Kybersodankäynnin kehityksestä ja tulevaisuudesta

Martti Lehto ja Jarno Limnéll

Abstract

Finland as a highly developed information society is very dependent on electrical energy as well as functioning information networks and systems, because of this threats in the cyber domain are especially significant from the perspective of overall national security. In addition, Finnish defense forces are increasingly technology dependent, which is why cyber defense is a more crucial area in military capabilities. In addition to increasing dependency, non-state and especially state actors' improved capability to influence through cyber domain Finland's vital functions forms threat to Finnish society that needs to taken seriously.

Cyber warfare is the result of long evolution. Armed forces have taken advantage of electromagnetic spectrum since the invention of radio. Electronic world developed during the Second World War created the electronic warfare operational environment. Cyber world made of bits has created a new domain, to which the armed forces has also attached itself. Armed forces' command and control, communication, intelligence and surveillance have become a part of cyber world. This evolution has taken more than 100 years, which has created a new cyber-physical operational domain, in which human, information, and technology create a completely new embedded domain. Cyber warfare together with information warfare and electronic warfare create a new non-kinetic domain, which operates in warfare's tactical, operational, strategic, and national comprehensive security levels. These non-kinetic capabilities are an essential part of the hybrid warfare whole.

This article describes the evolution of non-kinetic warfare and the different factors influencing cyber warfare and cyber operations and the development of cyber threats. Based on this evolution we present a network-based operational environment framework.

The article also evaluates the future of cyber domain and cyber warfare, cyber diplomacy and politics, in addition to the cyber deterrence and the probable military center of gravities for the next decade.

Key findings of our research indicate that the complexity, effectiveness, and capability of cyber-attacks is growing faster than the defensive capabilities. Often only serious cyber-attacks give the push to improve security measures. Cyber threats should be seen as a part of hybrid operation and this requires effective and centralized observation-situation picture-command and control capability. In addition to the development of national cyber security capability, it is also needed to deepen international cooperation and wide-ranging interdisciplinary cyber security research.

Johdanto

Euroopan komissio analysoi pohdinta-asiakirjassaan kesällä 2017 tulevaisuuden uhkamaailmaa. Sen mukaan teknologian kehitys muuttaa merkittävästi niin turvallisuuden kuin puolustuksen luonnetta. Big data, pilviteknologia, miehittämättömät ajoneuvot ja tekoäly mullistavat puolustussektoria vahvistaen myös siviiliteknologian merkitystä puolustusalalla. Tämän verrattain helposti saatavilla olevan teknologian käyttö mahdollistaa epätavanomaisten, valtioiden rajat ylittävien ja epäsymmetristen uhkien nopean kasvun. Näitä ovat muun muassa hybridi- ja kyberuhat, terrorismi sekä kemialliset, biologiset ja radiologiset iskut. Internetin käyttäjien määrän nopean kasvun myötä kyberrikollisuudesta ja internetin terrorikäytöstä on tullut 2000-luvulla sodankäynnin uusia muotoja. (Euroopan komissio 2017, 10.)

Teknologian kehitys ja digitalisaation vaikutukset ilmenevät myös suomalaisissa turvallisuus-asiakirjoissa. Sisäisen turvallisuuden selonteon mukaan robotisaatio, virtualisaatio, keinoälyn kehitys, nanomateriaalit, bioteknologia ja energiateknologia ovat esimerkkejä teknologioista, joiden merkitystä sisäisen turvallisuuden toimintaympäristölle ei voi ylikorostaa (Sisäministeriö 2016, 52). Uusimmassa puolustusselonteossa kyberympäristön merkityksen todetaan kasvavan. Puolustusselonteon mukaan kyber- ja informaatiovaikuttamista on kohdistettu Suomeen muun muassa kriittistä infrastruktuuria, teollisuuslaitoksia sekä poliittista päätöksentekojärjestelmää ja kansalaisia vastaan (Valtioneuvoston kanslia 2017, 9).

Elektronisen sodankäynnin, informaatiosodankäynnin ja kybersodankäynnin operaatiot muodostavat viitekehyksenä kyberajan ei-kineettisten verkostoperustaisten operaatioiden kokonaisuuden. Sodankäynnissä nämä operaatiot muodostavat verkottuneen kokonaisuuden, jossa eri operaatiomuotojen avulla pyritään saavuttamaan sodankäynnille asetetut tavoitteet usein osana hybridivaikuttamista. Kybersodankäynti ei ole syrjäyttänyt aikaisempia ei-kineettisiä sodankäynnin muotoja, mutta kybermaailma on laajentanut sodankäynnin

ympäristöä ja samalla se läpäisee myös yhä merkittävämmin muita sodankäynnin toimintaympäristöjä (Limnéll 2016, 50–60). Kyberympäristöstä on tullut erottamaton osa niin nykyajan sodankäyntiä kuin turvallisuuden kokemista.

Kybermaailman kehitys ei ole irrallinen ilmiö vaan se yhdistyy vahvasti yhteiskuntarakenteisiin ja eri turvallisuustoimijoiden tarpeisiin ja odotuksiin. Kehitykselle on ominaista nopeus sekä tietynlainen arvaamattomuus tulevaisuudesta. Kybermaailmaa ja teknologian kehitystä ei myöskään tule nähdä pelkästään uhkien näkökulmasta vaan teknologia tuottaa uudenlaisia ratkaisuja ja toimintamalleja turvallisuuden tuottamiseen. Uusista teknologisista ratkaisuista otetaan käyttöön ne, mitkä parhaiten tuottavat lisäarvoa, tehokkuutta ja vaikuttavuutta.

Tässä artikkelissa arvioidaan ensin kyberympäristön historiallista kehitystä ja siinä vaikuttaneita tekijöitä. Nykyhetkessä on ymmärrettävä puolestaan erilaiset kybersodankäyntiin ja kyberoperaatioihin sekä kyberuhkien kehitykseen vaikuttavat tekijät, joiden pohjalta esitetään verkostopohjaisen toimintaympäristön viitekehys. Artikkelin lopussa arvioidaan myös kyberympäristön ja kybersodankäynnin tulevaisuutta ja todennäköisiä sotilaallisia painopistealueita ensi vuosikymmenellä.

Digitalisaation murros

Digitalisaation vaikutukset koskevat laajasti niin yksilöitä, organisaatioita, yrityksiä kuin yhteiskuntaa yhteisesti. Digitaalitekniikka integroidaan osaksi ihmisten arkea niin kotona kuin työelämässä. Kyse on yhteiskunnallisesta prosessista, jossa hyödynnetään teknologisen kehityksen uusia mahdollisuuksia. Digitalisaatio on luonut spesifisiä ilmiöitä, luonut erilaisia toimintaympäristöjä ja mahdollistanut käyttäytymistä, joita ei ollut ennen digitaalista aikaa. (Lehto & Neittaanmäki 2016, 56–64.)

Digitalisaatiosta on tullut yhä tärkeämpi osa yritysten ja ihmisten toimintaa. Digitaalisuuteen pohjautuvia innovaatiomahdollisuuksia syntyy koko ajan lisää. Näköön, kuuloon ja kosketukseen perustuvat teknologiat luovat uusia mahdollisuuksia ja tapoja käsittää maailma ja olla yhteydessä sen kanssa. Tavaroista ja palveluista tulee älykkäämpiä. Myös yritykset voivat luoda syvempiä reaaliaikaisia suhteita kumppaneihin, asiakkaisiin, palvelun- ja tavarantoimittajiin sekä julkishallintoon. Samaan aikaan digitalisaation seurauksena syntyy uudenlaisia uhkia. Digitaalinen kybermaailma houkuttelee rikollisia, jotka etsivät uusia mahdollisuuksia varastaa, hyödyntää ja myydä tietoa. Tiedon ja informaation siirtyminen verkkoon on tuonut sinne myös tiedusteluorganisaatiot. Terroristeille kybermaailma on yhteydenpidon, viestinnän ja vaikuttamisen

toimintaympäristö, minkä lisäksi se on heille houkutteleva hyökkäyskohde. Asevoimien digitalisaatio on luonut sotilaallisen kybermaailman, jossa vaikuttavat verkottuneiden sotilaiden lisäksi älykkäät ja yhä itsenäisemmät asejärjestelmät.

Digitaalinen murros perustuu ihmisten muuttuneisiin odotuksiin, yhteiskunnan palvelurakenteiden ja -tuotannon kasvaneisiin tehokkuusvaatimuksiin ja teknologioiden tarjoamiin mahdollisuuksiin. Uudet teknologiat, työkalut ja toimintatavat muuttavat ihmisten tapaa toimia arjessa ja työssä, organisaatioiden tapaa toteuttaa tehtäviään ja julkishallinnon tapaa tuottaa palveluita. (Lehto & Neittaanmäki 2016, 56–64.)

Tulevaisuuden digitaaliset palvelut perustuvat ihmisten, innovatiivisten toimijoiden ja älykkäiden koneiden ekosysteemiin. Kehittyvässä digitaalisessa yhteiskunnassa mahdollisuuksien tila laajenee. Tilaa laajentavat kyberfyysiset toisiinsa kytkeytyneet järjestelmät, vuorovaikutteisuus, itse tuottaminen ja jakaminen, sekä koneiden älykkyyden ja kyvykkyyden kasvu. Digitaalitalouden kehitystä edistävät kansalaisten identiteetin ja tietokäytäntöjen siirtyminen verkkoon sekä organisaatioiden palvelurakenteiden digitalisaatio yhdistettynä luottamukseen systeemin turvallisuudesta. Näin muodostuu digitaalinen alustatalous, jossa elementteinä ovat teollinen internet, erilaiset sosiaalisen median ja viestinnän alustat sekä hajautetut ja yhteisölliset palvelut.

Asevoimat ovat vastaavalla tavalla kehittyneet riippuvaisiksi informaatiosta, verkostoista ja sähköenergiasta – siis koko digitaalisesta maailmasta – jossa tietotekniikan erilaiset sovellukset ovat kiinteä osa asevoimien laitteita ja järjestelmiä. Kyberavaruus fuusioi kaikki tietoliikenneverkot, tietokannat ja informaatiolähteet globaaliksi virtuaalisysteemiksi.

Kyberuhat digitaalisessa maailmassa

Tutkimukset osoittavat, että yrityksen tai organisaation sisällä työskentelevät ihmiset ovat merkittävä kyberuhka. IBM:n mukaan sisäpiiriläiset tekivät jopa 60% kaikista hyökkäyksistä. Tietoturvayhtiö Kaspersky on puolestaan arvioinut, että 21% organisaatioista oli menettänyt luottamuksellista tietoa sisäpiiriläisten toiminnan vuoksi. Sisäpiiriläisiä voivat olla nykyiset sekä entiset työntekijät, nykyiset sekä entiset palveluntarjoajat, sopimuskumppanit sekä konsultit, nykyiset sekä entiset toimittajakumppanit sekä liiketoimintakumppanit ja asiakkaat. (Lehto ym. 2017, 22.)

Tulevaisuudessa kyberturvallisuutta eniten muokkaavat voimat ovat yhä laajeneva kyberhyökkäysala, hakkeroinnin teollistuminen, kyberturvallisuusmarkkinan monimutkaisuus sekä hajautuneisuus. Tulevaisuudessa nähdään hyökkääjien kehittyneisyyden lisääntyminen, tietovuotojen kustannusten

kasvu, yhteensopivien tietoturvateknologioiden ja taitavien tietoturva-ammattilaisten puute. Keskeisiä kyberhyökkäyskohteita ovat esineiden internet, pilvipalvelut, big data ja mobiiliratkaisut. Koska verkkoon liitettävien esineiden määrä kasvaa ja pienten sensoreiden turvaaminen on haasteellista, saavat kyberhyökkääjät valtavasti uusia hyökkäysmahdollisuuksia. Tämä digitalisaation kehitys koskee myös asevoimia, jotka osin jopa kulkevat digitalisaation kärjessä. (Lehto ym. 2017, 13–19.)

Kyberuhkien aiheuttajat kehittävät jatkuvasti uusia tapoja hyökätä haluamiinsa kohteisiin. Kyberrikoksista on tullut vahva ja elinvoimainen liiketoiminnan alue. Vaikka uudet palvelut tuovat mukanaan myös uudenlaisia kyberuhkia, organisaatiot eivät voi ottaa taka-askeleita ja luopua verkkopalveluiden, mobiliteetin, big datan tai pilvipalveluiden tuomista hyödyistä. Digitalisaatio on synnyttänyt työtä ja kansalaisten elämää helpottavia uusia innovaatioita. Tässä tilanteessa on lähdettävä aivan uusilla tavoilla hakemaan informaatioteknologian, kyberturvallisuuden ja liiketoiminnan liittoa. Kyberuhkia vastaan toimiminen edellyttää myös uudenlaisia tapoja toimia yritysten ja julkisten toimijoiden välillä sekä myös kansainvälisessä yhteistyössä. Tietoa on jaettava aktiivisesti kyberuhkista, tapahtuneista hyökkäyksistä sekä uusista vaaroista. Keskeisintä on yhteisen tilannetietoisuuden kehittäminen.

