritään pääsemään laittomasti käsiksi salassa pidettävään tietoon. Keskeisenä motiivina on usein poliittinen vaikuttaminen, taloudellinen hyöty ja ideologian ajaminen. Tässä tutkielmassa keskitytään etenkin poliittisin syin tapahtuvaan kybervakoiluun. Hanska (2013, s. 177) kuvaa kybervakoilua eräänlaiseksi hiljaiseksi sodankäynniksi. Kybervakoilu voidaankin nähdä vastapuolen tilannekuvan muodostamisen operaationa, jonka onnistuminen on pitkälti riippuvaista operaation kyvystä pitää itsensä näkymättömänä.

Valtioiden suorittamat kyberoperaatiot, jotka kohdistuvat toiseen valtioon ovat pääasiassa motivoituneet joko tiedollisesti tai sotilaallisesti (Prislan & Bernik, 2012). Tiedollisesti motivoituneet kyberoperaatiot pyrkivät vakoilun keinoin keräämään tietoa toisen valtion taloudellisista, sotilaallisista, poliittisista tai yhteiskunnallisista päämääristä. Sotilaallisesti motivoituneet kyberoperaatiot viittaavat perinteisen sodankäynnin keinovalikoimaan, joita toteutetaan kyberympäristössä tai sen avulla. Usein kybervakoilu ja tiedollisesti motivoituneet kyberoperaatiot voidaan nähdä sotaa lievempänä valtioiden välisenä vaikuttamisen muotona. (Prislan & Bernik, 2012.) Kybervakoilulla ja sen kerryttämällä tiedolla voi kuitenkin olla suuri vaikutus valtioiden välisiin voimasuhteisiin ja globaalin politiikan ilmapiiriin (Harknett & Smeets, 2020).

Perinteisesti vakoilutoiminta on usein edellyttänyt fyysistä läsnäoloa esimerkiksi vakoilun kohdemaassa. Kuitenkin teknologian kehityksen ja globaalin verkottuneisuuden myötä vakoilun rooli on nykyään merkittävimmillään kybermaailmassa. (Weissbrodt, 2013.) Itse vakoilun päämäärä, eli salaisen tai muuten julkisuudelta piilossa olevan tiedon keruu, on kuitenkin kautta aikojen pysynyt samana (Pun, 2017). Weissbrodt (2013) kertoo, että kybervakoilua tulisi kohdella perinteistä vakoiluakin vakavampana uhkana, sillä kybervakoilu on huomattavasti tunkeilevampaa ja sillä on suurempi kapasiteetti käsitellä kerättyä tietoa. Kybervakoilu ulottuu täten siis perinteistä vakoilua laajemmalle.

Kansainvälisen lain puitteissa kybervakoilulle ei ole erillisiä laillisia säädöksiä, vaan valtioiden tulee itse määritellä tekojen rankaistavuus (Gunneriusson & Ottis, 2013). Kuitenkin kybermaailman globaalius tuo haasteita paikallisille lainsäädännöille. Kybervakoilussa kiinnijäämisen riskit ovat huomattavasti pienemmät kuin perinteisessä vakoilussa esimerkiksi siksi, että vakoilija voi operoida täysin toiselta puolelta maapalloa. (Weissbrodt, 2013; Gunneriusson & Ottis, 2013.) Esimerkiksi pohjoismaisesta kyberyhteistyöstä voisi tässä tapauksessa olla hyötyä (Hanska, 2013, s. 177).

3 POLIITTISESTI MOTIVOITUNUT KYBER-VAKOILU

Vakoilun rooli on muuttanut muotoaan kehittyneissä yhteiskunnissa. Perinteisen vakoilun tehokkaammaksi muodoksi on noussut verkottuneen yhteiskunnan kehityksen seurauksena kybervakoilua. Kybervakoilu nähdäänkin erityisen kustannustehokkaana ja matalariskisenä vakoiluoperaationa. (Lohse, Meriniemi & Honkanen, 2019, s. 34.)

Hyökkäävän tahon motiiveja ja agendaa kybervakoiluoperaatioissa voi olla vaikea määritellä tai ymmärtää. Yleisesti voidaan kuitenkin luokitella poliittisesti motivoituneen kybervakoilun tavoitteet kahdeksi osa-alueeksi. Gunneriusson ja Ottis (2013) määrittelevät, että kybervakoilun tavoitteena on yleisimmin salaisen tiedon keruu tai tulevan kyberhyökkäyksen alustus ja valmistelu. Poliittisesti motivoitunut kybervakoilu kohdistuu niin ikään esimerkiksi poliittisen päätöksenteon kannalta oleellisten tietojen keruuseen (Suojelupoliisi, 2018). Kyberhyökkäystä alustava vakoilu sen sijaan pyrkii selvittämään etenkin vastapuolen kyvykkyyksiä ja valmiuksia (Moran, 2010).

Tässä kappaleessa käsitellään kybervakoilua etenkin poliittisena ilmiönä. Kybervakoilulla on kuitenkin huomattavasti myös taloudellisia ulottuvuuksia, jotka voivat liittyä esimerkiksi yritysvakoiluun (Suojelupoliisi, 2018). Tässä tutkielmassa käsitellään kuitenkin valtioiden välistä tai ainakin jollain tapaa valtioavusteista kybervakoilua, jonka vuoksi pohdinta taloudellisesta kybervakoilusta jätetään pois. Tämä kappale vastaa tutkimuskysymykseen ”Mitä on poliittisesti motivoitunut kybervakoilu ja kuinka se ilmenee?”. Tätä tutkimuskysymystä pohditaan etenkin tämän kappaleen kolmessa ensimmäisessä sisältöluvussa. Lisäksi pohditaan kybervakoilun osalta tutkimuskysymystä ”Millainen on kybervakoilun sekä tiedustelun toimintaympäristö Suomessa?”, johon pureudutaan kappaleen neljännessä luvussa.

3.1 Kybervakoilusta hyökkäykseen

Kybervakoilu nähdään poliittisessa kontekstissa yleisesti ottaen valtioiden välisenä laittomana informaation keräämisenä (Gunneriusson & Ottis, 2013). On tärkeä ymmärtää, että kybervakoilu on usein vain yksi osa laajempaa valtioidenvälistä operointia kybertilassa. Kyberoperaatiot ovat usein linkittyneet toisiinsa, eivätkä tapahdu tyhjiössä. Kyberkampanjoiksi luonnehditaan sellaisia kyberoperaatioita, jotka ovat toisiinsa kytköksissä ja pyrkivät samaan operatiiviseen tavoitteeseen. (Harknett & Smeets, 2020.) Hyökkäyksellisestä näkökulmasta esimerkiksi kybervakoilu voi olla osa laajempaa kyberkampanjaa ja sillä voi olla yksittäistä operaatiota laajemmat tavoitteet. Moranin (2010) kuvaama poliittisesti motivoituneen kyberkonfliktin vaiheittaisesta etenemisestä voidaan käyttää avaamaan kybervakoilun roolia osana valtiollisen kybertoiminnan kokonaiskuvaa. Alla oleva kuvio on itse piirretty suomennos Moranin (2010) tutkimuksesta koskien poliittisen kyberhyökkäyksen etenemisen vaiheita ja niihin varautumista.

KUVIO 1 Kybervakoilusta hyökkäykseen (Moran, 2010)

Piilevät jännitteet ovat Moranin (2010) mukaan jo olemassa olevia konfliktin alkuja, joita esiintyy esimerkiksi valtioiden poliittisten tavoitteiden ollessa vastakkain. Hän kuvaa piileviä jännitteitä laaja-alaisena jännitteiden verkostona, joita esiintyy miltei kaikkien niiden tahojen välillä, jotka osallistuvat kansainväliseen politiikkaan. Piilevät jännitteet ovatkin usein pitkäkestoisia ja hellittämättömiä poliittisia latauksia.

Kybervakoilua harjoitetaan osittain näiden jännitteiden takia, sillä vastapuolen aikeita, kyvykkyyksiä ja varautuneisuutta halutaan testata. Moranin (2010) mukaan kybervakoilun avulla voidaan valmistautua häämöttävään kyberhyökkäykseen tunnustelemalla vastapuolen toimintaa kybertilassa. Kybervakoilulle ominainen peitelty toteuttaminen on usein edellytyksenä sille, että vakoiluoperaatioita voidaan toteuttaa pitkään näkymättömänä ennen mitään varsinaista konfliktia (Hanska, 2013, s. 177). Jokin yksittäinen tapahtuma tai tapahtumaketju voi lopulta laukaista valtioiden välisiä jännitteitä ja manifestoitua sitä kautta kybertilaan. Tällainen käynnistävä tapahtuma toimii usein täten poliittisesti motivoituneiden kyberhyökkäysten alullepanijana. Käynnistävän tapahtuman seurauksena osapuolet saattavat kohentaa valmiustasoaan kybertilassa. (Mattern, Felker, Borum & Bamford, 2014.)

Kybermobilisaatiota kuvataan Moranin (2010) hahmotelmassa toimintana, joka aloittaa kyberhyökkäykseen valmistautumisen käynnistävän tapahtuman seurauksena. Mobilisaatio on yleisesti ottaen kriittinen vaihe minkä tahansa

hyökkäyksen valmistelua. Mobilisaation vaiheessa poliittinen entiteetti pyrkii ajamaan oman narratiivinsa läpi, täten hakien oikeutusta kyberhyökkäykselle (Mattern ym., 2014). Internetin hyödyntäminen mobilisaation vaiheessa on ominaista poliittisten aatteiden, ajatusten ja oikeutuksien levittämiselle (Betz, 2012).

Varsinainen poliittinen kyberhyökkäys voidaan nähdä tämän tapahtumaketjun kulminoitumispisteenä, jossa valtiollinen toimija pyrkii ajamaan tavoitteensa läpi kybertilassa (Moran, 2010). Mikäli esimerkiksi kybervakoilun avulla saatua tietoa onnistutaan hyödyntämään hyökkäyksen toteutuksessa, voi seurauksena olla hyökkäyksen kohteelle laaja ja tuhoisa kyberoperaatio. Poliittiselle kyberhyökkäykselle on toisaalta myös tyypillistä hyökkääjän halu anonymiteetin säilyttämiseen (Libicki, 2017). Oleellista hyökkääjän kannalta on tässä tapauksessa tietää, millainen kohdevaltion tai -järjestelmän sietokyky on. Mikäli suurilta vastaoperaatioilta halutaan välttyä, tarvitaan Libickin (2017) mukaan vankkaa analyysia vastustajan kyberkyvykkyydestä ja poliittisesta tilanteesta.

