Cyberwatch Finland

MAGAZINE 1/2025

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Intohimona kyberturvallisempi maailma

Cyberwatch MAGAZINE

JULKAISIJA Cyberwatch Oy
Nuijamiestentie 5 C
Helsinki, Finland

TOIMITUS Päätoimittaja
Aapo Cederberg
aapo@cyberwatchfinland.fi

TAITTO PuulaMedia / Mari Riepponen
KUVAT AdobeStock, PhotoShopAI
PAINO Scanseri Oy, Helsinki

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

SISÄLTÖ

Cyberwatch Finland
MAGAZINE 1/2025

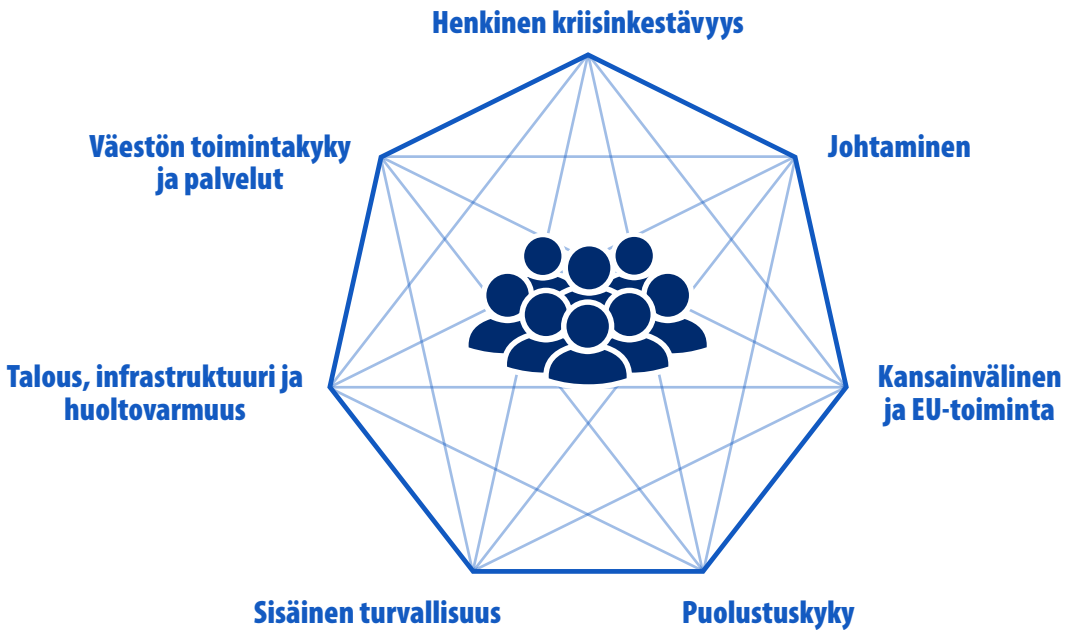
Cyberwatch Finland

Sota nopeuttaa kehitystä - pysymmekö perässä?

Historia on osoittanut, että teknologia kehittyy sota- ja kriisitilanteissa paljon nopeammin kuin normaalioloissa. Ukrainan sota ei tee tässä poikkeusta. Vaikutus näkyy niin sotilasteknologiassa kuin kaksoiskäyttötuotteissakin. Lennokkien massamainen käyttö niin tiedusteluun kuin vaikuttamiseen on muuttanut myös operaatioiden suunnittelua ja taistelutaktiikkaa. Kriittinen infrastruktuuri on ollut jatkuvan kineettisen vaikuttamisen ja kyberoperaatioiden kohteena. Siitä huolimatta monet asiantuntijat ovat sitä mieltä, että matkapuhelin verkot toimivat tällä hetkellä Ukrainassa paremmin kuin ennen sotaa.

Sodan kuva ja menetelmät ovat myös muuttuneet. Samaan aikaan käydään sekä perinteistä tuhoamissotaa että informaatio-, kyber- energia-, talous- ja hybridisotaa. Kaikki yhteiskunnan kriittiset sektorit voidaan nähdä sodan näyttämönä. Modernit yhteiskuntarakenteet sisältävät maaleja ja heikkouksia, joihin hyökkäämällä voidaan saavuttaa haluttuja poliittisia, taloudellisia, sotilaallisia sekä kognitiivisia vaikutuksia. Herääkin kysymys, voidaanko näillä sodankäynnin eri muodoilla voittaa sota tai voidaanko voittoa yleensä määritellä. Perinteisesti sodan voittajat ovat saaneet haltuunsa vallattuja alueita ja oikeuden kontrolloida ja sanella hävinneen osapuolen poliittisia ratkaisuja. Tämä vaikuttaa nytkin olevan Venäjän hyökkäyssodan päämääränä. Näyttääkin siltä, että sota voidaan voittaa vain kineettisillä operaatioilla. Herää kysymys mikä on näiden muiden sodankäynnin muotojen merkitys?

Eräät sotataidon asiantuntijat väittivät, että tulevaisuuden sodat voidaan voittaa kybersodankäynnillä tai avaruudessa tehtävillä operaatioilla. Ukrainan sodan kokemusten valossa näyttäisi siltä, että näin ei ole, vaan näillä moninaisilla sodankäynnin eri muodoilla on pääasiassa tukirooli perinteisen sodan voittamiseksi. Toinen näkökulma on, miten voidaan käydä sotaa ilman sodan julistamista ja perinteisen sodan kynnyksen alapuolella eli silloin, kun kineettistä voimaa ei voida tai haluta käyttää kuin erilaisissa sa-



Kuva:
s. 16 ”VALTIONEUVOSTON JULKAISUJA 2025:1
Kuvio 2. Yhteiskunnan elintärkeät toiminnot.”

botaasioperaatioissa. Hybridisodan konsepti on kehitetty juuri tätä tarkoitusta varten. Siinä halutaan saavuttaa sodan päämäärät ilman sotilaallisen voiman käyttöä, eli voittaa sota ampumatta laukaustakaan.

Eurooppalaiset maat ja Suomi niiden mukana ovat joka päivä informaatio- ja kyberoperaatioiden kohteena. Venäjä ja muut epävakautta tuottavat toimijat haluavat vaikuttaa meidän poliittiseen päätöksentekoomme, hyvinvointiyhteiskunnan toimivuuteen ja kansalaisten mielipiteisiin aiheuttamalla pelkoa ja epävarmuutta kansalaisten jokapäiväisiin palveluihin ja elämän laatuun. Jokaisella vakavalla kyberhyökkäyksellä saadaan aikaan informaatiovaikutuksia niin lyhyellä kuin pidemmälläkin aikavälillä. Tästä hyvänä konkreettisena esimerkkinä ovat pankkeihin kohdistuneet hyökkäykset, jotka saavat pelkäämään rahojemme ja varallisuutemme menettämistä.

Suomessa julkaistiin tammikuussa päivitetty yhteiskunnan turvallisuusstrategia. Se on jo viides päivitys yhteiskunnan kokonaisturvallisuuden mallista. Konsepti ja keskeiset periaatteet ovat pysyneet pääosin entisellään ja muodostavat perustan yhteiskunnan varautumiselle ja kriisinkestävyydelle. Ehkä merkittävin muutos on ihmisten nostaminen timantin keskiöön ja henkisen kriisinkestävyyden siirtäminen timantin yläkulmaan. Tämä on varmasti perusteltua, kun sitä katsoo sodankäynnin ja modernien vaikuttamisen muotojen näkökulmasta. Sota voitetaan, jos sotilaiden taistelutahto pysyy korkealla ja siviiliyhteiskunta pystyy turvaamaan elintärkeät toimintonsa kaikissa oloissa.