Kybermaailman sodankäynnin evoluutio

Bousquetin sodankäynnin evoluutio

Tutkija Antoine J. Bousquet Lontoon yliopistosta jakaa sodankäynnin evoluution neljään periodiin. 1600–1700-lukujen manööveri-intensiivinen toimintatapa perustui mekanistiseen (kellokoneisto) sodankäyntiin. Tämä aikakausi huipentui Frederik Suuren (1721–1786) kehittämään Preussin armeijaan, joka oli aikansa tehokkain. 1800-luvun alussa alkoi termodynamiikan kehittyminen, joka näkyi joukkojen operatiivisen ja jopa strategisen liikkuvuuden parantumisena. Aikaisemmin joukkojen liikkuvuus oli perustunut ”ihmisvoimaan” ja ”hevosvoimaan”, nyt niitä voitiin korvata aluksi höyryvoimalla, sitten polttomoottorin avulla. Sodankäynnistä tuli energiaintensiivinen, mikä näkyi sekä aseissa että joukkojen liikkuvuudessa. Toinen maailmansota oli tämän vaiheen huipentuma. Materiaalisista resursseista tuli sodan voiton avain. (Bousquet 2009, 37–62.)

Bousqetin mallissa kolmannen periodin muodostaa tietokoneisiin perustuva kybernetiikan aikakausi. 1800-luvun lopulta oli alkanut elektromagneettisen kommunikaation aikakausi, jossa radiosta tuli toisen maailmansodan aikana

keskeinen johtamisväline ja tutkasta ilmasodankäynnin keskeinen valvonta- ja johtamisväline. Sysäyksen kohti tietokoneiden ja kybernetiikan aikaa antoi brittiläinen matemaatikko ja logiikan tutkija Alan Turing (1912–1954), joka vuonna 1936 julkaisi formalisoimansa symboliseen logiikkaan perustuvan algoritmin ja tietojenkäsittelytieteessä käytetyn Turingin kone -käsitteen. Toisen maailmansodan aikana hän johti Saksan laivaston Enigma-salakirjoituskoneella tehtyjen viestien purkamistyötä. Sodan jälkeen hän suunnitteli yhden ensimmäisistä ohjelmoitavista digitaalisista tietokoneista rakentaen siitä myös ensimmäisen prototyypin Manchesterin yliopistossa. Yhdysvalloissa matemaatikko John von Neumann (1903–1957) kehitti kvanttimekaniikkaa ja tietojenkäsittelytiedettä Manhattan-projektin yhteydessä. Hän oli mukana ensimmäisen täysin elektronisen tietokoneen ENIAC (Electronic Numerical Integrator And Computer) kehittämisessä. Neumannin suurin kontribuutio oli sillan luominen Turingin abstraktin koneen ja loogisen elektronisen laskennan välille. (Bousquet 2009, 37–62.)

Toisen maailmansodan jälkeen kehittyi kybernetiikan systeemikoulukunta, jonka etulinjassa toimi yhdysvaltalainen matemaatikko Norbert Wiener. Kybernetiikka yhdisti tietokoneet ja verkon konemaiseksi kokonaisuudeksi, jossa systeemin hallinta perustui servomekanismiksi kuvattuun feedback-prosessiin. Verkossa käytetään loogisia tietomalleja ja toimintasääntöjä. Sen semioottinen kone saattoi käsitellä mitä tahansa symbolista informaatiota. Kyberneettisen valvontamekanismin tavoitteena oli saada voitto vallitsevasta entropiasta (epäjärjestyksestä). Sodan jälkeinen verkosto kasvoi ja laajeni perinteisestä viestiverkosta laajaksi tiedustelu-, valvonta-, johtamis-, informaatio- ja maalittamisjärjestelmäksi (Command-Control-Communication-Computer-Information-Intelligence-Surveillance-Reconnaissance-Target Aquisition, C^4I^2SRTA). Kyberneettisellä mallilla pyrittiin luomaan ”täydellinen sotakone”. Tutkalla voitiin saada havainto maalista ja antaa tieto johtamisjärjestelmän tietokoneelle, joka laski maasta-ilmaan ohjukselle optimaalisen lentoradan. Järjestelmä voisi käskyttää ohjuksen ilmaan ja korjata sen lentorataa muuttuneen maalitiedon perusteella. Kun ohjus on optimietäisyydellä maalista, järjestelmä voi antaa käskyn ohjukselle ”räjähdä”. Nykyinen tekoälykehitys mahdollistaa tällaiselle koneelle täydellisen autonomisuuden.

Bousquetin neljännen periodin muodostaa kaaosympäristöön perustuva kompleksisten systeemien maailma. Epälineaarisuuden tutkiminen tietokonejärjestelmissä johti bifurkaatioilmiön kuvaamiseen dynaamisissa systeemeissä. Tutkimus osoitti, että hyvin pieni muutos parametreissa tai toiminta-arvoissa saattoi johtaa äkilliseen kvalitatiiviseen muutokseen systeemin pitkän aikavälin dynaamisessa toiminnassa. Bifurkaatiosta tuli keskeinen selityslogiikka järjestelmien transformaatioon ja evoluutioon. John Urry (2000, 121) on todennut,

että ”systeemit saavuttavat bifurkaatiopisteen niiden toiminnan ja tulevaisuuden kehityspolun tullessa arvaamattomaksi (unpredictable) ja uusi erilainen korkeamman tason järjestys ja rakenne tulevat esiin.” Bifurkaatiossa järjestelmä tuottaa kaksi vaihtoehtoista stabiliteettia, joilla pyritään vastaamaan häiriötilaan. Tilanteen/parametrien muuttuessa vaihe vaiheelta syntyy lukematon määrä vaihtoehtoisia stabiliteetteja. Järjestelmä on kaaoksen reunalla niin kauan kuin bifurkaatiolla voidaan tuottaa uusia stabiliteetteja. Kybermaailman kiihtyvä monimutkaisuus luo jatkuvasti uusia bifurkaatiotilanteita ja siten uusia mahdollisia kehityspolkuja (Bousquet 2009, 163–176.)

Bousquetin periodimallissa mekanismi ja kellokoneisto, termodynamiikka ja moottori, kybernetiikka ja tietokone sekä kompleksinen kaaosmalli (chaoplexity) ja verkosto muodostavat parin, joista kukin kuvaa oman aikakautensa sodankäyntitapaa. Nykyinen digitaalinen yhteiskuntarakenne muodostaa kyberfyysisen rakenteen, jossa yhdistyvät mekaaniset (fyysiset) rakenteet, kehittynyt tietotekniikka ja verkostot sekä informaatioympäristö moniulotteiseksi ja vaikeasti hallittavaksi kokonaisuudeksi. Seuraavaksi käydään läpi ei-kineettisen sodankäynnin evoluutio 1900 luvulta nykypäivään (ks. Kuva 1 sivulla 190).

Kommunikaatiosodankäynti

Asevoimien käyttämät kommunikaatiojärjestelmät ovat aina olleet tiedustelun, häirinnän ja lamautuksen kohteina. Lennätin oli salakuuntelun kohde ja lennätinlinjat katkaisun kohde heti lennättimen käyttöönoton jälkeen. Sodankäynnissä lennätin vaikutti ensimmäisen kerran Krimin sodassa 1853–1856. Sähköisillä viestivälineillä on ollut merkitystä lähes kaikissa sen jälkeisissä sodissa kuten Yhdysvaltain sisällissodassa 1861–1865. Lennätin mahdollisti rautateiden tehokkaan käytön ja joukkojen nopean keskittämisen valtakunnan haluttuun osaan. Ensimmäisessä maailmansodassa tästä tuli erittäin merkittävä osa sodan alkuvaiheen suunnitelmia.

Radioviestintää kuunneltiin ja häirittiin välittömästi radion sotilaallisen käyttöönoton jälkeen. Laivasto oli ensimmäinen puolustushaara, joka näki radioviestinnän potentiaalin, kun radion avulla tuli mahdolliseksi koordinoida laivasto-operaatioita aivan uudella tavalla. Kaikki 90 saksalaista sotalaivaa varustettiin langattomalla viestinnällä vuonna 1909. Venäjän ja Japanin välisessä merisodassa 1904–1905 radiokuuntelulla ja -häirinnällä oli vaikusta taistelujen lopputulokseen. Vuonna 1912 lordi ja amiraali Sir John Fisher (1841–1920) kutsui langatonta viestintää sodan ytimeksi, “the pith and marrow of war!” (Bacon 1929, 144).

Erityisesti saksalaiset kehittivät langatonta teknologiaa 1900-luvun alussa. Saksa käytti kuuntelutiedustelua menestyksellisesti Venäjää vastaan

Tannenbergin taistelussa 1914, sillä Venäjä käytti radioliikenteessä selväkielitekstiä. Menestyksen jälkeen perustettiin ensimmäinen kuunteluasema (Funkställe) vuonna 1915. Kuuntelutiedustelupalvelu (Horchdienst) perustettiin 1917. Nämä toimivat myöhemmin esimerkkeinä muiden maiden kuuntelutiedustelun kehittämiselle.

Elektroninen sodankäynti

Toisen maailmansodan aikana sähkömagneettinen ulottuvuus laajeni entisestään erityisesti ilmasodankäynnin alueella. Etenkin tutkajärjestelmän kehittäminen ja tulo operatiiviseen käyttöön mullistivat ilmasodan toisen maailmansodan aikana. Tutkan saaminen palveluskäyttöön oli ollut pitkän evoluutioprosessin tulosta. Ennen kuin tutkan toimintaperiaate ilmiönä ymmärrettiin ja se kyettiin muokkaamaan haluttuun käyttöön, sitä oli edeltänyt usean sadan vuoden tutkimisen, keksimisen ja kokeilujen sarja.

Elektronisen sodankäynnin (Electronic Warfare, EW) keinoin hyökkääjä pyrkii vaikuttamaan informaation kulkuun siten, että johtamisen ja tulenkäyttöjärjestelmien luotettavuus alenee ja informaatiorakenteiden käytettävyys pienenee.

Elektronisen sodankäynnin operaatiot jaetaan elektroniseen vaikuttamiseen, elektroniseen suojautumiseen ja elektroniseen tukeen. Elektroninen vaikuttaminen tarkoittaa häirintää ja harhauttamista, elektroninen tuki tarkoittaa tiedustelua ja valvontaa. Elektroninen suojautuminen on elektronisten järjestelmien käyttäjien suojautumistoimenpiteitä vastustajan elektronisen sodankäynnin operaatioita vastaan. Kaikilla näillä on yhteys informaatio- ja kyberoperaatioihin sekä ilmasodankäynnin kokonaisuuteen. (Kosola & Jokinen 2004, 30.)

Elektroninen vaikuttaminen käsittää kaikki ne toimenpiteet, joilla sähkömagneettisen spektrin välityksellä pyritään estämään, hidastamaan tai vähentämään vihollisen sähkömagneettista säteilyä hyödyntävien tai elektroniikasta riippuvien järjestelmien käyttöä taikka suuntaamaan käyttö oman toiminnan kannalta edulliselle alueelle. Elektroninen vaikuttaminen jakautuu häirintään, harhauttamiseen, lamauttamiseen ja tuhoamiseen. (Kosola & Jokinen 2004, 39–40.)

Elektroninen suojautumisen toimenpitein varmistetaan omien järjestelmien tehokas käyttö huolimatta vihollisen elektronisesta, vaikuttamisesta. Elektronien suojautuminen jakautuu aktiiviseen ja passiiviseen suojautumiseen. Operatiiviselta kannalta kysymys on suojautumisesta elektroniselta tiedustelulta ja vaikuttamiselta sekä niiden tukemalta asevaikutukselta. (Kosola & Jokinen 2004, 47.)

Elektroninen tuki tuottaa elektronisten lähetteiden ilmaisun ja paikantamisen perusteella tilannekuvaa ja sitä täydentäviä tietoja. Se on reaaliaikaista tiedustelua ja valvontaa, joka kohdistuu sähkömagneettista säteilyä käyttäviin järjestelmiin. Elektroninen tuki jakautuu elektroniseen tiedusteluun ja valvontaan, elektroniseen maalinosoitukseen ja elektroniseen uhkavaroitukseen. (Kosola & Jokinen 2004, 31.)

Informaatiosodankäynti

Vietnamin sodasta aina Irakin ensimmäiseen sotaan 1991 saakka johtamisen ja päätöksenteon tarvitseman informaation riittämättömyyttä taistelukentällä pyrittiin ratkaisemaan tietotekniikan avulla. Taistelukentän epävarmuuden uskottiin johtuvan informaation puutteesta. Uusi aika pyrki ratkaisemaan ongelmia tietokoneiden laskentakyvyn avulla ja luomalla uusia kommunikaatioteknologioita. Kylmän sodan aikana informaatioteknologiaa kehitettiin ratkaisuksi taistelukentän kaaoksen ja epävarmuuksien ratkaisemiseen. Tietoteknisten järjestelmien miniatyyrisoinnin, diffuusion ja uusien kommunikaatiovälineiden seurauksena on ollut informaatioparadigman kehittyminen. Kaaos- ja kompleksisuusteorioiden kehittyminen on lisännyt ymmärtämystä verkostojen ja hajautetun johtamisen mahdollisuuksista. (Bousquet 2009, 161.)

Tieto on aina ollut tärkeää taistelukentällä. Taistelukenttä on laajentunut taistelutilaksi, jossa joukot ja sotilaat ovat tulleet riippuvaiseksi informaatiosta, sähköisestä tiedonsiirrosta ja energian jakelusta. Martin C. Libicki (1995, ix–xi.) määritteli vuonna 1995 informaatiosodankäynnin (Information Warfare, IW) osa-alueiksi:

1. Johtamissodankäynti (command-and-control warfare, C2W)
2. Tiedusteluperusteinen sodankäynti (intelligence-based warfare, IBW)
3. Elektroninen sodankäynti (electronic warfare, EW)
4. Psykologinen sodankäynti (psychological operations, PSYOPS)
5. Hakkerisodankäynti (hackerwar)
6. Taloudellinen informaatiosodankäynti (information economic warfare, IEW)
7. Kybersota (cyberwar)

Hänen määrittelyssään informaatiosodankäynnistä tuli yläkäsite, joka sisältää sekä elektronisen sodankäynnin että kybersodankäynnin osa-alueet.

