Maanpuolustuskorkeakoulu
Julkaisusarja 3: Työpapereita nro 12

#kyberpuolustus

Kyberkäsikirja Puolustusvoimien henkilöstölle

Tommi Laari (toim.)

MAANPUOLUSTUSKORKEAKOULU
SOTATAIDON LAITOS
JULKAISUSARJA 3: TYÖPAPEREITA NRO 12

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF WARFARE
SERIES 3: WORKING PAPERS NO. 12

#kyberpuolustus

Kyberkäsikirja Puolustusvoimien henkilöstölle

TOIMITTANUT TOMMI LAARI

TEKIJÄT:
TOMMI LAARI, JOUNI FLYKTMAN, KATRIINA HÄRMÄ,
JUSSI TIMONEN & JUSSI TUOVINEN

MAANPUOLUSTUSKORKEAKOULU
SOTATAIDON LAITOS
HELSINKI 2019

Tommi Laari, Jouni Flyktman, Katriina Härmä, Jussi Timonen & Jussi Tuovinen: *#kyberpuolustus*
Maanpuolustuskorkeakoulu
Sotataidon laitos
Julkaisusarja 3: Työpapereita nro 12
National Defence University
Department of Warfare
Series 3: Working Papers No. 12

VASTUUVAPAUSLAUSEKE

Työpaperit ovat luonteeltaan keskustelun avauksia tai alustavia tutkimusraportteja. Työpapereiden avulla kirjoittajat voivat myös raportoida ja analysoida ajankohtaisia tapahtumia. Työpapereiden sähköisellä julkaisemisella Maanpuolustuskorkeakoulu toivoo kirjoittajien saavan rakentavaa palautetta kirjoituksilleen.

Maanpuolustuskorkeakoulu ei vastaa työpapereiden sisällöstä, mielipiteistä, havainnoista tai johtopäätöksistä, vaan vastuu niistä kuuluu yksinomaan niiden kirjoittajille.

Työpaperit tarkastetaan Maanpuolustuskorkeakoulun laitoskohtaisissa julkaisutyöryhmissä, mutta niitä ei arvioida käyttämällä akateemista ”blind peer-review” -prosessia. Lähtökohtaisesti työpaperit kirjoitetaan kuitenkin noudattaen samoja tieteellisen kirjoittamisen sääntöjä ja hyviä tieteen tekemisen käytäntöjä, mutta niiden läpikäymä arviointiprosessi on kevyempi ja nopeampi kuin tieteellisten julkaisuiden.

Uusimmat julkaisut pdf-muodossa: http://www.doria.fi/handle/10024/73990

Taittaja: Emil Marjo

ISBN 978-951-25-3119-6 (nid.)
ISBN 978-951-25-3120-2 (pdf)
ISSN 2489-4354 (painettu)
ISSN 2343-0753 (verkkojulkaisu)

Maanpuolustuskorkeakoulu – Sotataidon laitos
National Defence University – Department of Warfare

Sisällys

Jokamiehen kyberpuolustus

- Käytä harkintaa jakaessasi tietoja itsestäsi julkisesti
- Käytä riittävän pitkiä ja monimutkaisia salasanoja tai hyödynnä salasananhallintasovellusta.
- Käytä eri salasanoja eri palveluissa.
- Käytä varovaisuutta ja maalaisjärkeä sähköpostien avaamisessa.
- Pidä kaikki laitteesi suojattuina ja laitteiden päivitykset ajan tasalla.
- Pidä henkilökohtaiset laitteet erillään Puolustuvoimien laitteista.
- Käytä USB-tikkua vain pakottavissa tilanteissa ja silloinkin aina virustarkastuksen kautta.
- Mieti ennen kuin klikkaat, epämääräiset linkit altistavat monille uhkille.
- Käytä älypuhelinta kuin tietokonetta, samat ohjeet pätevät.

Taulukko 1: Hyviä käytänteitä henkilökohtaisessa kybersuojautumisessa

Esipuhe

Kybertoimintaympäristö kehittyy kovalla vauhdilla, ja se on sotilaille ajankohtaisempaa kuin koskaan aiemmin. Kesällä 2019 Israelin armeija tuhosi ilmaiskulla Hamasin kybertoimijoita ja heidän toimitilojaan. Se oli ensimmäinen kerta sotahistoriassa, kun kyberuhkaan on vastattu välittömästi sotilaallisella tulenkäytöllä eli tässä tapauksessa ilmaiskulla. Toki Yhdysvallat on jo aiemmin käyttänyt lennokki-iskuja Isis-järjestön kyberosaajia vastaan, mutta Israelin isku oli siis ensimmäinen kerta, kun kybertoimintaympäristössä havaittuun sotatoimeen kohdistettiin välitön vastahyökkäys ampumalla.

Kirja kyberpuolustuksesta ja sotilaallisesta kybertoimintaympäristöstä on erittäin tarpeellinen koko Puolustusvoimien henkilöstölle. Ensisijaisesti se toimii yksilöille oppaana ja lisää koko henkilöstön osaamista ja ymmärrystä kybertoimintaympäristöstä, mikä on edellytys koko organisaation menestykselle tänä päivänä. Toiseksi kirja tukee Maanpuolustuskorkeakoulun ja mahdollisesti myös muiden oppilaitosten opetusta muodostamalla selkeän kokonaisuuden siitä, kuinka tätä ajoittain monimutkaista kybertoimintaympäristöä voidaan lähestyä. Kolmanneksi kybertoimintaympäristön jatkuva ja nopea kehitys haastaa kirjan sisällön ja ajankohtaisuuden hyvinkin nopeasti, mutta kirja tarjoaa siitäkin huolimatta erinomaisen lähtökohdan jatkokeskusteluille ja tutkimukselle.

Kirjan tärkeimpinä johtopäätöksinä painotan kolmea asiaa. Ensinnäkin kybertoimintaympäristö on ja tulee olemaan oleellinen osa sotilaallista toimintaympäristöä. Mitä paremmin se ymmärretään, sen paremmin siinä osataan toimia. Toisena asiana nostan esiin Puolustusvoimien roolin kybertoimintaympäristössä. Puolustusvoimat on aktiivinen toimija kybertoimintaympäristössä, ja se valmistautuu toimimaan siinä oman toimivaltansa puitteissa kaikissa tilanteissa. Viimeisenä johtopäätöksenä tuon esille sen, että kybertoimintaympäristön globaalin luonteen myötä yhteistoiminta niin Suomessa kuin kansainvälisestikin on ehdoton edellytys kaikelle menestyksekkäälle toiminnalle kybertoimintaympäristössä.

Antoisia lukuhetkiä!

Sotataidon laitoksen johtaja
Eversti Riku Suikkanen

Lukijalle

#kyberpuolustus-teoksessa kuvataan kybertoimintaympäristön perusteet ja luodaan Puolustusvoimien henkilöstölle edellytykset tämän jatkuvasti ja nopeasti kehittyvän toimintaympäristön seuraamiseksi myös tulevaisuudessa. #kyberpuolustus kuvaa puolustusvoimiin ja sen henkilöstöön kohdistuvia uhkia sekä kertoo, kuinka puolustusvoimat toimii tässä sodankäynnin uudessa ulottuvuudessa. Lisäksi teos kuvaa kyberoperaatioiden yleisimpiä toimintamalleja maailmalta. #kyberpuolustus on ensimmäinen julkinen kuvaus kyberpuolustuksesta Suomessa ja aihealueen yleisestä sensitiivisyydestä huolimatta se on julkinen. Kirjan tavoitteena on antaa lukijalleen riittävä perustietämys laajasta ja monimutkaisesta kybertoimintaympäristöstä sekä siihen liittyvistä ilmiöistä.

#kyberpuolustus on laadittu koko puolustusvoimien henkilöstölle siviileistä sotilaisiin. Monet kybertoimintaympäristöön liittyvät ilmiöt ja uhkat koskettavat kaikkia työntekijöitä päivittäin. Esimerkkinä voidaan mainita huijaussähköpostiviestit, joissa jokaisen yksittäisen käyttäjän toimenpiteillä on merkitystä järjestelmien turvallisuudelle.

#kyberpuolustus koostuu neljästä luvusta. Ensimmäisessä luvussa kuvataan kybertoimintaympäristöä ja sen kehitystä. Toisessa luvussa tarkastellaan ympäristön muodostamaa uhkaa puolustusvoimien näkökulmasta ja kolmannessa luvussa käsitellään sitä, kuinka puolustusvoimat toimii kybertoimintaympäristössä. Neljännessä luvussa kuvataan kyberoperaatioita ja niiden toimintatapoja maailmalta.

Teos sisältää useita englanninkielisiä lyhenteitä, jotka on suomennettu ja selitetty. Englanninkieliset lyhenteet on kuitenkin sisällytetty tekstiin, koska englanninkieliset termit ja lyhenteet ovat alkaneet vakiintua kybertoimintaympäristön käsitteistöön ja englannista on muodostunut kyberin valtakieli. Näin ollen englanninkielisten termien ja lyhenteiden esittäminen helpottaa asioiden liittämistä suurempaan kokonaisuuteen sekä niiden vertaamista kansainväliseen materiaaliin tai uutisiin. Vastaavasti kansainvälisen yhteensopivuuden johdosta puolustushaarat, etenkin Ilma- ja Merivoimat, käyttävät jo pitkälti englanninkielistä termistöä. Sama pätee nyt kyberoperaatioissa, koska suomenkielisiä termejä ei ole vielä olemassa kaikille asioille. #kyberpuolustus-teoksessa on esitelty englanninkielisten termien suomenkieliset vastineet, mutta kaikki käytetyt termit eivät ole virallisesti Puolustusvoimissa hyväksyttyjä.

Lähteistöltään #kyberpuolustus perustuu pääosin amerikkalaiseen ja britannialaiseen materiaaliin. Syy on hyvin yksinkertainen. Yhdysvaltojen ja Ison-Britannian doktriinit ja muut lähteet ovat avoimia ja näin ollen ne ovat saatavilla. Lisäksi ne on kirjoitettu englanniksi ja ne on alun perinkin laadittu kansainvälisesti yhteensopiviksi. Lisäksi Yhdysvalloilla on pitkä kokemus kybertoimintaympäristössä toimimisesta ja näin ollen Yhdysvaltoja voidaan pitää kyberin edelläkävijänä.

Tekstissä ei ole lähdeviitteitä, sillä pääosin käsitellyt asiat esiintyvät kaikissa tärkeimmissä lähteissä ja tekstistä on haluttu laatia yleistajuinen ja helposti lähestyttävä. Lisäksi eri lähteiden välillä on jonkin verran ristiriitoja, joten kaikki tähän kirjoitettu perustuu kirjoittajien tulkintoihin lähdemateriaalista. Kaikki tärkeimmät käytetyt lähteet on mainittu kirjan lopussa.

Tätä kirjaa on ollut kirjoittamassa joukko kyberpuolustuksen asiantuntijoita ja kärkiosaajia. Kaikista kyberpuolustukseen liittyvistä asioista ei ole olemassa yksimielisyyttä, vaan kirjaa kirjoitettaessa on jouduttu tekemään myös kompromisseja erilaista näkemyksistä. #kyberpuolustuksen toivotaan kuitenkin toimivan tukena sekä kyberpuolustuksen parissa työskenneltäessä, että aihealuetta opiskellessa. Lisäksi kirjan toivotaan herättävän ajatuksia ja keskustelua.

1 #TILANNE

Elinympäristömme digitaalisuus on kasvanut viime vuosikymmeninä räjähdysmäisesti. Digitaalisuuden merkitys niin yksilöiden kuin yhteisöidenkin jokapäiväisessä elämässä on lisääntynyt. Myös palvelut ovat siirtyneet hyödyntämään digitaalisuuden tuomia mahdollisuuksia. Samanaikaisesti tämän uuden, ihmisen luoman ja digitaalisen osa-alueen eli kybertoimintaympäristön turvallisuus on noussut tärkeäksi tekijäksi, sillä tiedon ja palveluiden on oltava luotettavia ja käyttäjien saatavilla. Tähän haasteeseen vastataan kyberturvallisuudella. Kyberturvallisuus on laaja kokonaisuus, joka koskettaa koko yhteiskuntaa kriittisestä infrastruktuurista aina kuluttajiin asti. Kybertoimintaympäristön laajuus ja levinneisyys tarkoittavat kuitenkin sitä, että sen turvallisuutta ei ole mahdollista hoitaa yhden tahon toimenpitein vaan se vaatii yhteistyötä eri toimijoiden välillä. Kybertoimintaympäristö on tärkeä myös maanpuolustukselle, sillä Puolustusvoimat on riippuvainen tieto- ja viestintäjärjestelmistä. Toisaalta kybertoimintaympäristössä toimivat vastustajat aiheuttavat merkittävän uhkan näille järjestelmille. Tästä huolimatta kybertoimintaympäristö tulee nähdä sotilaallisen toiminnan kannalta mahdollisuutena ja voimavarana.

Tässä luvussa kuvataan kybertoimintaympäristön tilanne, jossa tällä hetkellä toimimme. Tämä tehdään kuvaamalla tärkeimmät käsitteet ja toimintaympäristön piirteet sekä esittelemällä kybertoimintaympäristöön liittyvää lainsäädäntöä, toimijoita ja tapahtumia. Lukuun perehdyttyään lukijalla tulisi olla selkeä ymmärrys siitä, millainen on kybertoimintaympäristö, jossa uhkia ja toimintaa teoksen tulevissa luvuissa käsitellään.

1.1 Mikä on kybertoimintaympäristö?

Kybertoimintaympäristön ymmärtäminen alkaa käsitteestä kyber. Mitä tämä sana kyber tarkoittaa? Kyber-käsitteelle ei ole olemassa maailmanlaajuisesti hyväksyttyä määritelmää. Kyber ja siihen liittyvä termistö ei tule todennäköisesti vähään aikaan vakiintumaan, mikä johtuu muun muassa siitä, että ala muuttuu jatkuvasti ja no-

peasti. Tässä esitettyjen peruskäsitteiden lisäksi käsitteitä on määritelty kirjassa sitä mukaa, kun uusia käsitteitä tulee asiasisällössä esille.

Kyber-sanaa käytetään lähes poikkeuksetta yhdyssanan määriteosana eikä yksinään. Sanan merkitys liittyy yleensä digitaalisessa muodossa olevan informaation käsittelyyn: tietotekniikkaan, digitaaliseen viestintään, tiedonsiirtoon, tietojärjestelmiin tai tietokonejärjestelmiin. Yleensä vasta koko yhdyssanalla voidaan ajatella olevan oma merkityksensä. Yleisesti voidaan mieltää, että mikä tahansa fyysisen maailman toiminto voidaan liittää ihmisen luomaan digitaaliseen toimintaympäristöön kyber-sanan avulla. Esimerkiksi perinteinen sodankäynti laajennetaan digitaaliseen ympäristöön termin kybersodankäynti avulla. Toisaalta kybersodankäynti on nykyisin osa kaikkea sodankäyntiä.

Tietoturvallisuus on tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Monissa tilanteissa tietoturvallisuutta käytetään kyberturvallisuuden synonyymina täysin perustellusti. Käsitteenä tietoturvallisuus ei ole ristiriidassa kyberturvallisuuden kanssa, vaan se on tärkeä osa kyberturvallisuutta.

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus on tiedon, laitteistojen, verkostojen, ohjelmistojen ja käyttäjien luottamuksellisuuden, eheydyn ja saatavuuden turvaamista koko elinjakson ajan. Kyberturvallisuus muodostuu ylläpitäjien ja käyttäjien välisestä yhteistoiminnasta ja siinä huomioidaan kybertoimintaympäristön vaikutukset fyysiseen maailmaan.

Kybertoimintaympäristö on digitaalisista tietojärjestelmistä muodostuva toimintaympäristö, johon kuuluvat myös fyysiset rakenteet sekä kaikki toimintaympäristön toimijat. Ympäristölle on tunnusomaista elektroniikan ja sähkömagneettisen spektrin käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon viestintäverkkojen avulla.

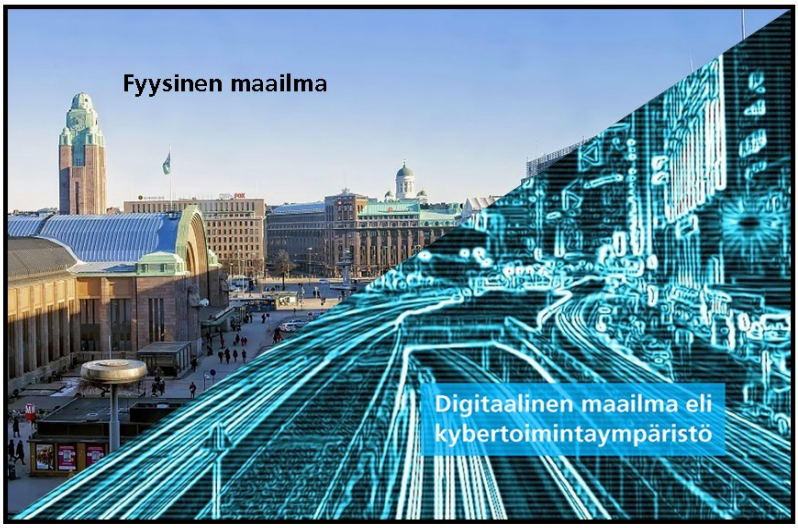
Kyber (cyber)	Käsitteellä viitataan yleensä kybertoimintaympäristöön. Lisäksi käsite viittaa yleisesti digitaalisessa muodossa olevien tietoaineistojen käsittelyyn. Yleensä kyber-sana on yhdyssanan alussa, ja sen avulla mikä tahansa fyysisen maailman toiminto tai tapahtuma voidaan liittää ihmisen luomaan digitaalisen maailmaan.
Tietoturvallisuus (information security)	Tietoturvallisuus tarkoittaa tietoainestojen luottamuksellisuuden, eheyden ja saatavuuden varmistamista hallinnoisilla, toiminnallisilla ja teknisillä toimenpiteillä.
Kyberturvallisuus (cyber security)	Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus on tiedon, laitteistojen, verkostojen, ohjelmistojen ja käyttäjien luottamuksellisuuden, eheydyn ja saatavuuden turvaamista koko elinjakson ajan. Kyberturvallisuus muodostuu ylläpitäjien ja käyttäjien välisestä yhteistoiminnasta ja siinä huomioidaan kybertoimintaympäristön vaikutukset fyysiseen maailmaan.
Kybertoimintaympäristö (cyberspace)	Digitaalisista tietojärjestelmistä muodostuva toimintaympäristö, johon kuuluvat myös fyysiset rakenteet sekä kaikki toimintaympäristön toimijat.

Taulukko 2: Peruskäsitteitä

Kybertoimintaympäristö ei ole maantieteellisesti rajoitettu kuten muut toimintaympäristöt. Tämä aiheuttaa sen, että kybertoimintaympäristössä etäisyyttä on tarkasteltava eri tavoin kuin perinteisissä toimintaympäristöissä. Usein tietty komponentti saattaa sijaita fyysisesti toisella puolella maailmaa kuin sen käyttäjät. Esimerkiksi sosiaalisen median käyttäjiä voi olla ympäri maailmaa, mutta palvelua ylläpitävät järjestelmät sijaitsevat yhdessä tai useammassa maassa. Lisäksi ympäristö on maailmanlaajuinen ja haavoittuva useista kohdista. Kybertoimintaympäristön kokonaisuus on rakennettu laajan verkon ympärille, eikä sitä varsinaisesti omista kukaan. Toisaalta sen omistavat kaikki sen käyttäjät, kuten liike-elämä, valtiot ja yksilöt, yhdessä.

Esimerkkejä kybertoimintaympäristöistä ovat tietojärjestelmiin perustuvat ydinvoimalan ohjausjärjestelmät, elintarvikkeiden kuljetus- ja logistiikkajärjestelmät, liikenteen ohjausjärjestelmät sekä pankki- ja maksujärjestelmät. Kybertoimintaympäristö ei ole pelkästään valtiollista toimintaa ylläpitävää, vaan kaikki sähköinen asiointi – sosiaalinen media, musiikkipalvelut, lippuvaraukset, puhelut sekä kaikki arkipäiväisetkin asiat kuuluvat nykyään kybertoimintaympäristöön.

Kybertoimintaympäristö on hyvin laaja ja moninainen kokonaisuus, jonka ymmärtäminen voi olla ajoittain hankalaa. Asiaa voidaan hieman yksinkertaistaa jakamalla maailma kahteen osaan. Toisen osan muodostaa jokaiselle tuttu jokapäiväinen fyysinen maailma ja toisen osan ihmisten luoma keinotekoinen digitaalinen maailma. Nämä maailmat lähentyvät toisiaan ja fyysinen maailma on nykyisin erittäin



Kuva 1: Pelkisteytty malli kybertoimintaympäristöstä

riippuvainen digitaalisesta maailmasta. Tätä digitaalista ihmisen luomaa maailma voidaan kutsua kybertoimintaympäristöksi.

Internetillä on keskeinen asema kybertoimintaympäristössä, sillä se on kokonaisuutta yhdistävä tekijä. Kybertoimintaympäristö on kuitenkin paljon muutakin kuin internet. Kybertoimintaympäristö sisältää esimerkiksi teollisuusautomaatiota, ohjausjärjestelmiä, toiminnanohjausjärjestelmiä ja esineiden internetiin (internet of things, IoT) -kuuluvia laitteita. Ympäristöä hahmotettaessa on keskeistä tunnistaa se, mitä päivittäisessä käytössä ei juuri huomaa: -sähköposti ja www-sivut muodostavat verkosta vain pienen osan. Käytännössä laaja osa kriittisestä infrastruktuurista on verkottunut, esimerkkejä tästä ovat sähkönohjausjärjestelmät, logistiikan ohjausjärjestelmät sekä lennonjohdonjärjestelmät.