Yli 80 prosenttia onnistuneista kyberhyökkäyksistä johtuu tavalla tai toisella ihmisen toiminnasta. Me teemme virheitä joko vahingossa tai osaamattomuuttamme. Koulutus on siis edelleen kyberturvallisuuden voimakkain työkalu. Teknologian kehitysloikka vaatii myös ihmisten osaamisen kehitysloikkaa. Sotaa ei voida voittaa pelkästään teknologialla, aina tarvitaan myös huippuosaajia ja päteviä teknologian käyttäjiä. Henkisen kriisinkestävyyden merkitystä ei voi liiaksi korostaa ja sitäkin parantaa hyvä osaaminen. Toivottavasti nyt ja tulevaisuudessa eri elementit sodan ohella nopeuttavat ja motivoivat myös meitä ihmisiä omaksumaan uusia taitoja ja toimimaan tehokkaammin yhdessä.

Tämä julkaisu on tehty yhteistoiminnassa Euroopan hybridiuhkien torjunnan osaamiskeskuksen kanssa. Haluan kiittää heitä hyvästä ja hedelmällisestä yhteistyöstä ja tässä lehdessä julkaistavista erinomaisista artikkeleista. Erityiskiitos tohtori Josef Schröflille, jonka kanssa olemme tehneet erinomaista yhteistyötä jo seitsemän vuoden ajan. Nämä artikkelit perustuvat vuonna 2024 keväällä, Josef Schröflin johdolla järjestettyyn kuudenteen Cyber Power in Hybrid Warfare Symposiumiin.

Kyberturvallisuusteollisuuden toimintaympäristö vuonna 2025

RISTO RAJALA &
PETER SUND

Suomessa toimiva kyberturvallisuusteollisuus astui vuoteen 2025 alati muuttuvassa toimintaympäristössä. Tuore kansallinen kyberturvallisuusstrategia ja erityisesti sen valmisteilla oleva toimeenpanosuunnitelma, sekä valtion varainkäyttöä koskevat päätökset tulevat muovaamaan toimintaympäristöä kotimaassa. Merkittävin vaikutus on kuitenkin toimeenpanovaiheeseen edenneellä uudella EU-sääntelyllä, mikä pakottaa yhä useamman yrityksen ja organisaation panostamaan digitaalisten riskiensä hallintaan, tarjoten kyberturvallisuusalan tuotteita, palveluita ja ratkaisuja tarjoaville yrityksille uusia liiketoimintamahdollisuuksia.

Kansallinen kyber-turvallisuusstrategia selvillä

Valtioneuvoston periaatepäätöksenä lokakuussa 2024 annetun kyberturvallisuusstrategian tavoitteena oli uudistaa strategia vastaamaan muuttunutta toimintaympäristöä ja hallitusohjelman kirjauksia sekä täyttää NIS2-direktiivin asettamat vaatimukset. Suomen kyberturvallisuusstrategia on tärkeä asiakirja, ei pelkästään EU-oikeuden vaatimusten näkökulmasta, vaan myös siksi, että sillä voidaan suunnata politiikkatoimia, hallinnon ja eri toimijoiden yhteistyön kehittämistä sekä julkisten varojen huolellista ja vaikuttavaa käyttöä. Julkisen hallinnon sitoutuminen kyberturvallisuuden kehittämiseen on luonnollisesti välttämätöntä yhteiskuntamme digitaalisen turvallisuuden edistämiselle. Tärkeintä olisi toimenpiteiden valinta kyberturvallisuusriskien hallintavaikutuksen perusteella. Valitettavasti strategia jättää osin vaikutelman, että tarkoituksena on ollut pikemminkin listata, mitä viranomaiset haluaisivat itse tehdä ja mitä resursseja niihin haluttaisiin. On laajasti tiedossa ja kiistatonta, että Suomen talous, niin yksityinen kuin julkinen on merkittävissä vaikeuksissa eikä kestävyysvajeeseen ole odotettavissa parannusta ainakaan lyhyellä aikavälillä. Kuluvalla vuosikymmenellä nähtäneen edelleen julkisen talouden välttämättömiä sopeutustoimia. Tämä tosiasia ei kuitenkaan ole vaikuttanut virkakunnan ajattelutapoihin riittävästi, vaikka tarve on pakottava ja poliittinen ohjaus on olemassa.

Strategian resursointi, toimeenpano ja seuranta ovat onnistumisen kannalta keskeisiä mikä kohdistaa katseet kansallisen kyberturvallisuusstrategian toimeenpanosuunnitelmaan. Strategian toimeenpanoon kytketyt resurssit määrittävät sen, kuinka strategiassa esitettyihin tavoitteisiin päästään. Toimeenpanosuunnitelmassa olisi perusteltua olla tavoitellut toimet priorisoituna ja resurssit osoitettuna. Tähän on toki pyrittykin, mutta budjettimomenteille asti suunnittelu ei vaikuta kaikilta osin päätyneen. Koska samalla Euroopan muuttunut turvallisuustilanne edellyttänee edelleen panostuksia aseelliseen puolustuskykyyn ja kasvavaan velanottoon, yhteiskunnan kybersietoisuuden kokonaisvaltaisen kehittämisen kannalta tärkeää, että kyberturvallisuusstrategiaan sisällytetyt puolustushallinnon toimet toteutetaan hallinnonalan omalla rahoituksella, ja että samalla varmistetaan, että muut säästöjen kohteena olevat hallinnonalat, erityisesti laajamittaisimpien vaikutustensa vuoksi Liikenne- ja viestintäministeriön sekä Valtiovarainministeriön hallinnonalat, kykenevät toteuttamaan omat toimensa.

Laajemmin valtion varainkäyttöä tarkastellessa korostuvat erityisesti Liikenne- ja viestintäministeriön hallinnonalalle tehdyt säästöt vaikuttavat negatiivisesti yhteiskunnan kokonaisturvallisuuteen, kun asianmukaisia toimia elinkeinoelämän ja muun (siviili)yhteiskunnan kybersietoisuuden parantamiseksi ei kyetä toteuttamaan. On siksi tärkeää, että sotilaallisen kyberpuolustuksen toimet eivät vie resursseja muun yhteiskunnan suojaamiseen tähtäävältä toimilta. Tasapainoisemman tuloksen toisi hallitusohjelmassa ja Suomen digitaalisessa kompassissa kirjatun digitalisaation yhteiskehitysbudjetin tehokkaampi hyödyntäminen myös kyberturvallisuuden parantamiseen. Yhteiskehitysbudjetin avulla voidaan keskittää resursseja ja varmistaa, että hankkeet ovat linjassa hallitusohjelman prioriteettien kanssa sekä yhteen toimivia koko valtionhallinnon digitaalisen infrastruktuurin ja digitalisaatiokehityksen kanssa. Yhteiskehitysbudjetti on ollut tarkoitus ottaa käyttöön tämän vuoden aikana hallitusohjelman mukaisesti, mutta vahvistettua päätöstä ei ole.

Valtiovarainministeriön koordinoiman tietojärjestelmien vaatimuksenmukaisuuden arvioinnin nykytilaa arvioivan hankkeen yhteydessä on noussut esille Puolustusvoimien ilmaisema tarve yhteydessään toimivan itsenäisen tietojärjestelmien ja salaustuotteiden arviointi- ja hy-

väksyntäviranomaisen kehittämisestä. Mikäli Puolustushallinnolla on ylimääräisiä reusursseja tietoturvallisuuden arviointi- ja hyväksyntätoimintaan, Puolustushallinnon ydintoimintojen rajoissa niitä voitaisiin käyttää Traficomin resurssien tukena. Kyberturvallisuusteollisuuden ja laajemmin elinkeinoelämän näkökulmasta on välttämätöntä, että uudet hyväksyntä- ja arviointitoimintaan kohdennettavat resurssit ohjataan ensisijaisesti Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle, jotta toiminnan hyödyt saadaan ulosmitattua koko yhteiskunnan käyttöön. Puolustusvoimien yhteydessä kaavailluksi harkittavan arviointi- ja hyväksyntätoiminnan tulisi ensisijaisesti kohdistua NATO:sta lähtöisin olevien tietoturvallisuusvelvoitteiden arviointiin.