2000-luvun alussa suomalaisen näkemyksen mukaan ”informaatiosodankäynti on yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista ja tältä suojautumista

käyttämällä hyväksi informaatioympäristöä. Informaatiosodankäyntiä voidaan käydä yhteiskunnallisin, poliittisin, psykologisin, sosiaalisin, taloudellisin ja sotilaallisin keinoin kaikilla sodankäynnin tasoilla. Informaatiosodankäynti koskee koko yhteiskuntaa ja on siten luonteeltaan pääosin turvallisuuspoliittista sekä toiminnallisesti valtakunnallista strategista tasoa koskettavaa toimintaa. Informaatiosodankäynnissä päämääränä on kansallisten tavoitteiden mukaisesti hankkia ja ylläpitää informaatioylivoima." (Valtioneuvoston kanslia 2004, 156.)

Informaatio-operaatiot ovat sarja sotilaallisia toimintoja, joilla tuetaan Puolustusvoimien operaatioita suojaamalla oman päätöksenteon edellytykset ja heikentämällä vastustajan tilannetietoisuutta ja tahtoa.

Informaatio voidaan määritellä resurssiksi, jolla on kaksi ulottuvuutta. Se muodostuu eri keinoin kerätystä datasta sekä systeemistä, jonka avulla dataa on tulkittu ja analysoitu, siten tuottaen datalle merkitystä. Teknologian avulla voidaan lisätä informaation arvoa. Tietokantojen, tietoverkkojen ja data-analyysin avulla asevoimat voivat luoda korkeamman tason jaettua tilannetietoisuutta, paremmin synkronoitua johtamista ja tiedustelua sekä muuttaa informaatioylivoima ylivoimaksi myös fyysisessä taistelutilassa.

Informaatiosodankäynnin operaatioiden avulla pyritään hankkimaan informaatioylivoima eli tilanne, jossa on kyetty luomaan itselleen edullisen asetelman informaatioympäristössä. Tällöin informaatioylivoiman omaavalla on luotettavampaa, tarkempaa ja oikea-aikaisempaa tietoa. Informaatioylivoiman haltijalla on käytettävissä hyvät tiedon saamis- ja hyödyntämismahdollisuudet, ajankohtainen ja tarkka tilannekuva sekä operatiivinen toimintavapaus operaatioalueella. (Puttonen 2015, 16.)

2020-luvun kybermaailman suurimmat taistelut käydään ihmisten mielissä. Strategisessa kommunikaatiossa ei-kineettisten operaatioiden avulla tavoitellaan sodan voittamista käyttäen mahdollisimman vähän kineettistä voimaa. Strategisesta kommunikaatiosta on tullut valtioille toimintatapa, jolla se pyrkii luomaan kansallista turvallisuutta ja kansakunnan yhtenäisyyttä sekä vahvistamaan tarvittavia uhkakuvia kansalaisten ja sotilaiden mielissä. Strategisen kommunikaation paradigmassa koko maailma on kybertaistelutila, jossa informaatiota on vaikea hallita. Sosiaalisen median eri muodot ulottuvat taistelukentälle ja se haastaa valtiollisen kontrollin.

Strategisen kommunikaation paradigma ei hylkää kineettisten suorituskykyjen suunnittelua, kehittämistä, rakentamista ja käyttöä, mutta niiden ensisijaisuus asetetaan kyseenalaiseksi. Siinä missä kineettisten suorituskykyjen käyttö on näkyvää, niin strateginen kommunikaatio on näkymättömämpää ja se halutaankin verhota esimerkiksi patriotismin ja kansallisten etujen suojaamisen taakse.

Kyberajan informaatio-operaatiot kohdistuvat tietoon/informaatioon. Informaatio-operaatiossa on tarkoitus vaikuttaa siihen, miten ihmiset ajattelevat ja toimivat. Tällöin keinoina voivat olla myös suorat taktiset toimet, joilla pyritään vaikuttamaan tai tuhoamaan vastustajan kyky välittää omaa viestiään. Käytännössä informaatio-operaatiossa voidaan esimerkiksi väärentää tietoa tai estää vihollisen tiedonsiirto. Sotilaalliset informaatio-operaatiot vahvistavat ja tukevat joukkojen operaatiokykyä. Informaatio-operaatioita ovat operaatioturvallisuus, harhauttaminen, psykologiset operaatiot ja viestintä. Operaatiot sovitetaan yhteen muiden ei-kineettisten operaatioiden ja kineettisten operaatioiden kanssa.

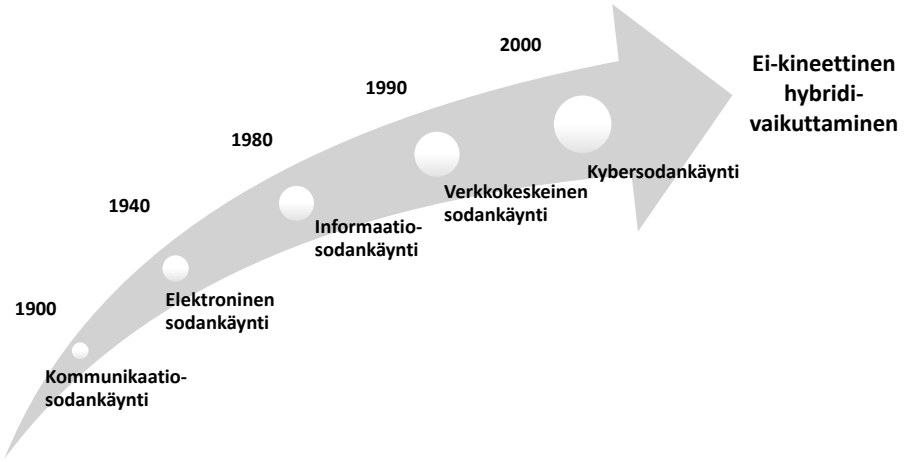
Operaatioturvallisuudessa keskitytään kriittisen tiedon tunnistamiseen, informaatiouhkien arvioimiseen, haavoittuvuuksien analysoimiseen, riskien arvioimiseen ja sopivien operaatioturvallisuustoimien valintaan ja toteuttamiseen. Operaatioturvallisuudella tarkoitetaan informaatioita, joita pyritään pitämään salassa vastustajan tiedustelulta, jotta operaation tavoitteita ja toimintaa voidaan suojella. Näitä ovat mm. paikkatiedot, kokoonpanot, kaluston ja joukkojen lukumäärät, joukkojen tehtävät sekä toimintatavat ja taktiikka. (Puttonen 2015, 21.)

Psykologiset operaatiot (PSYOPS) tukevat sekä kansallista että puolustusvoimien strategista kommunikaatiota. PSYOPS:lla pyritään ensisijaisesti vaikuttamaan vastustajan/kohdeyleisön identiteettirakenteisiin, tahtoon, tilannetietoisuuteen, toimintakykyyn ja henkiseen kriisinkestävyyteen. Keino valikoimaan kuuluu perinteistä propagandaa, disinformaation levittämistä, yksittäisten henkilöiden uhkailua, painostamista ja mustamaalaamista sekä vaikuttamista sosiaalisessa mediassa. Tällaisia toimia suunnitellaan yleensä kauan. Tavoitteena on vaikuttaa kohteen tai kohderyhmän identiteettirakenteisiin (eli käsitykseen omasta itsestä), asenteisiin ja käyttäytymiseen. Näitä operaatioita toteutetaan niin rauhan kuin kriisin aikana. (Sirén 2011, 199–207.)

Informaatio-operaatioiden avulla vahvistetaan kansallisia sodankäynnin päämääriä, puolustusvoimien toimintakykyä komentajatasolta aina yksittäisiin taistelijoihin saakka. Tavoitteena on erityisesti suojata omat kriittiset informaatiotoiminnot.

Verkkokeskeinen sodankäynti

Yhdysvaltalaisessa diskurssissa tuli 1990-luvun lopulla käyttöön käsite verkkokeskeinen sodankäynti (Network Centric Warfare, NCW), jossa informaation rinnalle nostettiin verkosto. NCW-konsepti tuli julkisuuteen vuonna 1998 US Naval Instituten julkaisussa "Network-Centric Warfare: Its Origin and Future". Sen olivat laatineet vara-amiraali Arthur K. Cebrowski ja John Gartska. Heidän



Kuva 1. Ei-kineettisen sodankäynnin evoluutio 1900-luvulta lähtien.

mukaansa ”melkein 200 vuoden ajan välineet ja sodankäynnin taktiikka ovat kehittyneet sotilaallisten teknologioiden kanssa. Nyt perustavanlaatuiset muutokset vaikuttavat sodan luonteeseen”. (Cebrowski & Garstka 1998, 28.)

Yhdysvaltalainen termi verkostokeskeinen sodankäynti ja brittiläinen vastine verkostoavusteinen puolustus (Network Enabled Defence, NED) viittaavat samaan käsitteeseen. Kyseessä on verkottuneesti toimivan yhteiskunnan kaikkien voimavarojen hyödyntäminen sotilaallisiin tarkoituksiin. Eron ajattelussa tekee suhtautuminen verkoston asemaan – onko verkosto määräävässä asemassa vai verkostomaisena alustana eri järjestelmille. (Iivonen 2009, 20.)

Verkkokeskeinen sodankäynti nähtiin informaatioajan sodankäyntiteoriana ja toimintakonseptina. Laajasti käsittäen NCW kuvasi strategioiden, operaatiotaidon ja taktiikan, teknologian, toimintatapamallien ja organisaatioiden kombinaatioita, joiden avulla verkottunut asevoima saattoi tuottaa ylivoimaa taistelukentällä. NCW:n ydinajatus oli taisteluvoiman kasvattaminen yhdistämällä sensorit, päätöksentekijät ja asealustat, jotta voidaan saavuttaa yhteinen tilannetietoisuus, kasvattaa johtamisen nopeutta ja operaationopeutta, kasvattaa kineettisen voimankäytön vaikuttavuutta, lisätä joukkojen selviytymiskykyisyyttä ja itse-organisoitumista. (Office of Force Transformation 2005, 3–5; Alberts ym. 2000, 2; Garstka 2003, 58.)

Verkostokeskeisyys sodankäynnissä tarkoitti siirtymistä tietokoneiden laskentaintensiivisestä mallista verkostointensiiviseen malliin. Tässä mallissa Antoine Bousquet yhdistää kompleksisuuden ja kaoottisuuden muodostaen

monimutkaisen kaaosmallin (chaoplexity). Tämän mallin kehityssuuntia ovat olleet verkkokeskeinen sodankäynti ja sen monet muunnelmat, kuten verkostopuolustus. Verkostopuolustukseen teoreettiseen viitekehykseen liittyvät mm. itseorganisoituminen, itsesynkronisoituminen ja parveilu. (Bousquet 2009, 233–234.)

Hybridisodankäynti

2000-luvun asymmetrinen sodankäynti on luonut uuden asetelman, jossa raja perinteisen ja epätavanomaisen sodankäynnin välillä on hämärtynyt, tai paremminkin sitä on pyritty tietoisesti hämärtämään. Hybridisodankäynti-käsite on hankala, koska hybridisodankäynnissä toimitaan sodan ala- ja ulkopuolella. Sodankäynti sodan ulkopuolella on vaikeasti määriteltävissä, koska kansainvälinen oikeus ei määrittele tämän tyyppistä tilannetta. Toiminta perinteisin sodankäyntikäsittein sodan ja osittain fyysisen maailman ulkopuolella virtuaalisessa kybermaailmassa on haasteellista.

Hybridisodankäynti voidaan määritellä valtiolliseksi tai ei-valtiolliseksi toiminnaksi, jossa käytetään useita sodankäynnin muotoja kuten tavanomaista asevoimaa, epätavanomaista taktiikkaa ja rikollista toimintaa (Lalu & Puistola, 2015). Hybridivaikuttamisella puolestaan ymmärretään suunnitelmallista toimintaa, jossa valtiollinen tai ei-valtiollinen toimija voi hyödyntää samanaikaisesti erilaisia keinoja vaikuttaakseen kohteena olevan valtion heikkouksiin ja saavuttaakseen omat tavoitteensa (Hallituksen esitys eduskunnalle laiksi Euroopan hybridiuhkien torjunnan osaamiskeskuksesta, 2017). Määritelmiä on toki muitakin. Oleellista on huomioida sodan kynnyksen ala- ja ulkopuolella toimiminen, ja hybridi-termin hyödyllisyys viitekehyksenä nykypäivän uhkien ja niiltä puolustautumisen moniulotteiseen tarkasteluun ja varautumiseen.

Hybridisodankäynnistä on esimerkkejä, jossa kineettistä sodankäyntiä on jatkettu matalan intensiteetin kineettisten ja ei-kineettisten operaatioiden avulla. Venäjän sotatoimet Ukrainassa vuonna 2014 ovat esimerkki sodankäynnistä, jossa erikoisjoukkojen rajoitetun voimankäytön, poliittisen, sotilaallisen ja taloudellisen painostuksen, strategisen kommunikaation sekä erilaisten ei-kineettisten operaatioiden avulla on luotu epävakaa Itä-Ukrainan alue, jota Venäjä hallitsee. (Geers, 2015.)