Kybervakoilu on täten oleellinen osa valtioiden välistä poliittista toimintaa ja konflikteja. Libickin (2017) mukaan kybervakoilu on luultavasti yleisin valtiollisten toimijoiden poliittisiin tarkoituksiin jalostettu kyberoperaatio. Kyberoperaatioiden verkottunutta kokonaisuutta pohtivat myös Boeke ja Broeders (2018), jotka huomauttavat, että kybermaailman tapahtumat ovat niin limittyneitä, että välillä on mahdotonta erottaa erityyppisiä operaatioita toisistaan. He painottavatkin, että kyberoperaatiot ovat spesifisille tehtäville räätälöityjä toimintamalleja, jotka yhdistelevät käytännössä esimerkiksi vakoilua ja kohdistettuja kyberhyökkäyksiä. Tällä perusteella Moranin (2010) luomaa kyberkonfliktin vaiheittaista etenemistä voidaan pitää myös kuvauksena poliittisten kyberkampanjoiden mahdollisista ulottuvuuksista. On selvää, että tapahtumaketju ei aina noudata samaa virtaviivaisuutta, mutta kehikko edustaa selkeästi siitä huolimatta kyberoperaatioiden välisiä syy-seuraussuhteita.

3.2 Kohdistettu kybervakoilu

Varsinaista kybervakoilua toteutetaan usein esimerkiksi kohdistettujen hyökkäysten, eli APT-hyökkäysten (engl. *advanced persistent threat*) avulla, sillä ne ovat kehittyneisyytensä ansiosta usein vaikeita havaita (Lehto & Limnéll, 2017a). Kohdistetut hyökkäykset voivat olla hyvinkin pitkäkestoisia ja jatkua jopa useiden vuosien ajan huomaamattomina (Wangen, 2015). Kohdistettujen kybervakoilukampanjoiden tarkoituksena on pitkällä aikavälillä kerätä tietoa kohdeohjelmistosta vakoiluoperaattoreiden käyttöön jalostamalla kerättyä tietoa hyödylliseen muotoon (Mattern ym., 2014). Valtiollisiin toimijoihin kohdistuvat vakoilutarkoituksessa suoritettujen APT-hyökkäysten on yleisesti mielletty tavoittelevan pääsyä esimerkiksi kriittistä informaatiota sisältäviin järjestelmiin (Rudner, 2013).

Lehto ja Limnéll (2017a) esittävät Suomen kyberturvallisuuden nykytilaa käsittelevässä raportissaan, että kohdistettujen hyökkäysten taustalla on mitä

useimmin toinen valtio tai rikollisryhmä, joka työskentelee läheisesti jonkun valtiollisen toimijan kanssa. Raportissa todetaankin, että poliittisesti kohdistettujen hyökkäysten kohteina voidaan usein nähdä kansalliset salaisuudet, henkilötiedot sekä aineeton pääoma. Valtiolliset toimijat nähdään usein APT-hyökkäysten eräinä potentiaalisimmista toteuttajista, sillä he voivat tarjota hyökkäykselle tarvittavat taloudelliset ja teknologiset puitteet (Rudner, 2013). Eräät tunnetuimmat kybervakoilutapaukset, kuten vuonna 2012 paljastunut Flame sekä vuonna 2011 havaittu Duqu, voidaan nähdä kohdistettuina, ja ainakin osittain poliittisesti motivoituneina kyberoperaatioina (Wangen, 2015). Tämänkaltaiset hyökkäykset toteutetaan kuitenkin usein ulkoisten toimijoiden kanssa yhteistyössä, sillä esimerkiksi erilaisista hakkeriryhmistä löytyy laajaa kyvykkyyttä kyberoperaatioiden toteuttamiseen (Rudner, 2013).

APT-hyökkäykselle voidaan hahmotella kuusiosainen toimintaperiaate, joka on Wangenin (2015) mukaelma oletettavasti Kiinan suorittamasta APT1-hyökkäyksen käyttämästä toimintaprosessista. Samankaltaista mallia APT-hyökkäyksen vaiheille kuvaavat myös Messaoud, Guennoun, Wahbi ja Sadik (2016). Hyökkäyksen kulku alkaa yleensä tiedonkeruuvaiheesta, jossa kohteesta pyritään tunnistamaan ja keräämään olennaista informaatiota hyökkäyksen toteuttamiseksi (Wangen, 2015). Olennaista on etenkin järjestelmiin sekä organisaatioinfrastruktuuriin liittyvien mahdollisten heikkouksien paikantaminen (Messaoud ym., 2016).

Tiedonkeruun perusteella saatua tietoa hyödynnetään edelleen hyökkäyksen valmisteluvaiheessa. Hyökkäys suunnitellaan Wangenin (2015) mukaan hyödyntäen yleensä ainakin sosiaalista manipulaatiota sekä teknologista taidokkuutta. Tunnetuissa APT-hyökkäyksissä on esimerkiksi hyödynnetty sähköpostiviestiin kätkettyjä haittaohjelmia, jotka iskevät havaittuihin heikkouksiin saaden täten jalansijan järjestelmään (Wangen 2015; Messaoud ym., 2016). Tällaisissa hyökkäysmetodeissa korostuukin sosiaalisen manipuloinnin osaalue, sillä esimerkiksi hyödynnettäessä sähköpostia haittaohjelman saattamiseksi järjestelmään, on kriittistä, että viestin vastaanottaja haluaa avata viestin. Wangenin (2015) mukaan tässä korostuu ensimmäisessä vaiheessa kerätyn tiedon laatu sekä se, kuinka hyvin hyökkääjä tuntee kohteensa.

Saatuaan jalansijan kohdejärjestelmään, hyökkääjä voi aloittaa hyökkäyksensä. Operaation alkuvaiheessa APT-hyökkäys tyypillisesti saattaa etsiä kohteesta lisää haavoittuvuuksia, täten saaden porattua pääsyään edelleen syvemmälle järjestelmän sisältämään informaatioon (Wangen, 2015). Jotta APT-hyökkäystä voidaan tituleerata nimensä mukaiseksi, eli pitkäkestoiseksi ja sinnikkääksi uhkaksi, tulee sen pysyä näkymättömänä järjestelmässä. Tästä syystä Messaoud ja muut (2016) huomauttavat itsensä naamioinnin ja näkymättömyyden tärkeydestä hyökkäyksen jokaisessa vaiheessa.

Onnistuttuaan vakaasti soluttautumaan kohteeseensa, APT-hyökkäys voi aloittaa pääasiallisen vakoiluoperaationsa. Tähän vaiheeseen liittyy laajaa tietoaineiston keruuta, joka voi olla esimerkiksi kuvien tai pdf-tiedostojen muodossa (Wangen, 2015; Messaoud ym., 2016). Usein tässä vaiheessa hyökkääjillä on selvä päämäärä tiedonkeruulle, ja he tietävät millaista informaatiota he ovat etsi-

mässä. Usein haittaohjelmien mukana tulee myös erilaisia käyttäjän toimintoja monitoroivia toiminnallisuuksia, kuten näppäimistöllä kirjoitetun tekstin tallennusta tai kuvankaappauksien ottamista ennalta määritellyistä kohteista. (Wangen, 2015.)

Kerätty tieto täytyy jollain tapaa myös saada poimittua järjestelmästä ilman, että operaatio itsessään paljastuu. Tietoa kerätään Wangenin (2015) mukaan pääasiassa erilaisiin arkistoihin, jotka suojataan siten, että vain haittaohjelman operoija pääsee niihin käsiksi. Tämän jälkeen ne saatetaan lähettää lukuisien välityspalvelimien kautta hyökkääjälle, jotta kiinnijäämisen riski olisi mahdollisimman pieni. APT-hyökkäyksen viimeisessä vaiheessa hyökkääjä pyrkii pyyhkimään jälkiään kohdejärjestelmässä. Messaoudin ja muiden (2016) mukaan hyökkääjä pyrkii salaamaan identiteettinsä, jotta välttyisi vastuulta, jota hyökkääjä joutuisi ottamaan kiinnijäädessään.

Rudnerin (2013) mukaan poliittisesti motivoituneilla APT-hyökkäyksillä tavoitellaan ennen kaikkea strategista yliotetta kybertilassa toiseen valtiolliseen toimijaan nähden. Hänen mukaansa APT-hyökkäysten teknologiset edellytykset ovat ainakin tunnetuimpien tapausten kohdalla olleet vertaansa vailla, joka puoltaa vaikeuksia niiltä puolustautumiselle. APT-hyökkäysten yksittäisiä vaiheita vastaan puolustautuminen nähdään suhteellisen yksinkertaisena, mutta hyökkäysten kokonaisvaltainen kompleksisuus ja suunnitelmallisuus lisää ongelmia puolustukselle (Rot & Olszewski, 2017). APT-hyökkäykset suunnitellaan käytännössä tiettyjä kohteita varten, jonka vuoksi ne omaavat usein spesifisiä ominaisuuksia, jotka ovat ennalta-arvaamattomia. Tarvitaan siis myös kompleksista puolustusta, jotta näitä hyökkäyksiä onnistutaan torjumaan tehokkaasti. Esimerkiksi älykkään tiedustelun menetelmistä, joita käsitellään tutkielman neljännessä luvussa, voi olla hyötyä.

3.3 Kybervakoilun poliittisuus

Maailmanpolitiikassa kybervakoilun rooli on merkittävä, mutta samalla lainsäädännöllisesti ylenkatsottu. Kansainvälinen lainsäädäntö ei varsinaisesti tunnista kybervakoilun laittomuutta, jonka seurauksena valtioiden ja muiden toimijoiden operaatiot vakoilun kentällä ovat vailla kunnon normeja ja säädöksiä. (Boeke & Broeders, 2018.) Kybervakoilun toteutus on pitkälti jokaisen valtion omissa käsissä ja verrannollinen kyseisen valtion lainsäädäntöön kybertilassa. (Weissbrodt, 2013.)

Kybermaailmassa korostuu usein valtioiden hämärätoiminta uskottavan kiistettävyyden nimissä (Cormac & Aldrich, 2018). Valtiot siis käyttävät laillisuuden harmaalla alueella olevia metodeja esimerkiksi kybervakoilussa, jotta voivat tarvittaessa kiistää toimensa uskottavasti. Maurer (2018) valottaa kybermaailmassa esille noussutta ”*cyber proxy*”-ilmiötä, jossa valtio ulkoistaa kyberoperaatioitaan, kuten vakoilua, ei-valtiollisille toimijoille. Tämän toimijan ja valtion välistä suhdetta kuvataan eräänlaisena vuorovaikutuksena, jossa esimerkiksi kybervakoilua harjoittava entiteetti toimii jossain määrin valtiovallan

alaisuudessa. Maurerin (2018) mukaan ulkoisen toimijan ja valtion välistä vaikutussuhdetta voidaan luonnehtia kolmella eri tavalla. Ensinnäkin ulkoiset toimijat voivat olla valtion valtuuttamina toimissaan kyberoperaatioissa. Tässä tapauksessa valtio käyttää suoraan voimaansa ulkoista toimijaa kohtaan, jolloin kyse on käytännössä valtion hallitsemista operaattoreista (Boeke & Broeders, 2018). Toisaalta valtion ja ulkoisen toimijan välinen suhde voi olla löyhempi, mutta silti osoittaa merkkejä organisoituneisuudesta ja yhteistyöstä. Tämä tilanne syntyy esimerkiksi sellaisissa tapauksissa, joissa valtio saattaa antaa ulkoiselle toimijalle tiettyjä ohjenuoria tai käytännön tukea, mutta joissa vankkaa yhteistyötä ei ole rakennettu (Biller & Maurer, 2018). Tämän lisäksi valtio voi oikeuttaa ja sympatisoida ulkoisten toimijoiden toimintaa. Maurerin (2018) mukaan tuki on passiivisempaa, mutta ei silti kieltävää.