Kybertoimintaympäristö on miltei kaikkien ulottuvilla, ja sinne on mahdollista päästä monin eri tavoin. Useimmiten kybertoimintaympäristöön liitytään tietokoneella, kannettavalla tietokoneella, tabletilla tai matkapuhelimella. Yhteys voidaan saavut-

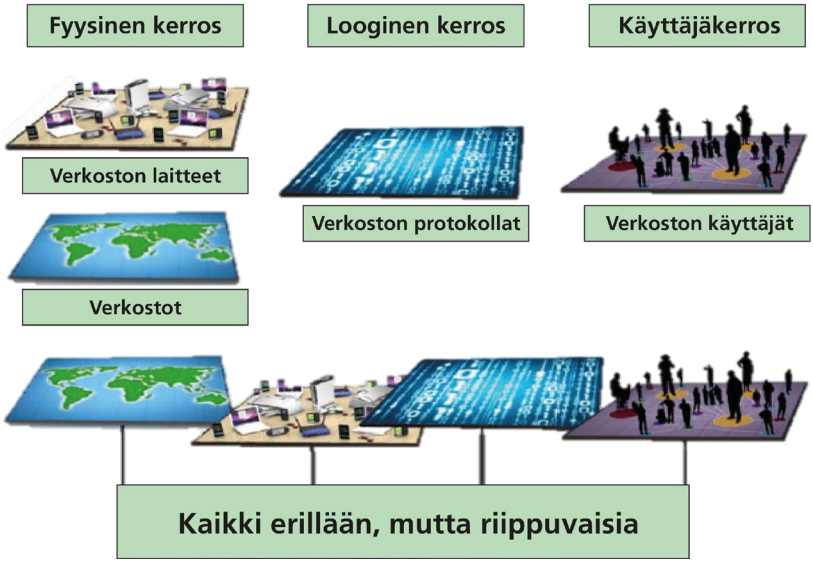
taa langattomien yhteyksien tai fyysisten kaapeleiden avulla. Nykyään langattomat verkot (4G, WLAN, Bluetooth, satelliitti) tarjoavat laajan mahdollisuuden päästä käyttämään palveluja. Kaikissa tilanteissa kybertoimintaympäristö on riippuvainen myös fyysisistä tekijöistä kuten virtalähteistä, kaapeleista, verkoista ja datakeskuksista sekä ihmisistä, jotka toimivat ja hallinnoivat niitä. Myös laitekanta on kasvanut tietokoneiden ja mobiililaitteiden määrän ja kyvyn kasvaessa. Lisäksi esineiden internetin kehittyessä pääosa muun muassa kodinkoneista liittyy automaattisesti kybertoimintaympäristöön, jos olosuhteet sen mahdollistavat esimerkiksi kodin langattoman verkon avulla.

www (world wide web)	www on internetin palvelumuoto. Se on internetverkossa toimiva hajautettu hypertekstijärjestelmä. Hypertekstiä luetaan selaimella, joka hakee verkkosivuiksi kutsuttuja dokumentteja web-palvelimilta ja esittää niitä käyttäjälle piirtämällä ne näytölle.
SCADA (supervisory control and data acquisition)	Scada on tietokoneohjelmistotyyppi, joka tunnetaan ehkä paremmin nimillä valvomo-ohjelmisto tai PC-valvomo. Valvomossa on tietokoneella toteutettu graafinen käyttöliittymä automaatiojärjestelmiin. Valvomoja käytetään kaikenlaisessa automaatiossa niin kiinteistöautomaatiossa, paperitehtaiden ja sähkönjakelun ohjauksessa kuin laivoissa ja ydinvoimaloissa.
4G	4G on laajakaistaisen internet-yhteyden käyttöön suunniteltu niin sanottu neljännen sukupolven langaton tiedosiirtoteknologia. ITU:n vuonna 2008 julkaiseman määritelmän mukaan 4G:n huippunopeus päätelaitteeseen tulisi olla 1 Gbit/s hitaasti liikuttaessa ja 100 Mbit/s nopeasti liikuttaessa. Käytännössä verkkojen nopeudet ovat alhaisempia.
5G	5G on viidennen sukupolven langaton tiedonsiirtoteknologia, jota voidaan käyttää muun muassa tietokoneissa sekä internetin avulla toimivissa koneissa ja ajoneuvoissa. 5G-tekniikkaan siirtyminen mahdollistaa muun muassa itseohjautuvat ajoneuvot, terveydenhuollon automaattisesti toimivat valvontalaitteet, edistyneen teollisuusautomaation sekä virtuaalitodellisuuden kokemisen älypuhelimen avulla.
IoT (internet of things)	IoT on englanninkielinen lyhenne esineiden internetille. Esineiden internetillä tarkoitetaan internet-verkon laajentumista laitteisiin ja koneisiin, joita voidaan ohjata, mitata ja sensoroida internet-verkon yli. Esimerkkinä esineiden internetistä ovat älytelevisiot tai jääkaapit, jotka voivat lähettää internetin välityksellä omistajalleen valokuvan jääkaapin sisällöstä kaupassa käyntiä helpottamaan.

Taulukko 3: Yleisiä käsitteitä

Kybertoimintaympäristön moninaisuutta ja rakennetta voi kuvata myös kerrosten avulla. Ympäristö voidaan jakaa ainakin fyysiseen kerrokseen, loogiseen kerrokseen ja käyttäjäkerrokseen kuvan 2 mukaisesti.

Fyysinen kerros koostuu nimensä mukaisesti fyysisistä asioista, joita voi kosketaa, kuten tietokone tai kaapeli. Fyysiseen kerrokseen kuuluvat laitteistot, järjestelmät ja infrastruktuuri, jotka muodostavat fyysisiä reittejä ja verkostoja. Verkkojen fyysisten paikkojen ja reittien lisäksi fyysinen kerros sisältää maantieteelliset osat.



Kuva 2: Kybertoimintaympäristön kerrokset (lähde: Joint Publication 3-12 Cyberspace Operations 8 June 2018)

Maantieteellinen osa liittyy verkon osien maantieteelliseen sijaintiin kuten sijaintiin meren tai maan alla tai rakennuksessa. Sotilaallisesta näkökulmasta fyysisen kerroksen suojaaminen tehdään fyysisesti ja tähän kerrokseen voidaan kohdistaa hyökkäys samalla tavoin kuin mihin tahansa muuhun fyysiseen kohteeseen.

Looginen kerros koostuu asioista, joita ei voi fyysisesti koskettaa, kuten palvelu tai ohjelmakoodi. Tämän kaltaiset komponentit eivät ole sidottuja tiettyyn fyysiseen paikkaan. Tällaisia komponentteja ovat esimerkiksi internet-palvelu, joka toteutetaan useista fyysisistä palvelimista. Tällä kerroksella sijaitsee myös ohjelmointikoodi. Looginen kerros muodostuu yhteyksistä, jotka muodostuvat verkon solmujen välillä. Solmu on verkkoon kytketty fyysinen laite, kuten tietokone, älypuhelin tai jokin muu mobiililaite. Solmu sisältää verkkoasetuksia, tietoturvaprosessit, tiedonsiirtoprotokollat, internetin verkkotunnukset, omistustiedot sekä tiedot, sovellukset ja protokollat, jotka ohjaavat vuorovaikutusta fyysisen kerroksen kanssa. Sotilaallisesta näkökulmasta looginen kerros käyttää siis loogisia rakenteita ensisijaisesti takaamaan tietoturvaa ja tiedon eheyttä. Tähän kerrokseen pelkkä fyysinen vaikuttaminen on lähes mahdotonta. Looginen kerros voi joutua muita kerroksia helpommin tiedustelun kohteeksi, ja tällä tasolla valtaosa kyberhyökkäyksistä ta-

pahtuu.

Käyttäjäkerros tarkoittaa ihmisiä ja persoonia kybertoimintaympäristössä. Se koostuu yksityiskohdista, jotka yhdistävät ihmiset kybertoimintaympäristöön sekä ihmiset ja ryhmät verkkojen välityksellä käytävään vuorovaikuttamiseen. Yksilölliset osoitteet tai käyttäjänimet yhdistetään virtuaalisiin osoitteisiin, jotka puolestaan toimivat karttana fyysiselle ja loogiselle kerrokselle. Yksittäisellä henkilöllä voi olla useita persoonia esimerkiksi erilaisten sosiaalisen median tilien sekä eri tietokoneiden ja mobiililaitteiden kautta. Toisaalta useat ihmiset voivat jakaa yhden kyberpersoonan esimerkiksi monen käyttäjän yksittäisen sähköpostitilin avulla. Näin ollen vastuun kohdistaminen kybertoimintaympäristössä on vaikeaa. Sotilaallisesta näkökulmasta sosiaalinen kerros on usein se kerros, josta hyökkäys aloitetaan. Monesti ihminen on edelleen helpoin tie tunkeutua järjestelmiin kybertoimintaympäristössä.

Kybertoimintaympäristön muodostavat tekniikat ja järjestelmät ovat kehittyneet nykyaikaisen elämäntavan mahdollistajista elämäntavan peruspilareiksi. Nykyajan yhteiskunnan kaikki toiminnot ovat riippuvaisia tietovirroista, joten kybertoimintaympäristö on olennainen osa nykypäivän globaalia ympäristöä. Elämme digitaalisessa maailmassa ja olemme tottuneet älypuhelimiin ja tietokoneisiin sekä työpaikalla että kotona. Sosiaalisen median sovellukset ja sähköposti ovat osa päivittäistä elämäämme.

Kybertoimintaympäristössä toimiminen vaatii jokaiselta toimijalta erityisiä taitoja sekä reilusti varovaisuutta ja järjenkäyttöä. Tarvittavia taitoja on esitelty useissa erilaisissa julkaisuissa. Tällaisia ovat esimerkiksi Suomen kyberturvallisuusstrategiat ja sen toimeenpano-ohjelmat, Valtioneuvoston selvitys Suomen kyberturvallisuuden nykytilasta tai Turvallisuuskomitean julkaisema Kodin kyberopas.

Kyberturvallisuus on joukkuelaji. Kybertoimintaympäristön globaali luonne edellyttää laajaa kansallista ja kansainvälistä yhteistoimintaa. Suomessa tietojärjestelmien verkottuneisuuden johdosta yritykset, ministeriöt ja laitokset toimivat kaikki omissa ja yhteisissä verkoissaan. Periaatena on, että jokainen vastaa omista verkoistaan, mutta yhteistyötä tehdään jatkuvasti uhkien torjunnassa. Puolustusvoimien vastuulla on kyberturvallisuuden osa-alue nimeltään kyberpuolustus, joka esitellään luvussa kolme. On kuitenkin olemassa paljon muitakin kyberturvallisuuden kannalta tärkeitä toimijoita. Suomessa tärkeimpiä valtiollisia toimijoita ovat muun muassa

Valtioneuvosto, Kyberturvallisuuskeskus, Keskusrikospoliisi, Väestörekisterikeskus ja Erillisverkot. Lisäksi on lukuisia erilaisia toimijoita, kuten yrityksiä, oppilaitoksia ja yhdistyksiä, joilla on oma tärkeä osansa Suomen kyberturvallisuudessa.

Valtioneuvosto muodostaa kyberturvallisuuden johtamisen ylimmän tason, jonka tehtävänä on kyberturvallisuuden poliittinen ohjaus ja strategiset linjaukset sekä kyberturvallisuuden voimavaroista ja toimintaedellytyksistä päättäminen. Eri ministeriöt vastaavat valtioneuvoston ohjeiden mukaisesti kyberturvallisuudesta ja siihen liittyvien häiriötilanteiden hallinnasta itsenäisesti mutta yhteistoiminnassa.

Liikenne- ja viestintävirasto Traficomiin kuuluva Kyberturvallisuuskeskus kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Lisäksi Kyberturvallisuuskeskus tuottaa tietoturvallisuuden tilannekuvaa.

Keskusrikospoliisiin perustettiin huhtikuussa 2015 Kyberrikostorjuntakeskus. Sen päätehtävinä kyberrikollisuuden torjunnassa ovat vakavimpien tietoverkkorikosten tutkinta, tietoverkkorikollisuuden tilannekuvan ylläpito, internet- ja verkkotiedustelu, tietotekninen tutkinta sekä esitutkintaan liittyvät asiantuntijapalvelut poliisille ja muille viranomaisille.

Väestörekisterikeskuksen digiturvapalvelut tukevat koko julkista hallintoa turvallisten palveluiden ja toimintaympäristön kehittämisessä. Valtiovarainministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden koordinaatioelin, jonka operatiivinen toiminta on Väestörekisterikeskuksen tehtävänä.

Suomen Erillisverkot Oy vastaa korkean varautumisen verkosta. Erillisverkot Oy varmistaa Suomen turvallisuuden kannalta tärkeiden viranomaisten ja valtion ylimmän johdon viestintää kaikissa tilanteissa. Sen palveluiden loppukäyttäjiä ovat esimerkiksi ministeriöt, puolustusvoimat, hätäkeskukset, rajavartiolaitos, poliisi ja pelastusviranomaiset. Erillisverkot on korkean varautumisen verkko-operaattori, joka takaa osaamisen, infrastruktuurin ja palvelun avulla häiriöttömän verkon.

1.2 Kybertoimintaympäristö sotilaille

Kybertoimintaympäristön sotilaskäytön ensiaskeleita otettiin jo vuonna 1997, kun Yhdysvallat järjesti ensimmäisen kaksipuolisen kyberharjoituksen nimeltä Eligible Receiver. Tässä harjoituksessa NSA (US National Security Agency) hyökkäsi puolustushallinnon verkkoja vastaan ja läpäisi kaiken puolustuksen melko helposti. Se herätti Yhdysvallat huomaamaan asian merkityksen. Kansainvälisesti asia päätettiin vuonna 2016, kun Nato julisti Varsovan kokouksessa kyberin sotilaalliseksi toimintaympäristöksi, jossa on kyettävä taistelemaan kuten maa-, meri-, ilma- ja avaruustoimintaympäristöissä.

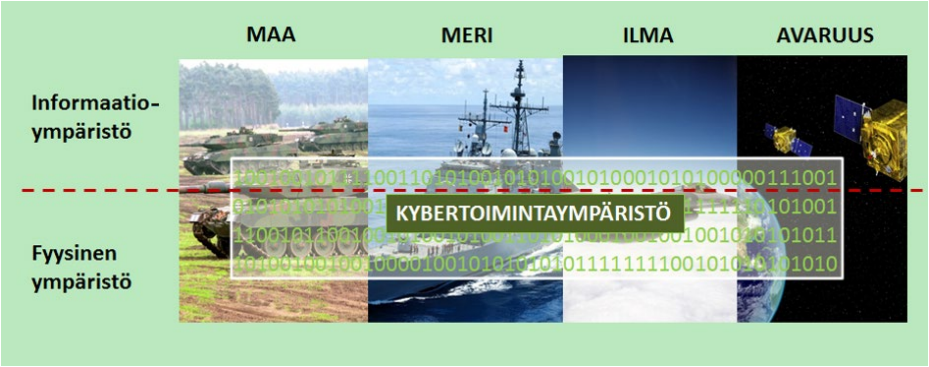
Suomessa Puolustusvoimat kehittää jatkuvasti keinoja parhaan mahdollisen hyödyn saamiseksi kybertoimintaympäristössä. Ympäristön dynaamisen luonteen johdosta usein on kysymyksessä suojautumisen ja vaikuttamisen kilpailu, jossa löydetään uusia haavoittuvuuksia ja niihin kehitetään vastatoimia. Erilaiset toimijat koettelevat jatkuvasti verkostojemme toimintakykyä etsimällä niistä haavoittuvuuksia sekä suorittamalla tietoverkkotiedustelua sotilaallisen ja kaupallinen edun saavuttamiseksi.

Kybertoimintaympäristössä on olemassa useita osa-alueita, jotka on huomioitava tarkasteltaessa kybertoimintaympäristöä sotilaallisena toimintaympäristönä.

- Kybertoimintaympäristö on globaali ja haavoittuva toimintaympäristö.
- Siviili- ja sotilasinfrastruktuurit ovat päällekkäisiä, mikä aiheuttaa vastuunjaolle ja valvonnalle haasteita, mutta tarjoaa myös yhteis toimintamahdollisuuksia.
- Kyberturvallisuus edellyttää korkeaa teknistä lähtötasoa, josta seuraa koulutukseen, harjoitteluun, järjestelmien ylläpitoon ja kybertilannekuvan muodostamiseen liittyviä vaatimuksia.

Kybertoimintaympäristö liittyy osittain muihin aiemmin jo olemassa oleviin toimintaympäristöihin eli maa-, meri-, ilma- ja avaruustoimintaympäristöihin. Kybertoimintaympäristö ei kuitenkaan vastaa täysin niitä, vaan se pikemminkin läpi leikkaa osiltaan kaikkia niitä. Nykyisin missään muissa toimintaympäristöistä ei voida välttää toimintaa kybertoimintaympäristössä. Lisäksi kaikki aiemmat toimintaympäristöt voidaan jakaa teoreettisesti myös informaatio- ja fyysiseen ympäristöön.

Samankaltainen jako on löydettävissä myös kybertoimintaympäristössä, ja näin ollen se ei ole alisteinen informaatioympäristölle vaan informaatioympäristö on osa sitä aivan kuten muitakin toimintaympäristöjä. Lisäksi edellisessä alaluvussa esitetty kybertoimintaympäristön kolmikerroksinen kerrosrakenne kuuluu myös kuvassa 3 esitettyyn kybertoimintaympäristöön, mutta se on jätetty merkitsemättä.



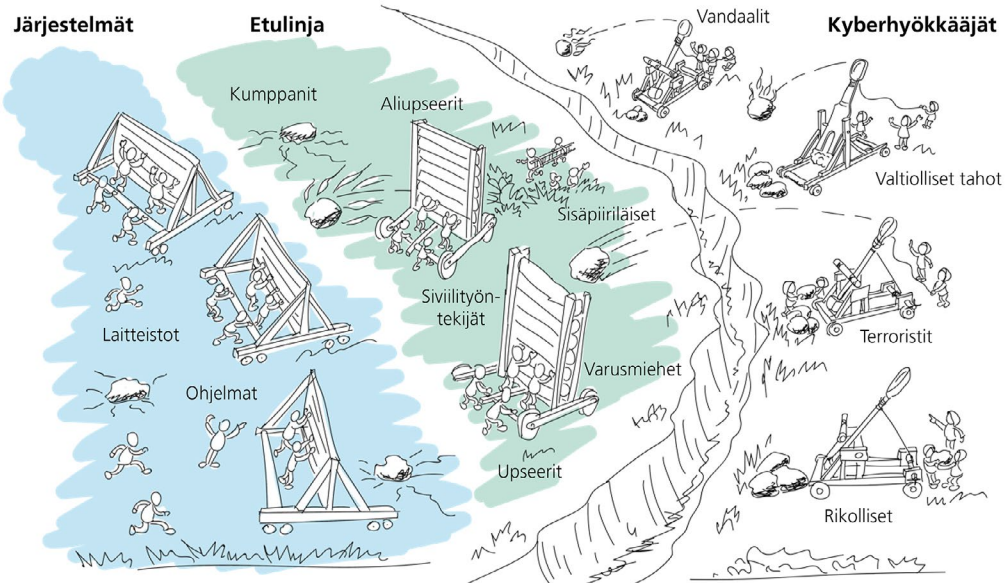
Kuva 3: Sotilaallinen kybertoimintaympäristö

Koko Puolustusvoimien henkilökunnan osaamista kybertoimintaympäristössä kehitetään kaikilla tasoilla tapahtuvalla koulutuksella. Koulutusta kohdennetaan sekä huippuosaajien kykyjen ylläpitoon ja parantamiseen, että peruskäyttäjän ymmärrykseen lisäämiseen. Henkilökunnan odotetaan toimivan tehokkaasti ja turvallisesti kybertoimintaympäristössä. Tämä tarkoittaa sitä, että henkilökunnan tulee osata käyttää ja hyödyntää tietoja ja tietojärjestelmiä sekä osata torjua mahdollisia uhkia. Kybertoimintaympäristön kaikkialla läsnä oleva luonne tarkoittaa sitä, että Puolustusvoimien on otettava huomioon laaja valikoima erilaisia kybertoimintoja ja vaatimuksia turvallisen kybertoimintaympäristön luomiseksi.

Esineiden internetin kehittyminen vaikuttaa kybertoimintaympäristöön myös sotilaallisesta näkökulmasta, esimerkiksi järjestelmien ylläpidon ja kunnossapidon kannalta. Kybertoimintaympäristön ja sen tarjoaminen mahdollisuuksien lisääntyessä paine korvata sillä ihmisten tekemää työtä kustannustehokkuuden parantamiseksi on suuri myös Puolustusvoimissa. Tämä voi tarkoittaa kuitenkin sitä, että järjestelmien kunnossapito ja valvonta toteutetaan etäkäytettävillä yhteyksillä, joista vastaa Puolustusvoimien ulkopuolinen yritys. Kehittyneet järjestelmät kykenevät ennaltaehkäisemään riskejä ja muodostamaan aiempaa paremman tilannekuvan

kokonaisuudesta. Lisäksi parhaimmillaan samanaikaisesti säästetään myös kustannuksia. Asian varjopuolena on, että täysin digitaalinen järjestelmä on haavoittuvainen kybertoimintaympäristön erilaisille uhkille. Näihin uhkiin varautuminen jää yrityksen vastuulle. Lisäksi Puolustusvoimien oman henkilöstön ammattitaito kunnossapitotehtäviin heikkenee.

Kybertoimintaympäristössä tai sen avulla suoritettavia sotilaallisia toimia eli kyberoperaatioita käsitellään tarkemmin luvussa neljä. Kyberoperaatiot vaativat hyvin koulutettuja ja harjoitettuja ammattilaisia, joilla on asianmukaiset kyvyt ja osaaminen. Lisäksi kyberoperaatioiden onnistumiseen tarvitaan sekä teknisten että taktisten asioiden asiantuntijoita ja henkilöstöä, joka ymmärtää ihmisen ajattelua ja käyttäytymistä. Puolustusvoimat rakentaa tämän kaltaista osaamista osana kyberpuolustuksen kehittämistä. Käytännössä tämä tarkoittaa sitä, että puolustusvoimat tarvitsee eri organisaatiotasoille johtajia, jotka hallitsevat kybertoimintaympäristössä tarvittavia kykyjä kuten ohjelmointi, tietokannat, verkkorakenteet, haavoittuvuudet. Toisaalta puolustusvoimat tarvitsee myös näihin ja vastaaviin osa-alueisiin erikoistuneita työntekijöitä, jotka puolestaan ymmärtävät sotilaallisia toimintatapoja ja johtamisrakenteita.