Keskeisiä kyberturvallisuusteollisuuden kotimaiseen toimintaympäristöön vaikuttavia lainsäädäntö- ja toimintapolitiikkahankkeita tulevat olemaan kuluvan vuoden aikana myös Huoltovarmuuden tavoitepäätös, Valmiuslain kokonaisuudistus ja kaikkien hallinnonalojen häiriö- ja kriisitilanteiden sääntelyn kokonaistarkastelu, Poliisin rikostiedustelulainsäädännön arviointi ja kehittäminen, Sisäisen turvallisuuden selonteko ja Puolustusselonteko.

EU:n suunta hahmottumassa

Euroopan Unionin alkaneen vaalikauden askelmerkit ovat alkaneet hahmottua. Kesällä 2024 julkaistiin jatkokauden saaneen Euroopan komission puheenjohtajan Ursula von der Leyenin poliittiset suuntaviivat vuosille 2024-2025, minkä voi nähdä eräänlaisena EU:n hallitusohjelmana. Muun komission kokoonpano vahvistui marraskuussa 2024, jolloin varmistui Henna Virkkusen nimitys komission teknologisesta suvereniteetista, turvallisuudesta ja demokratiasta vastaavaksi johtavaksi varapuheenjohtajaksi. Kyseessä on merkittävin suomalaiselle myönnetty kansainvälinen tehtävä koko maamme historiassa, ja on erityisen ajankohtainen yhteiskuntien digitalisoitumisen, murrosteknologioiden kehityksen ja epävakaan turvallisuusympäristön myötä. Tehtävään kuuluvat myös kyberturvallisuusasiat, joista Virkkunen on kokonaisvaltaista lähestymistapaa yhteiskunnan kyberkestävyyden vahvistamiseen, security-by-design -toimintamallia, kyberturvallisuusteollisuuden merkitystä digitaalisen infrastruktuurin turvallisuuden takajana sekä pienten ja keskisuurten yritysten merkitystä uusien innovaatioiden kehittäjinä.

Komission puheenjohtaja von der Leyen pyysi ”kolmea viisasta miestä” laatimaan raportit komission työn tueksi ja agendan hahmottamiseksi. Tehtävät valikoituivat kolme entistä eurooppalaista valtionpäämiestä: Italian entisen pääministerin Enrico Letan raportti koski EU:n sisämarkkinoiden nykytilaa kehittämistä, Italian entisen pääministerin ja Euroopan keskuspankin pääjohtajan Mario Draghin raportti EU:n kilpailukyvyn vahvistamista ja Suomen entisen presidentin Sauli Niinistön raportti EU:n sotilaallista ja siviilivalmiutta. On odotettavissa, että komission tulevat vuosittaiset työohjelmat tulevat mainittujen aiheiden kannalta määrittymään Letan, Draghin ja Niinistön raporttien asettamien suuntaviivojen mukaan.

Draghi, Letta ja Niinistö nostivat kaikki raporteissaan esille digitaalisen viestinnän ja televiestinnän turvallisuusviranomaisten lainvalvontatoimia koskevan lainsäädännön yksinkertaistamista ja harmonisointia EU-alueella. Lainvalvontaa koskevan lainsäädännön harmonisointi hyödyttäisi yrityksiä, mutta on kyseenalaista, miten asian voisi käytännössä toteuttaa. Vahva salaus edellyttää, että vain viestinnän osapuolilla on pääsy viestinnän sisältöön. Pyrkimyksiä ja kehittämisideoita käsiteltäessä onkin välttämätöntä nojata teknologisiin realiteetteihin. Digitaalisen viestinnän luottamuksellisuutta turvaavaa vahvaa päästä-päähän salausta (E2EE) ei ole mahdollista viestintäpalvelun tarjoajien myötävaikutuksella purkaa ilman kyberturvallisuuden vakavaa vaarantamista. Tähän tematiikkaan liittyy vahvasti myös viestiliikenteen salauksen heikentämiseen johtava, teknisesti toteutuskelvoton komission esitys säännöiksi lasten seksuaalisen hyväksikäytön torjumiseksi verkossa, johon Kyberala on vaikuttanut aktiivisesti.

Tätä taustaa vasten esimerkiksi Suomessa Eduskunta on asettanut Suomen kannan aihetta koskevan EU:n verkkopohjaista lasten seksuaalista hyväksikäyttöä koskevaan lakiehdotukseen:

”...ehdotetun kaltainen malli johtaisi tosiasiassa viestinnän massavalvontaan ja merkitsisi heikennystä viestinnän luottamuksellisuuden suojan sääntelyyn EU-tasolla. Suuri valiokunta katsoo, että ehdotettu malli tosiasiassa kiertäisi viestinnän päästä päähän salauksen käytön tarkoituksen, koska CSA-materiaalin kohdistuva valvonta toteutettaisiin teknisesti edellyttämällä päästä päähän salausta käyttäviä viestintäpalveluita mahdollistaman välitettävien viestien tekninen tunnistaminen jo viestijän päätelaitteessa ennen kuin viestin sisältö salautuu... ettei Suomen tule hyväksyä puheenjohtajamaan [Unkari] kompromissiesitystä tunnistamismääräystä koskevilta osin… Suuri valiokunta edellyttää, että valtioneuvosto ottaa edellä esitetyn huomioon, ja että valtioneuvosto ei hyväksy esitetyn kaltaista tunnistamismääräystä koskevaa ehdotusta.”

Käytännössä Suomessa lainsäätäjä siis ymmärtää hyvin sähköiseen viestintään liittyvät arvot ja teknologiset riskit. Lasten suojaamisen näkökulmasta lakiehdotuksen vastustaminen ei tarkoita pedofilian tukemista tai ongelman vähättelyä. Valinta ei ole pedofilian tukijoiden ja vastustajien välillä, vaan siinä, tuetaanko lasten

hyväksikäytön torjuntaa tehokkain vai tehottomin keinoin.

Taloudellinen turvallisuus oli vahvasti esillä kaikissa kolmessa raportissa. Ratkaisuiksi ehdotettiin talouden riippuvuuksien vähentämistä, toimitus- ja tuotantoketjujen turvaamista, raaka-aineiden saatavuuden varmistamista sekä tiiviimpien kauppasuhteiden solmimista samanmielisten maiden kanssa. Niinistö esitti julkisen ja yksityisen sektorin yhteistyön selvää lisäämistä riippuvuuksien ja taloudellisen painostuksen vähentämiseksi ulkomaisissa suorissa sijoituksissa ja ulospäin suuntautuvissa investoinneissa. Niinistön mukaan EU:n on myös säilytettävä kykynsä ylläpitää kriittistä infrastruktuuria ja varmistaa taloudellinen ja kyberturvallisuus, edistäen innovaatioita ja teknologista johtajuutta. Yritysten tukeminen kyberkestävyytensä parantamisessa nousi esille Niinistön raportissa osana julkisen ja yksityisen sektorin yhteistyön vahvistamista, mutta esitetyt keinot keskittyivät ainoastaan tietoisuuden lisäämiseen, harjoituksiin ja koulutukseen.

Euroopan puolustusteollisuuden vahvistaminen oli esillä kaikissa kolmessa raportissa: Puolustuksen sisämarkkinoiden ja eurooppalaisten yhteishankintojen edistämisen sekä yhteisten kyvykkyyksien (ml. kyber-, avaruus-, ilmapuolustus) kehittämisen kautta. Niinistö vaati investointitakuujärjestelmän perustamista, joka kannustaisi investointeja Euroopan puolustusteknologiseen teollisuuspohjaan. Euroopan komissio julkaisikin maaliskuussa Euroopan puolustuksen Valkoisen kirjan, jonka tarkoituksena on toimia suunnitelmana Euroopan uudelleen aseistamiseksi vuoteen 2030 mennessä. Valkoinen kirja puolustuksen tulevaisuudesta ja ReArm Europe -suunnitelma merkitsevät askelta eteenpäin Euroopan puolustuksen- ja turvallisuuden kehittämisessä. Niissä tunnistetaan kriittisten teknologioiden – kuten tekoälyn, kyberturvallisuuden, turvallisen viestinnän ja elektronisen sodankäynnin – keskeinen roolin Euroopan turvallisuuden ja resilienssin kannalta, yhdessä yhteishankintojen kanssa. Tämä on linjassa Euroopan teknologisen etumatkan kiihdyttämiseksi sotilaallisen puolustuksen alueella. Valkoisen kirjan ydinajatus on, että EU:sta tulee uskottava, itsenäinen toimija puolustuksessa jo vuoteen 2030 mennessä.