Kybertaistelutila ja miehittämättömyys ovat alentaneet sodankäynnin kynnystä samalla muuttaen perinteistä sota-rauha -asetelmaa. Tähän liitettiin kylmän sodan aikana käsite harmaasta vaiheesta, jolla ymmärrettiin aikaa ennen varsinaista sotaa. Hybridisodankäynti on tuonut tilan, joka voi edeltää perinteistä sotaa, ilmetä sodan aktiivisen vaiheen jälkeen tai ilman perinteistä sodankäyntiä. Uusi sodankäynnin paradigma on syrjäyttämässä perinteisen mallin

sodan julistamisesta rauhan sopimukseen luomalla tilan, jossa sotaa ei julista eikä rauhaa solmita vaan hybridisodankäynnin kohde joutuu elämään hyvinkin pitkään konfliktin ja epävakauden keskellä, jossa yhä enenevässä määrin kybertoimintaympäristö on toiminnan kohteena.

2020-luvun sodankäyntiin sekoittuu uusia elementtejä erityisesti kybertoimintaympäristössä tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Pitämällä tarkoituksellisesti yllä epävakautta ei-kineettisten operaatioiden avulla erityisesti suurvalta voi perustella läsnäoloaan ja vaikuttamista tietyllä alueella. Toimintaa perustellaan rauhanturvaamisella, tasapainon säilyttämisellä, omien etujen ja kansalaisten suojaamisella tai liittolaisten tukemisella, kaikella näennäisesti hyväksyttävällä toiminnalla. Kybertoimintaympäristö on luonut uuden tilan vaikuttaa toisen valtion alueella käyttäen hyväksi erilaisia sotilaallisia ja ei-sotilaallisia painostuskeinoja poliittisten ja sotilaallisten tavoitteiden saavuttamiseksi. Kybertoimintaympäristön hyväksi käyttäminen soveltuu hyvin hybridisodankäyntiin ja sen eri muotoihin.

Kybersodankäynti ja kansallinen turvallisuus

”Suomen puolustaminen edellyttää kykyä toimia maa-, meri-, ilma- ja kybertoimintaympäristöissä.” (Valtioneuvoston kanslia 2017, 10.)

Kyberturvallisuuden tekninen luonne on kehittynyt nopeasti strategiseksi käsitteeksi. Strategian ”yläpuolella” on puolestaan politiikka. Kyberympäristön merkityksen kasvu on johtanut lisääntyvään tarpeeseen ymmärtää kyberympäristö nimenomaan poliittisena ympäristönä. Politiikalla sekä luodaan kyberympäristön tulevaisuutta että pyritään kyberympäristössä edistämään poliittisia tavoitteita (Limnéll 2016, 50–60). Kybertoimintaympäristö voidaan jakaa toiminnan ja päätöksenteon näkökulmista viiteen eri tasoon, jotka ovat vuorovaikutuksessa toisiinsa (ks. Kuva 2 seuraavalla sivulla). Kyberympäristön sekä kybersodankäynnin nykytilaa ja tulevaisuutta pohdittaessa nämä kaikki tasot on otettava huomioon.

Kybervoiman ja -kyvykkyyksien kasvattaminen

Globalisaatio ja internet ovat antaneet yksilöille, organisaatioille ja valtioille uusia mahdollisuuksia toimia digitalisoituvassa maailmassa. Vastaavasti niin tämän päivän kuin tulevaisuuden poliittisissa ja sotilaallisissa konflikteissa on mukana kyberelementti, jonka tarkkaa vaikuttavuutta poliittisten tavoitteiden saavuttamisessa on vaikea ennustaa. Tulevaisuudessa kybertaisteluista voi tulla merkittävimpiä kuin taisteluista fyysisessä maailmassa. Useat reaalimaailman

Kuva 2. Kyberympäristön viisi toiminnan tasoa.

esimerkit Yhdysvalloista Venäjään ja Lähi-Idästä Kaukoitään osoittavat, että internetin ja digitalisaation globaali ulottuvuus ja haavoittuvuus aiheuttavat konkreettisia poliittisia ja sotilaallisia vaikutuksia. Digitalisaation vahvistuessa ja riippuvuuden kasvaessa kyberhyökkäyksistä saattaa kehittyä keskeinen tekijä tulevissa konflikteissa ja sodankäynnissä. Toisaalta kyse on teknologian kehityksen vaikutuksista laajemmin niin sodankäyntiin kuin (esimerkiksi tekoälyn kehittyessä) jopa ihmisyyden tulevaisuuteen.

Kybertaistelukentällä toimijan koolla ei ole samanlaista merkitystä kuin fyysisessä maailmassa – sekä suuret että pienet voivat olla tehokkaita. Siitä, miten ”kybervoima” (cyber power eli kyberkyvykkyydet valtaelementtinä) tulee maailmassa jakaantumaan niin eri valtiollisten kuin ei-valtiollisten toimijoiden kesken, on esitetty erilaisia arvioita (ks. mm. Koch & Rodosek 2016). Suurilla mailla on mahdollisuus hyödyntää teknologiaa laaja-alaisesti, kun taas pienet maat voivat käyttää hyväkseen esimerkiksi järjestelmähaavoittuvuuksia. Lisäksi digitaalisista toiminnoista riippuvaiset maat ovat hyökkääjille houkutteleva kohde, koska niiden kriittisen infrastruktuurin lamautuminen aiheuttaa merkittävää vahinkoa yhteiskunnan elintärkeille toiminnoille. Kybersodankäynnissä etäisyys on merkityksetön, koska kaikki toimivat samassa globaalissa kyberympäristössä. Laitteistot, ohjelmistot ja palvelut muodostavat kybermaailman maiseman – eivät vuoret, laaksot tai vesitiet, jotka kuvaavat fyysistä taistelukenttää. Kyberaseet eivät perustu kineettiseen voimaan vaan älykkyyteen ja innovatiivisuuteen. Kybertaistelun voittaa se, joka käyttää huipputeknologiaa älykkäämmin ja tehokkaammin (Geers 2001, 10). Innovatiivisuus on

kybersodankäynnissä imperatiivi – niin hyökkääjälle kuin puolustajalle.

Useat valtiot kasvattavat maa-, meri- ja ilmavoimiensa rinnalle kybervoimaa ja siihen yhdistyviä kyvykkyyksiä. Maailmassa on parhaillaan käynnissä kyberasevarustelukilpa ja sen arvioidaan kiihtyvän (IISS 2016, 13). Kyberkyvykkyyksiä ja niiden käyttöä määritellään eri tavoin, joten yhtenäistä viitekehystä vertailua varten on vaikea löytää.

Joseph Nye on todennut, että kybervoima "*is the ability to obtain preferred outcomes through use of electronically interconnected information resources of the cyber domain*" (Nye 2010, 4). Kybersodankäynnissä siis käytetään kybertoimintaympäristön menetelmiä, mutta tavoitellaan lopputuloksia, jotka ovat vastaavia maa-, meri- ja ilmavoiman kanssa (Chen & Dinerman 2016). Oleellista on ymmärtää, että kybervoimalla voidaan vaikuttaa sekä kyber- että fyysiseen ympäristöön, ja että kybertoimilla voidaan edistää nimenomaan strategisia ja poliittisia tavoitteita.

Kybersodankäynti yhtenä sodankäynnin muotona

Kybersodankäyntikäsitteelle ei ole yleisesti hyväksyttyä määritelmää ja sitä käytetään hyvinkin laajasti kuvaamaan erilaisia kyberympäristön tapahtumia ja toimia. Kybersodankäynnin käsite nousi voimakkaasti esille vuosina 2008–2010. Se syrjäytti osin aikaisemmin käytetyn informaatiosodankäynnin käsitteen, joka oli muotoiltu 1990-luvun puolivälissä. Toisille kybersodankäynti on sotaa digitaalisessa maailmassa, toisille se on vastakohta kineettiselle sodankäynnille. Tutkijoiden mukaan kybersodankäynnin määrittelyn tulisi perustua sodan tavoitteisiin ja motiiveihin, ei niinkään kyberoperaatioiden muotoihin. Sota on aina laaja-alainen kokonaisuus käsittäen kaikki sodankäynnin muodot. Kybersodankäynti on yksi sodankäynnin muoto, jota käytetään perinteisen kineettisen vaikuttamisen rinnalla.

Chen ja Dinerman (2016) ovat tutkimuksessaan käsitelleet eroja konventionaalisen sodankäynnin ja kybersodankäynnin välillä (ks. Taulukko 1 seuraavalla sivulla).

Kybersodankäynnissä kohteina ovat tavallisesti tietojärjestelmät ja/tai tieto, joka sisältyy näihin järjestelmiin. Kyberhyökkäyksen kustannukset ovat suhteellisesti halvempia kuin tavanomaisen sodankäynnin kustannukset. Luonteenomaista kybersodankäynnille on, että useimmiten kyberhyökkäyksessä on vaikeaa tunnistaa todellisia hyökkääjiä ja siten soveltaa voimankäyttövaltuuksia. Kyberhyökkäykset saattavat tuottaa väärän vaikutelman siitä, ettei kysymys ole vakavasta tapahtumasta, koska ihmishenkiä ei välttämättä menetetä. Hyökkäykset yhteiskunnan kriittistä infrastruktuuria vastaan saattavat kuitenkin aiheuttaa aineellisten tappioiden lisäksi myös ihmishenkien menetyksiä.

Taulukko 1. Konventionaalisen sodankäynnin ja kybersodankäynnin eroja.

	Konventionaalinen sodankäynti	**Kybersodankäynti**
Sodankäynnin tarkoitus (miksi)	Saada maantieteelliseen paikkaan sidottu poliittinen, taloudellinen, ideologinen, yhteiskunnallinen, uskonnollinen valta-asema pysyvästi tai määrätyksi ajaksi	Auttaa saamaan poliittinen, taloudellinen, ideologinen, yhteiskunnallinen, uskonnollinen valta-asema pysyvästi tai määrätyksi ajaksi; informaatioylivoiman saavuttaminen
Strategia (miten)	Käyttäen avoimia ja/tai salaisia operaatioita; vähäinen tarve salata toimijuus pl. salaiset operaatiot	Käyttäen avoimia ja/tai salaisia operaatioita; suuri mahdollisuus tarvittaessa salata toimijuus
Toimijat (kuka)	Sotilaalliset tai puolisotilaalliset joukot	Jokainen, jolla laitteet ja kyberaseet sekä pääsy verkkoon
Kohteet (mikä)	Vaikuttaminen ihmiseen ja ihmiselämään	Vaikuttaminen informaatioon ja informaatiojärjestelmiin ja epäsuorasti ihmiselämään
Toimintaympäristö	Rajallinen maatieteellinen toimintaympäristö	Globaali toimintaympäristö ja liityntä kyber-fyysiseen maailmaan
Kesto	Rajallinen aika	Jatkuvaa toimintaa, jossa lyhyitä aktiivisia hyökkäysjaksoja
Valmistautumisaika	Suhteellisen pitkä aika	Suhteellisen lyhyt aika
Kustannukset	Korkeat kustannukset	Suhteellisen alhaiset kustannukset
Piirteet	Suhteellisen läpinäkyvä	Suhteellisen näkymätön
Toimijan identifiointi	Suhteellisen helppo selvittää	Vaikeasti selvitettävissä
Voimankäyttösäännöt (RoE)	Suhteellisen selkeät (sodan oikeussäännöt)	Epäselvät
Vaikutus kohteessa	Laajoja materiaalisia tuhoja ja ihmishenkien menetyksiä; kohdistuu alueellisesti rajattuihin kohteisiin	Vähäisiä materiaalisia tuhoja, laajoja informaation menetyksiä, YET-lamautumista ja epäsuorasti ihmishenkien menetyksiä; kohdistuu kaikkiin verkon toimijoihin
Pelote	Ilmeinen ja vaikuttava	Epämääräinen
Dominanssi	Saavutettavissa	Vaikeasti saavutettavissa
Tuloksen näkyvyys	Ilmeinen	Epämääräinen
Voittaja	Helposti identifioitavissa	Vaikeasti määriteltävissä
Jälleenrakennus	Vaativaa, vaatii resursseja ja aikaa	Suhteellisen lyhyt aika ja vähän resursseja

Esimerkiksi laajamittaisella datamanipulaatiolla voi olla merkittäviä vaikutuksia yhteiskuntajärjestykseen kuin myös fyysisen voiman käyttöön vastatoimina (Limnéll & Salonius-Pasternak 2016).

Kyberajattelun myötä informaatioympäristön keskiössä olevan informaation rinnalle on haluttu tuoda kriittinen infrastruktuuri sekä sodankäynnin johtamis- ja toimeenpanoprosessit. Lisäksi kyberajattelussa on esitetty uudelleen ajatus totaalisesta sodasta, jossa vaikuttamisen kohteena ei ole vain sotilaallinen toimintaympäristö vaan koko yhteiskunta ja sen rakenteet. Erilaiset tietojärjestelmien ja -liikenteen verkostot ovat levittäytyneet kaikille elämän alueille. Yhteiskunnan kaikki elintärkeät toiminnat ovat tietoyhteiskunnissa verkottuneita. (Lehto 2014, 164.)

Samalla kun huomiota on yhä enemmän kiinnitetty haittaohjelmien havaitsemiseen ja torjuntaan sekä ohjelmistohaavoittuvuuksien löytymiseen ja korjaamiseen, hyökkäykset ovat siirtyneet laitteiden komponenttitasolle. Tällaisia hyökkäysvektoreita on erilaisia, kuten haittaohjelman asentaminen laitteen installointivaiheessa, toimintalogiikkaa muuttavan osan asentaminen laitteeseen sen varastointivaiheessa, hyökkäyksen kohdistaminen laitteen kehittämisprosessiin jo laboratoriovaiheessa tai haittaohjelman asentaminen mikropiireihin niiden valmistusvaiheessa.