Kuva 4: Puolustusvoimien kybertoimintaympäristö

1.3 Lainsäädäntö kybertoimintaympäristössä

Puolustusvoimien kyberpuolustuksen on aina noudatettava kansainvälistä ja kansallista lainsäädäntöä. Kuitenkaan erillistä tai yhtenäistä kyberlainsäädäntöä ei ole olemassa, vaan asiaan sovellettava normisto määräytyy kulloisenkin toiminnan mukaan. Erityisesti kybertoimintaympäristöä koskevia kansainvälisiä sopimuksiakaan ei ole, mutta voimassa olevaa kansainvälistä oikeutta sovelletaan myös kybertoimintaympäristössä. Rauhan ajan sotilaalliseen toimintaan, kuten koulutukseen ja testaukseen, sekä sotilaallisten operaatioiden tukemiseen tai aseelliseen konfliktiin sovelletaan eri normeja. Myös kyberuhkan laatu, alkuperä tai se, onko kyseessä valtiollinen tai muu toimija, voivat vaikuttaa arviointiin ja säännösten valintaan.

Kansainvälisesti vuonna 2017 ilmestynyt *Tallinn Manual 2.0* on tällä hetkellä ehkä kattavin tutkimus siitä, miten voimassa olevaa kansainvälistä oikeutta voidaan soveltaa ja tulkita kybertoimintaympäristössä. Sen laatimisesta vastasi kansainvälisen oikeuden asiantuntijoista muodostettu ryhmä ja sen valmistelua johti Tallinnassa toimiva Naton kyberpuolustuksen osaamiskeskus CCD COE (NATO Cooperative Cyber Defence Centre of Excellence).

Tallinn Manual 2.0 on tarkoitettu erityisesti käytännön apuvälineeksi lainsoveltajille. Se sisältää 154 asiantuntijaryhmän muotoilemaa kansainvälisen oikeuden sääntöä. Jokaiseen sääntöön liittyy kommentaari, jossa selitetään säännön oikeudellinen perusta ja sen soveltuminen kybertoimintaympäristöön. *Tallinn Manual 2.0* korvaa sitä edeltäneen vuoden 2012 painoksen ja sisältää sen päivityksen. Edellisessä Tallinn Manualissa käsiteltiin valtioiden turvautumista voimankäyttöön sekä aseellisen konfliktin aikana noudatettavia oikeussääntöjä. *Tallinn Manual 2.0* sisältää niiden lisäksi myös kokonaan uuden osuuden, joka koskee kansainvälistä oikeutta ja rauhan ajan kyberoperaatioita eli nykyisellään tavanomaisia ja paljon todennäköisempiä operaatioita. *Tallinn Manual 2.0* on oikeustieteellinen tutkimus, eikä se luonnollisestikaan luo uutta kansainvälistä oikeutta, joka on vain valtioille kuuluva etuoikeus.

Tallinn Manual 2.0 rakentuu ymmärrykselle siitä, että kybersuorituskykyjä edeltävän aikakauden kansainvälistä oikeutta sovelletaan sekä valtioiden toteuttamiin, että niitä vastaan kohdistettuihin kyberoperaatioihin. Kansainvälisen oikeuden varsin järeä järjestelmä säätelee myös kyberoperaatioita. Ne eivät tapahdu oikeudellisessa tyhjiössä, vaan valtioilla on kansainvälisen oikeuden mukaisesti tiettyjä

oikeuksia ja velvollisuuksia.

Kansainvälinen asiantuntijaryhmä päätyi muun muassa seuraaviin johtopäätöksiin:

- Valtioiden harjoittamat kyberoperaatiot voivat loukata kohdevaltion suvereenisuutta, kiellettyä puuttumista toisen valtion sisäisiin asioihin tai voimankäytön kieltoa.
- Valtioilla on velvollisuus kunnioittaa ja suojata kansainvälisiä ihmisoikeuksia, erityisesti sananvapautta ja yksityisyyden suojaa myös kyberoperaatioita toteuttaessaan.
- Mikäli valtio loukkaa kyberoperaatiollaan sille kuuluvia kansainvälisen oikeuden velvoitteita, se kantaa toimistaan kansain välisoikeudellisen vastuun. Sen lisäksi, että valtion on hyvitettävä aiheuttamansa vahinko, voi uhrivaltiolla olla oikeus turvautua tiettyihin vastareaktioihin. Tällaisia ovat esimerkiksi oikeus turvautua yksityiseen tai kollektiiviseen itsepuolustukseen, niin sanotut vastatoimet sekä pakkotilaan perustuvat toimet, jos valtion elintärkeät edut ovat vakavasti uhattuna. Vastareaktion tulee aina täyttää juuri sille vastaustyypille asetetut oikeudelliset edellytykset. Esimerkiksi jotta valtio voisi käyttää vastauksena kyberoperaatioon aseellista voimaa, tulee alkuperäisen operaation olla aseellisen hyökkäyksen tasalla. Valtaosa kyberoperaatioista ei koskaan ylitä aseellisen hyökkäyksen kynnystä, jolloin kyseeseen voivat tulla olosuhteista riippuen muut kansainvälisen oikeuden mukaiset reaktiot.
- Valtiolla on velvollisuus varmistaa, ettei sen aluetta käytetä kolmansien osapuolten toimesta tavalla, joka aiheuttaa vaka vaa haittaa muille valtioille. Periaate ei tarkoita sitä, että valtion tulee aktiivisesti tarkkailla kaikkia sen kybertoimintaympäristössä tapahtuvia toimia. Pikemminkin se edellyttää, että valtio tekee sen, mikä on kohtuudella sen vallassa päättääkseen sen alueen kautta kulkeutuvat muita valtioita vahingoittavat toimet sen jälkeen, kun se on tullut niistä tietoisiksi.

Kansainvälinen oikeus koskee ensisijaisesti valtioiden välisiä suhteita. Kansainvälisen oikeuden säännöt voivat kuitenkin tietyissä olosuhteissa ulottua myös ei-valtiollisiin toimijoihin. Valtiot voivat esimerkiksi toimia itsepuolustuksellisesti kohda-

tessaan tiettyjä erityisen vahingollisia terroristiryhmien kyberhyökkäyksiä. Lisäksi, mikäli valtio käyttää tietynasteista kontrollia ei-valtiolliseen toimijaan nähden, voidaan ei-valtiollisen toimijan toimet johtaa kyseessä olevaan valtioon valtiovastuuseen kuuluvan syyksiluettavuuden periaatteen mukaisesti. Tärkeimmät kansainvälisen oikeuden käsitteet ovat seuraavissa taulukoissa.

Useat valtiot ovat omissa kannanotoissaan ottaneet kantaa kybertoimintaympäristön kansainvälisen lainsäädännön tulkinnanvaraisuuteen ja puutteisiin. Esimerkiksi Yhdysvallat ja Iso-Britannia ovat ilmoittaneet varaavansa itselleen oikeuden käyttää tarvittaessa kineettistä voimaa vastaamaan niitä vastaan kohdistettuihin kyberhyökkäyksiin. On selvää, että kansainvälisen oikeuden tulkinnat tulevat vahvistumaan, kun valtiot muodostavat asiasta soveltamiskäytäntöä.

Laiton interventio (unlawful intervention)	Tapaoikeudellinen kansainvälisen oikeuden periaate kieltää valtioita puuttumasta toisten valtioiden sisäisiin asioihin. Periaate kieltää toiseen valtioon kohdistuvat pakottamistarkoituksessa tehdyt toimet, joilla puututaan asioihin, joista kukin valtio voi itsenäisesti päättää. Tällaisia valtion sisäisiä asioita ovat esimerkiksi maan yhteiskunta-, talous- ja kulttuurijärjestelmä sekä se, miten valtio toteuttaa ulkopolitiikkaansa. Kyberoperaatio, joka ei täytä voimankäytön tai aseellisen hyökkäyksen määritelmää, voi rikkoa sisäisiin asioihin puuttumisen kieltoa.
Vastatoimet (countermeasures)	Mikäli valtio syyllistyy kyberoperaatiollaan kansainvälisen oikeuden velvoitteiden vastaiseen tekoon, voi uhrivaltiolla olla oikeus turvautua tiettyihin vastareaktioihin, kuten oikeasuhtaisiin vastatoimiin (countermeasures). Vastatoimien tulee olla suhteellisia: ne eivät saa olla kostonluonteisia eivätkä ne saa sisältää voimankäyttöä. Tämä tarkoittaa sitä, että niiden tarkoituksena voi olla ainoastaan kansainvälisen oikeuden velvoitteita vastoin toimivan valtion taivuttaminen noudattamaan jälleen kansainvälistä oikeutta.
Valtiovastuu (principle of state responsibility)	Valtio on kansainvälisoikeudellisessa vastuussa toimistaan. Tämä periaate koskee myös kybertoimintaympäristöä. Jos valtio avustaa toista valtiota, avustavan valtion on arvioitava avustettavan valtion toiminnan laillisuus. Jos avustava valtio katsoisi, että toiminta on kansainvälisen oikeuden vastaista, voisi se itse joutua vastaamaan toimesta kansainvälisen oikeuden mukaisesti.
Voimankäytön tai sillä uhkaamisen kielto (prohibition on the threat or use of force)	Yhdistyneiden kansakuntien peruskirjan 2 artiklan 4 kappaleen mukaan kaikkien jäsenmaiden on pidätyttävä kansainvälisissä suhteissaan väkivallalla uhkaamisesta tai sen käyttämisestä. Tämä sääntö on myös yleisesti hyväksytty kansainvälisen tapaoikeuden normiksi. Jotta kyberoperaatio rinnastettaisiin aseelliseen voimankäyttöön, sen tulee aiheuttaa samankaltaisia vaikutuksia kuin aseellisen voimankäyttö.
Aseellinen hyökkäys (armed attack)	Kansainvälisessä oikeudessa ei ole määritelty aseellista hyökkäystä, mutta on yleisesti hyväksytty, että sen tulee olla mittasuhteiltaan ja vaikutuksiltaan riittävän vakava. Kyberoperaatio voi ylittää aseellisen hyökkäyksen kynnyksen, mikäli se on toteuttamistavaltaan, vakavuudeltaan tai voimankäytön voimakkuudeltaan sellainen, että vaikutukset ovat verrannolliset kineettiseen aseelliseen hyökkäykseen.

Taulukko 4: Kansainvälisen oikeuden käsitteitä 1

Itsepuolustus (self-defence)	Luonnollinen oikeus yksilölliseen ja kollektiiviseen itsepuolustukseen on tunnustettu kansainvälisessä tapaoikeudessa ja Yhdistyneiden kansakuntien peruskirjan 51 artiklassa. Aseellinen hyökkäys tai sen välitön uhka oikeuttavat itsepuolustuksellisen voimankäytön. Itsepuolustusoikeutta rajoittaa aina suhteellisuusperiaate: asevoimaa voidaan käyttää vain hyökkäyksen torjumiseksi ja välittömän uhan poistamiseksi. Kybertoimintaympäristössä itsepuolustukselle haasteita aiheuttavat: • Syyksiluettavuuden (attribuution) ongelma, hyökkäyksen alkuperän ja mahdollisen toisen valtion osallisuuden osoittaminen. • Kyberhyökkäyksen nopeus, joka vaikeuttaa kykyä vastata välittömään uhkaan. • Hyökkääjän jälkien salaaminen ja harhauttaminen, joiden avulla syyllisyys voidaan yrittää häivyttää tai siirtää toiselle. • Tekijän tietyn tarkoituksen näyttäminen, vaikka toimet olisivat todistettavissa ja toimijat tunnistettavissa.
Sodan oikeussäännöt (law of armed conflict)	Aseellisen konfliktin aikana toteutettuihin tai aseelliseen konfliktiin liittyviin kyberoperaatioihin sovelletaan sodan oikeussääntöjä, kuten sotapetoksen kieltoa ja puolueettomuuden periaatetta. Sotapetoksia ovat teot, jotka herättävät petollisesti luottamusta kansainvälisen oikeuden antamaan suojaan. Aseellisen konfliktin aikana toteutettavissa voimakäyttöä käsittävissä kyberoperaatioissa tulee noudattaa seuraavia periaatteita: • Sotilaallinen välttämättömyys. Valtio voi käyttää voimaa vain siinä määrin ja sellaisin keinoin, joita ei ole muutoin sodan oikeussäännöissä kielletty, ja mikä on välttämätöntä vihollisen täydelliseksi tai osittaiseksi lyömiseksi mahdollisimman nopeasti ja pienimmillä mahdollisilla materiaali- ja henkilöstötappioilla. • Erottelu. Vihollisuuksia saa kohdistaa ainoastaan sotilaskohteita vastaan; siviilejä ja siviilikohteita vastaan ei saa hyökätä. Sotilaskohteita ovat kohteet, joiden luonne, sijainti, tarkoitus tai käyttö muodostaa tärkeän osan sotilaallista toimintaa ja joiden täydellinen tai osittainen tuhoaminen, haltuunotto tai vaarattomaksi saattaminen merkitsee kulloinkin vallitsevissa olosuhteissa ratkaisevaa sotilaallista hyötyä. • Suhteellisuus. Teko on suhteellinen, jos siitä ei aiheudu liiallisia oheisvahinkoja siviileille ja siviilikohteille verrattuna saavutettuun sotilaalliseen hyötyyn. • Inhimillisen kohtelun periaate. Liiallisten vammojen ja tarpeettoman kärsimyksen aiheuttaminen on kielletty.
Taistelumenetelmät ja suojellut kohteet (methods of war and protections)	Taistelumenetelmien ja -välineiden käyttökiellot soveltuvat yhtä lailla kybertoimintoihin kuin perinteiseen sodankäyntiinkin. Alla on kaksi esimerkkiä, mutta listaa ei ole tarkoitettu tyhjentäväksi: • Kiellettyä on sellainen väkivallan käyttö tai väkivallalla uhkaaminen, jonka ensisijaisena tarkoituksena on levittää kauhua siviiliväestön keskuudessa. • Asevoimaa ei saa kohdistaa vaarallisia voimia sisältäviä laitoksia eli ydinvoimaloita ja suojapatoja vastaan, jos ne voivat tuhoutuessaan vapauttaa suuria ja vaarallisia voimia, joiden seurauksena aiheutuu vakavia siviiliuhreja. Myöskään muita sotilaskohteita, jotka sijaitsevat em. kohteissa tai niiden välittömässä läheisyydessä, ei tulisi ottaa hyökkäyksen kohteeksi, jos uhkana on, että hyökkäyksestä voi aiheutua vaarallisten voimien vapautumista.

Taulukko 5: Kansainvälisen oikeuden käsitteitä 2

Kansallinen lainsäädäntö toteaa kybertoimintaympäristöstä seuraavia asioita. Alueellinen toimivalta eli suvereniteetti antaa valtiolle muun muassa oikeuden kontrolloida sen alueella sijaitsevaa kyberinfrastruktuuria ja siinä tapahtuvaa toimintaa. Nämä kuuluvat kansallisen lainsäädännön piiriin. Kyberuhkat myös tyypillisesti ylittävät valtioiden rajat. Kansainvälinen oikeus, Suomen solmimat kansainväliset sopimukset sekä Euroopan unionin lainsäädäntö sääntelevät osaltaan rajat ylittävää toimintaa.

Kuten edellä todettiin, lainsäädännössä ei ole yhtenäistä säädöspohjaa, joka koskisi kaikkia kybertoimintoja, vaan useat tekijät vaikuttavat kulloinkin sovellettavan säädöksen valintaan. Kansallisesti oikeudelliseen arviointiin vaikuttavat myös eri hallinnonalojen eriytyneet toimivaltuudet, vaikka uhkat voivatkin kohdistua kaikkiin yhteiskunnan toimintoihin. Sinänsä sama tai samalta vaikuttava toimi voi myös tulla tekijästä ja alkuperästä riippuen oikeudellisesti arvioitavaksi joko yksittäisenä rikoksena, laajempana terrorismirikoksena tai jopa sotilaallisen puolustuksen näkökulmasta.

Puolustusvoimien kannalta keskeisiä, myös kybertoimintaympäristöön liittyviä säännöksiä sisältyy muun muassa seuraaviin säädöksiin:

- laki Puolustusvoimista 11.5.2007/551
- laki Puolustusvoimien virka-avusta poliisille 5.12.1980/781
- laki sotilaskurinpidosta ja rikostorjunnasta Puolustusvoimissa 28.3.2014/255
- aluevalvontalaki 18.8.2000/755
- valmiuslaki 29.12.2011/1552
- puolustustilalaki 22.7.1991/1083
- laki julkisen hallinnon tiedonhallinnasta 906/ 2019
- laki sähköisen viestinnän palveluista 7.11.2014/917
- laki julkisen hallinnon turvallisuusverkkotoiminnasta 13.1.2015/10
- rikoslaki 19.12.1889/39, 38 luku Tieto- ja viestintärikoksista
- laki sotilastiedustelusta 26.4.2019/590

1.4 Kehitys maailmalla

Kybertoimintaympäristö kehittyy hurjaa vauhtia, menneitä aikoja on turha kaivata ja historiasta on syytä ottaa oppia. Tämän kehityksen ymmärtämiseksi tässä alaluvussa esitellään muutamia tärkeitä tapahtumia, jotka ovat omalta osaltaan vaikuttaneet siihen, millainen kybertoimintaympäristö on tällä hetkellä. Tapahtumien esittely perustuu julkisissa lähteissä esitettyihin faktoihin, jotka voivat kuitenkin poiketa siitä mitä todellisuudessa on tapahtunut. Erityisesti julkisuuteen päätyneitä sotilaallisia kyberoperaatioita voidaan pitää osin epäonnistuneina sen takia, että operaatio on laajasti paljastunut. Lisäksi kybertapahtumilla on usein paljon laajempia seuraamuksia kuin ainoastaan yksittäisen hyökkäyksen välittömät vaikutukset.

Vuonna 2007 Viron valtion tietoverkot joutuivat laajan palvelunestohyökkäyksen kohteeksi. Hyökkäys oli seurausta sotamuistomerkin siirtämisestä ja siitä aiheutuneista kiistoista. Hyökkäyksen seurauksena valtion ja pankkien internetpalvelut olivat poissa käytöstä. Tämä tapahtuma toimi voimakkaana kannustimena Viron kyberosaamisen ja -turvallisuuden kehittämisessä sekä kiihdytti kansainvälistä keskustelua kybertoimintaympäristöstä ja siinä tapahtuvista toiminnoista.

Vuonna 2007 Israelin asevoimat toteuttivat operaatio Orchardin. Siinä ilmavoimat tekivät Syyrian ydintutkimuslaitosta vastaan ilmaiskun, joka mahdollistettiin erikoisjoukoilla sekä ilmapuolustusjärjestelmää vastaan tehdyllä kyberoperaatiolla. Operaatio on esitelty luvun 4.4 taulukossa 23.

Kesällä 2008 Georgian sodan yhteydessä georgialaisiin tietoverkkoihin tunkeuduttiin. Vaikka hyökkäys aiheutti ainoastaan vähäisiä häiriöitä palveluihin, Venäjän asevoimien hyökkäyksen rinnalla se muodosti huomattavaa painetta Georgian valtion johdolle. Nämä Syyrian ja Georgian tapahtumat toimivat esimerkkinä siitä, kuinka kyberoperaatiot ovat olleet osa asevoimien toimintaa ja sodankäyntiä jo yli vuosikymmenen ajan.

Vuoden 2009 alussa Israelin ja Hamasin väkivalta yltyi sodaksi ja Israelin armeija hyökkäsi Gazaan. Samanaikaisesti israelilaisia tietoverkkoja ja erityisesti Israelin hallituksen internetsivuja vastaan kohdistettiin kyberhyökkäys vähintään viidellä miljoonalla tietokoneella. Tapahtuma toimii esimerkkinä siitä, kuinka sotilaallisesti alivoimainen osapuoli voi hyödyntää kybertoimintaympäristöä omien päämäärien-sä tavoittelussa.

Maailman toistaiseksi kuuluisin kyberhyökkäys on vuodelta 2010 ja se tunnetaan nimellä Stuxnet. Se oli kyberoperaatio, jossa iranilaiseen Natanzin ydinvoimalaan ujutettiin haittaohjelma muistitikulla. Sen seurauksena ydinvoimalan toiminta häiriintyi, mutta samalla se myös kannusti Irania kyberpuolustuksensa kehittämiseen. Tämä operaatio on esitelty luvussa 2.1 taulukossa 9.

Vuonna 2013 entinen CIA:n työntekijä Edward Snowden kopioi ja levitti suuren määrän salaisia NSA:ta (US National Security Agency) koskevia tietoja. Tämän vaikutuksesta yleiseen tietoon tuli useita valtion käyttämiä salaisia tiedonhankintamenetelmiä, joita myöhemmin on hyödynnetty esimerkiksi kyberrikollisuudessa. Lisäksi Snowdenin vuotamat tiedot heikensivät ihmisten uskoa valtionhallintoon erityisesti Yhdysvalloissa.

Sotilaallisesta näkökulmasta yksi merkityksellisimmistä kybertoimintaympäristöön liittyvistä tapahtumista on vuodelta 2015. Asia tuli julkisuuteen noin vuotta myöhemmin, kun Yhdysvaltojen asevoimat kertoi ottaneensa käyttöön kybertoimintaympäristön sotilaallisena hyökkäysväylänä taistelussa terroristijärjestö Isisiä vastaan. Asia tuotiin julkisesti esille operaatioiden toteuduttua. Tämä oli ensimmäinen kerta, kun minkään valtion asevoimat julisti käyttävänsä kybertoimintaympäristöä sodankäynnissä muiden toimintaympäristöjen rinnalla. Yhtenä käytännön esimerkkinä tästä voidaan pitää Yhdysvaltojen asevoimien suorittamaa lennokki-iskua, jonka avulla surmattiin Isis-järjestön tärkeimpänä hakkerina pidetty Junaid Hussain vuonna 2015. Verkoissa tapahtuneista operaatioista ei ole kerrottu tietoja.

Sotilaallisesta näkökulmasta toinen tähän mennessä merkityksellisimmistä kybertoimintaympäristöön liittyvistä tapahtumista on kesältä 2016, kun Nato julisti Varsovan huippukokouksessa, että kybertoimintaympäristö on samankaltainen sotilaallinen toimintaympäristö kuin perinteisemmät maa-, meri-, ilma- ja avaruustoimintaympäristöt. Lisäksi Nato velvoitti luomaan sellaiset kyvyt, joilla kybertoimintaympäristössä pystytään taistelemaan ja puolustautumaan kuten muissakin toimintaympäristöissä.