Suurten, Euroopan yhteistä etua koskevien hankkeiden tarve korostui kaikissa kolmessa raportissa: Draghi vaatii rahoitusohjelmien yksinkertaistamista, hankkeiden koon kasvattamista sekä Euroopan innovaationeuvoston (EIC) uudistamista ja laajentamista vastaamaan Yhdysvaltain puolustusministeriön edistyneiden tutkimusprojektien virastoa (DARPA), joka hyödyntää julkisia hankintoja merkittävien murrosteknologioiden rahoituksessa. Letta mainitsi eurooppalaisten salausratkaisujen vahvistamisen yhtenä mahdollisena hankkeena.

Osaavan työvoiman puute korostui Draghin ja Niinistön mukaan kriittisenä kysymyksenä – sekä taloudellisesta että varautumisen näkökulmasta: Draghi vaati keskittymistä aikuiskoulutukseen ja jäsenvaltioiden ja yksityisten organisaatioiden riittävän rahoituksen vahvistamista (mukaan lukien yritysten kannustaminen kohdentamaan enemmän resursseja koulutukseen esimerkiksi tarjoamalla verokannustimia). Niinistö totesi, että osaajapula kriittisillä aloilla, erityisesti kyberturvallisuuden toimialalla uhkaa EU:n kriisinkestävyyttä ja edellyttää toimenpiteitä. Näitä ovat hänen mukaansa esimerkiksi työvoiman tarpeiden kartoittaminen, uusien työntekijäsegmenttien kouluttaminen, työperäisen maahanmuuton helpottaminen ja työvoiman liikkuvuuden mekanismien kehittäminen kriisitilanteita varten.

Uudesta EU-sääntelystä on puhuttu paljon ja syystä: kyseessä on yksi kyberturvallisuusalan historian suurimmista toimintaympäristöä muovaavista kehityskuluista. Verkkoon kytkettäville laitteille ja ohjelmistoille tietoturvallisuutta koskevat vähimmäisvaatimukset asettava kyberkestävyyssäädös ja yhteiskunnan toiminnan kannalta kriittisille yrityksille ja organisaatioille digitaalisten riskien hallintaa ja tietoturvaloukkausten raportointia koskevia velvoitteita asettava NIS2-direktiivi ovat kyberturvallisuuden kannalta uusista säädöksistä keskeisimmät. Kuitenkin myös EU:n kybersolidaarisuusssäädöksellä tulee olemaan vaikutuksensa monen kyberturvallisuusalan yritysten liiketoimintaan, sillä sen tarjoaman rahoituksen jäsenvaltioiden kriittiset toimijat voivat parantaa kyberturvallisuuttaan hyödyntämällä ”kyberturvallisuusreserviin” kuuluvien luotettujen yritysten tuotteita, palveluita ja ratkaisuja.

Uuden EU-lainsäädännön onnistunut ja yhdenmukainen toimeenpano on ratkaiseva askel kohti aitoa ja kattavaa julkisen ja yksityisen sektorin yhteistyökulttuuria valmiuden ja kriisinkestävyyden varmistamiseksi – toki muistaen julkisen vallan siirtämistä koskevat rajoitteet. Tähän tuoreen komission on panostettava merkittävästi niin standardoinnin tukemisen ja vauhdittamisen, tietoisuuden ja jäsenvaltioiden välisen yhteistyön lisäämisen, sekä EU:n rahoitusohjelmista tarjottavan taloudellisen tuen avulla. Keskeisin ja ensisijainen käytännön toimenpide olisikin lisätä ja kanavoida EU:n avustusmuotoista rahoitustukea jäsenvaltioille modernien tietoturvaratkaisujen käyttöönottoon yrityksissä, eritoten NIS2- ja CER-direktiivien riskienhallintatoiminpiteiden toteuttamiseen.

Kansainvälistymistä vaikeasti ennustettavassa maailmassa

Kansainvälinen toimintaympäristö on muovautumassa entistäkin haastavammaksi ja vaikeammin ennustettavaksi. Autoritääristen valtioi-

den, erityisesti Kiinan ja Venäjän toimet haastavat läntistä maailmaa ja sääntöperustaista maailmanjärjestystä, minkä lisäksi Yhdysvaltojen uuden hallinnon toimintaa seuratessa jää arvoitukseksi, millaiseen rooliin Yhdysvallat tulevaisuudessa globaalisti pyrkii, ja ennen kaikkea millä keinoin. Avoinna on myös se, ketkä ovat hyötyjiä ja ketkä kärsivät vahinkoa – Yhdysvallat itse mukaan lukien. Kansainväliset kauppa- ja turvallisuuspolitiikan kysymykset ovat erittäin merkittäviä kotimaisen kyberturvallisuusteollisuuden yrityksille. Vientiin tähtäävä kansainvälistyminen on edellytys kyberturvallisuusteollisuuden yritysten kannattavuudelle sekä mahdollisuuksille panostaa tutkimukseen, kehitykseen ja innovaatioihin. Kansainvälinen markkina kyberturvallisuusteollisuuden tuotteille ja palveluille kasvaa Euroopan komission arvion mukaan jopa 15–20 prosenttia vuodessa. Suomessa kansainvälisesti tunnistettua, jopa ainutlaatuista huippuosaamista useilla kyberturvallisuusteollisuuden osa-alueilla, joihin kohdistuu merkittävää vientipotentiaalia.

Hallitus valmistelee Team Finland -yrityspalveluiden ulkomaanverkoston uudistusta, jossa Business Finlandin ulkomaantoiminnot yhdistetään ulkoasiainhallintoon. Kyberala kannattaa uudistusta ja tukee Ulkomaankauppa- ja kehitysministeri Ville Tavion asettamaa tavoitetta ”saada yrityksille entistä paremmat vienninedistämispalvelut, jotka luodaan yhteistyössä elinkeinoelämän ja henkilöstöjen kanssa.” Elinkeinoelämän, erityisesti kasvavien suuren vientipotentiaalin omaavien teollisuudenalojen, tarpeiden huomioiminen vienninedistämispalveluiden uudistamisessa on erityisen tärkeää. Palveluista on eniten hyötyä, kun ne räätälöidään ja kohdennetaan optimaalisesti vientiyritysten tarpeisiin. Tavoitteenamme on, että palveluita uudistettaessa luodaan toimintamalli, jossa Kyberala ry:ltä ja muilta kasvavien teollisuusalojen toimialajärjestöiltä tiedustellaan systemaattisesti näkemyksiä toiminnan painopisteiden määrittelyn tueksi, esimerkiksi potentiaalisimpien kohdemarkkinoiden, teollisuudenalan ajankohtaisten teemojen sekä markkinoillepääsyä haittaavien tekijöiden tunnistamiseksi.

Kyberalan edunvalvonnan tehtävänä on tuoda esille Suomessa toimivan kyberturvallisuusteollisuuden tarpeita poliittisille päätöksentekijöille ja virkahenkilöille, sekä laajempaan tietoisuuteen. Yhteiskunnan kokonaisturvallisuuden vahvistamista koskevissa keskusteluissa ja kehityshankkeissa korostamme vahvan talouden ja teollisuuden pohjan, terveen kilpailun, kansainvälisen kilpailukyvyn sekä suotuisten investointiolosuhteiden kriittistä merkitystä maamme turvallisuudelle ja huoltovarmuudelle. Samalla pyrimme varmistamaan, että näille huoltovarmuuden ja kansallisen turvallisuuden kivijaloille haitallisista toimista pidättäydytään. NATO:n ylimmän sotilasjohtajan, amiraali Rob Bauerin sanoja lainataksemme: ”Armeijat voittavat taistelut mutta talous voittaa sodan”. Toisin sanoen isänmaallinen teko on menestyvän liiketoiminnan harjoittaminen.