Kybervakoilun ulkoistamisessa korostuu ilmiön poliittisuus. Ulkoistettujen toimijoiden sekä valtioiden väliset suhteet vaihtelevat valtioittain (Maurer, 2018). Boeken ja Broedersin (2018) mukaan esimerkiksi Venäjän menetelmät kybervakoilussa ovat kiinnostusta herättäviä. Heidän mukaansa Venäjän hallinto on useaan otteeseen toiminut ainakin löyhästi yhteistyössä ulkoisten toimijoiden kanssa kybervakoilun kentällä. Esimerkiksi APT29-nimellä tunnetulla kybervakoiluryhmällä on oletettavasti kytköksiä Venäjän tiedustelupalveluihin (Boeke & Broeders, 2018). Tämän yhteistyön tuloksena oletetaan olleen esimerkiksi vuoden 2016 Yhdysvaltain presidentinvaalien alla tapahtunut tietomurto maan demokraattipuolueen sähköpostipalvelimeen. Murron seurauksena arkaluontoista tietoa vuodettiin Wikileaks-sivustolle. Kybervakoiluna alkanut kyberoperaatio vaikutti täten poliittiseen ilmapiiriin, kylväen epäluottamusta demokraattista puoluetta kohtaan ja nostamalla presidenttiehdokas Donald Trumpin kannatusta. (Lipton, Sanger & Shane, 2016.)

Kybervakoilu onkin kasvavassa määrin keino, jota käytetään hybridivaikuttamisessa (Libicki, 2017). Hybridivaikuttaminen ei itsessään välttämättä vielä sisällä vakoilua, mutta vakoilun keinomenetelmän avulla voidaan luoda informaatiovaikuttamiselle uusia päämääriä. Libicki (2017) kuvaa esimerkiksi tilannetta, jossa kybervakoilun avulla kerättyä tietoa vääristellään tai muokataan sopimaan omaan tarkoitusperään. Suurvallat, etenkin autoritääriset sellaiset, ovat tunnettuja hybridivaikuttamisen kentällä (Suojelupoliisi, 2018). Vaikutuskeinoihin kuuluu usein esimerkiksi disinformaatiokampanjoita ja poliittista painostusta. Tarkoituksena voi olla esimerkiksi kohteena olevan henkilön tai ryhmän uskon horjuttaminen heille vakaisiin arvoihin, kuten demokratiaan tai valtioon. Suojelupoliisin (2020) mukaan hybridivaikuttamisen päämääränä on kuitenkin loppupelissä toisen valtion itsemääräämisoikeuteen puuttuminen tai sen kaventaminen.

Kybervakoilun poliittisuutta korostaa myös sen reaktiivisuus globaalin politiikan tapahtumiin. Kybervakoilun oveluus piilee juuri siinä, että vakoilun perusteella kerättyä tietoa ei välttämättä hyödynnetä heti (Axelrod & Iliev, 2013). Ilmiön poliittisuus on kenties näkyvimmillään juuri sellaisissa kybervakoilutilanteissa, joissa vieras valtio odottaa otollisinta aikaa hyödyntää keräämäänsä informaatiota toista valtiota vastaan.

3.4 Kybervakoilu Suomessa

Tietoyhteiskunnan kehityksen tuloksena erilaiset yhteiskunnan turvallisuus- ja toimintaympäristöön kohdistuvat uhkat hyödyntävät yhä enemmän tietoverkkoja ja informaatioinfrastruktuuria (Turvallisuuskomitea, 2017). Limnéll ja Lehto (2017) kuvailevat digitalisaatiota asevoimien ja sotilasvoimien näkökulmasta. Heidän mukaansa nyky-yhteiskunnan verkottuneisuus on nopeassa ajassa digitalisoinut koko valtiollisen ekosysteemimme. Samalla asevoimat ovat tulleet vahvasti riippuvaiseksi informaatioteknologiasta ja kybermaailmasta, johon nykyiset valtioidenväliset konfliktit paljolti heijastuvat. Kybervakoilu nähdäänkin osana Suomen kyberuhkamallia ja sen käyttö on yleistä valtioiden välisessä tiedustelutoiminnassa (Jansson & Sihvonen, 2018). Suomen ja sen lähialueiden kokonaisturvallisuusympäristö on heikentynyt vuoden 2014 jälkeen (Anttonen, 2020). Kiristyneet suurvaltasuhteet ja epävakaus aiheuttavat kaikuja myös Suomen turvallisuusympäristöön.

Suojelupoliisin (2018) mukaan Suomeen kohdistuu kokoonsa nähden huomattava määrä ulkomaisten tiedustelupalvelujen suorittamaa vakoilua. Kiinnostusta Suomen poliittiseen ja yhteiskunnalliseen toimintaan ovat osoittaneet toistamiseen etenkin Venäjä ja Kiina. Ulkomaisia tiedusteluviranomaisia on trendinomaisesti kiinnostanut etenkin Suomen Nato-suhteet, ulko- ja turvallisuuspolitiikka, Suomen kanta EU:n pakotepolitiikkaan sekä Itämeren turvallisuustilanne (Suojelupoliisi, 2018). Puhuttaessa Suomeen kohdistetusta vakoilusta, onkin olennaista puhua Venäjästä. Suojelupoliisi (2018) kuvaa Venäjän tiedustelupalveluun yhdistettyä toimijaa Turlaa eräänä Suomen kannalta kyvykkäimpänä kybervakoilun harjoittajana. Turlan kohteeksi ovat joutuneet esimerkiksi valtionhallinto sekä jotkut Venäjällä toimivat suomalaiset edustustot. Valtionhallinnon organisaatiot ovat yleisesti ottaen olleet kohteena myös muissa Venäjään yhdistetyissä kybervakoilutapauksissa (Lohse & Viitanen, 2019, s. 34).

Suomessa kybervakoilu on laaja-alaista ja systemaattista toimintaa, jonka kohteena voi kohdeorganisaation tai -ympäristön lisäksi joutua esimerkiksi muut läheistä yhteistyötä tekevät organisaatiot sekä sivulliset henkilöt, kuten työntekijöiden puolisot. Suojelupoliisi (2018) painottaa tietoturvaosaamisen tärkeyttä etenkin kybervakoilun onnistumisen minimoimiseksi myös poliittisesti kriittisessä asemassa toimivien puolisoille sekä muille läheisille, sillä he voivat näyttäytyä kybervakoilijalle otollisina kohteina.

Kybervakoilua tulee Suomen mittakaavassakin tarkastella hybridivaikuttamisen kokonaisuutena. Vieraiden valtioiden kyky vaikuttaa Suomen kybertoimintaympäristöön on kasvava ja vakava uhka (Lehto ja Limnéll (2017a). Näitä uhkia vastaan taistellakseen valtio joutuu suuren paineen eteen. Joitakin valtiollisen tiedustelutoiminnan keinomenetelmiä saatetaan kuitenkin länsimaisen oikeuskäsityksen nojalla vierastaa (Jansson & Sihvonen, 2018). Tämä ristipaine aiheuttaa valtiollisella tasolla ongelmia, jotka voivat osaltaan helpottaa esimerkiksi kybervakoilun kentällä operoivien vieraiden valtiollisten tahojen toimintaa.

4 KYBERVAKOILUN ESTÄMINEN JA TIEDUSTELUTOIMINTA

Poliittisesti motivoituneen kybervakoilun kentällä tarvitaan myös vastavuoroisesti sitä hillitseviä tai estäviä tekijöitä, joita tässä kappaleessa käsitellään. Valtiolliset tiedusteluorganisaatiot, kuten Suomessa Suojelupoliisi ja Puolustusvoimat, työskentelevät vakoilua ja valtiollista turvallisuutta uhkaavaa toimintaa kitkevinä toimijoina (Bigelow, 2019). Heidän keinovalikoimansa on osittain sama kuin kybervakoilijoilla, sillä operatiivisesti tiedustelu ja vakoilu ovat kuin saman kolikon kääntöpuolet.

Tässä kappaleessa esitellään etenkin Suomen tiedustelutoiminnan kautta yleisesti käytössä olevia malleja ja teorioita, joilla esimerkiksi valtioidenvälistä vakoilua pyritään estämään. Erilaisten kyberoperaatioiden torjumiseksi ehdotetaan etenkin kansainvälisen yhteistyön merkityksen kasvattamista, jota tarkastellaan myös tässä kappaleessa. Tässä kappaleessa vastataan ensisijaisesti tutkimuskysymykseen ”Kuinka tiedusteluviranomaiset harjoittavat toimintaansa vakoilun estämiseksi ja havaitsemiseksi?”. Vastausta tähän tutkimuskysymykseen pohditaan etenkin älykkään kybertiedustelun sekä hämäyksen konseptien avulla. Tämän lisäksi tutkimuskysymystä ”Millainen on kybervakoilun sekä tiedustelun toimintaympäristö Suomessa?” pohditaan tiedustelutoiminnan lajien ja globaalin turvallisuuspolitiikan näkökulmasta.