Lähitulevaisuudessa korostuu kyberfyysinen toimintaympäristö, jossa kyberoperaatiot kohdistuvat sekä virtuaaliseen maailmaan että fyysiseen laiteympäristöön. Tämä korostaa valvonnan, hallinnan ja tilannetietoisuuden rakentamista aina laitteiden ja ohjelmistojen suunnittelu- ja laboratoriovaiheesta niiden tuotantovaiheeseen, implementaatio- ja käyttöönottovaiheeseen sekä itse järjestelmien käyttöön.

Kybertiedustelun suorituskyvyllä tuotetaan tietoa kybertoimintaympäristön toimijoiden järjestelmien ja verkkojen kokoonpanoista ja haavoittuvuuksista sekä arviota toimijoiden kyvyistä toteuttaa tietoverkko-operaatioita. Kybertiedustelun tavoitteena on luoda suojautumisen ja vaikuttamisen edellyttämä tilannetietoisuus, uhkavaroitus ja maalinosoitus.

Kybersuojautumisen suorituskyvyllä estetään, rajataan ja lievennetään hyökkääjän eri järjestelmiin ja verkkoihin toteuttamien kyberoperaatioiden vaikutuksia. Kybersuojaaminen käsittää sellaisia tietoverkoissa tapahtuvia toimia kuten havainnointi, valvonta, analysointi ja vastatoimenpiteiden toteuttaminen verkkohyökkäyksiä, tunkeutumisia ja muita luvattomia toimia sekä häiriöitä vastaan. Suojautumisen tavoitteena on kyky suojata oma tieto sekä johtamis- ja tietojärjestelmät säilyttäen riittävä operaatioiden johtamiskyky.

Puolustusvoimien tulee ensisijaisesti suojata omat järjestelmänsä ja verkkonsa. Suojaamiskyky tulee mitoittaa sellaiseksi, että se mahdollisimman tehokkaasti tukee Puolustusvoimien toimintaa alueellisen koskemattomuuden

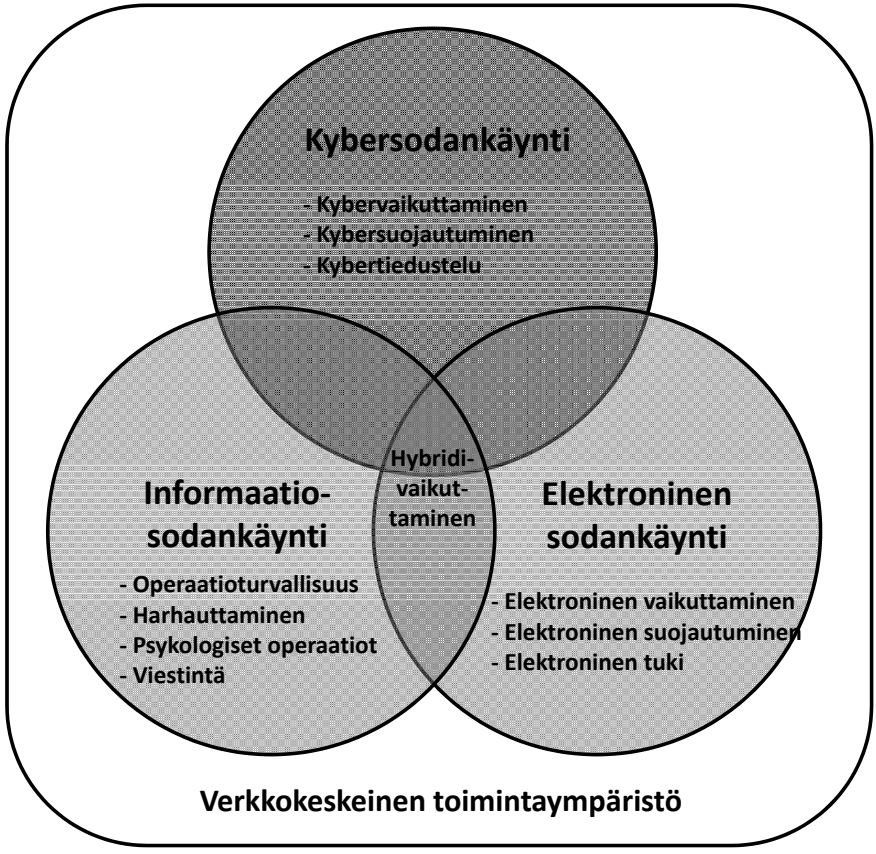
turvaamiseksi ja maan puolustamiseksi. Suojaamisen kehittämisessä korostuu yhteistoiminta Puolustusvoimien, muiden viranomaisten sekä yhteiskunnan muiden kybertoimintaympäristön toimijoiden kanssa.

Kybervaikuttamisen suorituskyvyllä vaikutetaan vastustajan toimintaan kohdistamalla toimenpiteitä sen järjestelmiin ja verkkoihin niiden haavoittuvuuksia hyödyntäen. Vaikuttamisen tavoitteena on vastustajan tietojärjestelmien, tietoverkon ja sen laitteiden toiminnan häiritseminen, tietoverkon tai sen sisältämän tiedon käytön rajoittaminen, käytettävyyden heikentäminen tai tuhoaminen sekä kyberylivoiman saavuttaminen kybertilassa.

Kybervaikuttamisen kehittämisessä korostuu systeeminen ajattelu. Kybermaalien valinnassa niitä tulee tarkastella systeemin osina, jolloin saadaan aikaan suoraa ja epäsuoraa vaikutusta. Maalien valinnassa on järkevää valita sellaisia, jotka nopeimmin, pitkävaikutteisimmin ja tehokkaimmin aikaansaavat systeemimuutoksen. Sotilaalliset operaatiot edellyttävät tarkkaa analysointia, joiden kohteina ovat vastustajan painopisteet, kriittiset rakenteet ja elintärkeät toiminnat ja niiden haavoittuvuudet. Vain tällaista kokonaisvaltaista lähestymistapaa käyttämällä voidaan strategiset tavoitteet saavuttaa kineettisillä ja ei-kineettisillä operaatioilla. Esimerkiksi liittouman hyökkäyksessä Bagdadiin vuonna 1991 ilmahyökkäyksellä tuhottiin vain 10% sähköverkosta, mutta aiheutettiin strateginen lamautus koko kaupungissa. Nyt tällainen strateginen lamautus on mahdollinen kyberhyökkäyksen avulla. Muutos saadaan tehokkaimmin toteutettua, kun toteutetaan kineettisiä ja ei-kineettisiä rinnakkaisoperaatioita kaikissa taistelutilan ulottuvuuksissa. Jokaista ulottuvuutta vastaan voidaan hyökätä suorasti tai epäsuorasti, ja paras toimintamalli riippuu kulloisestakin tilanteesta. Strategisessa ajattelussa tulee huomio kohdistaa systeemivaikutuksiin eikä yksittäisiin maaleihin.

Kuvassa 3 esitetään verkkokeskeinen toimintaympäristö, jossa eri ei-kineettiset sodankäyntimuodot muodostavat verkkokeskeisen kokonaisuuden osana hybridivaikuttamista.

Informaatiosodankäynnin, elektronisen sodankäynnin ja kybersodankäynnin operaatiot muodostavat toisiaan täydentävän monikerroksisen ei-kineettisen operaatiokokonaisuuden osana hybridivaikuttamista, mikä edellyttää eri osa-alueiden saumatonta yhteistoimintaa. Näiden sodankäyntimuotojen tarkkarajainen määrittely on vaikeaa, kun kullakin niistä on oma kehitysprosessinsa mukainen historia. Oleellisinta on ymmärtää kybertaistelukentän eri elementtien luonne, keskinäisriippuvuus ja vaikutus yhteiskunnan kokonaisturvallisuuteen ja elintärkeisiin toimintoihin.



Kuva 3. Kybersodankäynnin, informaatiosodankäynnin ja elektronisen sodankäynnin operaatiot toimivat osana hybridivaikuttamista verkottuneessa toimintaympäristössä.

Kybertilannekuvasta kyberomavaraisuuteen

Kybermaailman sotilaallinen ulottuvuus 2020-luvulla koostuu monista tekijöistä: kybertilannekuva, kyberoperaatiot, erilaisten kybertoimijoiden roolit, kyberpolitiikka ja -diplomatia, kyberpelote, kybersuorituskykyjen kehittäminen, yhteiskunnan elintärkeät toiminnat ja kyberomavaraisuus. Seuraavaksi luomme katsauksen näihin tekijöihin.

Kybertilannekuva

Sotilaallista kybertilannetietoisuutta rakennetaan tällä hetkellä hyvin aktiivisesti. 2010-luvulla monissa valtioissa on perustettu kyberturvallisuuskeskuksia vastaamaan kansallisesta kybertilannekuvasta ja koordinoimaan kyberturvallisuustoimenpiteitä. Samalla on luotu asevoimien kyberpuolustuskeskuksia, joiden tehtävänä on sotilaallisen kybertilannekuvan muodostaminen ja sotilaallisten kyberoperaatioiden sekä toteuttaminen että johtaminen. Kybersodankäynnin asema puolustushaarana, aselajina tai operaatiokonseptina vaihtelee maittain, mutta kybersodankäynnin kyvykkyyksiä kehitetään parhaillaan aktiivisesti perinteisten kineettisten suorituskykyjen rinnalla. Tavoitteena on ylivoiman saavuttaminen kybertaistelutilassa.

Reaaliaikaisen tilannekuvan muodostamisen ja jaetun tilannetietoisuuden aikaansaamisen tulee olla yhä nopeampaa. Myös tilannekuvan luotettavuuden merkitys korostuu. Johtamisprosessissa tarvitaan sisällöltään mahdollisimman tarkkaa ja oikein aikautettua informaatiota, jotta keskitetty johtaminen ja hajautettu toiminta voidaan toteuttaa sekä suojata oma toiminta kybertaistelutilassa. Resurssien käytön perusteiden pitää syntyä vastustajaa nopeammassa päätösprosessissa tilannekuvaa ja vastustajan toimintatapoja, tavoitteita ja kyvykkyyttä analysoimalla. Tilannetietoisuuden kehittäminen edellyttää tehokasta havainnointikykyä. Niinpä asevoimat tarvitsevat oikeudet tietoverkkotiedusteluun, jotta ne voivat turvata kybertiedustelun ja -valvonnan suorituskyvyn kehittämisen sekä varmistaa ennakkovaroituksen.

Kyberoperaatiot

Kyberoperaatiot muodostavat kokonaisuuden, jolla horjutetaan vastustajan kybertoimintaympäristön tieto- ja informaatioperusteisia järjestelmiä sekä eri toimijoiden tilannetietoisuuden muodostumista. Samalla suojataan omia järjestelmiä sekä defensiivisin että offensiivisin keinoin. Kybersodankäynnissä kyberoperaatiot eivät ole kokonaan itsenäisiä, muusta sodankäynnistä erillään olevia operaatioita, vaan kiinteä osa kokonaisoperaatioita.

Kyberoperaatioissa korostuu vaatimus toiminnan nopeudesta ja laajuudesta. Puolustajan järjestelmät ovat alttiita kyberhyökkäyksille asevoimien koko taistelutilan laajuudessa. Kybersodankäynnissä ei ole rintamalinjoja vaan sodankäynti tapahtuu kaikkialla kybertilassa. Kyberhyökkäykset ja hyökkäysvektoreiden muutokset ovat hyvin nopeita. Sodankäynnissä on siirrytty päivä- ja tuntiluokasta minuutteihin ja sekunteihin.

Useat valtiot kehittävät kykyään suorittaa operaatioita kyberavaruudessa maan, meren, ilman ja avaruuden lisäksi osana sotilaallista voimankäyttöä.

Suorituskyky perustuu tiedusteluun ja vaikuttamiseen. Tiedustelulla pyritään selvittämään kohteen järjestelmien ja verkkojen kokoonpanoa ja haavoittuvuuksia sekä vastapuolen kykyä suorittaa kyberoperaatioita. Vaikuttamisen tavoitteena on saada aikaa haluttu poliittinen ja/tai sotilaallinen vaikutus vastapuolen järjestelmien ja verkkojen kautta.

Kyberoperaatiot voidaan jakaa hyökkäyksellisiin toimiin (kybervaikuttaminen), puolustuksellisiin toimiin (kybersuojautuminen) ja tiedusteluun (kybertiedustelu) kybertoimintaympäristön eri rakenteissa. Kyberoperaatioita voidaan toteuttaa kolmella tasolla: strateginen, operatiivinen ja taktinen. Lisäksi kyberoperaatioita toteutetaan sotaa alemmissa konflikteissa osana sotilaallista, poliittista ja taloudellista painostusta. Kybersodassa kohteina voivat olla yhteiskunnan kriittinen infrastruktuuri, kansalaisten käyttämät palvelut sekä viranomaisten järjestelmät ja verkot.

Kybersodankäynnin strategisen tason kyberoperaatioissa valtio pyrkii vaikuttamaan toisen valtion toimintaan sekä toimintakykyyn. Operatiivisella ja taktisella tasolla kyberoperaatioita suoritetaan osana muuta sotilaallista voimankäyttöä. Tavoitteena voi esimerkiksi olla sotilaallisen johtamisen häiritseminen, lamauttaminen tai harhauttaminen tai sotilaallisen voimankäytön estäminen tai viivästyttäminen.