Vuonna 2017 tapahtui maailman ensimmäinen laajasti julkisuutta saanut kiristyshaittaohjelmahyökkäys. WannaCry -kiristyshaittaohjelma saastutti yhdessä päivässä yli 230 000 tietokonetta yli 150 valtiossa. Se aloitti samalla hyvin laajalle levinneen kiristyshaittaohjelmahyökkäysten sarjan. Myöhemmin samana vuonna koettiin uudenlainen yli 12 500 Microsoftin käyttöjärjestelmää käyttäneeseen tie-

tokoneeseen kohdistunut kiristyshaittaohjelmahyökkäys NotPetya. Sen erikoisuutena oli se, että tiedostojen salaamisen lisäksi NotPetya esti käytännössä tietokoneiden käytön kokonaan. Kiristyshaittaohjelmia on esitelty tarkemmin luvussa 2 ja NotPetya liittyvä operaatio on esitelty luvun 2.4 taulukossa 13.

Maailman toistaiseksi suurin yksittäinen julkaistu tietovuoto on vuoden 2019 alussa julkaistu Collection #1 -aineisto, jossa 773 miljoonan sähköpostiosoitteen salasanat julkaistiin internetissä. Toistaiseksi suurimpana tietomurtona pidetään vuosina 2013–2014 Yahoota vastaan tapahtunutta tietomurtoa, jossa hakkeriryhmä onnistui samaan pääsyn kaikkien kolmen miljardin käyttäjän tiedostoihin.

Sotilaallisen kybertoimintaympäristön näkökulmasta myös kesällä 2019 Israelin Hamasia vastaan toteuttamaa ilmaiskua voidaan pitää merkittävänä tapahtumana. Israel suuntasi ilmaiskun Hamas-järjestön kybertoimijoita vastaan saatuaan ensin puolustuksellisella kyberoperaatiolla estettyä Hamasin kyberhyökkäyksen ja sen jälkeen selville sen tekijät ja heidän sijaintinsa. Se oli ensimmäinen kerta, kun kyberhyökkäykseen tai sen välittömään uhkaan vastattiin välittömästi tuli-iskulla.

Kybertoimintaympäristöön liittyviä tapahtumia on olemassa runsaasti. Edellä esimerkiksi esitetyillä tapahtumilla on kuvattu ainoastaan kybertoimintaympäristön kehitystä. Hyvinkin todennäköisesti pystymme ymmärtämään erilaisten tapahtumien todellisen merkityksen vasta useita vuosia tapahtumien jälkeen, ja näin ollen tapahtumien tulkinnat voivat olla kymmenen vuoden kuluttua täysin erilaisia.

Viron patsas -kriisi (2007)	Viron tietoverkot joutuivat laajan palvelunestohyökkäyksen kohteeksi.
Operaatio Orchard (2007)	Israelin ilmaisku Syyrian kyberoperaation tukemana.
Gazan kriisi (2009)	Israelin ja Hamasin väkivalta yltyi sodaksi. Israel hyökkäsi Gazaan ja joutui laajan palvelunestohyökkäyksen kohteeksi.
Stuxnet (2010)	Kyberoperaatio iranilaista ydinvoimalaa vastaan.
Snowdenin paljastukset (2013)	Snowden kopioi ja levitti suuren määrän salaisia NSA:ta koskevia tietoja.
Operaatio ISIS:iä vastaan (2015)	Yhdysvaltojen asevoimat otti käyttöön kybertoimintaympäristön sotilaallisena hyökkäysväylänä taistelussa terroristijärjestö Isisiä vastaan.
Kyberistä viides sotilaallinen toimintaympäristö (2016)	Nato julisti Varsovan huippukokouksessa, että kybertoimintaympäristö sotilaallinen toimintaympäristö.
WannaCry (2017)	Maailman ensimmäinen laajasti julkisuutta saanut kiristyshaittaohjelmahyökkäys WannaCry saastutti yhdessä päivässä 230 000 tietokonetta yli 150 valtiossa.
Collection #1 (2019)	Maailman toistaiseksi suurimmassa yksittäisessä julkaistussa tietovuodossa Collection #1:ssä 773 miljoonan sähköpostin salasanat vuodettiin julkisuuteen.
Ilmaisku Hamasia vastaan (2019)	Israelin asevoimat havaitsivat ja estivät Hamas-järjestön kyberhyökkäyksen. Samalla Israelin asevoimat onnistuivat selvittämään Hamasin kyberhyökkääjien sijainnin, jota vastaan suoritettiin välittömästi ilmaisku. Se oli ensimmäinen kerta, kun kyberhyökkäykseen tai sen välittömään uhkaan vastattiin välittömästi sotilaallisella voimankäytöllä.

Taulukko 6: Kybertoimintaympäristön kehitykseen vaikuttaneita tapahtumia

2 #UHKA

Uutta teknologiaa on otettu käyttöön laajasti yhteiskunnan eri osa-alueilla ja toiminnoissa. Samalla digitalisaatio on luonut uusia uhkia siitä riippuville toiminnoille. Teknologian kautta kohdistuvia uhkia voidaan kutsua kyberuhkiksi. Yhä useammat yritykset, organisaatiot ja yksityishenkilöt voivat joutua kyberuhkien kohteiksi, ja uhkan on arvioitu kasvavan vuosi vuodelta.

Tässä luvussa kuvataan kybertoimintaympäristön kautta tai sen avulla muodostuvia uhkia. Erilaisia kyberuhkia ja niiden kehitystä kuvataan toimijoiden, tekniikan ja vaikutusten näkökulmasta. Lukuun perehdyttyään lukijalla tulisi olla selkeä ymmärrys siitä, millaisia kybertoimintaympäristön uhkat ovat.

2.1 Kyberuhka osana teknologian kehitystä

Pääosa käyttämistämme digitaalisista järjestelmistä sisältää haavoittuvuuksia, vaikka läheskään kaikkiin niistä ei kohdistu suoraan hyökkäyksen kohteiksi joutumisen uhkaa. Valtaosa ihmisistä kokee vain hetkenkin kestävän internetyhteyden menettämisen omassa kodissaan kiusallisena, mutta sähköpostitiliin murtautuminen tai henkilökohtaisten tietojen varastaminen on vakavuudessaan aivan eri luokkaa. Kybertoimintaympäristössä tapahtuva hyökkäys, joka johtaa sähköverkon tai puolustusalan tietoverkkojen ja kybertoimintaympäristöstä riippuvaisten kykyjen pitkäaikaiseen menetykseen, voi aiheuttaa vakavia seurauksia. Niihin voi kuulua sekä ihmishenkien menetyksiä, että jopa kohteeksi joutuneen valtion sotilaallisia vastatoimia.

Uhka	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku. Sotilaallisesti uhka esitetään usein muodossa uhka = kyky x tahto.
Tietoturvauhka	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu tietoturvaan ja toteutuessaan vaarantaa sen.
Kyberuhka	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon. Kyberuhkat voivat aiheutua paitsi toteutuneista tietoturvauhkista myös digitaalisessa viestintäympäristössä toteutettavista, yhteiskunnan turvallisuutta vaarantavista teoista.
Haavoittuvuus	Alttius uhkille. Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa.
Nollapäivä-haavoittuvuus	Nollapäivähaavoittuvuus on tietojärjestelmässä haavoittuvuus, joka ei ole yleisesti tiedossa ja johon ei ole saatavilla korjausta.
Hakkeri	Henkilö, joka tunkeutuu tai vaikuttaa tietoverkkoon, tietojärjestelmään tai niiden sisältämään tietoon ja käyttää ohjelmaa, palvelua tai muita resursseja.

Taulukko 7: Yleisiä uhkaan liittyviä käsitteitä

Kybertoimintaympäristöä hyödynnetään myös rikollisuudessa ja vakoilussa, sillä niissä käytettävät menetelmät ovat suhteellisen halpoja kehittää tai ostaa ja kiinnijäämisen riski on alhainen verrattuna perinteisiin rikollisiin menetelmiin. Kybertoimintaympäristössä tapausten liittäminen aukottomasti tiettyyn toimijaan on yleensä vaikeaa ja se lisää kybertoimintaympäristön houkuttelevuutta laittomaan toimintaan ja kasvattaa kyberuhkan yleisyyttä.

Tietoturvan näkökulmasta kyberuhka voi kohdistua tiedon luottamuksellisuuteen, tiedon eheyteen tai tiedon saatavuuteen. Tästä kolmijaosta puhutaan tietoturvan CIA-mallina. Tiedon luotettavuus vaarantuu, jos ulkopuoliset tahot pääsevät käsiksi tietoon, johon heillä ei tulisi olla pääsyä. Tiedon eheys vaarantuu, jos tieto voi muuttua joko teknisen virheen takia tai ihmisen aiheuttamana, eikä paikkansa pitävyyteen voida luottaa. Tiedon saatavuus vaarantuu, jos tieto ei ole tarvitsijoiden saatavilla tarvittavana aikana. Tietoturvan näkökulmasta tehdyn luokittelun lisäksi kyberuhkat voivat kohdistua myös fyysiseen maailmaan, jos kybermenetelmillä kyetään vaikuttamaan järjestelmien toimintaan ja aiheuttamaan fyysistä tuhoa. Kyberuhka ei ole kohdeorganisaatioille erillinen, tekninen ilmiö, vaan sillä voi olla merkittäviä vaikutuksia organisaation ydintoimintaan.

Luottamuksellisuus (confidentiality)	Kukaan sivullinen ei saa tietoa.
Eheys (integrity)	Tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa.
Saatavuus (availability)	Tieto on hyödynnettävissä haluttuna aikana.

Taulukko 8: Tietoturvan CIA-malli

Ilmiönä kyberuhka ei ole uusi, joskin sitä tarkoittava termi on vuosien mittaan vaihtunutkin. Ensimmäisiä tietokoneviruksia havaittiin jo 1980-luvulla, mutta tuolloin haittaohjelmien tuottajien motiivit erosivat nykypäivän kyberuhkista huomattavasti. Vaikka virusten vaikuttavuus kohdejärjestelmiin saattoi kohdistua luottamuksellisuuteen, eheyteen tai saatavuuteen, yleensä toimijan motiivina oli halu näyttää osaamisensa tai mahdollisuus vaikuttaa kohdejärjestelmään. Kuitenkaan kyberuhkien historia ei ole yhtenevä haittaohjelmien historian kanssa. Vaikka haittaohjelma- ja virustehtailijat tuottivat ohjelmia omaksi huvikseen, pidetään vuonna 1986 paljastunutta verkkovakoilutapausta yhtenä ensimmäisistä tietoverkon kautta tapahtuneista vakoiluista. Hyökkäyksessä ulkomaalainen toimija onnistui tunkeutumaan yhdysvaltalaisiin sotilaskohteisiin etsiäkseen tietoa ydinaseista ja ohjuspuolustuksesta. Hyökkääjä väitetysti myi haltuunsa saamat tiedot Neuvostoliiton KGB:lle. Tapahtumaa ja siitä kirjoitettua kirjaa *Cuckoo's Egg* on esitelty tarkemmin luvussa 4.3 taulukossa 19.

Viime vuosikymmenien aikana erityisesti verkossa tapahtuvan vakoilun ja haitanteon menetelmät, tekniikat sekä keinot ovat monipuolistuneet ja edistyneet. Tämän vuosituhannen uutena ilmiönä on havaittu kybertoimintaympäristön käyttö fyysisen vaikutuksen saamiseksi. Vuonna 2010 paljastunutta ja edellisessä luvussa mainittua Stuxnet-operaatiota pidetään ensimmäisenä valtiollisen tason operaationa, jonka tarkoituksena oli vaikuttaa fyysiseen maailmaan suoraan kybertoimintaympäristön keinoin. Operaatiossa pyrittiin hidastamaan Iranin ydinaseohjelmaa vaikuttamalla ydinlaitosten toiminnanohjausjärjestelmään. Stuxnet-operaatio on esitetty taulukossa 9.

Kuka?	The New York Timesin artikkelissa (1.6.2012) kettottin, että Stuxnet on osa Yhdysvaltojen ja Israelin tiedusteluoperaatiota nimeltä Olympic games.
Mitä?	Kyberoperaatio Iranissa sijaitsevaa Natanzin ydinlaitosta vastaan tavoitteena uraanin rikastukseen käytettävien tietokonejärjestelmien häirintä ja prosessin vahingoittaminen.
Miten?	Stuxnetin pääsy järjestelmään tapahtui luultavasti muistitikulla, koska tietokoneita ei ollut kytketty turvallisuussyistä internettiin. Mato hyökkäsi Windows-käyttöjärjestelmää vastaan hyödyntäen neljää haavoittuvuutta, joista kaksi oli ennalta tuntemattomia nollapäivähaavoittuvuuksia.
Kohde?	Iranin Natanzin rikastuslaitos.
Miksi?	Iranin ydinaseohjelman hidastaminen.
Milloin?	Stuxnetin alkuperäinen versio marraskuu 2008, varsinainen hyökkäys havaittiin 17.7.2010.
Vaikutus	Noin 1 000 uraanin rikastumiseen tarkoitettua sentrifugia tuhoutui. Lisäksi mato saastutti noin 100 000 muuta kohdetta ympäri maailmaa kuitenkin ilman merkittäviä vaikutuksia.
Lisätiedot	https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

Taulukko 9: Esimerkki Stuxnet - maailman kuuluisin kyberhyökkäys

2.2 Uhkatoimijat

Kyberuhkatoimijat voidaan jakaa toiminnan tavoitteiden ja käytössä olevien resurssien mukaisesti seuraaviin kategorioihin:

- kybervandaalit
- kyberrikolliset
- kyberterroristit
- valtiolliset toimijat

Kybervandaalit käyttävät kybertoimintaympäristöä ideologiansa levittämiseen, osaamisensa esittelyyn ja usein aiheuttaakseen häiriöitä tai tuhoa. Kybervandalismia ei tule sekoittaa haktivismiin, jossa vandaaleista poiketen usein tavoitteena on tuhon ja häiriön sijaan huomion herättäminen. Kybervandalismissa toiminnan on yleensä tarkoitus olla näkyvää ja siihen voi kuulua esimerkiksi verkkosivujen sotkemista. Toiminnan kohde valikoituu usein osittain satunnaisesti sen perusteella, mihin tietojärjestelmiin kybervandaalit kykenevät tunkeutumaan.

Kyberrikolliset tavoittelevat kybertoimintaympäristön avulla taloudellista hyötyä. Ihmisten siirtyessä jatkuvasti yhä enemmän hyödyntämään kybertoimintaympäristön tarjoamia mahdollisuuksia, myös raha seuraa kybertoimintaympäristöön ja sen myötä myös rikollisuus. Kyberrikollisten kohteena voivat olla esimerkiksi pankkien maksujärjestelmät ja verkkopankit, mutta myös yksityishenkilöt. Rikoshyötyä voidaan tavoitella esimerkiksi erilaisilla nettihuijauksilla, joissa kohde huijataan lähettämään rahaa huijarille tai kiristyshaittaohjelmilla, jotka estävät käyttäjän pääsyn omiin tietoihinsa, jos käyttäjä ei maksa vaadittua rahasummaa. Kyberrikollisten kohteet valikoituvat usein hyöty-kustannusanalyysin perusteella, jolloin oma vaiva ja ajankäyttö pyritään minimoimaan ja saadut voitot vastaavasti maksimoimaan. Kyberrikolliset myyvät nykyään toimintaa myös palveluna (cybercrime as a service, CaaS).

Kyberterroristeilla tarkoitetaan terroristeja, jotka käyttävät terroritekojen välineenä kybertoimintaympäristöä. Toistaiseksi kyberterrorismi ei ole yleistynyt eikä merkittäviä terroritekoja ole toteutettu kybermenetelmien avulla, vaikka terroristit hyödyntävätkin uusinta teknologiaa esimerkiksi propagandan välittämiseen ja uusien jäsenten rekrytoimiseen. Yhdenlaisena kyberterrorismin uhkana tulevaisuudessa voikin olla kyberkeinojen yhdistäminen perinteiseen terrorismiin. Esimerkiksi

pommi-iskun vaikutuksia voidaan pahentaa entisestään suuntaamalla samanaikaisesti palvelunestohyökkäys terveydenhuollon tai viranomaisten tietojärjestelmiin, joilla häiritään tilanteen hallitsemista ja ensiapua.

Valtiolliset toimijat hyödyntävät kybertoimintaympäristöä osana tiedustelua ja sodankäyntiä. Valtiollisiksi toimijoiksi voidaan virallisten toimijoiden lisäksi usein myös mieltää erilaiset järjestäytyneet ryhmittymät, jotka toimivat valtiollisten toimijoiden kaltaisilla resursseilla ja kyvyillä, ja joilla koetaan olevan jonkinlainen yhteys virallisiin toimijoihin. Useat ulkomaiset tiedustelupalvelut ovat kehittäneet edistyneitä kybertiedustelumenetelmiä, joilla voidaan kerätä tiedustelutietoa valituista kohdejärjestelmistä. Kybertiedustelua on usein erittäin vaikea havaita, sillä tiedustelumenetelmistä kehitetään tarkoituksella sellaisia, etteivät tietoturvatuotteet ja -järjestelmät havaitsisi niitä. Kybervakoilulla voidaan kerätä tietojärjestelmissä käytännössä kaikkea niissä olevaa tietoa: -asiakirjoja, sähköpostikirjeenvaihtoa ja käyttäjätietoa. Lisäksi voidaan salakuunnella ja -katsella tiloja tietokoneiden ja muiden laitteiden sisäisten mikrofonien ja kameroiden kautta. Älylaitteiden yleistymisen myötä myös kybervakoilulla saatavan tiedon määrä on lisääntynyt ja erityisesti älypuhelimet ovat viime aikoina olleet kybervakoilun suosiossa. Vakoilussa kybermenetelmien etuna suhteessa muihin menetelmiin on muun muassa alhainen hinta, pieni riski ja toiminnan alkuperän kiistämisen helppous. Kybervakoilu kohdistuu usein organisaatioiden virallisten tietojärjestelmien lisäksi henkilökohtaisiin laitteisiin. Lisäksi yritysten tuote- ja liikesalaisuudet ovat usein kybervakoilun kohteena. Kybervakoilua tuetaan muilla menetelmillä kuten henkilötiedustelulla, avoimien lähteiden tiedustelulla ja sosiaalisen median tiedustelulla.

Kybervakoilun lisäksi valtiolliset toimijat, usein asevoimat, kehittävät kybersuorituskykyjä osaksi sotilaallista voimankäyttöä. Kybervaikuttamismenetelmien etuja ovat lähes rajoittamaton maantieteellinen ulottuvuus, vaikuttamisen alkuperän kiistettävyys, torjumisen vaikeus ja edullinen hinta. Rajoituksia on mahdollisuuksissa vaikuttaa suljettuihin järjestelmiin oikea-aikaisesti. Kybervaikuttaminen vaatii tuekseen huolellista tiedustelua ja valmistelua.

Eri uhkatoimijat voivat hyödyntää toisiaan omissa operaatioissaan. Esimerkiksi valtiolliset toimijat ulkoistavat usein kybertoimintaansa rikollisryhmille, jolloin valtiollinen alkuperä on riittävän uskottavasti kiistettävissä. Toiminnassa voidaan käyttää myös niin sanottuja sisäpiiriläisiä eli henkilöitä, joilla on laillinen pääsy haluttuun tietojärjestelmään. Sisäpiiriläiset voivat toimia vieraan valtion tai rikollisten lukuun

tai aiheuttaakseen haittaa edustamalleen organisaatiolle koston tai ideologisen syiden vuoksi.

Edellä kuvattujen toimijoiden muodostaman uhkan lisäksi internetissä esiintyy paljon haittaohjelmia, joita ei ole suunnattu mitään tiettyä organisaatiota vastaan. **Kohdistamattomat haittaohjelmat** voivat kuitenkin aiheuttaa merkittävää haittaa organisaatioiden toiminnalle. Tämänkaltaisen haittaohjelman uhriksi voi joutua myös vahingossa, jos tieto- ja kyberturvallisuuden perusasiat kuten järjestelmien päivitykset eivät ole ajan tasalla.

2.3 Tekniset menetelmät

Kyberuhkat ja niissä käytettävät menetelmät perustuvat järjestelmissä olevien haavoittuvuuksien hyödyntämiseen. Haavoittuvuuksilla tarkoitetaan yleensä tietojärjestelmien ja ohjelmistojen ei-toivottuja ominaisuuksia, joiden vuoksi järjestelmiä voidaan käyttää muulla tavalla kuin ne on tarkoitettu käytettäviksi. Toimittajat pyrkivät korjaamaan järjestelmään mahdollisesti jääneet haavoittuvuudet päivitysten avulla. Teknisten haavoittuvuuksien lisäksi järjestelmäkokonaisuuksiin voi liittyä inhimillisiä haavoittuvuuksia. Näitä voivat olla esimerkiksi puutteellinen koulutustaso tai puutteelliset tietoturvaohjeistukset tai virheet prosesseissa.

Palvelunestohyökkäys (denial of service, DoS) on hyökkäystyyppi, joka usein esiintyy julkisuudessa. Sillä tarkoitetaan verkkohyökkäystä, jossa pyritään estämään kohteeksi valitun palvelun, kuten verkkosivuston käyttö. Tavallisimmin tämä toteutetaan kohdistamalla palveluun niin paljon liikennettä, ettei se käytännössä kykene palvelemaan asiakkaitaan. Useista lähteistä tapahtuvaa hyökkäystä kutsutaan nimellä hajautettu palvelunestohyökkäys (distributed denial of service, DDoS). Tällöin käytetään usein saastuneista tietokoneista muodostettua verkkoa eli botnetiä. Palvelunestohyökkäyksellä ei tarkoiteta palveluun murtautumista vaan sillä vaikutetaan tietojen saatavuuteen. Erityisesti esineiden internetin kasvaessa verkosta on löydettävissä paljon suojaamattomia laitteita, joita voidaan hyödyntää hajautetuissa palvelunestohyökkäyksissä. Usein tämänkaltaisten hyökkäysten motiivina voi olla kiusanteko, maineen luominen tai taloudellisen hyödyn tavoittelu. Palvelunestohyökkäyksiä voidaan käyttää myös harhautuksena tai savuverhona peittämään todelliset toimet.