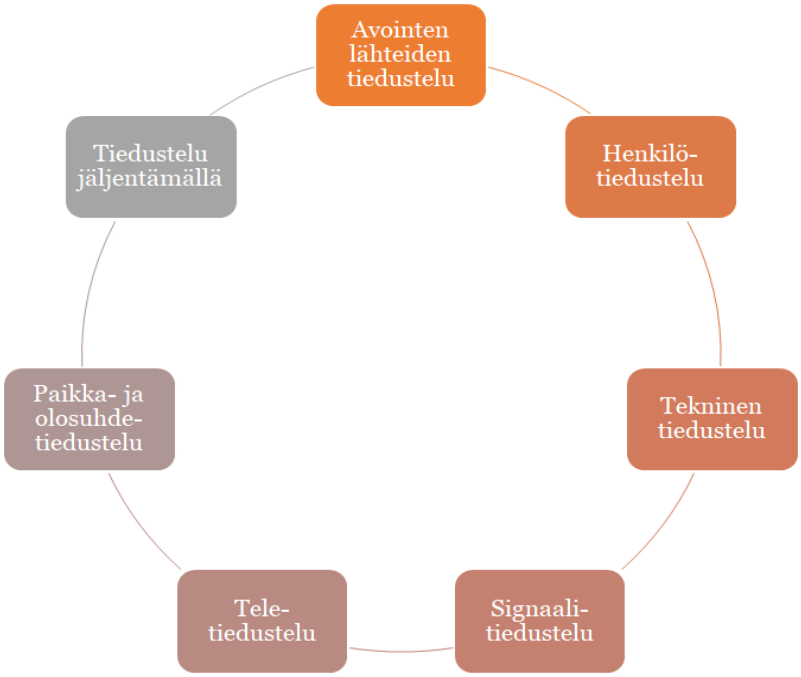
4.1 Tiedustelutoiminnan lajit

Lowenthal ja Clarke (2015) referoivat etenkin yhdysvaltalaisessa tiedustelukäsityksessä esiintyviä tiedustelun lajeja. Suomeen nämä lajit ovat tulleet hieman muokattuina, mutta silti ainakin osittain hyväksyttyinä käytäntöön. Yleisesti tiedustelussa nähdään Lowenthalin ja Clarken (2015) mukaan olevan viisi päälajia, jotka ovat:

- avointen lähteiden tiedustelu (*open-source intelligence, OSINT*),
- signaalitiedustelu (*signals intelligence, SIGINT*),

- henkilötiedustelu (*human intelligence, HUMINT*),
- paikka- ja olosuhdetiedustelu (*geospatial intelligence, GEOINT*),
- sekä mittaus- ja tunnusmerkkitiedustelu (*measurement and signatures intelligence, MASINT*).

Kuitenkin suomalaisessa tiedustelutoiminnassa on todettu, että mittaus- ja tunnusmerkkitiedustelua ei sen virallisen määritelmän mukaan juurikaan toteuteta, jonka vuoksi sitä ei ole relevanttia esittää Suomen tiedustelulajien hahmotelmassa (Lohse ym., 2019, s. 19). Tämän lisäksi suomalaiseen tiedusteluun on otettu kolme yleistä mallia täydentävää tiedustelun lajia, jotka ovat teletiedustelu, tekninen tiedustelu ja tiedustelu jäljentämällä (Lohse ym., 2019, s. 19–21). Alla esitetty kuvio on oma muunnelma Lowenthalin ja Clarken (2015, s. 1–4) sekä Lohsen ja muiden (2019, s. 19–21) esittämistä tiedustelutoiminnan lajeista. Kuvio edustaa tiedustelun kokonaisvaltaista toimintaympäristöä Suomessa. Lowenthalin ja Clarken (2015, s. 1–4) määritelmään tiedustelulajeista kaaviossa viittaavat avointen lähteiden tiedustelu, henkilötiedustelu, tekninen tiedustelu sekä signaalitiedustelu. Lohsen ja muiden (2019, s. 19–21) määritelmiin perustuvat kuviossa teletiedustelu, paikka- ja olosuhdetiedustelu sekä tiedustelu jäljentämällä.



KUVIO 2 Suomen tiedustelulajit (Lowenthal & Clark, 2015, s. 1–4; Lohse ym., 2019, s. 19–21)

Tiedustelun kokonaishahmotelmasta tavoitettava avointen lähteiden tiedustelu on kansantajuisesti kenties helpoiten lähestyttävissä. Nimensä mukaisesti se kohdistuu julkisissa lähteissä saatavilla olevaan materiaaliin, kuten kirjallisuuteen, viranomaisten julkaisuihin, verkkosivuihin ja sosiaaliseen mediaan (Lohse ym., 2019, s. 88–89). Avoimet lähteet ovat nopeasti saatavilla, edullisia ja

maantieteellisesti rajoittamattomia, mutta samalla myös laajuudestaan johtuen vaikeita hallita. Avoimien lähteiden kautta hankittu tiedustelutieto on toisaalta operatiivisesti riskittömämpää hankkia kuin monet muut tiedustelun lajit (Wirtz & Rosenwasser, 2010).

Wirtz ja Rosenwasser (2010) arvioivat, että avoimien lähteiden tiedustelun avulla voidaan reagoida uudentyyppisiin poliittisiin uhkakuviin kenties vanhempia tiedustelumetodeja tehokkaammin. Informaatiovaikuttamisen aikakaudella uudenlaiset kyberuhkat eivät enää ainoastaan keskity teknologisesti edistyneiden kyberaseiden tai -ohjelmien luomiseen, vaan pinnalle on noussut poliittisesti motivoitunutta liikehdintää avoimessa verkossa. Wirtzin ja Rosenwasserin (2010) mukaan esimerkiksi useat äärijärjestöt ja poliittiset ryhmät etsivät tukea verkosta, sekä kommunikoivat erilaisten sosiaalisen median kanavien avulla. Tiedustelutietoa voidaan fokusoidusti kerätä tällaisten järjestöjen sivustoilta ja alustoilta vanhojen tiedustelumetodien käyttöä vaivattomammin.

Henkilötiedustelussa taas havainnoidaan kohdehenkilöä tai -ryhmää. Henkilötiedustelun menetelminä nähdään yleensä etenkin esimerkiksi erilaiset peiteoperaatiot sekä tarkkailutoiminta. (Lohse ym., 2019, s. 138.) Avointen tiedustelulähteiden tapaan henkilötiedustelun voidaan nähdä olevan kustannustehokasta, mutta kompleksisuudestaan johtuen pitkäkestoista. Henkilötiedustelu voi osoittautua ehdottoman hyödylliseksi tiedustelumenetelmäksi, mikäli siinä onnistutaan, mutta se vaatii usein kaikista tiedustelumenetelmistä eniten panostusta ja aikaa. (Wirtz & Rosenwasser, 2010.) Henkilötiedustelun kompleksisuus tulee esiin sen ennalta-arvaamattomuudessa. Wirtzin ja Rosenwasserin (2010) mukaan riskinä voidaan yleisesti nähdä etenkin mahdollisuus kohdehenkilöltä saatu valheellisen tai harhaanjohtavan tiedon keruu, joka saattaa jäädessään huomaamatta vaarantaa koko tiedusteluoperaation.

Tekninen tiedustelu on osittain limittäinen ilmiö henkilötiedustelun kanssa. Tekninen tiedustelu voi olla muodoltaan kuuntelua, katselua, seurantaa tai laitetarkkailua. (Lohse ym., 2019, s. 167.) Tekninen tiedustelu voi esimerkiksi kohdistua ulkomaisiin tietojärjestelmiin. Lohsen ja muiden (2019, s. 167) mukaan tekninen tiedustelu käyttää nimensä mukaisesti teknologiaa tiedustelun välineenä, mutta kohteena ovat usein henkilötiedustelun tapaan myös henkilöt. Teknisen tiedustelun avulla voidaan myös kerätä tietoa esimerkiksi ajoneuvoista, paikoista ja tietojärjestelmistä. Etenkin teknisen tiedustelun ulottuvuudet ovat laajentuneet valtioidenvälisten kyberkonfliktien yleistyttyä (Caton, 2020). Potentiaalisen kyberhyökkääjän keinovalikoiman laajentuessa, on tiedustelutoiminnalle erityisen tärkeää pyrkiä pysymään perillä uhkista. Etenkin kriittiseen infrastruktuuriin kohdistuvat uhkat voidaan nähdä tärkeinä uhka-arvion luomisen kannalta. (Caton, 2020.)

Signaalitiedustelu jaetaan yleisesti radiosignaali- ja tietoliikennetiedusteluun (Lohse ym., 2019, s. 90). Signaalitiedustelu nähdään yleisesti elektronisen signaalien tiedusteluna, jota voidaan harjoittaa etenkin kommunikaatiovälineiden sekä -laitteiden tiedusteluna (Wirtz & Rosenwasser, 2010). Radiosignaalitiedustelun tiedonhankinta kohdistuu radioaaltoihin ja sitä kohdistetaan ainoastaan muihin valtiollisiin toimijoihin (Lohse ym., 2019, s. 91–95). Tietoliikenne-

tiedustelu kohdistuu maan rajan ylittävän tietoliikenteen valvontaan ja analysointiin (Lohse ym., 2019, s. 96–100). Täten tietoliikennetiedustelu ei saa kohdistua valtion rajojen sisäisessä viestintäverkossa tapahtuvaan tietoliikenteeseen. Tietoliikennetiedustelu ei välttämättä varsinaisesti kohdistu yksilöön, vaan kohteena voi olla esimerkiksi tunnistaa tahoja, joiden kanssa tietyltä alueelta lähetetyt viestit kommunikoivat (Honkanen, 2020).

Teletiedustelu viittaa sellaiseen tiedusteluun, jossa tietoa hankitaan yleisessä viestintäverkossa liikkuvista viesteistä, kuten puheluista sekä sähköpostija tekstiviesteistä (Lohse ym., 2019, s. 119). Paikka- ja olosuhdetiedustelu taas käsittää tiettyyn alueeseen tai paikkaan kohdistuvan tiedonhankinnan ja niiden olosuhteiden analysoinnin (Lohse ym., 2019, s. 188). Paikkatiedusteluun liittyvä satelliittikuvien analysointi on historiallisesti tuottanut poliittisesti merkittäville tiedusteluoperaatioille tulosta. Sitä käytettiin esimerkiksi Kuuban ohjuskriisin aikana ilmatiedustelussa (Wirtz & Rosenwasser, 2010). Paikka- ja olosuhdetiedustelulla voidaan nähdä olevan kuitenkin muutamia suuria heikkouksia, jotka vaikeuttavat sen hyödyntämistä kaikissa tilanteissa. Esimerkiksi huono sää tai tiedustelukohteen naamiointi saattavat estää validin tiedonkeruun. (Wirtz & Rosenwasser, 2010.)

Jäljentämistä käytetään tiedustelussa etenkin oleellisen tiedon taltiointiin siten, että tiedusteluoperaation paljastumisriski pysyy mahdollisimman minimaalisena. Jäljentäminen tarkoittaa käytännössä toimintoja, joilla jokin tiedusteluoperaation kannalta oleellinen tieto, kuten asiakirja, esine, lähetys tai kirje pyritään kopioimaan ilman, että operaatio itsessään paljastuu. (Lohse ym., 2019, s. 196–203.)