Kyberala tarjoaa tietoa jäsenilleen alati muuttuvasta toimintaympäristöstä laaja-alaisesti jäsentiedotteilla, minkä lisäksi järjestämme tilaisuuksia erilaisista ajankohtaisista aiheista itse ja yhdessä kumppaniemme kanssa, unohtamatta tarjoamiamme osallistumismahdollisuuksia esimerkiksi eräisiin valtionhallinnon ja eurooppalaisten yhteistyöjärjestöjemme tilaisuuksiin. Vuonna 2024 aloitimme yhdessä Traficomin kyberturvallisuuskeskuksen ja Huoltovarmuuskeskuksen kanssa yhteisen ”Kyberala murroksessa” -konseptin, minkä puitteissa olemme järjestäneet tiedotusluontoisia webinaareja kyberturvallisuusalan ajankohtaisista asioista, kuten EU:n kyberkestävyyssäädöksestä, tekoälyn turvallisuusnäkökulmista ja kvanttiturvallisesta salauksesta. Webinaarisarja on ollut hyvin suosittu ja se on houkutellut kuluneen vuoden aikana tuhansia katsojia. Kyberala murroksessa ja muut yhdistyksemme muut aktiviteetit jatkuvat ja otamme mielellämme vastaan jäseniltämme ehdotuksia niiden ja muun edunvalvonnan kehittämiseksi. Yhdistyksemme on avoin kyberturvallisuuden alalla toimiville yrityksille ja organisaatioille.

PETER SUND

Kyberala ry:n (FISC ry) toimitusjohtaja

Teknologiateollisuus ry

Jukka Rapo

RISTO RAJALA

Kyberala ry:n (FISC ry) neuvonantaja

Teknologiateollisuus ry

MARTTI LEHTO

Kansallinen kybertoimintaympäristö ja kyberoperaatiot

Tiivistelmä:
Sodankäynti on historiallisesti tapahtunut erilaisissa toimintaympäristöissä, kuten maa, meri, ilma ja avaruus. Viime aikoina informaatio ja kyberavaruus ovat nousseet uusiksi toimintaympäristöiksi. Kansallinen kybertoimintaympäristö voidaan jakaa kuuteen ulottuvuuteen: sotilaallinen, poliittinen, taloudellinen, yhteiskunnallinen, teknologinen ja kansalaiset. Offensiiviset kyberoperaatiot ovat muuttuneet yhä monimuotoisemmiksi, kehittyneemmiksi ja yleisemmiksi. Disruptiivisten teknologioiden saatavuus sekä hyökkääjille että puolustajille on lisännyt hyökkäysten monimutkaisuutta ja tehnyt hyökkääjän tunnistamisesta entistä haastavampaa. Tämä ilmiö on havaittu erityisesti Venäjän kyberoperaatioissa Ukrainassa.

Ongelmankuvaus:
Miten Venäjän kyberoperaatiot voidaan ymmärtää osana hybridioperaatioita?

Lopputulos:
Valtioiden tulisi varmistaa, että kybertoimintaympäristössä tapahtuva toiminta edistää vuoropuhelua, sisällyttää kaikki asiaankuuluvat kansalaisyhteiskunnan organisaatiot kyberturvallisuuden rakentamiseen ja lisää alan tutkimusta, koulutusta sekä toiminnan harjoittelua.

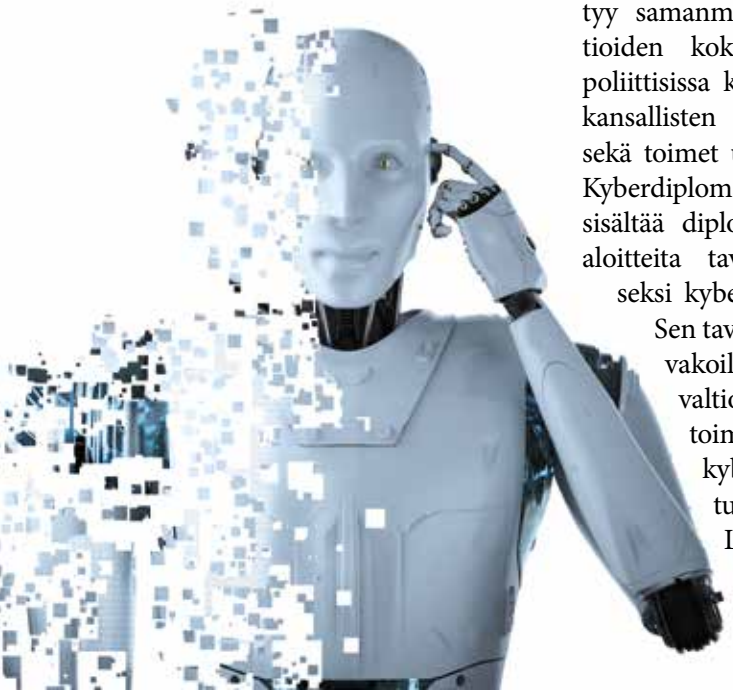
Mitä sitten?

Kansallisen kyberresilienssin vahvistaminen vaatii kansainvälistä yhteistyötä Naton ja EU:n kanssa. EU:n kybersolidaarisuussäädös parantaa kyberturvallisuuspoikkeamiin varautumista, havaitsemista ja niihin reagoimista. Kyberturvallisuus tulisi nähdä kokonaisuutena, joka koskee koko digitaalista yhteiskuntaa ja vaatii integrointia kokonaisturvallisuuden viitekehykseen.

PARADIGMA ON MUUTTUNUT, JA MUUTOS JATKUU

Perinteisessä sodankäynnin mallissa kansallisvaltiot osallistuvat konflikteihin erilaisista syistä, jotka liittyvät niiden kansallisiin etuihin. Sodankäynnin operaatioita toteutetaan eri toimintaympäristöissä. Toiminnot voidaan jakaa kineettisiin toimintoihin, joilla on fyysisiä vaikutuksia, ja ei-kineettisiin toimintoihin.

Ei-kineettinen ympäristö on kehittynyt radiosta tietotekniikkaan ja tekoälyyn (AI) sisältäen osin piilossa olevia teknologioita, joilla on vahingollisia ja toimintoja heikentäviä vaikutuksia.[1] Kognitiivinen sodankäynti käyttää ihmisen havaintokykyä, kognitiota ja käyttäytymistä strategisten tavoitteiden saavuttamiseksi. Uudet teknologiat, kuten tekoäly ja neuroteknologiat, helpottavat valtionvastaista toimintaa. Datan massatuotanto ja automatisoitu sisällöntuotanto ovat lisänneet johtaneet julkisesti saatavilla olevan datan määrää ja siten kognitiivisen manipuloinnin mahdollisuuksia, jolloin datasta ja tekoälyalgoritmeista on tullut kognitiivisen sodankäynnin aseita.[2]



KANSALLISEN KYBERTOIMINTAYMPÄRISTÖN YMMÄRTÄMINEN

Kyberuhat ovat monimutkaisia ja epäsymmetrisiä, koska digitaalinen kyberavaruus on rajaton ja moniulotteinen. Kansallisessa kyberympäristössä on erilaisia toimijoita ja toiminnallisia kokonaisuuksia, ja se eroaa perinteisestä kansallisesta ympäristöstä, jossa valtiolla on selkeästi määritellyt maantieteelliset rajat kuten maalla, merellä ja ilmassa, joissa valtioilla on kansainvälisten sopimusten määrittelemät toimivaltuudet.