Tekniseen järjestelmään kohdistuvien uhkien lisäksi, kyberuhkat voivat kohdistua

myös teknisen järjestelmän kautta. Esimerkkinä teknisen järjestelmän kautta tapahtuvasta uhkasta voidaan pitää käyttäjän manipulointia (social engineering), jossa teknisin menetelmin lähestytään kohdeorganisaation käyttäjää joko sähköpostitse, sosiaalisen median tai muiden teknisten järjestelmien kautta. Käyttäjien manipulointi voidaan jakaa seitsemään eri kategoriaan. Yksinkertaisimmillaan käyttäjien manipulointi on kalasteluviestien lähettämistä niitä sen kummemmin kohdentamatta (phishing). Tarkemmin kohdennettuna manipulointi kohdistuu tiettyyn organisaatioon tai henkilöihin (spear phishing). Yleisempi tiedonkeruu voidaan kohdentaa organisaation ylempiin toimihenkilöihin (whaling). Käyttäjä voidaan yrittää manipuloida käyttämään saastutettua nettisivustoa tai houkutella aidon kaltaiselle mutta väärennetylle nettisivustolle. Tiettyyn käyttäjäryhmään kohdistettua saastutettua nettisivustoa kutsutaan termillä watering hole. Myös esimerkiksi haittaohjelmia sisältäviä muistitikkuja tai muita tallennusmedioita voidaan jättää kohdeorganisaation työntekijöiden saataville ja tavoitella sitä, että ne kytketään organisaation tietojärjestelmään (baiting). Myös lähestyminen puhelimitse sekä sosiaalisen median kautta on kategorioitu käyttäjien manipuloinniksi.

Huijausviesti tai verkkourkinta (phishing)	Sähköpostin välityksellä ja väärien tietojen avulla toteutettavaa luottamuksellisten tietojen urkintaa.
Kohdistettu huijausviesti (spear phishing)	Sähköpostin välityksellä ja väärien tietojen avulla toteutettavaa yritykseen tai yhteisöön kohdistettua luottamuksellisten tietojen urkintaa.
Päätöksen tekijöiden huijaaminen (whaling)	Päätöksentekijöihin kohdistetut käyttäjänmanipulointiin perustuvat hyökkäykset, jollaisia voivat olla esimerkiksi huijausviestit.
Saastuneet verkkosivut	Saastuneilla verkkosivuilla tarkoitetaan sellaisia internetsivuja, jotka jakavat haittaohjelmia kaikille sivustoilla vieraileville. Esimerkkinä saastuneesta verkkosivusta voi olla virallista poliisi.fi-verkkosivustoa muistuttavat sivut kuten polliisi.fi.
Palkinnoilla houkuttelu (baiting)	Uhria houkutellaan käyttämään saastunutta kohdetta, joka voi olla esimerkiksi muistitikku tai aplikaatio.
Huijauspuhelut	Käyttäjien manipuloiminen puheluiden avulla.
Huijaukset sosiaalisessa mediassa	Käyttäjien manipulointi joko sosiaalisessa mediassa tai sosiaalisen median avulla.

Taulukko 10: Käyttäjien manipuloimisen menetelmiä

Kalasteluhyökkäyksissä lähestytään organisaation käyttäjää hänen työtehtäviinsä tai kiinnostuksensa kohteisiin liittyvillä viesteillä siten, että käyttäjä luulee viestittävänsä oikeista työasioista. Hyökkäyksissä viestien välitystietoja voidaan myös muokata näyttämään siltä kuin ne tulisivat todellisesta, vastaanottajan työasioihin liittyvästä organisaatiosta. Käyttäjä yritetään saada luovuttamaan organisaation kannalta haitallista informaatiota hyökkääjälle: kalastellaan esimerkiksi käyttäjätunnuksia ja salasanoja tai muita tietoja. Myös "nigerialaiskirjeet", joissa käyttäjiä pyydetään lähettämään rahaa viestin lähettäjälle esimerkiksi surullisen tarinan varjolla, voidaan luokitella sosiaaliseksi manipuloinniksi.

Toinen yleinen teknisen kyberuhkan ilmenemismuoto on haittaohjelma (malware), jonka hyökkääjä saa asennettua kohdeorganisaation tietotekniikkaa hyödyntävään järjestelmään. Kuten sosiaalista manipulointia, myös haittaohjelmatyyppejä on lukuisia erilaisia. Haittaohjelmat voidaan jakaa seitsemään eri tyyppiin: virukset (viruses), madot (worms), vakoiluohjelmat (spyware), piilohallintaohjelmat (rootkits), bottiverkot (botnets), troijalaiset (trojans) sekä kiristyshaittaohjelmat (ransomware).

Virus (virus)	Ohjelma, joka monistaa itseään ja leviää tietokoneesta toiseen.	*Brain*, *Iloveyou*
Mato (worm)	Suunniteltu leviämään tietokoneesta toiseen automaattisesti ilman tietokoneen käyttäjän toimenpiteitä.	*Conficker*, *Slammer*
Vakoiluohjelma (spyware)	Kerää ja lähettää tietoa ilman käyttäjän lupaa tai huomiota.	*DaVinci*, *FinFisher*
Piilohallintaohjelma (rootkit)	Ohjelmisto, joka asentuu tietokoneelle hyökkääjän saatua sen hallintaansa.	*Uroburos*
Bottiverkko (botnet)	Saastuneista tietokoneista muodostettu verkko, joka hyödynnetään erilaisissa hyökkäyksissä.	*Mirai*
Troijalainen (trojans)	Viattoman näköinen ohjelma, joka tekeekin jotakin muuta.	*Keymarble*, *Bandcall*
Kiristyshaittaohjelma (ransomware)	Lukitsee tietokoneen sisältöä ja vaatii lunnaita sen vapauttamiseksi.	*Petya*, *WannaCry*

Taulukko 11: Haittaohjelmia

Virukset ja madot ovat toiminnallisesti hyvin lähellä toisiaan. Virukset ovat työasemissa sekä niiden välillä leviäviä haittaohjelmia, joiden leviämiseen tarvitaan tyypillisesti käyttäjän toimenpiteitä, kun taas madot kykenevät leviämään päätelaitteista toisiin itsenäisesti. Vakoiluohjelmilla tarkoitetaan päätelaitteista tietoa kerääviä haittaohjelmia kuten esimerkiksi näppäimistön painalluksia tallentavia ohjelmia. Piilohallintaohjelmilla tarkoitetaan hyökkääjän päätelaitteeseen asentamia ohjelmia tai ohjelmistoja, joiden pääasiallisena tarkoituksena on mahdollistaa esimerkiksi ulkopuoliselle taholle pääsy päätelaitteeseen. Ohjelmistot pyritään piilottamaan siten, että niiden löytäminen on mahdollisimman haastavaa.

Bottiverkoilla tarkoitetaan haitallisella koodilla saastutetuista työasemista muodostuvaa laajaa, esimerkiksi palvelunestohyökkäyksiin käytettävää järjestelmää. Hyökkääjä asentaa yleisimmin kotikäyttäjien työasemille, yleensä automaattisin keinoin, haittaohjelmia joita voidaan myöhemmin käyttää omien tarkoitusperien saavuttamiseksi. Troijalaiset esitetään käyttäjälle todellisena sovelluksena, jonka käyttäjä haluaakin päätelaitteeseensa asentaa. Yleensä käyttäjän asentama sovellus vaikuttaa toimivan normaalisti. Todellisuudessa ohjelman taustalla on vihamielinen toimija, joka pyrkii troijalaisen kautta asentamaan päätelaitteeseensa haluamansa haittaohjelman, kuten piilohallintasovelluksen. Viimeisimpänä kategoriana on kiristyshaittaohjelma, joka salaa ja lukitsee tietokoneen sisältöä ja vaatii lunnaita tämän lukituksen poistamiseksi.

Kyberhyökkäyksellä tarkoitetaan yleisesti siis mitä tahansa kybertoimintaympäristössä tai sen avulla tapahtuvaa toimintaa, jolla pyritään kybertoimintaympäristössä olevien verkkojen, laitteiden, järjestelmien tai persoonien oikeudettomaan käyttöön tai vahingoittamiseen. Yleensä edellä mainittuja menetelmiä käyttävät yksittäiset kyberhyökkäykset kuuluvat laajempaan kokonaisuuteen eli kyberoperaatioon. Kyberoperaatioksi kutsutaan kybertoimintaympäristössä tai sen avulla tapahtuvaa suunnitelmallista toimintojen kokonaisuutta, jossa pyritään vaikuttamaan kohteen toimintaan. Kyberoperaatioita on käsitelty luvussa 4.

Kyberhyökkäys (cyber attack)	Kyberhyökkäys on mikä tahansa kybertoimintaympäristössä tai sen avulla tapahtuva toiminta, jolla pyritään kybertoimintaympäristössä olevien verkkojen, laitteiden, järjestelmien tai persoonien oikeudettomaan käyttöön tai vahingoittamiseen.
Kyberoperaatio (cyber operation)	Kyberoperaatio on kybertoimintaympäristössä tai sen avulla tapahtuva suunnitelmallinen toimintojen kokonaisuus, jossa pyritään vaikuttamaan kohteen toimintaan.

Taulukko 12: Kyberhyökkäys ja -operaatio

Kyberoperaatioiden eri vaiheet sekä niiden toimeenpano saattavat kuitenkin sisältää useita eri haittaohjelmatyyppejä sekä käyttäjien manipulointitapoja. Tällaista edistyneempää ja toiminnan takia pitkäkestoista kyberoperaatiota kutsutaan APT:ksi (advanced persistent threat). APT:lle on ominaista, kuten englanninkielinen termi kertoo, monimutkaisuus ja pitkäkestoisuus. Operaatiossa vihamielinen, yleensä valtiollinen tai valtion lukuun toimiva hyökkääjä on päässyt merkittävään kohteeseen ja piiloutunut järjestelmään mahdollisesti useiden vuosien ajaksi saavuttaakseen operaatiolle asetetut tavoitteet. Niitä voi olla useita, mutta yleensä päätarkoituksena on vakoilu.

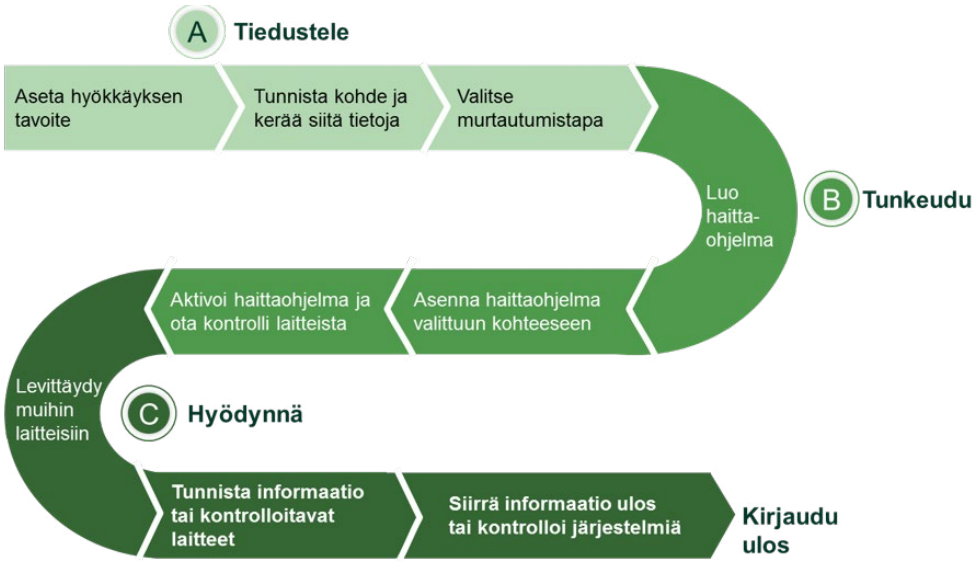
Kuten aiemmin mainittiin, kyberuhka vaatii toteutuakseen haavoittuvuuden joko teknologiassa tai prosessissa. Osa julkisuudessa raportoiduista kyberhyökkäyksistä on voinut ollut sellaisia, ettei niissä ole käytetty yhtään teknistä haavoittuvuutta operaation toimeenpanemiseksi, vaan onnistuminen on perustunut teknisen järjestelemän käyttöön juuri siten, kuin se on suunniteltu. Tällöin haavoittuvuus on ollut joko järjestelmän käyttöprosessissa tai käyttäjien varsinaisessa toiminnassa. Teknisten haavoittuvuuksien kautta pystytään kuitenkin kampanjasta riippuen tuottamaan mahdollisuuksia erityyppisten haittaohjelmien asentamiseksi järjestelmiin eri käyttäjätasoilla.

Sellaisia haavoittuvuuksia, joita ei ennalta tiedetä ja joihin ei ole olemassa korjauspäivitystä, kutsutaan yleensä nollapäivähaavoittuvuuksiksi. Niiden olemassaolo ja kyky niiden hyödyntämiseen saattaa olla vain hyökkääjän tiedossa, eikä niihin ole edes olemassa korjaavia ohjelmistopäivityksiä. On myös mahdollista, että haavoittuvuus on raportoitu ohjelmiston toimittajalle, mutta sitä ei ole kuitenkaan ehditty tai haluttu päivittää.

Kyberhyökkäystä voidaan kuvata myös sen teknisen toteutuksen mallin avulla. Tunnetuimman kyberhyökkäysmallin laati jo vuonna 2011 Lockheed-Martin, ja sen pohjalta on esitetty useita erilaisia muokattuja versioita useissa julkaisuissa. Yleinen valtiollisen kohdistetun kyberhyökkäyksen vaiheistettu malli on seuraava:

1. Tavoitteiden asettaminen eli määritetään se, mitä hyökkäyksellä on tarkoitus saada aikaiseksi.
2. Kohteen tunnistaminen eli kerätään tietoja eri menetelmillä, kuten julkisista lähteistä, kohteen työntekijöiden kanssa keskustelemalla tai muilla tiedustelumenetelmillä.

3. Murtautumistavan valitseminen eli kerätyn tiedon perusteella tehdään päätös toteutettavista menetelmistä ja helpoimmasta tavasta päästä kohdejärjestelmään.
4. Haittaohjelman luominen eli haittaohjelma luodaan joko ostamalla, muokkaamalla tai itse kehittämällä.
5. Haittaohjelman asentaminen valittuun kohteeseen eli luodaan uskot tava perusta kohdistetulle kalasteluviestille tai selvitetään käyttäjä ja se, kenen kautta ohjelma saadaan toimitettua esim. USB-tikulla.
6. Haittaohjelman aktivoiminen eli haittaohjelman avulla otetaan kontrolli laitteesta ja samalla luodaan etäyhteys haittaohjelmaan.
7. Levittäytyminen muihin laitteisiin eli vahvennetaan läsnäoloa kohdejärjestelmässä.
8. Tunnistetaan informaatio tai kontrolloitavat laitteet eli hakeudutaan hyökkäyksen tavoitteet mahdollistavaan taisteluasemaan ja muodoste taan komentoyhteys.
9. Informaation siirtäminen ulos järjestelmästä tai järjestelmän kontrollointi eli tehdään toimenpiteet tavoitteen saavuttamiseksi.



Kuva 5: Kyberhyökkäyksen kulku

2.4 Uhkan vaikutukset

Kyberuhkaa määrittävät ensisijaisesti käytettävät menetelmät, joten kyberuhkilla voi olla hyvin monenlaisia vaikutuksia. Vaikutukset voivat vaihdella yksilötason vaikutuksista globaaleihin vaikutuksiin, ja ne voivat kohdistua yhteiskunnan kaikkiin sektoreihin.

Yleensä kyberuhkan vaikutuksia tarkastellaan ensisijaisesti organisaatioiden tai valtioiden näkökulmasta. Vaikutukset voivat olla välittömiä ja suoraan toimintaan vaikuttavia, tai vaikutukset saatetaan havaita välillisesti tai pitkienkin aikojen kuluttua. Välittömiä vaikutuksia tuottavat esimerkiksi kiristyshaittaohjelmat, jotka vaikuttavat suoraan tietojärjestelmissä säilytetyn tiedon käytettävyyteen. Esimerkki kiristyshaittaohjelmaa jäljittelevän salaushaittaohjelman NotPetyan hyökkäyksestä tanskalaista merilogistiikkayritystä vastaan on esitetty taulukossa 13.

Organisaatioiden näkökulmasta kyberuhka voi kohdistua niiden omiin järjestel-

Kuka?	NotPetya salaushaittaohjelman arvioidaan levinneen maailmalle Ukrainan kriisiin liittyen.
Mitä?	Salausohjelma, joka lamautti yrityksen ICT-toimintoja.
Miten?	Haittaohjelma hyödynsi jo aiemmin keväällä julkisuuteen tullutta ja myös kiristyshaittaohjelma WannaCry-hyökkäyksessä käytettyä Windowsiin liittyvää Eternal Blue -haavoittuvuutta.
Kohde?	Kohteena oli A. P. Møller-Mærsk A/S, joka on tanskalainen konglomeraatti ja jonka tärkein liiketoiminta-alue on logistiikka. Yhtiö on maailman suurin rahtilaivavarustamo sekä laivaston koolla että TEU-määrällä mitattuna. Se on myös liikevaihdoltaan Tanskan suurin yritys.
Miksi?	Luultavasti Mærsk oli sivullinen uhri ja varsinainen kyberhyökkäys oli kohdistettu Ukrainalaisia yrityksiä vastaan.
Milloin?	Kesäkuu 2017.
Vaikutus	Tietokoneiden lukituksen seurauksena satamalogistiikka lamautui ja laivat jouduttiin reitittämään toisiin satamiin. Hyökkäyksestä on arvioitu aiheutuneen noin 350 miljoonan dollarin kustannukset.
Lisätiedot	https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Taulukko 13: Esimerkki NotPetya salaushaittaohjelma

miin, yhteistyökumppaneiden tai toimittajien tietojärjestelmiin, kriittiseen infrastruktuuriin tai työntekijöihin yksilöinä. Ulkoistetut tietojärjestelmät muodostavat merkittävän hyökkäysvektorin, sillä usein organisaatio kykenee valvomaan ja suojaamaan niitä muita järjestelmiä heikommin, erityisesti jos turvallisuusnäkökulma on huomioitu puutteellisesti ulkoistussopimuksissa

Valtion turvallisuuden näkökulmasta arvioituna kyberuhka voi vaikuttaa valtion puolustuskykyyn, jos vastustajat pystyvät hankkimaan tietoonsa sotasuunnitelmia tai jos valtion sotilaalliseen suorituskykyyn, esimerkiksi asejärjestelmien toimintaan, kyetään vaikuttamaan kybervaikuttamismenetelmillä. Puolustuskykyyn voidaan vaikuttaa myös epäsuorasti esimerkiksi kriittisen infrastruktuurin kautta.

Yhdysvaltojen presidentinvaali vuonna 2016 on viimeaikainen esimerkki tilanteesta, jossa väitetysti on vaikutettu kybermenetelmillä valtion poliittiseen sektoriin. Julkisuudessa esitettyjen tietojen mukaan Venäjä vaikutti vaalin lopputulokseen tunkeutumalla demokraattisen puolueen tietojärjestelmiin ja varastamalla tietoa, jota käytettiin mustamaalauskampanjassa. Tapaus on esimerkki operaatiosta, jossa käytettiin kybermenetelmiä osana informaatiovaikuttamista. Esimerkki tapahtuneesta on esitetty taulukossa 14.

Kuka?	ODNI:n (Office of the Director of National Intelligence), joka on osa Yhdysvaltain tiedustelupalvelua, mukaan Venäjän sotilastiedustelu (GRU) oli hyökkäysten takana.
Mitä?	Yhdysvaltojen presidentin vaalien tulokseen yritettiin vaikuttaa informaatio-operaatiolla, josta osa toteutettiin kybertoimintaympäristön keinoin.
Miten?	Demokraattisen puolueen sähköpostipalvelimelle tunkeuduttiin ja näin hankittiin pääsy henkilöstön yksityisille Gmail-tileille mustamaalaamiseen käytettävään materiaaliin hankkimiseksi.
Kohde?	Yhdysvaltojen vuoden 2016 presidentinvaalit.
Miksi?	Operaation todennäköisimpänä tavoitteena oli heikentää Yhdysvaltojen kansalaisten luottamusta yhteiskuntaan ja vaalijärjestelmään.
Milloin?	2016.
Vaikutus	Hyökkäys sai runsaasti julkisuutta, ja sen avulla onnistuttiin kyseenalaistamaan presidentinvaalien luotettavuus sekä vaalit voittaneen presidentti Trumpin vaalivoiton aitous.
Lisätiedot	NY Times & CNN

Taulukko 14: Esimerkki Yhdysvaltojen presidentinvaalit vuonna 2016

Kyberuhka vaikuttaa valtion taloudelliseen kilpailukykyyn, kun taas teollisuusvakoilulla varastetaan yritysten aineetonta pääomaa. Tämä onkin yksi merkittävä tekijä kyberuhkien toteutumisen kustannusten arvioimisessa. Perinteisesti teollisuusvakoilulla on saavutettu kilpailuetua joko valmistamalla kilpailevia tuotteita tai kopioimalla tietyt tuotteet suoraan omille markkinoille. Kybertoimintaympäristö luo hyvät puitteet tällaiselle toiminnalle.

Yhdysvaltojen kansallinen vastatiedustelu ja turvallisuuskeskus (National Counterintelligence and Security Center, NCSC) on arvioinut, että ulkomainen taloudellinen ja teollinen vakoilu muodostaa merkittävän uhkan Yhdysvaltojen vauraudelle, turvallisuudelle ja kilpailukyvylle. NCSC:n mukaan kybertoimintaympäristö on otollinen operatiivinen alusta laajalle joukolle yritysvakoilun uhkatoimijoita.

Nykyisin tietojärjestelmät ja tietoliikenneinfrastruktuurin hallinta ovat valtioiden välisen valtakamppailun välineitä. Esimerkiksi Kiina on panostanut voimakkaasti Afrikan tietoliikenneinfrastruktuurin kehittämiseen. Venäjä puolestaan on pyrkinyt vähentämään riippuvuuttaan länsimaisesta informaatioteknologiasta kehittämällä kansallisia tietojärjestelmäratkaisujaan.