Kybersodan operatiivisella ja taktisella tasolla kysymys on kyberoperaatioista osana yhteisoperaatioita, joissa toimenpiteet kohdistuvat ensisijaisesti joukkojen johtamisjärjestelmiin. Näillä kyberoperaatioilla pyritään lamauttamaan vastustajan joukkojen tilannetietoisuuden muodostaminen sekä kyky tehokkaaseen joukkojen ja toiminnan johtamiseen. Sodan aikana toteutetuista kyberoperaatioista esimerkkinä voidaan pitää Venäjän ja Georgian välisessä sodassa vuonna 2008 esiintyneitä verkkohyökkäyksiä. Eri arvioiden mukaan Yhdysvallat harkitsi kyberoperaatioita Libyan operaation yhteydessä vuonna 2011. Suunnitelmissa oli lamauttaa Libyan ilmatorjunnan tietoverkot ja siten turvata sen omat ilmaoperaatiot.

Sotaa alempitasoisemman konfliktin yhteydessä valtiollinen toimija tai tämän tukema ja/tai suojaama ryhmittymä voi kohdistaa kyberhyökkäyksiä toista valtiota vastaan ilman, että valtiot ovat sodassa keskenään. Näille hyökkäyksille on tavanomaista, että tekijät pyrkivät pysymään tuntemattomina ja että valtiot kykenevät kiistämään osallisuutensa niihin. Näkyvin tällainen operaatio tapahtui keväältä 2007, kun Viroon kohdistui verkkohyökkäysten sarja, jonka kohteina olivat kolmen viikon ajan mm. valtiojohto, poliisi, pankkilaitos, media ja yritysmaailma. Päätoimintamuotoina olivat palvelunestohyökkäykset.

Kyberhyökkäysten vaikuttavuus nousi uudelle tasolle, kun vuonna 2010 paljastui Iranin ydinlaitoksiin kohdistunut hyökkäys, jossa Stuxnet-haittaohjelma vaurioitti uraanin rikastamiseen tarkoitettuja sentrifugeja. Iranin epäillään

vastatoimenpiteenään perustaneen kybersodankäynnin yksikkönsä vuonna 2010 ja tehneen hyökkäyksiä ainakin Yhdysvaltoja ja Iso-Britanniaa vastaan.

Etelä- ja Pohjois-Korea syyttävät toisiaan jatkuvista kyberiskuista, joita ovat olleet mm. pankkien hakkerointi ja palvelunestohyökkäykset. Israelin sekä Palestiinan ja sitä tukevien maiden välillä on jatkuva pienimuotoinen kyberkonflikti, jossa eri hyökkäysmuodoin pyritään häiritsemään valtion hallintorakenteita, asevoimia sekä pankki- ja teollisuussektorin toimintaa.

Kybersotaan pätevät sodankäynnin yleiset periaatteet. Kyberoperaatioita ei toteuteta satunnaisesti, vaan niitä edeltää tilannekuvan muodostaminen tiedustelun ja vakoilun avulla sekä maalien analysointi ja valinta. (Filiol 2009, 71–79.)

Kyberhyökkäysten kohteena eivät ole vain asevoimat vaan yhteiskunnan elintärkeät toiminnat. Yhteiskunnan elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja siksi kybertoimintaympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Näin kansallisesta kyberpuolustuksesta muodostuu kiinteä osa kokonaismaanpuolustusta.

Kyberhyökkäyksiin pyritään löytämään vielä tunnistamattomia haavoittuvuuksia, joita hyödynnetään niin rauhan kuin sodan aikana. Kriisitilanteessa hyökkääjälle kohteen haavoittuvuuden arvon tunteminen on erittäin tärkeää.[1] Tulevaisuuden sodan voi voittaa hankkimalla ylivoiman kybertoimintaympäristössä ja tässä kyberylivoiman hankinnassa auttavat ulkoistetut toimijat rauhan aikana.

Viime vuosina kyberhyökkäyksissä on havaittu yhä systemaattisempaa toimintatapaa sekä toiminnan organisointia ja johtamista (ks. Valeriano & Maness 2015). Hyökkäysmenetelmät ovat kehittyneempiä ja käytetyt kyberaseet tehokkaampia. Ennusteiden mukaan myös valtioiden kybersodankäynnin kyvykkyydet tulevat kehittymään sekä hyökkäysten laajuudessa että kehittyneisyydessä. Valtioiden tekemät kyberhyökkäykset tulevat vaikuttamaan poliittisiin suhteisiin sekä valtarakennelmiin ympäri maailmaa. Valtioiden käyttämät työkalut päätyvät ajan kuluessa myös kyberrikollisryhmien käyttöön. (Lehto ym. 2017, 22.)

Kybertoimijat

Kybermaailman (uhka)toimijoita voidaan määritellä monella tavalla. Yksi käytetyimmistä on luokitella toimijat motivaation perusteella. Kybermaailman eri tapauksia pyritään liittämään eri ryhmiin ja siten luomaan kuvaa eri toimijoista ja heidän motivaatioistaan. Erityisesti lainvalvonta- ja turvallisuusviranomai-

set ovat kiinnostuneita keräämään dataa ja tekemään luokituksia, jotta tulevia tapahtumia voidaan sekä ennakoida että selvittää paremmin. Yhdistämällä kybermaailman tapahtumia (incidents) eri kybertoimijoihin (Cyber Agents) voidaan ymmärtää kybermaailman dynamiikkaa, tekniikkaa ja erilaisia riippuvuuksia.

Euroopan unionin verkko- ja tietoturvavirasto (ENISA) on laatinut taksonomian kybertoimijoista tehden pääjaon eettisten toimijoiden ja uhkatoimijoiden välillä.

Eettisten toimijoiden kategoria muodostuu tutkijoista, eettisitä hakkereista, turvallisuushenkilöstöstä, poliisista, kybertaistelijoista, työntekijöistä ja loppukäyttäjistä/asiakkaista. Kyberuhka-agentit ENISA jakaa korkean teknologian ja osaamisen toimijoihin sekä matalan/keskitason teknologiaan ja osaamiseen.

Kyberrikolliset ovat keskeinen uhkaryhmä. ENISA:n vuoden 2015 että 2016 raporteissa tämä ryhmä on mukana vähintään 2/3 rekisteröidyistä tapauksista. Kyberrikollisten tavoitteena on taloudellinen hyöty toiminnan kohdistuessa vakoiluun ja rahan hankintaan. Ryhmällä on kasvavassa määrin osaamista, taloudellisia resursseja ja tietokonekapasiteettia. Lisäksi kyberrikolliset muodostavat hyvin toimivia ja organisoituja ryhmiä. Nämä ryhmät toimivat kaikkialla digitalouden, digitaalisen kaupankäynnin, verkkokaupan ja verkkomaksun ympäristöissä käyttäen haittaohjelmia ja lunnashyökkäyksiä sekä soveltaen kyberrikollisuus palveluna -toimintamallia (ENISA 2016; ENISA 2017.)

Vuosien 2013–2014 Edward Snowdenin paljastukset toivat **valtioiden turvallisuuspalvelut** median huomion kohteeksi. Niiden toiminnasta on saatavissa vähän varmistettua tietoa. On kuitenkin varmaa, että nämä organisaatiot kehittävät kybersuorituskykyjään tehtäviensä toteuttamiseksi sekä kybertiedustelun että kybervastatiedustelun alueilla. Kybertiedustelun tavoitteena on hankkia salaisia tietoja (sensitiivinen, yksityisoikeudellinen tai turvaluokiteltu) yksityisiltä ihmisiltä, hallituksilta ja vastustajilta poliittisen, sotilaallisen tai taloudellisen edun saavuttamiseksi käyttäen eri menetelmiä internetissä, tietoverkoissa, ohjelmistoissa tai tietokoneissa. Erityisenä kohteena ovat yhteiskunnan kriittinen infrastruktuuri ja kriittinen informaatioinfrastruktuuri. (ENISA 2016; ENISA 2017.)

Kybertaistelijoita ovat sekä asevoimiin kuuluvat kybersotilaat että patrioottiset toimijat, joita ohjaa kyky ja motivaatio toimia valtion eduksi. Nämä toimivat yksittäin tai ryhminä suorassa tai epäsuorassa valtion viranomaisten ohjauksessa. Ryhmittymät voivat toiminnassaan siirtyä kyberterroristien, aktivistien sekä kybervakoilun välimaastoon. Esimerkkinä tästä on Syrian Electronic Army. Tämän ryhmän avainhenkilöillä on tai on ollut läheiset suhteet Syyrian hallitukseen.

Tämän tyyppisellä ulkoistuksella on monia etuja. Ensiksi, mikäli hyökkääjää ei voi varmuudella identifioida, mitään valtiota tai sen virallista organisaatiota ei voi syyllistää, jolloin toiminta luetaan kyberrikollisuudeksi. Toiseksi, ulkoistettu hyökkäys ei paljasta valtion asevoimien tai turvallisuusorganisaatioiden todellista suorituskykyä. Jokainen paljastunut kybervakoiluoperaatio tai fyysisen kohteen lamauttaminen kyberhyökkäyksellä tutkitaan tarkoin. Tutkimuksella pyritään selvittämään, kuinka hyökkäykset suunniteltiin ja toteutettiin, mikä antaa kuvan hyökkääjän kybersuorituskyvyistä. Lisäksi ulkoistetut hyökkäykset antavat tietoa kohteen kyberturvallisuuden ja kyberpuolustuksen suorituskyvyistä. Osa kyberhyökkäyksistä voikin olla toteutettu suorituskyvyn testaustarkoituksessa, mihin tarkoitukseen sopivat hyvin ulkoistetut toimijat.

Kyberterrorismin määrittely on vaikeaa. Kyberterrorismissa käytetään tietoverkkoja hyökkäyksiin kriittisiä informaatiojärjestelmiä kohtaan ja niiden kontrollointiin. Hyökkäysten tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen. Kyberterrorismihyökkäyksillä halutaan vaikuttaa kansallisella ja kansainvälisellä tasolla. Kyberterroristien kohteena on yhteiskuntien kriittinen infrastruktuuri. Tämän uhka-agenttiryhmän ominaispiirre on umpimähkäinen väkivallankäyttö. Toistaiseksi kyberterrorismista ei ole tapauksia. Silti kansalliset kyberturvallisuusstrategiat kuvaavat kyberterrorismin merkittävänä uhkana ja valtiot kehittävät torjuntamekanismeja tällaisia uhkia vastaan. (ENISA 2016; ENISA 2017.)

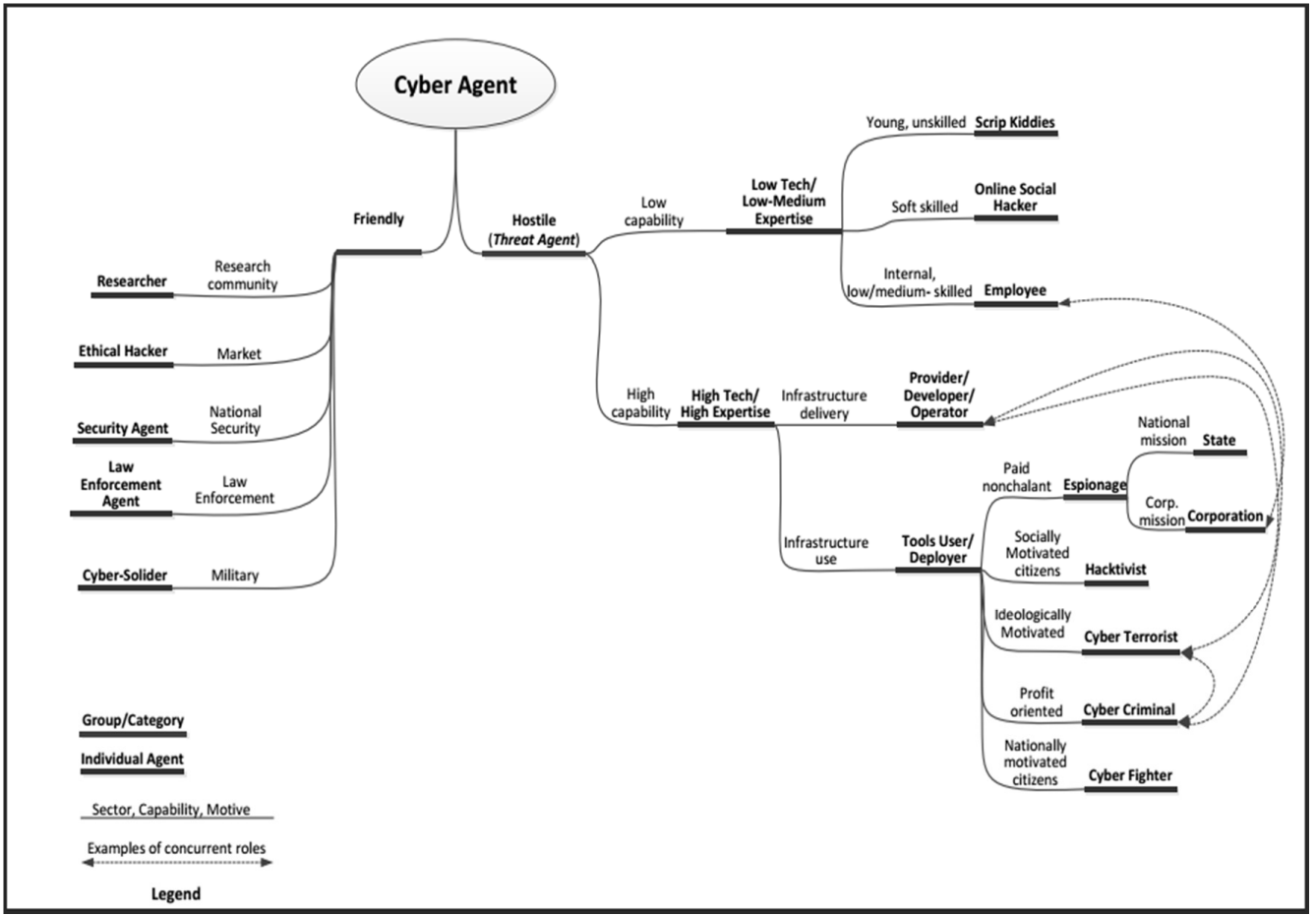
Kybersodankäynnin kannalta kyberrikolliset, kyberterroristit ja vastustajan kybersotilaat muodostavat yhteen kietoutuneen kokonaisuuden, jossa eri toimijoiden rooleja on vaikea erottaa toisistaan. Hybridivaikuttamisen kannalta hyökkääjä voi käyttää kaikkien näiden uhka-agenttien ”palveluita” hyväkseen joko suoraan tai epäsuorasti. Hybridivaikuttamiseen voidaan vielä liittää kineettistä vaikuttamista ja luoda epämääräinen ja vaikeasti tunnistettava hyökkäyskonsepti.