Poliittinen ulottuvuus

Kansallisen kybertoimintaympäristön poliittinen ulottuvuus kattaa prosessit, lainsäädännön ja säännökset, jotka edistävät ja valvovat kyberturvallisuutta. Nämä kysymykset korostuvat niin kansallisessa kuin kansainvälisessä politiikassa, ja niillä on kasvava merkitys kansainvälisillä foorumeilla ja organisaatioissa esimerkiksi EU:ssa, Natossa ja ETYJ:ssä.

Kuten muutkin diplomaattiset ponnistelut, kyberdiplomatiaan kuuluu strategisten globaalinen kumppanuuksien rakentaminen parantaaksemme yhteisiä toimia ja yhteistyötä samoja uhkia vastaan. Tähän sisältyy samanmielisten maiden koalitioiden kokoaminen elintärkeissä poliittisissa kysymyksissä, tiedon ja kansallisten aloitteiden jakaminen, sekä toimet uhkatoimijoita vastaan. Kyberdiplomatian keinovalikoima sisältää diplomaattisia työkaluja ja aloitteita tavoitteiden saavuttamiseksi kybertoimintaympäristössä. Sen tavoitteisiin kuuluu kybervakoilun, ja valtiollisten tai valtiosta riippumattomien toimijoiden toteuttamien kyberhyökkäysten vaikutusten minimoiminen. Lisäksi kyberdiplomatian tavoitteena on käsitellä kansainvälistä oikeutta ja normeja kyberturvallisuuden alalla ja ryhtyä toimiin, jotka rakentavat luottamusta. Keskinäisellä ymmärryksellä ja yhteisillä pelisäännöillä voidaan vähentää erilaisten konfliktien uhkaa.[3]

Kyberdiplomatiaan kuuluu strategisten globaalien kumppanuuksien rakentaminen yhteisten kyberuhkien torjumiseksi ja yhteistyön laaja-alaiseksi toteuttamiseksi. Tähän sisältyy samanmielisten maiden koalitiot, tiedon jakaminen ja toimet uhkatoimijoita vastaan. Työkaluja ovat diplomatian keinot ja aloitteet kybertoimintaympäristössä. Toiminnan tavoitteisiin kuuluu kybervakoilun sekä valtiollisten tai valtiosta riippumattomien toimijoiden toteuttamien kyberhyökkäysten vaikutusten minimoiminen. Lisäksi kyberdiplomatian tavoitteena on käsitellä kansainvälistä oikeutta ja normeja kyberturvallisuuden alalla sekä rakentaa luottamusta. Keskinäisellä ymmärryksellä ja yhteisillä pelisäännöillä voidaan vähentää erilaisten konfliktien uhkaa.

EU on luonut tärkeät viitekehykset ja toimintamenettelyt kuten Diplomatic Response Framework (Cyber Diplomacy Toolbox, 2017), the Cyber Defence Policy Framework (2018), EU Cybersecurity Act (2019) and Council Decision (2019) unionia tai sen jäsenmaita uhkaavien kyberhyökkäysten vastaisista rajoittavista toimenpiteistä. Lisäksi EU:n kyberturvallisuusstrategian mukaisesti digitaalisen vuosikymmenen (Digital Decade) kehitystyössä EU on ottanut käyttöön useita säädöksiä ja politiikka-asiakirjoja, kuten NIS2 -direktiivin, EU:n kyberresilienssisäädöksen (European Cyber Resilience Act), finanssialan häiriönsietokykyä koskevan säädöksen (Digital Operational Resilience Act), Euroopan kyberpuolustuspolitiikan, Euroopan unionin strategisen kompassin ja eurooppalaisen sirusäädöksen (European Chips Act).[4] EU:n Cyber Diplomacy Toolbox on kollektiivinen diplomaattinen kehikko haital-

listen kybertoimien torjuntaan. Se on osa EU:n lähestymistapaa kyberdiplomatiaan yhteisen ulko- ja turvallisuuspolitiikan puitteissa. Sen tavoitteena on edistää konfliktien ehkäisyä, kyberturvallisuusuhkien lieventämistä ja kansainvälisten suhteiden vakautta.[5]

Sotilaallinen ulottuvuus

Useat valtiot kehittävät sotilasstrategioitaan kybertoimintaympäristössä sekä maalla, merellä, ilmassa ja avaruudessa. Kybersodankäynnin strategisella tasolla valtio pyrkii vaikuttamaan toisen valtion elintärkeisiin toimintoihin. Kyberoperaatiot integroidaan muiden puolustushaarojen operaatioihin operatiivisella ja taktisella tasolla.

Nato on pitkään pitänyt kyberpuolustusta keskeisenä osana puolustusstrategiaansa. Naton vahva keskittyminen kyberpuolustukseen alkoi vuoden 2002 Naton huippukokouksessa Prahassa. Nato ja sen liittolaiset vastaavat kyberuhkiin parantamalla kykyään havaita, ehkäistä haitallisia kybertoimia ja reagoida niihin. Vahva ja kestävä kyberpuolustus on ratkaisevan tärkeää, jotta Nato ja sen liittolaiset voivat täyttää liittouman kolme ydintehtävää: pelote ja puolustus, kriisien ehkäisy ja hallinta, ja yhteistyöhön perustuva turvallisuus.[6]

Vuoden 2023 Naton huippukokouksessa Vilnassa jäsenmaat hyväksyivät uuden konseptin kyberpuolustuksen tehostamiseksi osana Naton pelote- ja puolustusrakennetta. He käynnistivät myös Naton virtuaalisen kybertapahtumien tuen (Virtual Cyber Incident Support Capability, VCISC) tukemaan kansallisia lieventämistoimia merkittäviin haitallisiin kybertoimiin vastaamiseksi.[7]

Puolustusvoimat tarvitsevat tehokasta kyberuhkien sietokykyä, ei-kineettisen voimankäytön tiivistämistä sekä kykyä operoida kiistanalaisessa ja kompleksisessa kybertoimintaympäristössä. Kybervoima ja kyberpelote ovat kaksi keskeistä tekijää, jotka yhdistävät kybertoimintaympäristön sotilaalliset ja poliittiset ulottuvuudet. Kansallinen kybervoiman indeksi (National Cyber Power Index) kuvaa kansakunnan kykyä toimia globaalissa kyberympäristössä.[8] Kybertoimintaympäristön pelotteella pyritään vaikuttamaan vastustajan käyttäytymiseen ja estämään heitä toteuttamasta haitallisia kyberoperaatioita.[9]

Yhteiskunnallinen ulottuvuus

Digitalisaation ja datatalouden murroksen vuosikymmen vaikuttaa koko maailmaan. Tämä muutos koskettaa kaikkia elämänalueita, sillä digitalisaatio ja data ovat läsnä jokaisella yhteiskunnan sektorilla. Tämä näkyy uusissa palveluissa, toimintamalleissa, teknologioissa ja osaamisvaatimuksissa. Digitalisaatio kattaa esimerkiksi sosiaalipalvelut, koulutussektorin ja terveyspalvelut. Kyberhyökkäykset ja kybertoimintaympäristön haavoittuvuudet muodostavat merkittävän turvallisuusriskin. Kybermaailman suurimmat uhat kohdistuvat keskeiseen infrastruktuuriin (Critical Infrastructure, CI).