2.5 Kehityksen suunta

Kyberuhkien määrä kasvaa teknologian kehittyessä ja yleistyessä. Jatkossakin uusia teknologioiden ja järjestelmien haavoittuvuuksia pyritään hyödyntämään myös vihamielisessä toiminnassa. Esimerkiksi esineiden internetin yleistymisen myötä entistä huomattavasti suurempaa määrää laitteita voidaan käyttää hyväksi kyberhyökkäyksissä. Käytäntö on osoittanut, että usein uudessa teknologiassa laiminlyödään tietoturvaominaisuuksien kehittäminen ja siksi ne ovat erittäin houkuttelevia kohteita kyberhyökkäyksille. Lisäksi laitteistojen määrä ja monimutkaisuus voi tuottaa loppukäyttäjille haasteita siinä, että heidän pitäisi ylläpitää laitteiden päivitykset ajantasaisina mahdollisten haavoittuvuuksien korjaamiseksi.

Tekoäly (artificial intelligence, AI) on tietojenkäsittelytieteen osa-alue, joka yrittää luoda älykkäitä koneita ja ohjelmia, jotka kykenevät matkimaan ihmisen tajuntaa ja tehtävien suorituskykyä. Tekoäly ja sen kehittyminen on jatkuvasti esillä tulevaisuuden visioissa. Sen nähdään ratkaisevan valtaosan ihmiskunnan ongelmista, mutta samalla se koetaan uhkana. Kuitenkin näkemykset tekoälystä, joka suuntautuu koko ihmiskuntaa vastaan, ovat jäämässä taka-alalle. Nyt suurimmat tekoälyn ke-

hittymisen uhkakuvat liittyvät tekoälyn hyödyntämiseen sotilaallisessa toiminnassa sekä rikollisuudessa. Lisäksi tekoälyn hyödyntämiskykyjen epätasainen jakautuminen voi tulevaisuudessa aiheuttaa lisää eriarvoistumista ja kriisejä.

Kvanttitietokoneilla tarkoitetaan kehitteillä olevia monikertaisesti nykyisiä tietokoneita tehokkaampia tietokoneita. Kvanttitietokoneet hyödyntävät 1:n ja 0:n sijaan kvanttitilojen superpositioita. Tämänkaltaisten tietokoneiden laskentateho tulee väistämättä vaikuttamaan kyberturvallisuuteen muun muassa käytettyinä salaamismenetelminä ja niiden avaamismekanismeina. Vaikka tällaisia tietokoneita on kehitteillä useita, todennäköisesti niitä ei saada yleiseen käyttöön ainakaan vielä vuosikymmeneen.

Valtiollisten toimijoiden toteuttamat tai tilaamat kyberoperaatiot lisääntyvät. Tämän kaltainen kyberuhkien hyödyntäminen ei ylitä sodankäynnin kynnystä, ja sen alkuperän ja näin ollen syyllisyyden osoittaminen on vaikeaa. Kyberoperaatioihin paneudutaan tarkemmin luvussa 4.

Myös informaatiovaikuttamisen merkitys kansainvälisissä suhteissa on korostunut 2010-luvulla. Tulevaisuudessa sen osana pyritään todennäköisesti entistä tehokkaammin hyödyntämään kybermenetelmiä. Jo nykyään eri toimijat ylläpitävät sosiaalisessa mediassa bottiarmeijoita, joiden tehtävänä on julkaista toimijan haluamaa materiaalia, väärentää keskustelua tai vaientaa toisinajattelijoita. Mitä todennäköisimmin kybermenetelmillä pyritään tulevaisuudessa vaikuttamaan myös robotteihin ja autonomisiin järjestelmiin niiden toiminnan muuttamiseksi. Kybermenetelmillä esimerkiksi robottiaseet voidaan kääntää omistajiaan tai kolmansia osapuolia vastaan.

Kyberuhkat ilmiönä eivät ole uusia. Erilaisia uhkia tietoteknisiä järjestelmiä kohtaan on ollut yhtä kauan kuin järjestelmiä on ollut olemassa. Digitalisaatio ja informaatioteknologian yleistyminen on kuitenkin tuonut kyberuhkat lähemmäs ihmisten, yritysten ja organisaatioiden jokapäiväistä elämää ja toimintaa. Toteutuessaan uhkilla voi olla monimuotoisia vaikutuksia, minkä vuoksi sekä ihmisten että organisaatioiden pitää ottaa uhkat toiminnassaan huomioon.

3 #TOIMINTA

Tässä luvussa kuvataan Puolustusvoimien roolia kyberturvallisuudessa eli kyberpuolustusta. Luvussa kerrotaan kyberpuolustuksen perusteet ja se, mistä ne ovat lähtöisin. Lisäksi luvussa tarkastellaan sitä, kuinka Puolustusvoimat toimii kybertoimintaympäristössä. Lukuun perehdyttyään lukijalla tulisi olla selkeä ymmärrys siitä, miten Puolustusvoimat toimii kybertoimintaympäristössä yhteiskunnan osana.

3.1 Kyberturvallisuudesta kyberpuolustukseen

Suomalainen yhteiskunta on riippuvainen tietojärjestelmistä. Se tarvitsee toimiakseen niin tietoa, sitä tukevia järjestelmiä kuin sähköäkin. Näiden perustarpeiden turvaaminen on tärkeää yhteiskunnan toiminnan kannalta. Sitä varten on laadittu *Yhteiskunnan turvallisuusstrategia* (YTS), jonka perusteella varautuminen häiriöihin ja poikkeustiloihin on ohjeistettu toteutettavaksi kyberturvallisuusstrategian ja sen toimeenpano-ohjelman kautta.

Suomen ensimmäinen kansallinen kyberturvallisuusstrategia julkaistiin valtioneuvoston periaatepäätöksenä 2013. Siinä määriteltiin tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. Suomen kyberturvallisuusstrategian mukainen kyberturvallisuuden visio:

- Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.
- Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.
- Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

Kyberturvallisuusstrategiassa on myös kymmenen strategista linjausta, joista viides määrittelee, että Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

Kyberturvallisuusstrategian toteutumiseksi laadittiin toimeenpano-ohjelma vuonna 2014. Se sisälsi 74 erilaista toimenpidettä. Keskeisimmät kehittämiskohteet olivat kyberturvallisuuskeskus, valtion ympärivuorokautinen tietoturvatoiminta, salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke (SA-TU), poliisin toimintakyky kyberrikollisuuden torjunnassa, kybertoimintaympäristöön ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen sekä tutkimus- ja koulutusohjelmat ja muu osaamisen vahvistaminen.

Kyberturvallisuusstrategian toteutumista ja kybertoimintaympäristön nopeaa muutosta on seurattu. Vuonna 2017 julkaistun valtioneuvoston selvityksen *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi* mukaan viime vuosien kyberuhkien merkittävimmät trendit ovat olleet kiristyshaittaohjelmien kasvu, haavoittuvuuksien hyödyntäminen, laitteistoihin kohdistuvat uhkat sekä liiketoiminnan tuhoamiseen tai henkilötietojen varastamiseen tähtäävät hyökkäykset. Myös huijaukset ja tietojen kalastelut, palvelunestohyökkäykset sekä kohdistetut hyökkäykset ovat edelleen ajankohtaisia uhkia.

Kyberturvallisuusstrategian toteutumisen tueksi laadittiin uusi *Kyberstrategian toimeenpano-ohjelma vuosille 2017–2020*. Siinä muutettiin pysyväksi tavoite siitä, että Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. Toimeenpano-ohjelma jakaantui kolmeen kokonaisuuteen:

- Johtamisella on varmistettu kyberturvallisuuden vision saavuttaminen.
- Yhteiskunnan digitalisoidut elintärkeät toiminnot ovat turvatut.
- Kansalaisten, elinkeinoelämän ja hallinnon kyberosaaminen edistää digitalisaation kehitystä.

Myös Puolustusvoimien kyberpuolustuksen perusteet ovat Kyberturvallisuusstrategiassa. Siinä määritellään strategisena linjauksena, että Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään. Puolustusvoimat vastaa kyberpuolustuksesta, jolla tarkoitetaan kansallisen kyberturvallisuuden maanpuolustuksellista osa-aluetta, joka muodostuu tiedustelun, vaikuttamisen

ja suojautumisen suorituskyvyistä. Puolustusvoimiin luodaan kokonaisvaltainen kyberpuolustuskyky sen lakisääteisiä tehtäviä varten osana yhteiskunnan elintärkeiden toimintojen turvaamista. Kyberpuolustuksen suorituskyvyillä tuetaan Puolustusvoimien operaatioita suojaamalla oman päätöksenteon edellytykset. Tämä mahdollistuu hallitsemalla omat tietojärjestelmät ja kriittiset asejärjestelmät, joihin kuuluvat myös ohjelmoitava elektroniikka ja integroidut järjestelmät, sekä heikentämällä vastustajan tilannetietoisuutta ja toiminnanvapautta kybertoimintaympäristössä ja vaikuttamalla vastustajan päätöksentekoa tukeviin rakenteisiin sekä suorituskykyihin.

Viimeisimpiä Puolustusvoimien toimintaa kybertoimintaympäristössä ohjaavia asiakirjoja on puolustusministeriön vuonna 2019 julkaisema *Kyberpuolustuksen kehittämisen strategiset linjaukset*. Asiakirja painottaa edelleen vuoden 2017 puolustusselonteon linjauksia, joissa kyberpuolustus määritettiin yhdeksi puolustusjärjestelmän kehittämisen ja ylläpidon painopistealueeksi. Selonteon mukaan Puolustusvoimat rakentaa kyvyn kybertilannekuvan muodostamiseen, kyberoperaatioiden suunnitteluun ja toimeenpanoon sekä omien järjestelmien suojaamiseen ja valvontaan kybertoimintaympäristössä. Lisäksi asiakirjassa mainitaan, että kesällä 2019 voimaanastunut tiedustelulainsäädäntö mahdollistaa kyberpuolustuksen kokonaisuutta vahvistavien tiedustelusuorituskykyjen kehittämisen.

Viimeisin kyberturvallisuutta ja kyberpuolustusta ohjaava asiakirja on *Suomen kyberturvallisuusstrategia 2019*. Siinä määritetään, että kyberpuolustus on keskeinen kyberturvallisuuden kehittämisen osa-alue Suomessa. Lisäksi strategia painottaa, että kybersuojaa parannetaan kasvattamalla kyberhyökkäysten kynnystä kehittämällä havainnointi-, attribuutio- ja vastatoimintakykyä.

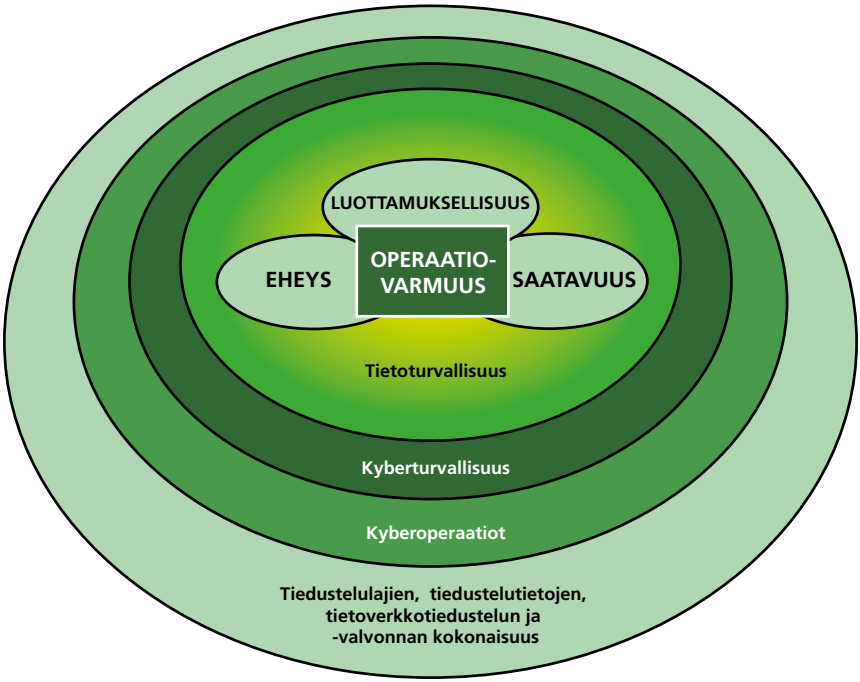
Puolustusvoimien sisällä kyberpuolustukseen liittyviä asioita on määritelty *Kyberpuolustuskonseptissa*, joka ei kaikilta osin ole julkinen asiakirja. Konseptin tavoitteena on jalkauttaa kyberpuolustuksen toiminta-ajatus Puolustusvoimissa, kuvata suorituskyvyn kehittämisen tavoitetila sekä muutosaskeleet tavoitetilaan. Konsepti kuvaa sitä, millä kyberpuolustuksen kyvyillä tuetaan Puolustusvoimien lakisääteisten tehtävien toteuttamista sekä sitä, miten kyberpuolustus liittyy Puolustusvoimien operaatioihin.

3.2 Kyberpuolustus

Kyberpuolustuksella tarkoitetaan kansallisen kyberturvallisuuden maanpuolustuksellista osa-aluetta, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Kyberpuolustuksella suojataan sotilaallisen maanpuolustuksen kannalta kriittinen tieto, tietojärjestelmät ja tietoliikennejärjestelyt sekä osaltaan mahdollistetaan Puolustusvoimien operaatiot ja tuetaan päätöksenteon edellyttämän tilannekuvan muodostamista.

Kyberpuolustuksen päämäärä on kaikissa tilanteissa oman operaatiovarmuuden (mission assurance, MA) takaaminen. Puolustusvoimien operaatiovarmuus on kokonaisuus, joka tuotetaan neljällä osa-alueella:

- tietoturvallisuus (information security, IS)
- kyberturvallisuus (cyber security, CS)
- kyberoperaatiot (cyber operations, CO)
- tiedustelun ja valvonnan kokonaisuus kaikissa ympäristöissä (intelligence, surveillance and reconnaissance, ISR).



Kuva 6: Kyberpuolustuksen kokonaisuus

Operaatiovarmuus (mission assurance)	Kokonaisuus, jolla turvataan operaatioiden toimeenpano ja joka muodostuu tietoturvallisuudesta, kyberturvallisuudesta, kyberoperaatioista ja kaikissa toimintaympäristöissä tapahtuvasta tiedustelun ja valvonnan kokonaisuudesta.
Tietoturvallisuus (information security)	Tietoturvallisuus tarkoittaa tietoaineistojen luottamuksellisuuden, eheyden ja saatavuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.
Kyberturvallisuus (cyber security)	Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus on tiedon, laitteistojen, verkostojen, ohjelmistojen ja käyttäjien luottamuksellisuuden, eheydyn ja saatavuuden turvaamista koko elinjakson ajan. Kyberturvallisuus muodostuu ylläpitäjien ja käyttäjien välisestä yhteistoiminnasta ja siinä huomioidaan kybertoimintaympäristön vaikutukset fyysiseen maailmaan.
Kyberoperaatio (cyber operation)	Kyberoperaatio on kybertoimintaympäristössä tai sen avulla tapahtuva suunnitelmallinen toimintojen kokonaisuus, jossa pyritään vaikuttamaan kohteen toimintaan.
Tiedustelun ja valvonnan kokonaisuus (ISR)	Kokonaisuus, joka muodostuu ISR (intelligence, surveillance, reconnaissance) avulla: • Intelligence – yleinen tiedon keruu ja analysointi halutusta aiheesta. • Surveillance – verkon tai toimijan valvonta. • Reconnaissance – tiettyyn kohteeseen kohdistettu tiedustelu. Tämän kokonaisuuden avulla muodostetaan johtamiseen ja menestykseen tarvittava tietoisuus toimintaympäristöstä.

Taulukko 15: Operaatiovarmuus ja sen tekijät

Operaatiovarmuuden perustan muodostavat tieto- ja kyberturvallisuuden toiminnalliset ja tekniset ratkaisut. Niiden tavoitteena on tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistaminen kaikissa tilanteissa. Tietoturvallisuudella varmistetaan käytettävää tietoa sisäisiltä virheiltä ja väärinymmärryksiltä ja kyberturvallisuudella luodaan suojakerros tietoturvallisuuden ympärille.

Tieto- ja kyberturvallisuuden käytännön toimia ovat esimerkiksi kulun- ja pääsynvalvonta, tilojen lukitus, tiedon turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tieto- ja kyberturvallisuus ovat uhkasta riippumattomia, mikä tarkoittaa sitä, että ratkaisut on tarkoitettu toimimaan kaikkia mahdollisia tunnistettuja uhkia vastaan.

Operaatiovarmuutta tuetaan aktiivisin kyberoperaatioin. Siinä missä tieto- ja kyberturvallisuuden ratkaisut ovat perusmenetelmiä, joita ei ole sidottu nimettyyn uhkaan tai tilanteeseen, kyberoperaatiot perustuvat uhkalähtöiseen ajatteluun. Uhkalähtöisessä ajattelussa keskitytään tiettyyn odotettuun tai odottamattomaan tilanteeseen, jossa aktiivisin toimenpitein aikaansaadaan vaikutuksia kybertoimintaympäristössä tai fyysisessä maailmassa. Kyberoperaatiossa korostuu jatkuvasti muuttuva uhkaympäristö toimijoineen.

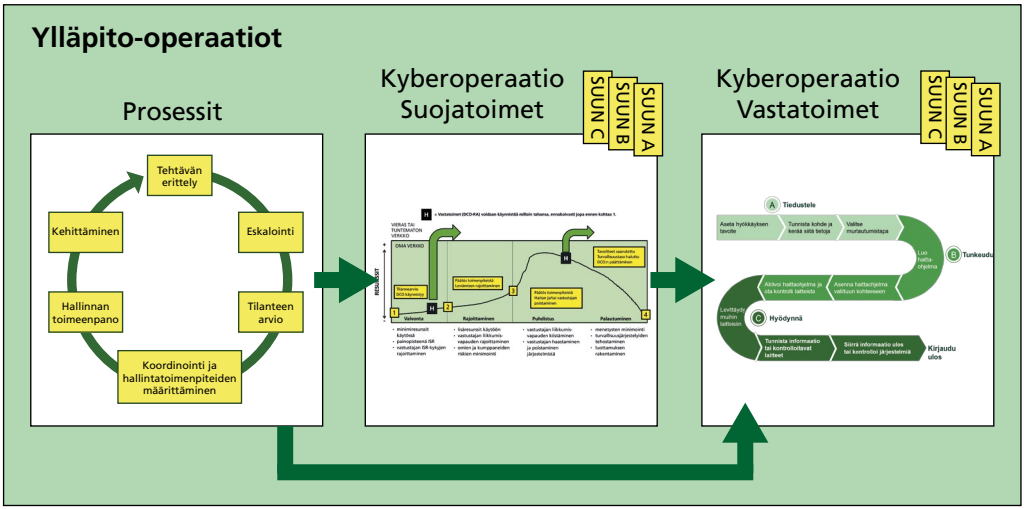
Tiedustelun kokonaisuus kybertoimintaympäristössä koostuu sekä tietoverkkotiedustelusta että kaikista muista perinteisistä tiedustelun osa-alueista, joiden avulla kybertoimintaympäristön tilannekuvaa muodostetaan. Asiaa voidaan kuvata englanninkielisen lyhenteen ISR (intelligence, surveillance, reconnaissance) avulla:

- Intelligence – yleinen tiedon keruu ja analysointi halutusta aiheesta
- Surveillance – verkon tai toimijan valvonta
- Reconnaissance – tiettyyn kohteeseen kohdistettu tiedustelu

Julkisuudessa kybertiedustelu-termillä tarkoitetaan usein kyberoperaatioiden tueksi tehtävää tiedon keräämistä kybertoimintaympäristössä tai sen avulla. Termillä ei ole Puolustusvoimissa vakiintunutta määritelmää, vaan sen sijaan käytetään termiä tietoverkkotiedustelu tai joissain tapauksissa termiä puolustukselliset kyberoperaatiot. Tietoverkkotiedustelu on osa signaalitiedustelua, ja se jakautuu tietoliikennetiedusteluun ja tietojärjestelmätiedusteluun.

3.3 Puolustusvoimien kyberoperaatiot

Kyberoperaatiot liittyvät kiinteästi Puolustusvoimien muuhun toimintaan ja niiden suunnittelu tapahtuu samoilla periaatteilla kuin muidenkin operaatioiden. Kyberoperaatiolla tarkoitetaan kybertoimintaympäristössä tai sen avulla tapahtuvaa suunnitelmallista toimintojen kokonaisuutta, jossa pyritään vaikuttamaan kohteen toimintaan. Puolustusvoimien jatkuvasti kybertoimintaympäristössä käynnissä olevilla prosesseilla pyritään toteuttamaan toiminnat niin pitkälle kuin mahdollista. Kyberoperaatioita käytetään kohdattaessa poikkeuksellinen tilanne, jota ei kyetä meneillään olevien prosessien ja resurssien avulla ratkaisemaan tai tilanne, jossa on tunnistettu tavoite, jonka saavuttaminen edellyttää tavanomaisesta toiminnasta poikkeamista. Kyberoperaatioita voidaan toteuttaa itsenäisinä, mutta yleensä ne toteutetaan yhteistoiminnassa puolustushaarojen ja toimialojen kanssa.