Modernissa ja verkottuneessa yhteiskunnassa uhkakuvat ovat moniulotteisia, jonka vuoksi tiedustelussa tarvitaan laajasti eri tyyppisiä puolustuskeinoja (Ohra-aho, 2020). Tiedustelutoiminta tulee siis ymmärtää kokonaisuutena, jossa eri tiedustelulajien tulisi toimia yhteistyössä toistensa kanssa tietyn operaation vaatimusten määrittelemällä tavalla. Kaikki yllä kuvatuista tiedustelumetodeista eivät välttämättä suoranaisesti liity modernien kyberoperaatioiden tiedusteluun, mutta kokonaisuus on silti tärkeä hahmottaa. Ohra-aho (2020) painottaa, että hyökkääjien epätavalliset ja uudenlaiset keinot vaikuttamiseen kehittyvät jatkuvasti. Hänen mukaansa modernissa tiedustelussa erityisen tärkeäksi onkin muodostunut hyökkääjän tavoitteiden ja kyvykkyyksien mahdollisimman kokonaisvaltainen ymmärtäminen, jonka voidaan nähdä tapahtuvan laajan tiedustelutoiminnan keinovalikoiman avulla.

4.2 Kyberuhkien älykäs tiedustelu

Kyberhyökkäysten tekijöiden ja niiden torjujien keinomenetelmien välillä voidaan nähdä olevan asymmetrinen tasapaino (Toveri & Pelttari, 2020). Käytännössä esimerkiksi kybervakoilija saattaa onnistua hyödyntämään kohdejärjestelmän tietoturvan heikkoa kohtaa massiivisella tavalla. Toisaalta kyberoperaatioiden torjunnasta vastaavat voivat olla vaikean tehtävän edessä yrittäessään

suojata järjestelmäänsä kaikilta mahdollisilta siihen kohdistuvilta uhkakuvilta. (Oosthoek & Doerr, 2020.) Kyberuhkien älykäs tiedustelu (engl. *cyber threat intelligence* tai *cyber intelligence)* pyrkii tasaamaan asymmetriaa siten, että kyberhyökkäysten torjunnassa voitaisiin hyödyntää laajempaa keinovalikoimaa ja täten estää jatkossa suurempi määrä hyökkäyksiä (Mattern ym., 2014).

Kyberuhkien torjuntaa on pitkään leimannut sen reaktiivinen luonne jo tapahtuneisiin uhkiin (Mattern ym., 2014). On kuitenkin yhtäältä tärkeää analysoida mahdollisten uhkien kyvykkyyttä sekä potentiaalisia aikomuksia paremman kokonaisymmärryksen takaamiseksi ja uhkakuvan ennakoimiseksi. Ensin on syytä tarkastella kyberoperaatioihin yleisesti liittyviä operatiivisia ja toiminnallisia ominaisuuksia. Mattern ja muut (2014) luokittelevat kolme älykkään uhka-arvion luomiselle oleellista aspektia hyökkääjän oletetusta käytöksestä. Ensinnäkin he kuvaavat kyberhyökkäystä jonkin tapahtumaketjun kulminoitumispisteeksi, jolle on löydettävissä selkeälinjainen etenemisprosessi. Tämä ajatus on yhtenevä esimerkiksi tutkielmassa aikaisemmin esiteltyyn poliittisesti motivoituneen kyberhyökkäyksen etenemisen kaavioon (Moran, 2010).

Yhteneväisyys näkyy myös Matternin ja muiden (2014) esittämän luokituksen toisessa kohdassa, jossa korostetaan aikaisempien tapahtumien, nykytilanteen sekä hyökkäysasetelman muodostamaa kokonaisuutta hyökkäykseen johtavina tekijöinä. Moranin (2010) luokituksessa tuotiin esille esimerkiksi piileviä jännitteitä osana tapahtumia, jotka voivat johtaa kyberkonfliktiin. Näyttäisi siis siltä, että älykkään kybertiedustelun perusperiaatteena on ehdottoman tarkka arvio ja analyysi kaikista niistä taustatekijöistä, joilla voi olla jotain vaikutusta operaation toteutumiseen. Borum, Fein, Vossekuil, ja Berglund (1999) ovat määritelleet kolmannen uhka-arvion luomiselle oleellisen aspektin, jota vielä nykyisessä Matternin ja muiden (2014) hahmottelemassa mallissakin käytetään. Tämä aspekti kuvaa itse niitä hienovaraisia toimia, joita hyökkääjä suorittaa ennen varsinaista iskua. Tästä kehikosta voidaan huomata, että älykäs kybertiedustelu ei ole passiivista tai reaktiivista toimintaa. Sen perusoletuksena on uhkien aktiivinen etsiminen, tulkitseminen sekä ymmärtäminen.

Jotta älykkään kybertiedustelun käsitettä voidaan syventää tiedustelutoimijoille käytettävään muotoon, on syytä määritellä myös niitä ominaisuuksia, joista kyberhyökkääjä voisi olla kiinnostunut. Oosthoek ja Doerr (2020) muotoilevat älykkään kybertiedustelun kannalta kolme olennaista kysymystä, joita jokaisen esimerkiksi kybervakoilun kaltaisilta operaatioilta suojautuvien tahojen tulisi pohtia. Ensinnäkin organisaatioissa tulisi tarkastella niitä ominaisuuksia, joista vakoilua suorittava taho voisi olla kiinnostunut. Tämän lisäksi tärkeää on arvioida omien tietolähteidensä arvokkuutta hyökkääjälle, eli sitä, mitkä tiedot tai kohteen ominaisuudet voivat kiinnostaa vakoiluoperaation suorittavaa tahoa. Kolmannessa pääkohdassa pyritään pohtimaan sitä, kuinka hyvin kybervakoilulta suojaudutaan.

Yksinkertaisuudessaan älykäs kyberuhkien tiedustelu pyrkii ymmärtämään kyberoperaatioiden toteutuksen lisäksi myös sitä, mitkä tahot voisivat olla niiden takana ja miksi (Oosthoek & Doerr, 2020). Tämän lisäksi tärkeänä aspektina pidetään myös tulevaisuudessa mahdollisesti tapahtuvien uhkaku-

vien arviointia ennaltaehkäisevänä toimenpiteenä (Mattern ym., 2014). Kyberuhkien älykäs tiedustelu pyrkiikin tunnistamaan niitä uhkia ja haavoittuvaisuuksia, jotka saattavat osoittautua kriittisiksi tulevaisuudessa (Mtsweni, Mutemwa & Mkhonto, 2016).

Bodeau, Graubart ja Fabius-Greene ovat muodostaneet tutkimuksessaan (2010) kehikon riittävän kybervalmiuden luomiselle erilaisissa kyberuhkatilanteissa. Tässä tutkielmassa keskitytään kybervakoiluun uhkatilanteena, jonka vuoksi kehikkoa ei käsitellä kokonaisuudessaan. Kehikon osa-alueita, jotka ovat kybervakoilun ja älykkään kybertiedustelun kannalta olennaisia on hahmoteltu alla olevassa taulukossa. Tutkielmaan on itse muunneltu edellä mainitusta tutkimuksesta eri osa-alueista yhteensopivia kohtia, jotta malli olisi toimiva ja hyödyllinen tässä kontekstissa.

TAULUKKO 1 Kybervalvonnalta ja -vakoilulta suojautuminen (Bodeau ym., 2010)

Hyökkäysmetodi	Taustalla tyypillisesti	Hyökkäyksen tavoite	Älykäs kybertiedustelustrategia
kybervalvonta	Valtiollinen entiteetti, teknologisesti edistyksellinen terroristiryhmä, hakkeriryhmä ja/tai järjestäytynyt rikollisjärjestö	Infrastruktuuriin kohdistuvan ymmärryksen lisäys, tulevan hyökkäyksen valmistelu ja/tai laaja-alaisen spesifisen tiedon keruu	Pyrkimys estää tunkeutujan pääsy oleelliseen ja kriittiseen informaatioinfrastruktuuriin
kybervakoilu	Armeija ja/tai (valtiollinen) tiedusteluorganisaatio	Spesifisen ja korkeaarvoisen tiedon keruu, vastaoperaation näkökohtien heikentäminen ja/tai operatiivisen kyvyn haavoittaminen	Pyrkimys rajoittaa kriittisen datan saatavuutta, operatiivisen kyvyn säilyttäminen mahdollisimman tehokkaasti, pyrkimys järjestelmäsuunnitteluun sinnikkyyden ja kestävyyden periaatteella

Taulukosta voidaan ymmärtää kaksi erillistä kybertilaa hyödyntävää poliittista vakoilutoiminnan lajia. Kybervalvonta (engl. *cyber incursion* tai *cyber surveillance*) on poliittisesta kybervakoilusta lievempi muoto, jota voi Bodeaun ja muiden (2010) mukaan harjoittaa myös ei-valtiolliset toimijat. Heidän mukaansa tämänkaltaisessa valvonnassa on kyse siitä, että operaation taustalla oleva taho on hetkellisesti onnistunut pääsemään käsiksi johonkin valtiollisen organisaation kannalta kriittiseen tiedonlähteeseen kybertilassa. Tämän kaltainen hyökkäys on lisäksi yleensä keskittynyt tiettyyn tai tiettyihin arvokkaina pidettyihin tietolähteisiin tai -järjestelmiin (Bodeau ym., 2010).

Tutkimuksessa määritellään lisäksi alustava toimintamalli jokaiselta spesifiseltä kyberuhkatilanteelta suojautumiseen. Kybervalvonnan toteuttajan ei nähdä olevan saaneen pääsyä kriittistä informaatiota sisältäviin järjestelmän osiin, jonka vuoksi tämän hyökkäyksen vahinkojen torjunnassa tulee keskittyä rajaamaan hyökkääjän pääsyä eteenpäin (Bodeau ym., 2010). Tällaisen toiminnan ehkäisemiseksi olemassa oleva keinovalikoima keskittyy etenkin mahdollisimman tarkkaan tietoverkon monitorointiin, piilohallintaohjelmien, eli rootkitien, havaitsemiseen sekä hunajapurkki-ansojen kehittämiseen. Hunajapurkeilla viitataan yleisesti ottaen ansaan, jonka on tarkoitus välittää tietoa kyberhyökkääjistä tai -hyökkäyksestä puolustajille (Rowe & Goh, 2007).

Kybervakoilu taas ymmärretään tutkimuksen pohjalta kybervalvontaa vakavampana ja monimutkaisempana ilmiönä. Kybervakoilua suorittava taho on onnistunut luomaan pitkäkestoisen väylän tiedonkeruuseen tai sabotaasiin kohdeorganisaatiossa. Kybervakoilun taustalla on toisen valtion tiedusteluorganisaatio tai jokin sen alainen toimija, kuten Maurerin (2018) tutkimuksessa mainitut ulkoistetut toimijat. Kyberhyökkäys kohdistetaan spesifiseen ja arvokkaana pidettyyn tietoon (Bodeau ym., 2010). Operaatioiden motiivina voi olla myös informaatiovaikuttamiseen liittyvä väärän tiedon syöttäminen tai tulevan kyberhyökkäyksen pohjustaminen vakoilutoimien avulla.