CI käsittää yhteiskunnan jatkuvan toiminnan kannalta kriittiset rakenteet ja toiminnot. Näihin kuuluvat fyysiset tilat sekä tekniset toiminnot ja palvelut, kuten poliittinen päätöksenteko, sisäinen ja ulkoinen turvallisuus, logistiikka, talous, energia, televiestintä ja ruoantuotanto. Kriittiseen infrastruktuuriin, kriittiseen informaatioinfrastruktuuriin ja Internetiin kohdistuvat hyökkäykset ovat viime vuosina yleistyneet, laajentuneet ja monimutkaistuneet, kun rikoksentekijöistä on tullut ammattimaisempia. Hyökkääjät voivat aiheuttaa vahinkoa fyysiselle infrastruktuurille tunkeutumalla fyysisiä prosesseja ohjaaviin digitaalisiin järjestelmiin, vahingoittamalla toimintajärjestelmiä ja häiritsemällä yhteiskunnan elintärkeitä palveluita ilman fyysistä hyökkäystä.[10]

Yhteiskunnallisessa ulottuvuudessa painopisteenä on kriittisen infrastruktuurin suojaaminen (Critical Infrastructure Protection, CIP). Tämä sisältää toimenpiteitä, joilla pyritään ehkäisemään ja lieventämään kriittisen infrastruktuurin haavoittuvuuksista johtuvia riskejä sekä helpottamaan palautumisprosessia mahdollisen hyökkäyksen jälkeen.

Kansalaisulottuvuus

Digitaaliteknologiat ovat integroituneet syvälle ihmisten elämään. Tieto- ja viestintätekniikan toimintavarmuus on välttämätöntä nyky-yhteiskunnan toiminnalle, sen infrastruktuurin turvallisuudelle ja kansalaisten hyvinvoinnille. Tämä toimintavarmuus on tärkeää myös yhteiskunnallisen luottamuksen ylläpitämiseksi. Digitaalisessa yhteiskunnassa kansalaisten on toimittava turvallisesti ja vastuullisesti digitaalisessa uhkaympäristössä. Digitalisaatio tarjoaa merkittäviä etuja, kuten elämän laadun parantamista ja globaalin viestinnän mahdollistamista. Se vaikuttaa myös kansalaisten yksityiselämään, sosiaaliseen ja julkiseen elämään sekä heidän yksityisyyteensä, itsemääräämisoikeuteensa ja turvallisuuteensa.[11]

EU:n digitaalisen kompassin mukaan ”digitaaliteknologioiden olisi suojeltava ihmisten oikeuksia, tuettava demokratiaa ja varmistettava, että kaikki digitaaliset toimijat toimivat vastuullisesti ja turvallisesti. Ihmisten olisi voitava hyötyä oikeudenmukaisesta verkkoympäristöstä, heitä olisi suojeltava laittomalta ja haitalliselta sisällöltä ja heitä olisi voitava voimaannuttaa vuorovaikutuksessa uusien ja kehittyvien teknologioiden, kuten tekoälyn kanssa. Digitaalisen ympäristön olisi oltava turvallinen kaikille käyttäjille lapsuudesta vanhuuteen ja varmistettava voimaannuttaminen ja suojelu.”[12]

EU:n digitaalisen vuosikymmenen tavoitteet digitaalisia taitoja

koskien eivät ole vielä täysin toteutuneet, sillä vain 55,6 prosentilla EU:n väestöstä on vähintään perusmuotoiset digitaaliset taidot. Jäsenmaat pyrkivät saavuttamaan tavoitteen, jonka mukaan kaikki keskeiset julkiset palvelut ja sähköiset terveystiedot ovat kansalaisten ja yritysten saatavilla verkossa sekä että näille tarjotaan turvallinen sähköinen tunnistaminen (Electronic Identification, eID). Kuitenkin digitaalisten julkisten palvelujen 100-prosenttisen kattavuuden saavuttaminen vuoteen 2030 mennessä voi osoittautua haastavaksi.[13]

Taloudellinen ulottuvuus

Cybersecurity Ventures on alan tutkimus- ja mediaorganisaatio, joka tunnetaan näkemyksistään ja panoksestaan kyberturvallisuuteen. Vuonna 2020 laaditun raportin mukaan maailmanlaajuiset kyberrikollisuuden kustannukset kasvavat 15 prosenttia vuosittain seuraavan viiden vuoden aikana ja nousevat vuositasolla 10,5 biljoonaan dollariin vuoteen 2025 mennessä. Tämä ennuste osoittaa taloudellisen vaurauden siirtymistä rikollisille. Kyberrikollisuuden kustannukset aiheutuvat tietojen vahingoittumisesta ja tuhoutumisesta, huijauksilla menetetyistä varoista, tuottavuuden menetyksestä, tekijänoikeuksien varkauksista, henkilökohtaisten ja taloudellisten tietojen varkauksista, kavallusten ja petosten aiheuttamista menetyksistä, hyökkäyksen aiheuttamista liiketoiminnan häiriöistä, rikosteknisen tutkinnan, tietojen ja järjestelmien palauttamisen sekä maineen hallinnan kustannuksista.[14]

Globaali rahoitusjärjestelmä on yhä enemmän riippuvainen digitaalisesta infrastruktuurista. Kyberhyökkäysten taloudelliset vaikutukset sisältävät organisaatioille aiheutuvien suorien kustannusten lisäksi pitkän aikavälin vaikutukset kansantalouteen sekä kyberturvallisuuden parantamiseen liittyvät kustannukset eri tasoilla. Kyberhyökkäyksiin varautuminen voi vaikuttaa myös verotukseen ja julkisiin menoihin, kun julkisen sektorin kyberturvallisuuteen tarvitaan lisäresursseja. Kyberturvallisuuden kehittäminen vaatii huolellista harkintaa sekä taloudellisesta että yhteiskunnallisesta näkökulmasta.[15]

Sääntelymekanismit voivat vaikuttaa kyberturvallisuuden parantamiseen, mutta niihin liittyy myös haasteita. Ennaltaehkäisevät säännökset, vahinkojen ja haavoittuvuuksien jälkeiset velvoitteet sekä tiedonsaantivaatimukset tuovat mukanaan etujen lisäksi kustannuksia. NIS2-direktiivi on esimerkki sääntelystä, jolla pyritään parantamaan kyberturvallisuuden tasoa EU:ssa oikeudellisten toimenpiteiden avulla. Poliittisella, yhteiskunnallisella ja taloudellisella ulottuvuudella on merkitystä taloudellisen ja rahoituksellisen vakauden saavuttamisessa. Tehokas julkinen hallinto on ratkaisevan tärkeää demokratian ylläpitämiseksi ja yhteiskunnan hyvinvoinnin turvaamiseksi.

Teknologinen ulottuvuus

Tieto- ja viestintätekniikka (ICT) kattaa laajan valikoiman aloja, jotka liittyvät tietokonejärjestelmiin, ohjelmistoihin, laitteistoihin sekä tietojenkäsittelyyn ja -tallennukseen. ICT:n työkalujen ja järjestelmien ensisijaisena tavoitteena on tehostaa yksilöiden ja organisaatioiden tapaa luoda, käsitellä ja jakaa dataa ja tietoa. Tieto- ja viestintätekniikalla on keskeinen merkitys lukuisilla alueilla, kuten liike-elämässä, koulutuksessa, terveydenhuollossa, puolustuksessa ja kansalaisten vapaa-ajan toiminnassa.[16]

Digitaaliset työkalut virtaviivaistavat liiketoimintaa, vähentävät manuaalisia toimintoja ja parantavat asiakaspalvelua. Ne automatisoivat tehtäviä ja suojaavat asiakastietoja. Digitalisaatio tuo myös kyberuhkia; rikolliset voivat varastaa ja myydä tietoa. Kyberturvallisuusratkaisujen on oltava älykkäitä ja tehokkaita suojatakseen kansalaisia ja organisaatioita yhä vaarallisimmilta uhkilta. Luottamus on digitaalisen yhteiskunnan perusta, sillä ylläpidetään yhteiskunnallista vakautta. Luottamus vaatii jatkuvaa ylläpito.

KYBEROPERAATIOT OSANA HYBRIDIOPERAATIOITA

Hybridioperaatiot käyttävät kyberoperaatioita pysyäkseen aseellisen konfliktin kynnyksen alapuolella. Epävakautta voidaan ylläpitää kyberoperaatioilla sekä rauhan että sodan aikana. Venäjän hybridisodankäynnin strategiaa voidaan kuvata luovaksi voimankäytöksi, joka yhdistää sotilaallisia ja ei-sotilaallisia työkaluja monipuolisesti moniulotteisella taistelukentällä.