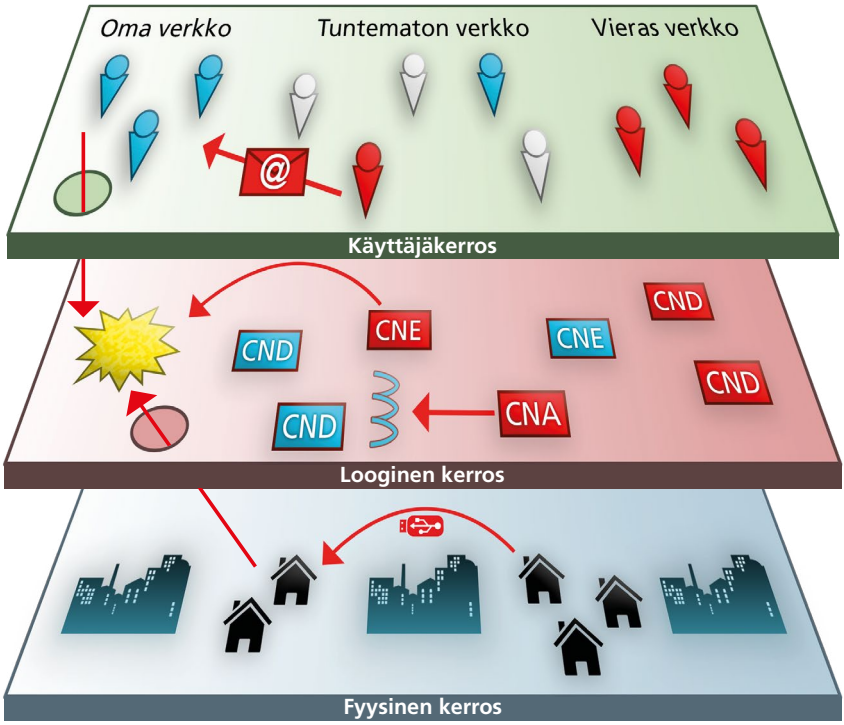
Kuva 7: Prosessit ja puolustukselliset kyberoperaatiot

Kyberoperaatiolla voidaan tukea laajempia Puolustusvoimien operaatioita ja vastaavasti muiden suorituskykyjen toiminnalla voidaan tukea kyberoperaatioita. Kyberoperaatiot ovat yhdenvertaisia maa-, meri-, ilma- ja erikoisoperaatioiden kanssa. Tämän johdosta kaikki Puolustusvoimien operaatiot ovat lähtökohtaisesti yhteisoperaatioita. Kyberoperaatiot ovat ainoastaan uusi taistelujärjestelmä tai asejärjestelmä, joka vaatii uudenlaista organisoitumista, taktista ajattelua sekä tukitoimia, jotta sitä voidaan hyödyntää yhteisoperaation osana.

Kybertoimintaympäristön toimintojen tavoin myös kyberoperaatiot ovat Suomessa uusi käsite. Toimintakenttä on nuori, ja määritelmät elävät vielä joitain vuosia ennen kuin ne vakiintuvat Puolustusvoimissa. Tämä johtuu siitä, että sotilaallisista kyberoperaatioista ei ole vielä merkittävästi käytännön kokemuksia Suomessa.

Operaatiosta tulee käyttää yhtenäisiä termejä, jotta yhteisoperaatioita tai vaikuttamista suunniteltaessa osataan ottaa huomioon muiden puolustushaarojen, toimialojen tai aselajien käyttö. Jokaisella toimijalla on omat erityispiirteensä ja tarpeensa luokitella asioita. Näin on myös kybertoimintaympäristössä.

Kyberoperaatiot ja -hyökkäykset tapahtuvat kaikilla kybertoimintaympäristön kerroksilla sekä myös kerroksia vaihtaen. Tasojen välillä voidaan liikkua esimerkiksi tuomalla vastustajan fyysinen Usb-tikku Puolustusvoimien verkkoon, jolloin on mahdollista kiertää loogisen tason suojaus. Toisaalta haittaohjelmaa voidaan yrittää ujuttaa Puolustusvoimien järjestelmiin suoraan loogisella tasolla tai hyökkäys voidaan aloittaa käyttäjäkerrokselta Puolustusvoimien henkilöstöä manipuloimalla ja sitä kautta saada haittaohjelma kohteeseen. Erilaisia vastustajan lähestymismahdollisuuksia kutsutaan hyökkäysvektoreiksi. Puolustaja pyrkii minimoimaan hyökkäysvektorit kaikilla tasoilla. Kybertoimintaympäristön eri kerroksilla ja niiden välillä tapahtuvia hyökkäyksiä on esitetty kuvassa 8.



Kuva 8: Kyberhyökkäyksiä kerroksittain

Vastustajan kybertoimintaympäristössä tapahtuviin hyökkäyksiin voidaan vastata omalla kyberoperaatiolla. Puolustuksellisilla kyberoperaatioilla kiistetään vastustajan toiminnanvapaus omissa verkoissa ja palautetaan verkon tärkeimmät osat omaan hallintaan. Puolustukselliset kyberoperaatiot perustuvat tilannekuvaan ja sekä aktiivisiin että passiivisiin toimiin.

4 #OPERAATIOT

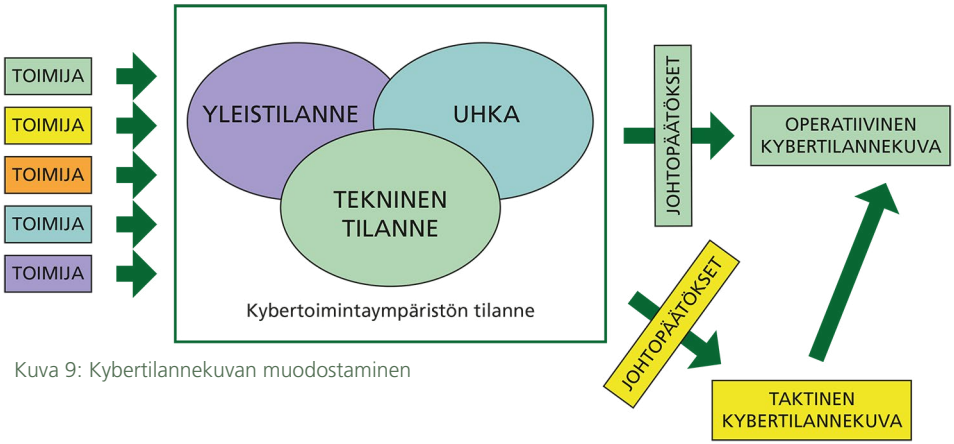
Tässä luvussa kuvataan erilaisia toimintoja ja operaatioita kybertoimintaympäristössä. Luvun sisältö perustuu kirjoittajien tulkintaan Yhdysvaltojen ja Ison-Britannian julkaisemista lähteistä, joista tärkeimpinä voidaan mainita *Joint Publication 3-12 Cyberspace Operations* ja *Cyber Primer, Second Edition*. Erityisesti Yhdysvaltojen voidaan arvioida toimivan edelläkävijänä kybertoimintaympäristössä, ja näin ollen voidaan olettaa samankaltaisten toimintojen ja operaatioiden leviävän käyttöön maailmalla laajemmin. Luvun sisältö ei kuvaa Puolustusvoimien kybertoimintojen nykytilaa. Lukuun perehdyttyään lukijan tulisi ymmärtää kybertoimintaympäristön toiminnot sekä tuntea erilaiset kyberoperaatiot.

4.1 Tietoisuus toimintaympäristöstä

Toimintaympäristötietoisuus ja sen ymmärtäminen ovat edellytys menestykselle myös kybertoimintaympäristössä. Operaatioiden suunnittelua ja toimeenpanoa varten muodostetaan kybertilannekuva. Se on operaatioiden johtamisen ja päätöksenteon tärkein työkalu. Kybertilannekuvan sisältö ja tarve vaihtelevat suuresti eri johtamistasojen ja toimijoiden välillä, joten ei ole mahdollista määritellä yksiselitteistä kaikkiin tilanteisiin ja kaikille toimijoille sopivaa kybertilannekuvaa. Eräällä tavalla kyse on sodan voiton kaavan etsimisestä, sillä periaatteessa toimija, jolla on parempi tilannekuva, menestyy vastustajaansa paremmin myös kybertoimintaympäristössä.

Kybertilannekuva ei muodostu ainoastaan teknisestä tilannekuvasta. Parhaimmillaan kybertilannekuvassa on kyetty yhdistämään onnistuneesti teknisten tietojen lisäksi uhkatiedot ja yleinen tilanne. Tärkeimpänä elementtinä toimii toistaiseksi edelleen ihminen, joka kykenee koostamaan tiedoista selkeän kokonaisuuden sekä tekemään siitä järkeviä johtopäätöksiä. Tämä kyky edellyttää sekä osaamista että tekemisen ja harjoittelun kautta muodostunutta kokemusta.

Seuraavassa kuvassa on esitetty pelkistetysti ajatus kybertilannekuvan muodostamisesta. Kaikki toimijat osallistuvat kybertilannekuvan rakentamiseen ennalta käskettyjen vastuiden mukaisesti. Tällä tavoin organisaatio kykenee varmistumaan riittävän kattavasta tilannekuvasta, ja kuitenkin se välttää turhaa päällekkäistä työtä. Kaikkien toimijoiden tuottamat osuudet kootaan samaan tietokantaan tai järjestelmään. Siten tiedot ovat kaikkien toimijoiden saatavilla, ja jokainen kykenee valitsemaan oman toimintansa kannalta tärkeät tiedot ja muodostamaan omanlaisensa tilannekuvan ja sen avulla tilanneymmärryksen. Tietokannasta muodostetaan myös taktinen sekä operatiivinen kybertilannekuva. Se tehdään valitsemalla, yhdistämällä ja analysoimalla toimijoiden tärkeimmät tiedot, jotta kyetään muodostamaan taktista tai operatiivista päätöksentekoa tukeva kybertilannekuva.



Kuva 9: Kybertilannekuvan muodostaminen

Kybertoimintaympäristön luonteesta johtuen riskien arviointi korostuu entisestään. Riskien arviointia tehdään kybertoimintaympäristössä samaan tapaan kuin muissakin toimintaympäristöissä. Kybertoimintaympäristöön liittyy paljon erilaisia tekijöitä, joihin kyberoperaatioiden resursseilla ei ole mahdollista vaikuttaa tai joita ei ehkä edes ole mahdollista tunnistaa. Esimerkkinä voidaan mainita kyberoperaatiossa hyödynnettävän ohjelman arvaamaton leviäminen ja sen vaikutukset kohdejärjestelmän ulkopuolella. Riskit on kuitenkin pyrittävä tunnistamaan ja arvioimaan kyberoperaatioiden suunnittelun yhteydessä parhaalla mahdollisella tavalla, ja ne on ehdottomasti tuotava päätöksentekijöiden tietoisuuteen ennen operaation aloittamista.

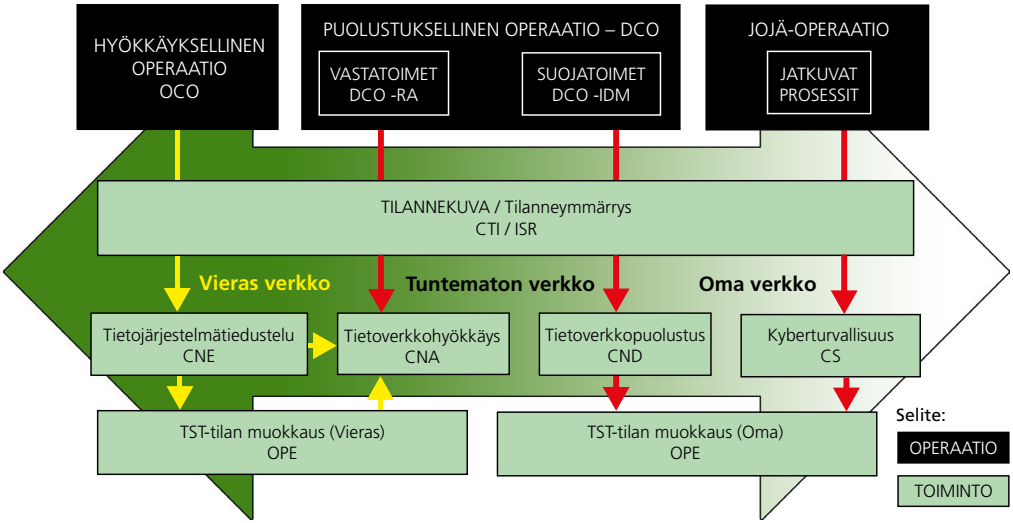
Toinen kyberoperaatioiden kannalta tärkeä asia on tärkeiden maastonkohtien arvioiminen ja tunnistaminen. Tärkeät maastonkohdat muodostavat edellytykset

puolustuksellisten ja hyökkäyksellisten kyberoperaatioiden toteuttamiselle, ja ne mahdollistavat operaatioiden tilannekuvan muodostamisen. Kybertoimintaympäristössä kiinteissä verkoissa toimittaessa tärkeällä maastonkohdalla voidaan tarkoittaa esimerkiksi tiettyä sotilasverkkoa tai sen osaa. Toimittaessa kiinteiden tai sotilaallisten verkkojen ulkopuolella tärkeitä maastonkohtia kybertoimintaympäristössä voivat olla esimerkiksi jotkin kriittisen infrastruktuurin tarjoamat mahdollisuudet.

4.2 Sotilaalliset toiminnot kybertoimintaympäristössä

Sotilaallisena toimintaympäristönä kybertoimintaympäristö koostuu kyberoperaatiosta ja erilaisista toiminnoista. Olennaista on erottaa termit operaatio ja toiminto. Kyberoperaatiot voidaan jakaa puolustuksellisiin ja hyökkäyksellisiin operaatioihin sekä johtamisjärjestelmäoperaatioihin (JOJÄ-operaatio). Esimerkiksi Yhdysvalloissa on käytössä jatkuvasti meneillään oleva JOJÄ-operaatio (DODIN OPS), jonka avulla turvataan Yhdysvaltojen puolustusministeriön maailmanlaajuisten verkkojen operaatiovarmuus. JOJÄ-operaatio on kokonaisuus jatkuvasti käynnissä olevia prosesseja, joiden avulla ylläpidetään kyberturvallisuutta. Niihin kuuluvat jokapäiväiset toimet, kuten verkon valvonta, käyttöoikeuksien hallinta, uusien laitteiden ja ohjelmistojen hankinta ja tietoturvan testaaminen sekä muut käyttäjälle näkymättömät toimet. JOJÄ-operaation päätavoite on tuottaa kyberturvallinen toimintaympäristö.

Kyberoperaatioiden suunnittelun ja toimeenpanon lähtökohtana on ajantasainen toimintaympäristötietoisuus ja tilannekuva. Kyberympäristön tilannekuvaa kootaan siis muillakin keinoilla, kuin teknisillä verkon sensoreilla tai laitteilla. Tämän johdosta ei käytetä termiä tiedusteluoperaatio. Tiedustelu ja valvonta ovat jatkuvia prosesseja, joiden avulla operaation johtamiseen tarvittavaa tilannekuvaa muodostetaan. Toiminto taas voi olla tiedustelu, suoja, johtaminen tai logistiikka. Kuvassa 10 esitetään operaatioiden ja toimintojen suhdetta kybertoimintaympäristössä ja taulukossa 16 on kuvattu tärkeimmät toiminnot.



Kuva 10: Kyberoperaatiot ja toiminnot

Tietoverkkohyökkäys (CNA, Computer Network Attack)	Tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön. Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Tietoverkkopuolustus (CND, Computer Network Defense)	Tekninen puolustus. Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction.
Tietojärjestelmätiedustelu (CNE, Computer Network Explotation)	Vastustajan tietojärjestelmien heikkouksien etsimistä ja hyödyntämistä hyökkäyksien torjumiseksi sekä tiedonhankintaa toimintaympäristötietoisuuden muodostamiseksi ja ennakkovaroituksen antamiseksi. Tietojärjestelmätiedustelu on osa tietoverkkotiedustelua, johon kuuluu lisäksi tietoliikennetiedustelu.
Taistelutilan valmistelu (OPE, Operational Preparation of the Environment)	Kybertoimintaympäristöön tehtävät muutokset, joita tehdään joko omiin tai vieraisiin tietojärjestelmiin. Tavoitteena on parantaa omia toimintaedellytyksiä ja toiminnanvapautta sekä estää tai heikentää vastustajan toiminnan edellytyksiä.

Taulukko 16: Toiminnot kybertoimintaympäristössä

Sotilastiedustelu suorittaa strategista tiedustelua useilla tiedustelulajeilla. Niitä ovat muun muassa signaalitiedustelu (SIGINT), geotiedustelu (GEOINT), henkilötiedustelu (HUMINT) ja avointen lähteiden tiedustelu (OSINT). Tietoverkkotiedustelu on osa signaalitiedustelua ja se jaetaan tietoliikennetiedusteluun ja tietojärjestelmätiedusteluun (computer network exploitation, CNE). Sotilastiedustelu tuottaa tiedustelutietoa operatiiviselle ja taktiselle tasolle operaatioita varten.

Kyberuhkatiedustelu (cyber threat intel, CTI) on puolustajan tai hyökkääjän suorittamaa omasuojatiedustelua. Uhkatiedustelun keinoin pyritään selvittämään mahdollisia hyökkäystapoja tai hyökkääjiä, jotta kyetään paremmin varautumaan. Uhkatiedustelua suorittavat kaikki kybertoimintaympäristössä aktiivisesti toimivat joukot, ja sitä tehdään kaikilla tasoilla alkaen järjestelmien ylläpitäjistä. Uhkatiedustelua voisi verrata tukikohdan lähipuolustukseen, jossa partiot kiertävät tukikohtaa ja koettavat paikantaa vihollisen ennen kuin se aloittaa hyökkäyksen tai etenevän joukkueen tunnustelijoihin, jotka mahdollistavat reagoinnin viholliseen.

Kybertiedustelu ei ole yleisesti ja yksiselitteisesti ymmärrettävä käsite. Sitä kuitenkin käytetään monissa yhteyksissä. Yleisesti kybertiedustelulla tarkoitetaan kyberoperaatioiden tueksi suoritettavaa tiedustelua, joka voidaan suorittaa millä tahansa tiedustelumenetelmällä tai niiden yhdistelmällä. Kybertiedustelun tavoitteena on esimerkiksi erilaisten kybertoimintaympäristön toimijoiden tunnistaminen sekä heidän kykyjen, heikkouksien ja aikomusten arviointi. Näitä arvioita käytetään kyberuhkatason määrittämiseen ja omien toimintamahdollisuuksien tunnistamiseen. Kybertoimintaympäristöön liittyvä tiedustelu ja sen kokonaisuus on laaja. Kokonaisuuden hahmottamiseksi kybertoimintaympäristöön liittyvän tiedustelun tärkeimmät toiminnot on kuvattu taulukossa 17.

Taistelutilan muokkaamisella (operational preparation of environment, OPE) tarkoitetaan muutoksia, joita tehdään joko omiin tai vieraisiin tietojärjestelmiin. Puolustuksellista taistelutilan muokkaamista on esimerkiksi omien järjestelmien koventaminen (hardening), jonka tarkoituksena on tehostaa omien järjestelmien turvallisuutta. Puolustuksessa valelaitteiden (honeypot) tai ansojen luonti omaan verkkoon on myös mahdollista. Hyökkäyksellistä taistelutilan muokkaamista on esimerkiksi erilaisten takaporttien (remote access trojan, RAT) tai monimutkaisten piilohaittaohjelmien (root kit) luonti vastustajan järjestelmiin.

Kybertiedustelu	Yleensä kybertiedustelulla tarkoitetaan kyberoperaatioiden tueksi suoritettavaa tiedustelua, joka voidaan suorittaa millä tahansa tiedustelumenetelmällä tai niiden yhdistelmällä.
ISR (Intelligence, Surveillance, Reconnaissance)	Tiedustelun kokonaisuus kybertoimintaympäristössä koostuu sekä tietoverkkotiedustelusta että kaikista muista perinteisistä tiedustelun osa-alueista, joiden avulla kybertoimintaympäristön tilannekuvaa muodostetaan. Asiaa voidaan kuvata englanninkielisen lyhenteen ISR avulla. Tällöin: • Intelligence = Yleistä tiedon keruuta ja analysointia halutusta aiheesta. • Surveillance = Verkon tai toimijan valvontaa. • Reconnaissance = Kohdistettua tiedustelua johonkin tiettyyn kohteeseen.
Kyberuhkatiedustelu (CTI, Cyber Threat Intelligence)	Kybertoimintaympäristössä tai sen avulla tapahtuvaa oman toiminnan suojaamiseksi tehtävää tiedustelua, jonka tavoitteena on luoda paremmat edellytykset varautua erilaisiin hyökkäyksiin.
Tietoverkkotiedustelu (DNI, Digital Network Intelligence)	Tietoverkossa oleviin lähteisiin kohdistuva tiedonhankinta, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhkista, riskeistä, mahdollisuuksista ja muutoksista. Tietoverkkotiedustelu koostuu tietoliikennetiedustelusta ja tietojärjestelmätiedustelusta ja se voi tapahtua niin maan sisällä kuin rajojen ulkopuolella.
Tietoliikennetiedustelu	Tietoliikennetiedustelu on viestintäverkossa tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä tiedustelutehtävän suorittamiseksi.
Tietoliikennetiedustelu (CNE, Computer Network Exploitation)	Vastustajan tietojärjestelmien heikkouksien etsimistä ja hyödyntämistä hyökkäyksien torjumiseksi sekä tiedonhankintaa toimintaympäristötietoisuuden muodostamiseksi ja ennakkovarautuksen antamiseksi. Tietojärjestelmätiedustelu on osa tietoverkkotiedustelua, johon kuuluu lisäksi tietoliikennetiedustelu.

Taulukko 17: Kybertoimintaympäristöön liittyviä tiedustelun käsitteitä

Koventaminen (hardening)	Tietojärjestelmien koventaminen tarkoittaa järjestelmien uudelleen konfigurointia eli kaikkien turhien laitteiden, palveluiden ja ohjelmistojen poistamista tietojärjestelmistä. Lisäksi koventamiseen kuuluu ohjelmistojen luotettavuuden ja ajantasaisuuden varmistaminen.
Hunajapurkki (honeypot)	Kybertoimintaympäristössä hunajapurkilla tarkoitetaan ansaa, johon vastustaja houkutellaan ja samalla kerätään tietoa vastustajan kyvyistä ja kiinnostuksen kohteista.
Etähallittava takaovi (RAT, Remote Access Trojan)	Etähallittavalla takaovella tarkoitetaan haittaohjelmaa, joka mahdollistaa kohdejärjestelmän kontrolloimisen etäyhteyttä käyttäen verkon yli. Etähallittava takaovi asennetaan uhrin tietämättä, ja se pyrkii toimimaan sekä uhrin että kohdejärjestelmän turvamekanismien huomaamatta.