Kuvassa 4 on esitetty ENISA:n laatima taksonomia kybermaailman kyberagenteista.

Kyberpolitiikka ja -diplomatia

”Kybertoimintaympäristöön liittyvistä kysymyksistä, mukaan lukien digitalisaatio ja kyberturvallisuus, on tullut yhä keskeisempi osa ulko-, turvallisuus- ja puolustuspolitiikkaa.” (Valtioneuvoston kanslia 2016, 12.)

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu kyberasioiden poliittinen luonne (cyberpolitics). Kybertoimintaympäristö itsessään ja siihen vaikuttaminen ovat voimakkaassa muutoksessa, ja tätä kehitystä pyritään



Kuva 4. Cyber Agent -taksonomia ENISA:n (2016) mukaan.

poliittisin keinoin ohjaamaan (ks. mm. CIGI & Chatham House 2016). Kyberturvallisuuden asiat ovat yhä vahvemmin esillä kansainvälisillä foorumeilla ja järjestöissä kuten ETYJ:ssä, EU:ssa, NATO:ssa, OECD:ssä ja Eurooppa-neuvostossa.

Kyberturvallisuudessa etenkin valtioiden välisen luottamuksen lisääminen on keskeinen kysymys. Siihen pyritään tiivistämällä valtioiden välistä keskustelua kybertoimintaympäristöön liittyvistä kysymyksistä niin monenvälisesti, alueellisesti kuin kahdenvälisesti. Kansainvälisillä yhteistyöfoorumeilla ja valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen kyberturvallisuuden kannalta myönteisiä asioita. Ulkoministeriö koordinoi Suomen osallistumista kansainväliseen yhteistyöhön ja osallistuu aktiivisesti kybertoimintaympäristöä koskevaan kansainväliseen keskusteluun. Kybertoimintaympäristö ja kyberturvallisuus ovat lyhyessä ajassa nousseet Suomen ulko- ja turvallisuuspolitiikan tärkeäksi osaksi. Huomionarvoisena voi myös pitää erityisen kybersuurlähettilään viran perustamista Ulkoministeriöön Suomen kyberdiplomatian edistämiseksi.

Useat valtiot sekä esimerkiksi NATO ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin (ks. mm. NATO 2016). Toistaiseksi kyberoperaatiot on tulkittu niin sanotuiksi pehmeiksi toimiksi, minkä vuoksi niiden käyttökynnys on alempi kuin perinteisten sotilasoperaatioiden. Myös poliittiset riskit näyttäytyvät hyökkääjälle pienempinä. Valtiot ja eri järjestöt ovat vähin erin kehittämässä poliittisia keinoja vastata kybervaikuttamiseen. Hyvän esimerkin tästä tarjoaa Eurooppa-neuvoston aloite ”kyberdiplomatian työkalupakin kehittämisestä” (Euroopan komissio 2017). Kyse on diplomaattisista keinoista ja sanktioista, joita Euroopan unioni voi langettaa toimijalle, joka hyökkää EU-jäsenmaita vastaan digitaalisessa ympäristössä.

Kyberpelote

Pelotteen luominen kyberympäristöön on kansainvälisesti tällä hetkellä hyvin ajankohtainen aihe. Kaikki suurvallat tulevat rakentamaan kyberpelotteen, joskin keinot sen luomiseen ovat vielä epäselvät. Uskottavaa kyberpelotetta ei välttämättä saada aikaan samankaltaisin metodein kuin pelotetta fyysisessä maailmassa. Kyberpelotteeseen kuuluu kuitenkin neljä keskeistä elementtiä. Ensiksi, kyky puolustautua kyberympäristössä yhteiskunnan laajuisesti ja hyökkäyksen vahva sietokyky, eli kyky toimia voimakkaan hyökkäyksen alaisena. Toiseksi, kyse on kyvystä tunnistaa hyökkääjä eli attribuutiosta. Kyberpelotteeseen kuuluu kyky paikallistaa hyökkääjä, mihin tarvitaan vahvaa kansainvälistä

yhteistyötä. Kolmanneksi, kyse on hyökkäyskyvykkyydestä ja valmiudesta vastata myös poliittisesti kyberhyökkäyksiin. Haasteeksi muodostuu tällöin se, miten valtio voi viestiä pelotetta ja näyttää kyberhyökkäyskykyjään julkisesti, kun mainitut kyvyt ovat salaista tietoa. Voidaan arvioida, että valtiot tulevat paljastamaan osan kyberhyökkäyskyvyistään ja tekemään esimerkiksi ”koehyökkäyksiä” luodakseen uskottavuutta kyvykkyyksilleen (Limnéll 2013, 200–207). Neljänneksi, pelotteeseen kuuluu myös valtion kyberomavaraisuus ja osaamisen taso. Hieman pelkistäen voi todeta, että osaavat ihmiset ovat paras ”kyberase”, ja korkeaa osaamista osoittava valtio pystyy tällä tavoin viestimään turvallisuusympäristöönsä kyvykkyytensä tasosta. Valtion on myös pelotteen luomisen näkökulmasta kyettävä riittävään omavaraisuuteen turvallisuusteknologian tuottamisessa.

Viestinnällä on tärkeä merkitys pelotteen luomiseen. Esimerkiksi Kiina on julkisesti ilmoittanut rakentavansa kyberpelotteen ydinpelotteen rinnalle. Kyberpelotteen kehittämistä kiihdyttää sen edullisuus. Siinä missä modernin häivehävittäjän hinta on yli 150 miljoonaa euroa, hyökkäysohjelmien koodaaminen maksaa korkeimmillaan kymmeniä miljoonia euroja. Koulutettuja osaajia ei tarvita kyberaseiden suunnitteluun, kehittämiseen ja käyttöön tuhansia, vaan kymmenillä huippuosaajilla voidaan tuottaa maailmanluokan kybersuorituskykyjä. Tässä uudessa tilanteessa maailmanpolitiikan voimasuhteet saattavat muuttua, jos useat maat todella investoivat kyberkyvykkyyksiin ja myös käyttävät niitä. (Mowbray 2010, 3–5; Jensen 2012, 773–824.)

Kybersuorituskykyjen kehittäminen

Uusin valtioneuvoston selonteko toteaa Puolustusvoimien jatkavan ”kyberpuolustuskyvyn kehittämistä kansallisen kyberturvallisuusstrategian mukaisesti. Puolustusvoimat rakentaa kyvyn kybertilannekuvan muodostamiseen, kyberoperaatioiden suunnitteluun ja toimeenpanoon sekä omien järjestelmien suojaamiseen ja valvontaan kybertoimintaympäristössä.” (Valtioneuvoston kanslia 2017, 23.)

Kansallisen puolustuksen näkökulmasta puolustusvoimien tulee säilyttää oma toimintavapautensa ja vaikuttaa vastustajaan kaikilla ei-kineettisillä operaatioilla kybertaistelutilassa kaikissa olosuhteissa. Puolustusvoimien tulee kyetä kiistämään vastustajan toimintavapaus koko kybertaistelutilassa. Tämä edellyttää puolustusvoimilta uhkien mukaista kyvykkyyttä tilannetietoisuuden luomiseen, vastustajan kyberhaavoittuvuuksien tiedusteluun, maalittamiseen ja vaikuttamiseen tavoitteena kyberkohteiden haltuunotto, lamauttaminen tai tuhoaminen.

Asevoimien uudet suorituskyvyt luovat uusia mahdollisuuksia sekä kineettiseen että ei-kineettiseen voimankäyttöön kybertilassa. Siinä tulee voida integroida saumattomasti yhteen ilmassa, pinnassa, pinnan alla ja kyberavaruudessa toimivat miehitetyt ja miehittämättömät alustat. Uusien järjestelmien avulla voidaan yhä tehokkaammin havaita, seurata ja identifioida maaleja sekä johtaa joukkoja ja ohjata asejärjestelmiä halutun vaikutuksen saavuttamiseksi.

Kyberuhkiin varaudutaan ja uhkia hallitaan kehittämällä ja ylläpitämällä erilaisia tiedustelu-, suojaus- ja vaikuttamiskeinoja. Lisäksi on tärkeää luoda tarvittava toipumiskyky kyberhyökkäyksistä (kyberresilienssi).

Yhteiskunnan elintärkeät toiminnat ja kyberomavaraisuus

Kyberhyökkäysten kohteena eivät ole vain asevoimat vaan yhteiskunnan elintärkeät toiminnat. Yhteiskunnan elintärkeät toiminnat on pystyttävä turvaamaan kaikissa tilanteissa. Tietoyhteiskuntana Suomi on riippuvainen tietoverkkojen ja -järjestelmien toiminnasta. Niinpä kriittisen infrastruktuurin kyberympäristössä toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä. Vakavassa kriisissä niitä voidaan käyttää vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella. Näin kansallisesta kyberpuolustuksesta muodostuu kiinteä osa kokonaismaanpuolustusta.

Suomella on hyvä perinne huoltovarmuuden järjestämisessä. Kyberhuoltovarmuutta ja -omavaraisuutta tulee kehittää osana tätä työtä. Kyberhuoltovarmuuden ja -omavaraisuuden avulla luodaan kyky ylläpitää yhteiskunnan elintärkeitä toimintoja väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen toiminnan turvaamiseksi vakavissa häiriötilanteissa ja poikkeusoloissa. Kyberhuoltovarmuus- ja omavaraisuus edellyttävät ensisijaisesti riittävän kyberosaamisen turvaamista sekä Puolustusvoimissa että koko yhteiskunnassa. Riittävä määrä huippuosaajia tarvitaan luomaan tehokasta kansallista kyvykkyyttä. Kyberosaamisen ja erityisesti kyberosaajien kehittäminen niin puolustusvoimissa kuin laajemmin suomalaisessa yhteiskunnassa nousee merkittäväksi jo lähivuosina. Osana kyberomavaraisuutta kriittiset yritykset, teknologiaratkaisut ja osaajat tulee ’ankkuroida’ Suomeen. Samalla mahdollistetaan kansainvälisistä toimijoista riippumaton kansallinen kyberturvallisuustuotteiden ja -palveluiden suunnittelu-, kehittämis- ja tuotantokyky erityisesti turvallisuustoimijoiden käyttöön.

Diskussio

Niin suomalaista yhteiskuntaa kuin myös sodankäyntiä leimaa tällä hetkellä kyberturvallisuuden näkökulmasta kaksi kehityspiirrettä, jotka molemmat tulevat voimistumaan. Ensinnäkin riippuvuus kybertoimintaympäristöstä ja laajemminkin teknologiasta kasvaa. Tämä merkitsee kyberasioiden painoarvon nousua kaikilla toiminnan tasoilla. Turvallisuuden näkökulmasta tämä tarkoittaa myös haavoittuvuuden kasvua. Toiseksi, eri toimijoiden – etenkin valtioiden – kyvykkyydet toimia kyberympäristössä lisääntyvät. Kyvykkyyksien kehittämiseen panostetaan ja oletettavaa on, että kyberympäristön painoarvo sodankäynnissä muodostuu yhä merkityksellisemmäksi.

Tällä hetkellä kyberhyökkäysten monimutkaisuus, tehokkuus ja kyvykkyys kasvavat nopeammin kuin puolustuskyky. Usein vasta vakavat kyberhyökkäykset antavat sysäyksen turvallisuustoimenpiteiden kehittämiselle. Kybermaailmassa on tapahtunut pahuuden konvergenssi. Mafia, hakkeriryhmät ja -verkostot, terroristit ja järjestäytynyt rikollisuus toimivat kybermaailmassa ja käyttävät sen palveluita tiedonvaihtoon, viestintään, tilannekuvan muodostamiseen ja johtamiseen. Tällä joukolla ei ole ”toimivaltuusongelmia”. Ne voivat vapaasti ja täysimääräisesti hyödyntää globaalin digimaailman kyvykkyyksiä.

Kybertoimintaympäristössä tapahtuu myös positiivista kehitystä. Tietoturvayhtiöt sekä hallinnolliset organisaatiot ovat parantaneet yhteistyötään, minkä seurauksena on luotu entistä tehokkaampia toimintatapoja, prosesseja ja järjestelmiä. Järjestelmien haavoittuvuuksien ja kyberturvallisuuden tutkimukseen panostetaan paljon niin yksityisellä sektorilla kuin asevoimissa. Suuret tietoturvayritykset lisäävät resursseja kyberturvallisuuden tutkimukseen ja kehitykseen. Näin markkinoille syntyy tehokkaita työvälineitä kyberhyökkäysten tunnistamiseen ja pysäyttämiseen sekä järjestelmien suojaamiseen.