Bodeaun ja muiden (2010) kehittämä älykäs tiedustelumalli kybervakoilun estämiseksi kuvaa tapoja, joilla hyökkäystä voidaan ehkäistä, mutta toisaalta myös sitä, kuinka haittoja voidaan minimoida. Ensinnäkin järjestelmäsuunnittelussa pyritään mahdollisimman sinnikkääseen ja kestävään toteutukseen, jotta kybervakoiluoperaatioilla olisi mahdollisimman pieni tilaisuus onnistua. Tässä käytetään Bodeaun ja muiden (2010) mukaan keinoina esimerkiksi järjestelmän sisäisen informaatioinfrastruktuurin hajauttamista siten, että kriittistä tietoa sisältävä data on lukuisen eri oven takana. Toisaalta mikäli kybervakoilun toimija on onnistunut saamaan jalansijaa tietojärjestelmässä, on tärkeä pyrkiä minimoimaan kerätyn tiedon määrä sekä sen laadukkuus (Bodeau ym., 2010). Yksi keino tähän voisi olla väärän tiedon syöttäminen vakoilijoille, joista puhutaan tämän luvun kolmannessa kappaleessa.

Yleisesti ottaen kyberuhkien älykkään tiedustelun ongelmana voidaan nähdä yhteistyön vähäisyys (Mtsweni, Mutemwa & Mkhonto, 2016). Kuten tässäkin tutkielmassa on määritelty, kyberhyökkääjät toimivat usein yhteistyössä keskenään. Kybervakoilun tapauksessa oiva esimerkki tästä on valtiollisten tiedustelupalveluiden ja ulkoistettujen toimijoiden välinen yhteistyö (Maurer, 2018). Tästä syystä Mtsweni, Mutemwa sekä Mkhonto (2016) arvioivat, että myös älykkäässä kyberpuolustuksessa olisi hyötyä entistä yhteisöllisemmästä otteesta. Toisena keskeisenä ongelmana voidaan nähdä osaamisen puute, joka on yleinen ongelma kyberpuolustuksessa muutenkin (Oosthoek & Doerr, 2020). Kuitenkin osaamisen parantamisella esimerkiksi koulutuksen lisäämisen avulla, sekä yhteistyön korostamisella voidaan nähdä olevan tulevaisuudessa suuria vaikutuksia kyberuhkien älykkäälle tiedustelulle (Oosthoek & Doerr, 2020).

4.3 Vakoiluoperaatioiden hämäys

Väärän tiedon syöttäminen kybervakoilijoille on noussut suosituksi keinoksi minimoida vakoilun haittoja. Tavoitteena on modifioida tiettyjä tietoverkon ominaisuuksia siten, että vakoilija sivuuttaa oleellisen tiedon keskittyessään väärän tiedon keräämiseen (Achleitner ym., 2016). Hämäys (engl. *Cyber deception)* täytyy tapahtua siten, että väärä tieto niin uskottavaa, että vakoilija tarttuu siihen (Wang & Lu, 2018). Ottamalla kontaktin hämäykseen, hyökkääjä tulee samalla usein myös paljastaneeksi itsensä puolustusoperaatiolle (Bushby, 2019). Hämäyksen käyttö voi tämän lisäksi johtaa hyökkääjän väärälle polulle seuraavissa askelissaan, sillä kerätty tieto on virheellistä. Hämäyksen perimmäinen tarkoitus kybervakoilun torjunnan lisäksi onkin oppia hyökkääjän käytöksestä, jotta tulevaisuudessa hämäysoperaatioiden toiminta olisi entistä tarkempaa. Poliittisen kybervakoilun kentällä hämäyksestä voidaan katsoa olevan erityistä hyötyä esimerkiksi pitkäkestoisten ja usein valtioiden harjoittamien APT-iskujen hillinnässä. (Almeshekah & Spafford, 2016, s. 9.)

Wang ja Lu (2018) kuvailevat tutkimuksessaan kehikkoa hämäyksen vaiheista, jota voidaan käyttää avaamaan kyberhämäyksen toteuttamista. Kehikon mukaan hämäyksen ensimmäisessä vaiheessa keskitytään ensisijaisesti potentiaalisen hyökkääjän ymmärtämiseen. Tutkimuksessa kuvaillaan, että olennaista on ensin ymmärtää hyökkääjän tavoitteita, kyvykkyyksiä sekä päätöksentekoprosessia parhaalla mahdollisella tavalla. Kokonaiskuvan perusteellinen ymmärtäminen voidaan nähdä hämäyksen onnistumisen kannalta oleellisena, sillä mikäli ymmärrystä hyökkääjän tilanteesta ja aikeista ei saada riittävän konkreettisesti luotua, on kohdistetun hämäyksenkin luominen hakuammuntaa (Wang & Lu, 2018).

Hämäyksen toisen vaiheen tavoite on edellä mainitun kehikon mukaan luoda harhautusstrategia. Ensisijaisesti hyvän hämäyksen taustalla on taata mahdollisimman suuri yliote kriittisestä tiedosta hyökkääjään verrattuna. Wang ja Lu (2018) perustelevat, että puolustuksellisessa operaatiossa on tärkeä pyrkiä minimoimaan mahdollisimman tehokkaasti niitä ”sokeita pisteitä”, joita hyökkääjä voisi hyödyntää. Mikäli tiedollinen ylivoima onnistutaan luomaan, on puolustuksellinen hämäys siis huomattavasti vaivattomampaa toteuttaa. Hämäyksen toisessa vaiheessa onkin ensisijaisesti kyse strategisesta hämäyksen suunnittelusta perustuen hyökkääjän oletettuun tiedon määrään. Käytännössä hämäyksen strategisena tavoitteena on saada hyökkääjä kohdistamaan resurssejaan väärän tiedon hankintaan (Almeshekah & Spafford, 2016, s. 9).

Hämäyksestä nähdään olevan erityisen suurta hyötyä silloin, kun se voidaan toteuttaa mahdollisimman varhaisessa vaiheessa hyökkääjän kyberkampanjaa (Rowe & Goh, 2007). Kuten KUVIO 1 (Moran, 2010) osoittaa, kybervakoilu on usein kyberhyökkäystä ennen suoritettava tunnusteluoperaatio, jossa pyritään ymmärtämään kohdeorganisaatiota tai -ympäristöä mahdollisimman tehokkaasti. Tämän vuoksi kybervakoilun estämiseksi suoritettu hämäys voi

toimia erityisen tehokkaana puolustuskeinona jo ennen kuin hyökkääjä ehtii suunnitella suurempaa kyberoperaatiota (Bushby, 2019).

Hämäysoperaatioita on käytetty laajalti jo ennen niiden hyödyntämistä kybertilassa (Wang & Lu, 2018). Kyberhämäysoperaatiot voivat täten saada samanlaisia psykologisia ominaisuuksia kuin perinteisemmät hämäysmetodit. Wang ja Lu (2018) osoittavat, että tietynlaisen kognitiivisen vinouman luominen hyökkääjän tietoisuuteen tulisi olla hämäyksen keskeinen tavoite. Hämäyksessä on pyrittävä luomaan eheän oloinen kokonaiskuva käyttäen valheellista narratiivia, jotta hyökkääjä uskoo valheeseen. Kognitiivinen vinouma perustuu ihmisille yleiseen psykologiseen taipumukseen muodostaa stereotypioita ja subjektiivisia johtopäätöksiä ilman riittävää taustatietoa (Yuill, Denning & Feer, 2007). Kognitiivisen vinouman aiheuttaminen hyökkääjälle on siis tietyllä tavalla hämäyksen tavoite. Hämäyksessä pyritään luomaan niin vakuuttavaa disinformaatiota, että hyökkääjä olettaa sen oikeelliseksi tai edes menee osittain harhaan sen takia (Wang & Lu, 2018).

Hämäys käyttää osittain samankaltaista lähestymistapaa kyberuhkilta puolustautumiseen kuin älykäs tiedustelu. Molemmat esimerkiksi painottavat aikaista reagointia sekä hyökkääjän tarkkaa tuntemusta ja analysointia (Bushby 2019; Mattern ym., 2014). Tietyllä tapaa molemmissa lähestymistavoissa korostuu myös inhimillinen älykkyys (Wang & Lu, 2018). Hämäykseen liittyvä tutkimus tulisi nähdä ennen kaikkea monitieteellisenä kokonaisuutena, joka pyrkii älykkäiden metodien avulla muuttamaan hyökkääjän ajattelutapaa ja informaationkeruuprosessia (Wang & Lu, 2018).

4.4 Kansainvälinen yhteistyö ja lainsäädäntö

Kybervakoilun tavoin myös siltä puolustautuminen tulisi nähdä moniulotteisena ja usein yhteistyötä vaativana operaationa. Kansainvälistä yhteistyötä kyberuhkien torjuntaan puolletaan usein etenkin samanhenkisten valtioiden tai liittoumien kesken (Gunneriusson & Ottis, 2013).

Suomessa kybertiedustelua harjoittavat laillisesti vain Suojelupoliisi ja Puolustusvoimat (Lohse & Viitanen, 2019, s. 38–39). Tiedustelu voidaan yleisesti jakaa siviili- ja sotilastiedusteluun sitä suorittavan organisaation mukaan. Siviilitiedustelu on Suojelupoliisin harjoittamaa toimintaa, jonka tarkoituksena on hankkia ja hyödyntää tiedustelumenetelmin kerättyä tietoa kansallisen turvallisuuden takaamiseksi (Poliisilaki, 2011/872). Siviilitiedustelun tärkeimmät tehtävät ovat Suomen kansallisen turvallisuuden suojaaminen, valtiojohdon päätöksenteon tukeminen ja muiden viranomaisten suorittamien kansalliseen turvallisuuteen liittyvien tehtävien suojaaminen. Sotilastiedustelu taas on Puolustusvoimien toimintaa. Sen tehtävänä on kerätä tietoa sellaisesta Suomen turvallisuusympäristön kannalta oleellisesta sotilaallisesta toiminnasta, joka uhkaa vakavalla tavalla Suomen maanpuolustusta tai muuten vaarantaa yhteiskunnallisia toimintoja. (Sotilastiedustelulaki, 2019/590.)