Taulukko 18: Kyberoperaatioihin liittyviä toimintoja

4.3 Puolustuksellinen operaatio (defensive cyberspace operation, DCO)

Puolustuksellisessa kyberoperaatiossa toimeenpano käynnistyy, kun havaitaan poikkeamia tai uhkatiedustelun mukaan jotain on tapahtumassa. Tilanne, jossa esimerkiksi huomataan luvaton tunkeutuja järjestelmässä tai luvattomia muutoksia verkossa aiheuttaa suojatoimia (defensive cyberspace operation - internal defensive measures, DCO-IDM). Tällaisia operaatioita suorittavat tyypillisesti siihen erikoiskoulutetut kyberpuolustuksen ammattilaiset ja toimintona on tietoverkkopuolustus (computer network defense, CND). Operaation tarkoitus on tyypillisesti etsiä vastustaja, rajoittaa sen toimia sekä karkottaa vastustaja omasta järjestelmästä. Suojatoimia voidaan tehdä yhdessä kumppaneiden kanssa pyytämällä esimerkiksi palveluntarjoajaa katkaisemaan verkkoliikenne määritetyistä lähteistä. Esimerkki toteutuneista suojatoimista eli puolustuksellisesta kyberoperaatiosta (DCO-IDM) on esitetty taulukossa 19.

Kuka?	Clifford Stoll, tähtitieteilijä ja tietokoneiden ylläpitäjä Lawrence Berkeley National Laboratory, jäljittää hakkeria 1980-luvulla Yhdysvalloissa.
Mitä?	The Cuckoo's egg on kirja, jonka kirjoittaja Clifford Stoll kertoo tarinaa siitä, kuinka hän jäljitti löytämäänsä hakkeria työpaikkansa tietojärjestelmistä aina sotilastukikohtiin ja lopulta Saksaan saakka.
Miten?	Kirjassa kuvataan laajasti kybertoimintaympäristön alkuaikoja 1980 -luvulla ja sen aikaisia menetelmiä.
Kohde?	Kirjassa jäljitettävä hakkeri pyrki hankkimaan sotilaallisia tietoja Yhdysvalloista myydäkseen niitä eteenpäin Neuvostoliittoon.
Miksi?	Kirja kuvaa hyvin sekä alkuaikojen kybertoimintaympäristön haavoittuvuuden osaavan hyökkääjän tunkeutumisille että ennakkoluulottoman ja periksiantamattoman selvitystyön saavutukset turvallisuuden parantamiseksi.
Milloin?	Tapahtumat alkavat vuonna 1986, ja kirja on julkaistu 1989.
Vaikutus	Kirja on kybertoimintaympäristöön liittyvän kirjallisuuden merkkiteoksia. Vaikkakin tekniikka on kehittynyt paljon, monet kirjan käsittelemistä asioista ovat edelleen ajankohtaisia.
Lisätiedot	http://pdf.textfiles.com/academics/wilyhacker.pdf Clifford Stoll: The Cuckoo's Egg

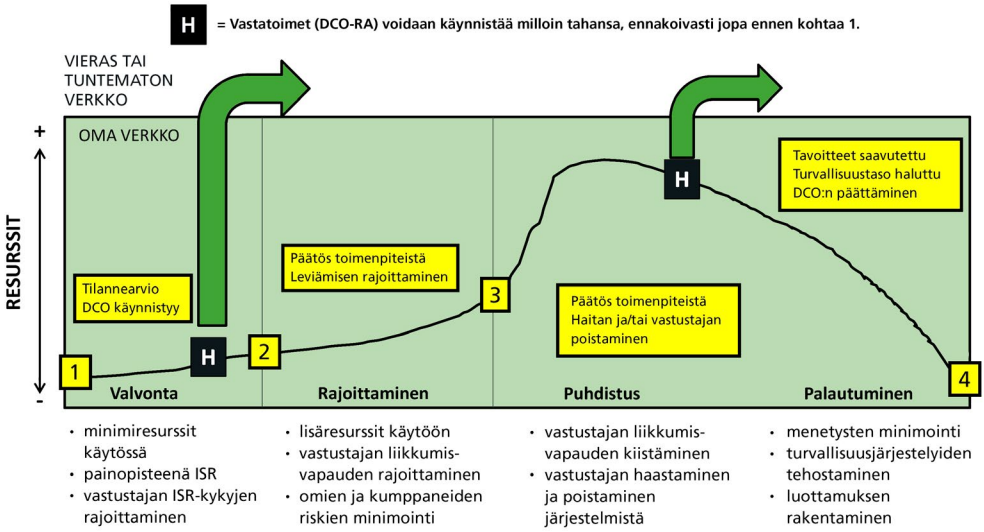
Taulukko 19: Esimerkki DCO-IDM operaatiosta

Toimintaa, jossa puolustuksellisen operaation vastatoimet ulotetaan tuntemattomaan tai vastustajan verkkoon, kutsutaan vastatoimiksi (defensive cyberspace operation - responsive actions, DCO-RA). Vastatoimet voidaan käynnistää missä tahansa vaiheessa havaittua hyökkäystä tai ennakoivasti muun muassa tiedustelua vastaan. Vastatoimet suoritetaan oman järjestelmän ulkopuolelle, ja jos esimerkiksi havaitaan hyökkääjän tulevan jostain tietystä verkosta tai koneesta, puolustaja voi ottaa hyökkääjän järjestelmän haltuun tai jopa kaataa sen tarvittaessa. Toiminnosta käytetään myös termiä *hackback*. Teknisesti kyseessä on tietoverkkohyökkäys (computer network attack, CNA). Esimerkki toteutuneista vastatoimista eli puolustuksellisesta kyberoperaatiosta (DCO-RA) on esitetty taulukossa 20.

Kuka?	Ranskan poliisi yhdessä tietoturvayritys Avastin asiantuntijoiden kanssa.
Mitä?	Ranskan poliisi onnistui kyberoperaation avulla estämään ja purkamaan maailmanlaajuisen 850 000 saastuneesta tietokoneesta muodostetun bottiverkon toiminnan ja käytön rikolliseen toimintaan.
Miten?	Operaation toteutuksesta vastasi Ranskan Gedarmerien Cybercrime Fighting Centre (C3N), joka toimi yhteistyössä Avastin ja Yhdysvaltojen liittovaltion poliisin (FBI) kanssa. Operaatiossa rikollisten komentopalvelin otettiin haltuun ja korvattiin operaatioon sopivalla palvelimella. Palvelin vastasi bottiverkkoon kuuluvien tietokoneiden yhteydenottopyyntöihin erityisellä paluuviestillä, jonka avulla levinnyt haittaohjelma kyettiin tuhoamaan.
Kohde?	Kyberoperaation kohteena oli rikollisjärjestö, joka oli onnistunut saastuttamaan yli 850 000 tietokonetta Retadup madolla.
Miksi?	Rikollisjärjestö käytti luvatta käyttöön otetuista saastuneista tietokoneista muodostettua bottiverkkoa virtuaalivaluutan louhintaan, ja samalla se heikensi merkittävästi saastuneiden tietokoneiden toimivuutta.
Milloin?	Retadup –mato otettiin erityisseurantaan maaliskuussa 2019 ja varsinainen operaatio toimeenpantiin elokuun 2019 lopussa.
Vaikutus	Operaatio onnistui ja bottiverkko saatiin purettua. Tämänkaltaisen ja näin laajan kyberoperaation toteuttaminen ja onnistuminen on hyvin harvinaista.
Lisätiedot	https://www.techradar.com/news/french-police-take-down-global-malware-botnet https://www.zdnet.com/article/avast-and-french-police-take-over-malware-botnet-and-disinfect-850000-computers/

Taulukko 20: Esimerkki DCO-RA operaatiosta

Kuvassa 11 on esitetty, kuinka puolustuksellinen operaatio käynnistyy perustilasta ja kuinka paljon missäkin operaation vaiheessa vaaditaan resursseja. Suojatoimet (DCO-IDM) voidaan jakaa valvontaan (screen), rajoittamiseen (contain), puhdistamiseen (clear) sekä palautumiseen (secure). Lisäksi missä tahansa vaiheessa voidaan tarvittaessa toteuttaa vastatoimet (DCO-RA). Kyberhyökkäykseen voidaan myös vaikuttaa iskemällä fyysisesti hyökkääjään tai infrastruktuuriin.



Kuva 11: Puolustukselliset kyberoperaatiot

Puolustuksellisten kyberoperaatioiden (DCO) toiminta-ajatus voidaan kuvata kuten jalkaväessä. Kyberturvallisuutta (CS) voi verrata puolustukseen ryhmittymiseen, tukikohtapalveluun ja tukikohdan vartiointiin. Vihollisen tunkeutuessa ryhmitykseen tehdään tukikohdan sisäinen vastaisku kuten suojatoimet (DCO-IDM), jotta saadaan vallattua menetetyt asemat takaisin. Jos vihollisen lisävoimien tulo täytyy estää tai seurata vetäytyvää hyökkääjää, kyseessä on vastahyökkäys oman ryhmityksen ulkopuolelle eli vastatoimet (DCO-RA).

4.4 Hyökkäyksellinen operaatio (offensive cyberspace operation, OCO)

Hyökkäyksellisellä kyberoperaatiolla voidaan tarkoittaa mitä tahansa suunniteltuja toimia vaikuttaa kohteen kyberympäristöön tai sen kautta fyysiseen maailmaan. Operaation toteuttaja voi olla valtiollinen toimija, rikollisryhmä tai jopa yksittäinen henkilö. Useissa tapauksissa toimijat haluavat salata osallisuutensa operaatioihin ja he pyrkivät peittämään identiteettiänsä käyttäen järjestäytyneitä ryhmiä tai teknisiä salaustoimenpiteitä. Hyökkäyksellisen kyberoperaation toteuttaja käyttää usein kaapattuja tietokoneita, palvelimia ja muita verkkoon kytkettyjä laitteita. Tästä syystä toteuttajaa ei pystytä paikantamaan IP-osoitteen perusteella, mikä tekee tämän tunnistamisesta ja paikantamisesta vaikeaa. Lisäksi valtioiden erilaiset oikeuskäytännöt estävät hyökkäyksen toteuttajan saamisen lailliseen edesvastuuseen, vaikka tämä olisi tunnistettu ja paikannettu. Jos hyökkääjää ei kyetä tunnistamaan, myös sekä hyökkääjän motivaatioiden selvittäminen, että vastatoimien toteuttaminen on hankalampaa. Lisäksi on tilanteita, joissa hyökkääjän tunnistamista ei haluta paljastaa, jotta omat kyberkyvyt eivät paljastuisi vastustajalle.

Useat valtiot ovat jo ilmoittaneet, että joutuessaan hyökkäyksellisen kyberoperaation kohteeksi ne varaavat itselleen oikeuden vastata tappavalla kineettisellä voimalla. Esimerkiksi Yhdysvallat on jo tuonut julkisuuteen tällaisia operaatioita, joissa hakkeri etsittiin kyberiskun jälkeen ja eliminoitiin kotimaassaan. Lisäksi Israelin asevoimat on vastannut kyberhyökkäyksen uhkaan tuhoamalla välittömästi kybertoimijat ja heidän toimitilansa ilmaiskulla. Esimerkki tällaisesta operaatiosta on löydettävissä taulukosta 21.

Kuka?	Israelin asevoimien suorittama ilmaisku Hamasin kybertoimijoita vastaan.
Mitä?	Israelin asevoimat onnistuivat estämään Hamasin hyökkäyksellisen kyberoperaation ja saamaan samalla selville hyökkääjien fyysisen sijainnin.
Miten?	Hamasin hyökkäyksellistä kyberoperaatiota yrittäneiden henkilöiden sijainti kyettiin määrittelemään osana Israelin puolustuksellista kyberoperaatiota. Tämän jälkeen paikannettuun sijaintiin suoritettiin välittömästi ilmaisku.
Kohde?	Rakennus, josta Hamasin kyberoperaatioita toteutettiin sekä kyberoperaatioita toteuttava henkilöstö ja välineistö.
Miksi?	Israelin asevoimien mukaan kybertoimintaympäristössä tai sen avulla tehtäviin hyökkäyksiin vastataan samalla tavoin kuin mihin tahansa muihin siihen kohdistuviin hyökkäyksiin tehokkaimmilla käytössä olevilla keinoilla.
Milloin?	Syyskuu 2019.
Vaikutus	Ilmaiskun kohteeksi joutunut rakennus tuhoutui ainakin osittain, sen sisällä olevista henkilöistä tai välineistöstä ei ole varmaa tietoa, mutta ottaen huomioon toteutetun ilmaiskun nopeuden, vaikutukset henkilöstöön ja välineistöön ovat myös todennäköisiä. Kyseessä oli ensimmäinen kerta, kun kyberhyökkäykseen vastattiin välittömällä sotilaallisella voimakäytöllä.
Lisätiedot	https://www.wired.com/story/israel-hamas-cyberattack-air-strike-cyberwar/ https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#122bffa6afb5

Taulukko 21: Esimerkki kyberoperaatio sodankäynnin osana 1

Hyökkäyksellistä kyberoperaatiota edeltää aina perusteellinen tiedustelu. Siihen käytetään kaikkia tiedustelun keinoja, ei vain kybertoimintaympäristössä tehtävää tietoverkkotiedustelua (digital network intelligence, DNI). Tiedustelu kyberoperaatiota varten saattaa kestää jopa vuosia, ja se voi sisältää useita eri toimijoita. Hyökkäyksellinen kyberoperaatio pyrkii vaikuttamaan vastustajan tietojärjestelmiin tai laitteisiin. Vaikutus voi ilmentyä kaikilla toimintaympäristön tasoilla aina loogisesta fyysiseen tasoon asti.

Hyökkäyksellisen operaation haluttuja vaikutuksia voi olla esimerkiksi jonkin tietyn verkon, laitteen tai palvelun kiistäminen (deny) halutuksi ajaksi. Kiistäminen voidaan suorittaa useilla tavoilla ja tasoilla, joita ovat häirintä (degrade), lamauttaminen (disrupt) tai tuhoaminen (destroy). Häirintä voi tarkoittaa esimerkiksi haitta-

ohjelmaa, joka hidastaa vastustajan tietokoneita ja tekee niiden käyttämisestä tehotonta. Lamauttaminen voi olla esimerkiksi palvelunestohyökkäys, jossa käyttäjät eivät pääse haluamaansa palveluun määräajaksi. Voimakkain kiistämisen muoto on tuhoaminen, jossa tuhotaan pysyvästi joko ohjelmistoja tai aiheutetaan jopa fyysisen laitteen tuhoutuminen, kuten Stuxnet-haittaohjelmassa. Stuxnet on esitelty jo luvun 2.1 taulukossa 9.

1. Estäminen (deny)	Tavoitteena on estää kohteelle pääsy, kohteen toiminta tai kohteen saatavuus tietyllä tasolla tietyn ajan.
1.1 Heikentäminen (degrade)	Heikentämisellä kohteelle pääsyä, kohteen saatavuutta vaikeutetaan ja kohteen toiminnan tasoa heikennetään ennalta määrättyyn prosenttitasoon kapasiteetista. Lisäksi voidaan myös määritellä haluttu vaikutusaika sekä tarvittaessa myös arvioida kohteen hajoamistaso.
1.2 Häirintä (disrupt)	Häirinnän avulla kohteelle pääsy, kohteen saatavuus tai kohteen toiminta estetään väliaikaisesti kokonaan ennalta määrättyjen alkamis- sekä päättymisaikojen mukaisesti.
1.3 Tuhoaminen (destroy)	Tuhoamista käytetään kun halutaan kokonaan ja peruuttamattomasti estää kohteelle pääsy, kohteen toiminta tai saatavuus.
2. Manipulointi (manipulate)	Manipulaation avulla pyritään hallitsemaan tai muuttamaan tietoa ja tietojärjestelmiä. Manipuloimisen vaikutukset eivät yleensä paljastu välittömästi vaan näyttäytyvät ja kertautuvat ajan myötä. Manipuloimisesta huolimatta kohde vaikuttaa yleensä toimivan normaalisti.

Taulukko 22: Hyökkäyksellisten kyberoperaatioiden vaikutuksia

Toinen hyökkäyksellisen operaation tavoite, tietojen manipulointi (manipulation), ei ole näkyvä, mutta se voi olla monella tapaa jopa vaarallisempi. Manipuloinnilla pyritään muuttamaan järjestelmien sisäistä tietoa tai vaikuttamaan niiden esittämään tietoon. Esimerkkinä voidaan mainita Israelin suorittama operaatio Orchard, jossa haittaohjelma ujutettiin Syyrian ilmapuolustukseen ja tutkat näyttivät vääriä havaintoja Israelin koneista, eikä ilmatorjunta kyennyt tämän johdosta toimimaan tehokkaasti. Operaatio on esitetty taulukossa 23.

Kuka?	Israelin ilmaoperaatio Syyrian ydintutkimuslaitosta vastaan.
Mitä?	Israelin yhteisoperaatio, jossa tavoitteena oli tuhota Syyriassa oleva ydintutkimuslaitos.
Miten?	Israel toteutti yhteisoperaation ORCHARD, jossa Syyrian ilmapuolustusjärjestelmään ujutettiin ilmatilannekuvaa vääristävä haittaohjelma. Lisäksi operaatiota tuettiin erikoisjoukoilla ja elektronisen sodankäynnin kyvyillä.
Kohde?	Dayr az-Zawr (Deir ez-Zur) ydintutkimuslaitos Syyriassa.
Miksi?	Syyrian ydinaseohjelman hidastaminen.
Milloin?	Ilmaoperaatio toteutettiin 6.9.2007.
Vaikutus	Kyberhyökkäyksen ja siinä käytetyn haittaohjelman avulla Syyrian ilmapuolustusjärjestelmä esitti manipuloitua ilmatilannekuvaa ja ei näin ollen kyennyt estämään Israelin ilmaoperaatiota, jonka seurauksena kohteena ollut tutkimuslaitos tuhoutui.
Lisätiedot	https://fi.wikipedia.org/wiki/Operaatio_Orchard

Taulukko 23: Esimerkki kyberoperaatio sodankäynnin osana 2

Manipulaatiota voidaan käyttää lukemattomin tavoin riippuen siitä, mihin tietoon päästään käsiksi. Jos esimerkiksi päästään käsiksi vastustajan maalitietokantoihin, voidaan muuttaa aseille evästettäviä koordinaatteja, mikä johtaa täsmäaseiden ohjautumiseen pois maaleista. Yksi useasti havaittu tietomanipuloinnin keino on paikannusjärjestelmien tietojen manipulointi, jolla voidaan ohjata esimerkiksi lento- tai meriliikennettä harhaan.

Hyökkäyksellisten operaatioiden (OCO) toiminta-ajatus voidaan kuvata kuten jalkaväessä. Ensin tulee tehdä tiedustelua kohteesta sekä selvittää mahdolliset heikot kohdat (DNI ja muut tiedustelulajit). Tämän jälkeen tehdään hyökkäysvalmistelut ja tulivalmistelua varten paikannetaan maalit (OPE). Lopuksi suoritetaan varsinainen isku ja vaikuttaminen kohteeseen (CNA).

Tärkeimmät lähteet

Cyber and Electromagnetic Activities, UK Joint Doctrine Note 1/18, Development, Concepts and Doctrine Centre, UK Ministry of Defence, 2018. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf].

Cyber Primer, Second Edition, Development, Concepts and Doctrine Centre, UK Ministry of Defence, 2016. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf].

Cyberspace and Electronic Warfare Operations, FM 3-12, Headquarters, Department of the Army, 2017. [https://fas.org/irp/doddir/army/fm3-12.pdf].

Cyberspace Operations, Joint Publication 3-12, US Joint Chiefs of Staff, 8.6.2018. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf].

Foreign Economic Espionage in Cyberspace, National Counterintelligence and Security Center, 2018. [https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf].

Kosola, Jyrki & Jokinen, Janne, *Elektroninen sodankäynti, osa 1 - taistelun viides dimensio*, No 2, Julkaisusarja 5, Tekniikan laitos, Maanpuolustuskorkeakoulu, 2004.

Kyberpuolustuksen kehittämisen strategiset linjaukset, Puolustusministeriö, 2019. [http://julkaisut.valtioneuvosto.fi/handle/10024/161771].

Kyberpuolustus 2025 Konsepti 1.0, Pääesikunta, PvAH asiakirja AM9122/PEJOJÄOS, 11.5.2016, Suojaustaso IV, käyttö rajoitettu.

Kyberturvallisuuden sanasto, Turvallisuuskomitea, TSK 52, Sanastokeskus TSK ry, Helsinki, 2018.

Laki sotilastiedustelusta, 590/2019, 26.4.2019, [https://www.finlex.fi/fi/laki/alkup/2019/20190590].

Lehto, Martti, Limnéll, Jarno, Innola, Eeva, Pöyhönen, Jouni, Rusi, Tarja, Salminen, Mirva, *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi*, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017, Valtioneuvoston kanslia, 17.2.2017. [https://tietokayttoon.fi/julkaisu?pubid=17805].

Langner, Ralph, *To kill a centrifuge - A technical analysis of what Stuxnet's creators tried to achieve*, The Langner Group, 2013, [https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf].

Palvelunestohyökkäykset ovat internetin arkipäivää, Tietoturva nyt -julkaisu, Liikenne- ja viestintävirasto Traficom, [https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/04/ttn201604291231.html].

Schmitt, Michael N (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Second edition, Cambridge University Press, 2017.

Stoll, Clifford, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*, Pocket Books, USA, 1990.

Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013, Turvallisuus-komitean sihteeristö, Forssa Print, 2013.

Suomen kyberturvallisuusstrategia 2019, Valtioneuvoston periaatepäätös 3.10.2019, Turvallisuuskomitean sihteeristö, 2019, [https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf].

Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 - 2020, Turvallisuuskomitea. [https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf].

Tietoturvan vuosi 2017, Viestintäviraston julkaisu 001/2018, Käytetty 26. 4 2018, [https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tietoturvan-vuosi-2017.pdf].

Tuovinen, Jussi & Kivimäki Veli-Pekka: Kyberoperaatioiden jalanjäljissä, *Kyberajan viestitaktiikka*, Kirjapaino Bookcover Oy, Seinäjoki, 2018.

Valtioneuvoston puolustusselonteko, Valtioneuvoston kanslian julkaisusarja 5/2017, Lönnberg Print & Promo, Helsinki 16.2.2017.

Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 2.11.2017, Turvallisuuskomitea, 2017. [https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf].

Maanpuolustuskorkeakoulu
PL 7, 00861 HELSINKI

Puh. +358 299 800

www.mpkk.fi

ISBN 978-951-25-3119-6 (nid.)
ISBN 978-951-25-3120-2 (pdf)
ISSN 2489-4354 (painettu)
ISSN 2343-0753 (verkkojulkaisu)

Puolustusvoimat
The Finnish Defence Forces