Kyberuhkat tulee nähdä osana hybridivaikuttamista. Tämä edellyttää vahvaa ja keskitettyä havainnointi-tilannekuva-johtaminen kyvykkyyttä. Kyberturvallisuuden strategisessa johtamisessa tarvitaan tilanneymmärrystä, selkeitä johtamisvastuita ja –rooleja sekä saumatonta tiedon kulkua ja -vaihtoa. Myös lainsäädännön tulee tukea kansallista kyberturvallisuusprosessia. Suomalaisen yhteiskunnan tulee varautua moninaisiin kyberuhkiin, jotka voivat vaikutuksiltaan olla yhteiskunnan toimivuudelle hyvin vakavia. Kun teknologian sekä kyberympäristön merkitys kasvaa, turvallisuuden kannalta on tärkeää huolehtia lainsäädännöstä, jonka on pysyttävä kehityksen mukana. Ajanmukaisella kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.

Tietoyhteiskuntana Suomi on erittäin riippuvainen tietoverkkojen ja -järjestelmien toiminnasta. Niinpä kybertoimintaympäristön kautta tulevat uhkat ovat kokonaisturvallisuuden kannalta hyvin merkityksellisiä. Kasvavan riippuvuuden ohella niin ei-valtiollisten kuin etenkin valtiollisten toimijoiden kehittyvä kyky vaikuttaa kybertoimintaympäristön kautta Suomen elintärkeisiin toimintoihin muodostaa suomalaiselle yhteiskunnalle yhä vakavamman uhkatekijän. Erityisesti kyberturvallisuuden kansalliseen johtamiseen, yhteistyön yhteensovittamiseen sekä energia-, sosiaali- ja terveydenhuolto- ja finanssialan kyberturvallisuuteen tulee kiinnittää erityistä huomiota. Suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävällä tavalla erilaisia kyberuhkia vastaan. Myös häiriötilanteiden resilienssi on joissakin kohteissa heikolla tasolla. Voidaan arvioida, että niin henkisen kuin toiminnallisen resilienssin merkitys kasvaa myös kyberuhkiin varautumisessa lähivuosien aikana. Tällöin on osattava varautua myös ennalta odottamattomiin vaikutuskeinoihin. Kriittisen kybertoimintaympäristön tunnistamiseen yhdistyy myös tietoisuus omasta kyberomavaraisuudesta. Tärkeää on pohtia, kuinka varmistetaan kriittisten infrastruktuurien ylläpidon kannalta riittävä kansallisen omavaraisuuden aste.

Kansallisen kehittämisen ohella tarvitaan kansainvälisen yhteistyön syventämistä. Tämä koskee niin Puolustusvoimia ja muita yhteiskunnan turvallisuutta tuottavia organisaatioita kuin myös Suomen kansainvälistä kyberpoliittista aktiivisuutta. Pelkistäen voidaan todeta, että kyberturvallisuus on niin kansallisesti kuin kansainvälisesti joukkuepeliä. Kansainvälisesti Euroopan unioni näyttäytyy Suomelle luontevana kansainvälisenä kyberturvallisuusyhteistyön viitekehyksenä. Suomen kannalta myönteisenä kehityssuuntana on pidettävä, että Euroopan unionissa on poliittista tahtoa puolustus- ja turvallisuusyhteistyön vahvistamiseen. Kyberturvallisuuden ja -sodankäynnin yhteistyön kehittämisen voi arvioida olevan tässä hyvin keskeisessä asemassa.

Yhteisen kyberpuolustuksen luominen EU:lle edellyttää kuitenkin tarkkarajaista kybersodankäynnin määrittelyä. Yhteisen kyberpuolustuksen tilannekuvan luominen on toteutettavissa, kuten on tehty esimerkiksi NATO-maiden kesken ilma- ja meritilannekuvien osalta. Kyberpuolustustoimenpiteiden osalta voidaan kehittää yhteisiä kyvykkyyksiä, harjoitella yhdessä ja vaihtaa tietoja hyvistä käytänteistä. Ongelmaksi muodostuu offensiivisten kyberoperaatioiden toteuttaminen. Mitkä toimet kybermaailmassa voidaan tulkita ylittävän sodan kynnykset (Act of War)? Kuinka käyttää eri keinoja kyberdiplomatiasta aina sotilaalliseen voimankäyttöön, jos kyberhyökkäyksen toteuttajasta ja sen tarkoituksista ei ole varmaa tietoa. Onhan hyökkääjän tunnistaminen (attribuutio) kybermaailmassa erityisen vaikeaa.

Kybermaailma ja sen kehitys sekä vaikuttavuus osana tämän päivän sodankäyntiä on laaja-alainen ilmiö. Kybersodankäynti on käsitteenä ja toiminnoiltaan osin jäsentymätön sekä nopeasti kehittyvä kokonaisuus. Kybervaikuttamisen keinot voivat jo muutaman vuoden päästä olla aivan toisenlaisia kuin tänään. Turvallisuudesta huolehtiminen kyberympäristössä on monen osatekijän summa. Yksi asia on kuitenkin varma: tutkimuksen merkitys sekä ilmiön ymmärtämisen että suorituskykyjen kehittämisen kannalta kasvaa. Samalla korostuu poikkitieteellisen tutkimusotteen tärkeys. Haluamme tämän artikkelin turvin kannustaa muita tutkijoita kybermaailman tärkeiden ilmiöiden ja kysymysten pohtimiseen sekä suuntaamaan intressejään tälle alueelle.

Viitteet

1 Nollapäivähaavoittuvuus (engl. zero-day vulnerability/attack/threat, 0-day) tarkoittaa tietoturva-aukkoa, jolle ei ole olemassa korjausta, mutta haavoittuvuudelle on olemassa hyväksikäyttömenetelmä. Nollapäivän aukko syntyy, kun joko tietoturva-aukon löytäjä julkaisee tiedot samalla kun ilmoittaa aukosta ohjelman kehittäjille, ei ilmoita siitä ollenkaan, tai kun tietoturva-aukkoa ei paikata ilmoituksesta huolimatta. Nimitys tulee siitä, montako päivää korjauksen jälkeen aukkoa hyödyntävä hyväksikäyttömenetelmä julkaistaan.

Lähteet

Alberts, David, John Garstka & Frederick Stein (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. 2nd revised ed., Washington D.C: CCRP.

Bacon R.H. (ed.) (1929). *The Life of Lord Fisher of Kilverstone. Vol. 2*. London: Hodder & Stoughton.

Bousquet, Antoine (2009). *The Scientific Way of Warfare*. New York: Columbia University Press.

CIGI & Chatham House (2016). *Global Commission on Internet Governance.* Centre for International Governance Innovation and Chatham House. https://www.cigionline.org/publications/one-internet, (31.8.2017).

Cebrowski, Arthur & John Garstka (1998). *Network-Centric Warfare: Its Origin and Future*. Naval Institute Proceedings, Vol 124/1/1,139. Annapolis Maryland, 28–35.

Chen, Jim & Alan Dinerman Alan (2016). On Cyber Dominance in Modern Warfare. *Proceedings of the 15th European Conference on Cyber Warfare and Security*, 7–8th July 2016, Munich: Bundeswehr University, 52–57.

ENISA (2016). *Threat Landscape 2015*. https://www.enisa.europa.eu/publications/etl2015, (23.7.2017).

ENISA (2017). Threat Landscape Report 2016. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016, (23.7.2017).

Euroopan komissio (2017). Pohdinta-asiakirja Euroopan puolustuksen tulevaisuudesta. https://www.eduskunta.fi/FI/tiedotteet/Sivut/komission-pohdinta-euroopan-puolustuksen-tulevaisuudesta.aspx, (23.7.2017).

Filiol, Eric (2009). Operational Aspects of Cyberwarfare or Cyber-Terrorist Attacks: What is truly Devastating Attack Could do. *Proceedings of the 8th European Conference on Information Warfare and Security*, Lisbon: University of Minho and the Military Academy, 71–79.

Garstka, John (2003). Network-Centric Warfare Offers Warfighting Advantage. *Signal* May 2003, 58.

Geers, Kenneth (2001). *Strategic Cyber Security*. Estonia: CCD COE Publication.

Geers, Kenneth (ed.) (2015). *Cyberwar in Perspective: Russian Aggression against Ukraine.* Tallin: NATO CCD COE Publications.

Hallituksen esitys eduskunnalle laiksi Euroopan hybridiuhkien torjunnan osaamiskeskuksesta. HE 59/2017 vp. http://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f8053bb1f, (20.7.2017).

IISS (2016). *The Military Balance 2016. Vol 116.* Taylor and Francis: Routledge.

Ilvonen, Janne (2009). *Vaikutusperusteiset konseptit: EBO-, EBAO-, SOD- ja CA-käsiteanalyysi*, diplomityö Yleisesikuntaupseerikurssi 54. Helsinki: Maanpuolustuskorkeakoulu.

Koch, Robert & Gabi Rodosek (ed.) (2016). *Proceedings of the 15th European Conference on Cyber Warfare and Security*, 7–8th July 2016. Munich: Bundeswehr University.

Jensen, Eric (2012). Cyber Deterrence. *Emory International Law Review*, 26(2), 773–824.

Kosola, Jyrki & Janne Jokinen (2004). *Elektroninen sodankäynti, osa 1 – taistelun viides dimensio.* Tekniikan laitos, julkaisusarja 5, No 2/2004. Helsinki: Maanpuolustuskorkeakoulu.

Lalu, Petteri & Juha Puistola (2015). *Hybridisodankäynnin käsitteestä*. Tutkimuskatsaus 1/2015, Riihimäki: Puolustusvoimien tutkimuslaitos.

Lehto, Martti (2014). Kybertaistelu ilmavoimaympäristössä. Teoksessa T. Kuusisto (toim.) *Kybertaistelu 2020*, Taktiikan laitos, julkaisusarja 2, n:o 1. Helsinki: Maanpuolustuskorkeakoulu, 157–178.

Lehto, Martti, Jarno Limnéll, Eeva Innola, Jouni Pöyhönen, Tarja Rusi & Mirva Salminen (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Helsinki: Valtioneuvoston kanslia.

Lehto, Martti & Pekka Neittaanmäki (2016). Digitalisaatio muuttaa yhteiskunnan ja yksilöiden tapaa toimia. *Tiedepolitiikka*, 1/2016, 56–64.

Libicki, Martin (1995). *What Is Information Warfare?* Washington DC: National Defense University, Institute for National Strategic Studies.

Limnéll, Jarno (2016). The Cyber arms race is accelerating – what are the consequences? *Journal of Cyber Policy,* 1(1), 50–60.

Limnéll, Jarno & Charly Salonius-Pasternak (2016). Challenge for NATO – Cyber article 5. Briefing paper, Center for Asymmetric Threat Studies, Swedish Defence University.

Limnéll, Jarno (2013). *Offensive Cyber Capabilities are Needed Because of Deterrence*. Teoksessa J. Rantapelkonen & M. Salminen (toim.), *The Fog of Cyber Defence*, Series 2, Article Collection N:o 10. Helsinki: National Defence University, 200–207.

Mowbray, Thomas (2010). Solution Architecture for Cyber Deterrence. SANS Institute InfoSec Reading Room. https://www.sans.org/reading-room/.../solution-architecture-cyber-deterrence-33348, (25.7.2017).

NATO (2016). Warsaw Summit Communiqué. http://www.nato.int/cps/en/natohq/official_texts_133169.htm, (23.7.2017).
Nye, Joseph (2010). *Cyber Power.* Harvard Kennedy School. www.belfercenter.org/publication/cyber-power, (22.7.2017).
Office of Force Transformation (2005). *The Implementation of Network-Centric Warfare*. Director, Force Transformation, Washington DC: Office of the Secretary of Defense.
Puttonen, Heidi (2015). *Informaatio-operaatiot ja niiden vaikutusmenetelmät*. Tietojenkäsittelytieteen kandidaattitutkielma, Tietojenkäsittelytieteiden laitos. Jyväskylä: Jyväskylän yliopisto.
Senenko, Christopher (2007). *Network Centric Warfare and The Principles Of War*. Master of Science Degree Thesis, Joint Advanced Warfighting School. Norfolk: Joint Forces Staff College.
Sirén, Torsti (toim.) (2011). *Strateginen kommunikaatio ja informaatio-operaatiot 2030*, Johtamisen ja sotilaspedagogiikan laitos, julkaisusarja 2, n:o 7. Helsinki: Maanpuolustuskorkeakoulu.
Sisäministeriö (2016). *Valtioneuvoston selonteko sisäisestä turvallisuudesta*. Sisäministeriön julkaisu 8/2016. Helsinki: Sisäministeriö.
Urry, John (2000). *Sociology Beyond Societies: Mobilities for the Twenty-first Century*, London and New York: Routledge.
Valeriano, Brandon & Ryan Maness (2015). *Cyber War versus Cyber Realities, Cyber Conflict in the International System*. New York: Oxford University Press.
Valtioneuvoston kanslia (2004). *Suomen turvallisuus- ja puolustuspolitiikka*. Valtioneuvoston kanslian julkaisusarja 16/2004. Helsinki: Valtioneuvoston kanslia.
Valtioneuvoston kanslia (2016). *Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko.* Valtioneuvoston julkaisusarja 7/2016. Helsinki: Valtioneuvoston kanslia.
Valtioneuvoston kanslia (2017). *Valtioneuvoston puolustusselonteko*. Valtioneuvoston kanslian julkaisusarja 5/2017. Helsinki: Valtioneuvoston kanslia.