Kansainväliset säädökset ja lait ovat olleet kybervakoilun estämisen kannalta jokseenkin epäselviä. Esimerkiksi valtiollisen voimankäytön periaatteiden mukaan toisen valtioon kohdistuvat kyberhyökkäykset tuomitaan usein laittomina, mutta kybervakoilun kaltaiset alemman asteen operaatiot jätetään usein lainsäädännöllisesti huomiotta. (Lin, 2011.) Yhdistyneiden kansakuntien kansainvälinen laki ei esimerkiksi miellä kybervakoilua laittomaksi. Kuitenkin eri maiden kybervakoiluyksiköt toimivat vieraan maan vakoilukentällä aina sillä riskillä, että kiinnijäädessään he voivat joutua syytöksiin kohdemaan oman lainsäädännön puitteissa. (Weissbrodt, 2013.) Tässä asetelmassa korostuu kuitenkin se, että kybervakoilun kentällä toimiminen ei edellytä perinteisen vakoilun tavalla läsnäoloa vakoilun kohdemaassa, jonka vuoksi vakoilijoiden vastuuseen saattaminen vaikeutuu huomattavasti. Lisäksi Weissbrodt (2013) kuvailee, että mikäli kybervakoilun toteuttaja toimii omassa kotimaassaan, esimerkiksi valtion tukemana, on hyvin epätodennäköistä, että edes kiinnijäädessään kotimaa lähettäisi kybervakoiluun syyllistynyttä kohtaamaan rangaistusta toiseen maahan.

Kollaboratiivista otetta tiedustelun kentällä puoltaa esimerkiksi Libicki (2017), joka tutkimuksessaan valaisee kriittisiä aspekteja modernin informaatiosodankäynnin globaalista luonteesta. Ensinnäkin kyberoperaatiot ovat verkottuneita tapahtumaketjuja kybertilassa. Esimerkiksi jonkin järjestelmän haltuunotto kybervakoiluoperaatiota varten voidaan nähdä moniulotteisena kyberoperaationa, joka heijastaa Libickin (2017) mukaan tekojen laajaa suunnitelmallisuutta ja koheesiota. Koska eri työkalujen ja toimijoiden yhteistyö on kyberhyökkääjien toimesta jo vahvaa, tulisi tutkimuksen mukaan samaa periaatetta noudattaa puolustuksessa. Kybertilan kokonaisvaltainen hyödyntäminen johtaa Libickin (2017) mukaan siihen, että eri valtiot voivat potentiaalisesti lisätä vaikutusvaltaansa kybertilan ulkopuolelle käyttämällä kyberoperaatioita. Esimerkiksi Venäjän kyberkampanjoilla on nähty olevan vaikutuksia reaalimaailman tapahtumiin, joka vahvistaa ilmiön poliittisuutta sekä yhteiskunnallista merkityksellisyyttä (Libicki, 2017). Kyberoperaatioiden informaatiovaikuttamisen keinot ovat vertaansa vailla modernissa yhteiskunnassa. Onkin mahdotonta edesauttaa globaalia yhtenäisyyttä ja tukea rauhan aikaa ilman valtioidenvälistä turvallisuusyhteistyötä (Lledo-Ferrer & Dietrich, 2020).

Tämän lisäksi selkeän kansainvälisen lainsäädännön puute kybervakoilun osalta voidaan nähdä ongelmallisena monimutkaistuvien uhkakuvien torjunnan kannalta (Boeke & Broeders, 2018). Esimerkiksi Venäjän ja Kiinan oletettavasti käyttämät ulkoistetut kybervakoilijat voidaan nähdä uhkaavan länsimaista oikeuskäsitystä. Boeke ja Broeders (2018) perustelevat tarvetta yhtenäiselle lainsäädännölle kybervakoilun osalta etenkin sillä, että sen avulla voitaisiin minimoida valtioiden uskottavaa kiistettävyyttä kybervakoilun toimijoina. Ongelmalliseksi on noussut nimenomaan diskurssi kybervakoilun kiistettävyydestä ja vaikeudesta varmentua tekijöiden motiiveista tai kansallisuudesta. Yhtenäisemmän lainsäädännön avulla voitaisiin potentiaalisesti siis ratkaista attribuutio-ongelma, jonka varjolla kybervakoilu nykyisin puittein pitkälti toteutuu ja onnistuu.

5 YHTEENVETO

Kybervakoilun sekä tiedustelutoiminnan muodostama informaationkeruun kehikko on oleellinen osa kansainvälistä poliittista liikehdintää. Kybertila on noussut globaalin tietoyhteiskunnan kehityksen myötä osaksi niin ihmisten arkielämää, kuin valtion perusinfrastruktuuriakin. Tästä syystä reaalimaailman tapahtumat, kuten poliittiset konfliktit, heijastuvat kybertilaan tai toteutuvat sen kautta. Kybervakoilu tulee nähdä osana valtioidenvälistä poliittista kanssakäymistä, jonka tarkoituksena on ensisijaisesti informaation tavoitteellinen kerääminen. Kybervakoilun poliittista kompleksisuutta kuvaa sen lainsäädännöllisesti epäselkeä asema kansainvälisen lain puitteissa, joka voi johtaa valtiot ulkoistamaan kybervakoiluaan ulkoisille toimijoille, kuten hakkeriryhmille.

Valtiollisen turvallisuustilanteen suojeleminen verkottuneessa ja globaalissa maailmassa on osittain tiedusteluviranomaisten tehtävää. Tiedustelutoiminta keskittyy toiminnassaan torjumaan muitakin kyber- ja reaalimaailman uhkakuvia kuin vakoilua, tehden tiedustelun kentästä monitahoisen. Kuten tutkimuksessa todetaan, kybervakoilusta ovat pääasiassa vastuussa valtiolliset toimijat tai niiden toimeenpanemat tahot. Täten puhuttaessa valtiollisesta tiedustelusta, voidaan havaita, että vakoilun ja tiedustelun rajapinta on ennen kaikkea häilyvä. Toisen valtion tiedustelutoiminta saattaa näyttäytyä kohdevaltiolle vakoiluoperaationa. Tästä syystä käsitteiden limittyneisyys täytyy keskustelussa tarkoin huomioida.

Tässä tutkielmassa tutkitaan poliittisesti motivoitunutta kybervakoilua, jonka voidaan ensisijaisesti tarkoittavan valtion laitonta informaationkeruuta vieraan valtion toimista, kyvykkyyksistä sekä varautuneisuudesta. Poliittisesti motivoituneen kybervakoilun nähdään tavoittelevan informaatioylivoimaa, jonka avulla valtion uskotaan pystyvän parantamaan toisaalta omaa varautuneisuuttaan, mutta myös operatiivisia kykyjään esimerkiksi mahdollisiin kyberoperaatioihin. Kybervakoilu ilmenee ennen kaikkea osana laajempia kyberoperaatioita, jotka voivat ilmentyä esimerkiksi kohdistettuina kyberiskuina toisen valtion tietojärjestelmiin. Tässä tutkimuksessa käsitellään pääpiirteittäin kybervakoilun kannalta oleellisia kyberoperaatioita, joista tarkemmin esitellään APT-iskuja. Keinovalikoimaan kuuluu lukuisia muitakin metodeja, joita ei kokonai-

suudessaan tämän tutkielman laajuuden puitteissa voida käsitellä. Mikäli kybervakoilua toteutetaan osana laajempaa operaatiota, on sen rooli ennen kaikkea operatiivisesti alustava. Toisaalta kybervakoilua voi ilmetä ilman varsinaista voimankäytöllistä kyberiskua, kuten esimerkiksi tiedonkeruuoperaatioina, jota saatetaan hyödyntää informaatiovaikuttamisessa.

Tiedusteluviranomaisten harjoittamaa tiedustelutoimintaa lähestytään tässä tutkielmassa ensin määrittelemällä keskeiset tiedustelulajit, joita toiminnassa käytetään Suomen mallin mukaan. Mallien perusteella todetaan, että tiedustelutoimintaa tulee tarkastella ennen kaikkea kompleksisena ja monitahoisena ilmiönä, jossa eri keinomenetelmiä sovelletaan kulloisenkin operaation vaatimalla tavalla. Tämän lisäksi pohditaan älykkään tiedustelutoiminnan kyvykkyyttä kohdata kybervakoilua ennakoivasti sekä kollaboratiivisesti luomalla asiaankuuluvia uhka-arvioita kybervakoilun toteutuksesta. Vakoilun estämistä havainnoidaan myös kyberhämäyksen konseptin avulla, jolla pyritään luomaan hämäävää ja harhaanjohtavaa tietoa, johon hyökkääjän odotetaan tarttuvan. Tässäkin korostuu ennen kaikkea puolustuksen ennakoiva luonne sekä hyökkääjän mahdollisimman kokonaisvaltainen tuntemus.

Suomen tiedustelutoimintaa sekä kybervakoilulta puolustautumista tarkastellaan etenkin kansainvälisen yhteistyön kehikon kautta. Olennaista uhkakuvien torjunnassa on niiden globaaliuden sekä poliittisen kontekstin ymmärtäminen, jonka vuoksi yhteistyöllä nähdään olevan suuri rooli esimerkiksi kybervakoilulta puolustautuessa. Suomessa tiedustelutoimijoita ovat Puolustusvoimat sekä Suojelupoliisi, joiden toimintaa tarkastellaan tiedustelulajien kautta. Tiedustelutoiminnan toimintaympäristö sekä kyberuhkien torjuminen vaatii tiedusteluviranomaisilta kokonaisvaltaista keinovalikoimaa, jota pyritään toteuttamaan yhdistelemällä eri tiedustelulajeja tilanteen mukaan. Suomeen kohdistuva kybervakoilu on luonteeltaan jatkuvaa sekä Suomen kokoon suhteutettuna huomattavaa.

Tässä tutkielmassa käsitellään kybervakoilua sekä tiedustelutoimintaa etenkin poliittisesta ja globaalista näkökulmasta. Vaikkakin esimerkiksi taloudellinen kybervakoilu yritysten välillä voi saavuttaa poliittisiksi luokiteltavia ulottuvuuksia, ei tämä tutkimus suoraan ota niihin kantaa. Poliittisella motivoituneisuudella pyritään tässä tutkielmassa kuvaamaan ennen kaikkea kybervakoilun globaalia luonnetta sekä sen merkitystä valtioidenvälisille suhteille. Tutkielmassa esitelty kybervakoiluun käytettävä keinovalikoima voi täten olla rinnastettavissa myös esimerkiksi taloudelliseen vakoiluun, mutta sen toimintamekanismeja tai sen syvempiä tarkoitusperiä ei tässä tutkielmassa tutkita.

Tällä tutkielmalla tavoitellaan parempaa kokonaisymmärrystä kybervakoilun sekä valtiollisen tiedustelutoiminnan roolista globaalin politiikan kentällä. Tässä tutkielmassa pyritään rajaamaan niitä vaikutussuhteita, joiden pohjalta kybervakoilua harjoitetaan. Tämän lisäksi tutkielma pyrkii rajaamaan niitä keskeisiä keinomenetelmiä, joiden avulla valtiollista kyberpuolustusta voidaan harjoittaa etenkin kybervakoilua vastaan. Tärkeänä aspektina tutkielmassa on myös kansainvälisen yhteistyön roolin korostaminen sekä osaamisen kehittäminen kollektiivisella ja kauaskantoisella tavalla. Tutkielma on linjassa aiem-

man tiedustelupoliittisen tutkimuksen kanssa, mutta painottaa näkökulmassaan etenkin myös Suomen tilannetta, joka harvoin on esillä tutkimuskohteena.

Tutkimustuloksia arvioidessa koetaan, että kaikkiin esitettyihin tutkimuskysymyksiin saatiin vastaus. Suomen tiedustelutoiminnan tarkastelua peilattiin kuitenkin ennen kaikkea globaalin yhteistyön kautta, sillä Suomessa tehtyä tutkimusta kybervakoilusta sekä tiedustelutoiminnasta on vähän. Täten esimerkiksi on mahdoton arvioida Suomessa käytettyjä puolustusmenetelmiä tiedustelun lajien määrittelyä pidemmälle, sillä tutkimusta keskittyen Suomen tilanteeseen ei ole suurta määrä tarjolla. Jatkotutkimuskohteena olisikin mielenkiintoista keskittyä rajaamaan Suomen geopoliittisen sijainnin perusteella tyypillisiä kybervakoilun ilmenemismuotoja. Tämän lisäksi erityisen kiinnostavaa olisi valottaa puolustusmenetelmiä etenkin Suomen tiedusteluviranomaisten näkökulmasta ja tutkia sitä, kuinka ne eroavat esimerkiksi tässä tutkielmassa esitetyistä menetelmistä.

LÄHTEET

Achleitner, S., La Porta, T., McDaniel, P., Sugrim, S., Krishnamurthy, S. V. & Chadha, R. (2016). Cyber deception: Virtual networks to defend insider reconnaissance. *Proceedings of the 8th ACM CCS international workshop on managing insider security threats,* 57-68.

Aid, M. (2002). 'Stella polaris' and the secret code battle in postwar Europe. *Intelligence and National Security, 17*(3), 17-86.

Almeshekah, M. H. & Spafford, E. H. (2016). Cyber security deception. *Cyber deception* (s. 23-50) Springer.

Anttonen, M. (2020). Ulkoasiainhallinto ja tiedustelu – yhteistyötä yhteisen asian eteen. *Kylkirauta 287(2)*, 19-21.

Axelrod, R. & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences, 111*(4), 1298-1303.

Bakdash, J. Z., Pizzocaro, D., & Precee, A. (2013). Human factors in intelligence, surveillance, and reconnaissance: Gaps for soldiers and technology recommendations. *MILCOM 2013-2013 IEEE Military Communications Conference.* s. 1900-1905. IEEE.

Bigelow, B. (2019). What are Military Cyberspace Operations Other Than War?. *11th International Conference on Cyber Conflict (CyCon)* s.1-17. IEEE.

Biller, J. & Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. *Naval War College Review, 71*(4), 16.

Betz, D. (2012). Cyberpower in strategic affairs: Neither unthinkable nor blessed. *Journal of Strategic Studies*, *35*(5), 689-711.

Bodeau, D. J., Graubart, R. & Fabius-Greene, J. (2010). Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels, *IEEE Second International Conference on Social Computing*. s. 1147-1152.

Boeke, S. & Broeders, D. (2018). The demilitarisation of cyber conflict. *Survival, 60*(6), 73-90.

Borum, R., Fein, R., Vossekuil, B., & Berglund, J. (1999). Threat assessment: Defining an approach for evaluating risk of targeted violence*. Behavioral Sciences & the Law, 17*(3), 323-337.

Bushby, A. (2019). How deception can change cyber security defences. *Computer Fraud & Security*, *2019*(1), 12-14.

Carlisle, R. P. (2005). *Encyclopedia of intelligence and counterintelligence.* Armonk, N.Y. Sharpe Reference. Haettu osoitteesta http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=971442

Caton, J. (2020). Dancing on the razor's edge: A foundational review of IoT exploitation and defense through the lens of TECHINT collection. *International Journal of Intelligence and CounterIntelligence*, *33*(3), 540-555.

Cormac, R. & Aldrich, R. J. (2018). Grey is the new black: Covert action and implausible deniability. *International Affairs, 94(*3), 477-494.

Denécé, E. (2014). The revolution in intelligence affairs: 1989–2003. *International Journal of Intelligence and CounterIntelligence*, *27*(1), 27-41.

Enisa. (2020). *ENISA threat landscape 2020 - cyber espionage.* European Union Agency for Network and Information Security. Haettu osoitteesta https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

Farago, L. (2012). *Burn after reading: The espionage history of world war II.* Naval Institute Press.

Gellman, R. (2002). Perspectives on privacy and terrorism: All is not lost—yet. *Government Information Quarterly, 19*(3), 255-264.

Gunneriusson, H. & Ottis, R. (2013). Cyberspace from the hybrid threat perspective. *Journal of Information Warfare*, *12*(3), 67-77.

Hanska, J. (2013). The emperor's digital clothes: Cyberwar and the application of classical theories of war. Teoksessa Rantapelkonen, J. & Salminen, M. (toim.) *The Fog of Cyber Defence, 2*, 169-190.

Harknett, R. J. & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies, 7*, 1-34.

Jansson, S. & Sihvonen, T. (2018). Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. *Media & Viestintä*, *41*(1).

Laki sotilastiedustelusta 2019/590. Annettu Helsingissä 26.4.2019. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2019/20190590

Lehto, M. & Limnéll, J. (2017a). Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede Ja Ase, 75.*

Lehto, M. & Limnéll, J. (2017b). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.* Valtioneuvoston kanslia. Haettu osoitteesta http://urn.fi/URN:ISBN:978-952-287-368-2

Libicki, M. C. (2017). The convergence of information warfare. *Strategic Studies Quarterly, 11*(1), 49-65.

Limnéll, J. (2014). Kybermaailman vaikutus sodankäyntiin. *Futura, 33*(2), 48.

Lipton, E., Sanger, D. E. & Shane, S. (Joulukuu 2016). The perfect weapon: How Russian cyberpower invaded the US. *The New York Times.*

Lledo-Ferrer, Y. & Dietrich, J. (2020). Building a European intelligence community. *International Journal of Intelligence and CounterIntelligence, 33*(3), 440-451.

Lohse, M., Meriniemi, M. & Honkanen, K. (2019). *Tiedustelumenetelmät*. Helsinki: Alma Talent Oy. Haettu osoitteesta https://verkkokirjahylly.almatalent.fi/teos/GAEBFXDTEB

Lohse, M. & Viitanen, M. (2019). *Johdatus tiedusteluun*. Helsinki: Alma Talent Oy. Haettu osoitteesta https://verkkokirjahylly.almatalent.fi/teos/EAEBFXDTEB

Lowenthal, M. M., & Clark, R. M. (2015). *The five disciplines of intelligence collection.* Sage. Haettu osoitteesta https://books.google.fi/books?id=rdI5DQAAQBAJ&printsec=frontcover&hl=fi#v=onepage&q&f=false

Mattern, T., Felker, J., Borum, R. & Bamford, G. (2014). Operational levels of cyber intelligence. *International Journal of Intelligence and CounterIntelligence, 27*(4), 702-719.

Maurer, T. (2018). Cyber proxies and their implications for liberal democracies. *The Washington Quarterly, 41*(2), 171-188.

Messaoud, B. I., Guennoun, K., Wahbi, M., & Sadik, M. (2016). Advanced persistent threat: new analysis driven by life cycle phases and their challenges. *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS)* (s. 1-6). IEEE.

Moran, N. (2010). A cyber early warning model. Teoksessa Carr, J. (toim), *Inside Cyber Warfare*, 179-189. O'Reilly Media.

Mtsweni, J., Mutemwa, M., & Mkhonto, N. (2016). Development of a cyber-threat intelligence-sharing model from big data sources. *Journal of Information Warfare, 15(*3), 56-68.

Nato Public Diplomacy Division. (2013). NATO-Russia practical cooperation. Haettu osoitteesta https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2013_12/20131127_131201-MediaBackgrounder-NRC_en.pdf

Ohra-aho, H. (2020). Tiedustelun paradigman muutoksesta. *Kylkirauta 287(2)*, 10-13.

Poliisilaki 872/2011. Annettu Helsingissä 22.7.2011. Haettu osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2011/20110872#L5P1

Prislan, K. & Bernik, I. (2012). Global and national take on state information warfare. *Journal of Information Warfare, 11*(2), 37-53.

Pun, D. (2017). Rethinking espionage in the modern era. *Chicago Journal of International Law, 18*(1), 353-391.

Rot, A., & Olszewski, B. (2017). Advanced Persistent Threats Attacks in Cyberspace. Threats, Vulnerabilities, Methods of Protection. *Position Papers of the 2017 Federated Conference on Computer Science and Information Systems* (s. 113-117).

Rowe, N. C. & Goh, H. C. (2007). Thwarting cyber-attack reconnaissance with inconsistency and deception. *IEEE SMC Information Assurance and Security Workshop.* (s.151-158) West Point, NY.

Rudner, M. (2004). Hunters and gatherers: The intelligence coalition against islamic terrorism. *International Journal of Intelligence and CounterIntelligence, 17*(2), 193-230.

Rudner, M. (2013). Cyber-threats to critical national infrastructure: An intelligence challenge. *International Journal of Intelligence and CounterIntelligence, 26*(3), 453-481.

Salminen, A. (2011). *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasan yliopiston julkaisusarja, Opetusjulkaisuja 62, Julkisjohtaminen 4.

Suojelupoliisi. (2020). *Kansallisen turvallisuuden katsaus 2020*. Haettu osoitteesta https://supo.fi/documents/38197657/39761269/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf/dd60c411-2ee5-d5c9-83a0-2e91b08ccd36/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf?t=1603899390368

Suojelupoliisi. (2018). *Suojelupoliisin juhlavuosikirja 2018*. Haettu osoitteesta https://supo.fi/documents/38197657/40760236/2018_Supo_Juhlavuosikirja-70.pdf/d986a8e0-65d5-5bf6-0857-b516d1c8907d/2018_Supo_Juhlavuosikirja-70.pdf?t=1602665751133

Toveri, P. & Pelttari, A. (2020). Sotilas- ja siviilitiedustelu– kehittämistä ajan hengessä. *Kylkirauta 287(2)*, 5-9.

Wang, C. & Lu, Z. (2018). Cyber deception: Overview and the road ahead. *IEEE Security & Privacy*, *16*(2), 80-85.

Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information, 6*(2), 183-211.

Weissbrodt, D. (2013). Cyber-conflict, cyber-crime, and cyber-espionage. *Minnesota Journal of International Law*, *22*, 347.

Yuill, J., Denning, D., & Feer, F. (2007). Psychological Vulnerabilities to Deception, for Use in Computer Security. *DoD Cyber Crime Conference.*