Naton Washingtonin huippukokouksen julistuksen (2024) mukaan ”Venäjän täysimittainen hyökkäys Ukrainaan on murtanut rauhan ja vakauden Euroatlanttisella alueella ja heikentänyt vakavasti maailmanlaajuista turvallisuutta. Venäjä on edelleen merkittävin ja suurin uhka liittoutuneiden turvallisuudelle.”[17]

Poliittinen ulottuvuus

Venäjä käyttää hybriditoimia vaikuttaakseen lännen ja muiden maiden politiikkaan ja toimintatapoihin, mikä aiheuttaa haasteita länsimaiden valtionjohdoille. Venäjä pyrkii varmistamaan, että kohdemaiden poliittiset päätökset tukevat sen kansallisia etuja, erityisesti maissa, joissa on heikko oikeudellinen rakenne tai sisäisiä ryhmiä, jotka jakavat saman maailmankatsomuksen. Taustalla on Venäjän strategisen kulttuurin perinne. Kreml vaikuttaa vaaleihin ja poliittisiin tuloksiin rajojensa ulkopuolella sekä harjoittaa aggressiivisia kyberoperaatioita, kuten kyberhyökkäyksiä ja -vakoilua. Näihin operaatioihin liittyvät epäsymmetriset sodankäyntimenetelmät, harhautus ja taktisen totuuden käsite. Ukrainan tilanne korostaa Venäjän jatkuvaa uhkaa sääntöihin perustuvalle kansainväliselle järjestykselle, ja Venäjän kybervalmiudet kehittyvät vastaamaan länsimaisia taktiikoita, tekniikoita ja toimintatapoja.[18] [19]

Suomen presidentti Alexander Stubb on useaan otteeseen käsitellyt Venäjän hybridivaikutusta puheissaan tuoden esiin, että Venäjä pyrkii horjuttamaan yhteiskuntia erilaisten hyökkäysmuotojen avulla. Hän on myös todennut, että nykyaikaiset konfliktit sisältävät usein yhdistelmän tavanomaista sodankäyntiä, hybridisodankäyntiä ja kybersotaa, ja näitä hybridihyökkäyksiä tapahtuu usein. Berliinin Hertie-koulussa 8. toukokuuta 2024 pitämässään puheessa Stubb totesi: ” Hybridihyökkäykset ovat arkipäivää rauhan aikana, eikä niihin yleensä liity sodanjulistusta. Myös perinteinen sota on monimutkaista ja monitahoista. Perinteistä sodankäyntiä on edelleen olemassa – tämä näkyy sekä Euroopassa että Lähi-idässä – mutta välineet ja menetelmät ulottuvat kranaatteja ja juoksuhautoja pidemmälle.”[20]

Sotilaallinen ulottuvuus

Kybertyökalujen käyttö sotilaallisena keinona hyökätessä vihollisen joukkoja ja resursseja vastaan voidaan luokitella samalla tavalla kuin muut sotilaalliset operaatiot. Kybertyökaluja voidaan soveltaa perinteisissä operaatioissa, kuten Ukrainassa on havaittu, tai erikoistuneemmissa operaatioissa, kuten Stuxnet-hyökkäyksessä Irania vastaan. Näissä hybridisodankäynnin operaatioissa menetelmiä käytetään tiettyjen tavoitteiden saavuttamiseksi usein peitellyllä tavalla, joka jää perinteisen aseellisen konfliktin kynnyksen alapuolelle. Sodassa kineettisten työkalujen ja ei-kineettisten taktiikkojen yhdistämisen tavoitteena on vastustajan toimintaympäristön häiritseminen, lamauttaminen tai vahingoittaminen.[21]

Venäjän hyökkäys Ukrainaan korostaa kybervalmiuksien merkittävää roolia nykyaikaisessa sodankäynnissä ja osoittaa, kuinka kybertyökalut voivat täydentää tavanomaisia sotilaallisia keinoja. Venäläinen toimintatapa on sisältänyt operaatioita, jotka ovat vaikuttaneet Ukrainan infrastruktuuriin, julkishallintoon ja siviiliverkostojen eri osa-alueisiin sekä Ukrainan ulkopuolisiin kohteisiin. Aikavälillä tammikuu 2022 - joulukuu 2023 CyberPeace Institute on kirjannut 2 258 kyberhyökkäystä ja operaatiota, joista 666 kohdistui Ukrainaan ja 1 592 muihin maihin. Nämä kyberhyökkäykset kohdistuivat 23 eri kriittisen infrastruktuurin sektoriin, jotka vaikuttivat Ukrainaan ja noin 49 muuhun maahan.[22]

Kanadassa kesäkuussa 2024 järjestetyssä tilaisuudessa Naton pääsihteeri Jens Stoltenberg huomautti: ”Haasteena on, että meitä uhkaa jokin, joka ei ole täysimittainen sotilaallinen hyökkäys, joita ovat nämä kyber- sekä hybridiuhat, jotka tapahtuvat viidennen artiklan viitekehyksen alapuolella, ja ne ovat kaikkea poliittisiin prosesseihimme sekaantumisesta, pyrkimystä heikentää luottamusta eurooppalaisiin poliittisiin instituutioihimme, disinformaatiota, kyberhyökkäyksiä, sabotaaseja kriittistä infrastruktuuriamme vastaan ja niin edelleen.”[23]

Yhteiskunnallinen ulottuvuus

Kyberturvallisuuden kehittäminen edellyttää kohdennettua pitkäjänteistä työtä. Riskit voivat ilmetä nopeasti ja toimintaympäristö kehittyy jatkuvasti. Viime vuosina hyökkäykset kriittiseen infrastruktuuriin, tietojärjestelmiin ja Internetiin ovat yleistyneet ja muuttuneet monimutkaisemmiksi sekä kohdennetummiksi hyökkääjien ammattimaisuuden kasvaessa. Nämä hyökkäykset voivat vahingoittaa fyysistä infrastruktuuria tai aiheuttaa häiriöitä digitaalisia järjestelmiä tunkeutumalla fyysisiä prosesseja ohjaaviin digitaalisiin järjestelmiin, laitteistoja vahingoittamalla ja tärkeitä palveluja häiritsemällä ilman fyysistä hyök-

käystä. Tulevaisuudessa nämä uhat voivat muuttua entistä monimutkaisemmiksi ja kehittyneemmiksi.

Venäjä voi kohdistaa kyberhyökkäyksiä kriittistä infrastruktuuria vastaan aiheuttaakseen epävarmuutta ja epäluottamusta kansalaisten keskuudessa sekä osoittaakseen kykynsä lamauttaa keskeisiä yhteiskunnallisia toimintoja. Vaikka Venäjä keskittyy Ukrainan konfliktiin liittyviin kyberoperaatioihin, se on edelleen merkittävä globaali kyberuhka. Venäjän kohteina Ukrainassa ovat olleet muun muassa televiestintäsektori (Triolan ja Vinasterisk ISP, Ukrtelecom, Kyivstar), radioyhtiöt, media, kuljetus- ja logistiikkatoimittajat, datakeskukset, energiasektori ja rajaturvallisuus.[24] [25] [26]

Moskova käyttää kyberhyökkäyksiä ulkopolitiikan välineenä vaikuttaakseen muiden maiden päätöksiin. Se kehittää kybervakoilu-, informaatiovaikuttamis- ja kyberhyökkäyskykyjään eri kohteita vastaan. Venäjän kohteena voi olla kriittinen infrastruktuuri, kuten vedenalaiset kaapelit ja teollisuuden ohjausjärjestelmät, Yhdysvalloissa sekä liittolais- ja kumppanimaissa. Venäjän kyberhyökkäysten kohteita vuonna 2024 ovat olleet:[27]

- Saksan poliittiset puolueet ja Saksan sotilasviranomaiset;
- Vakoilukampanja Georgian, Puolan, Ukrainan ja Iranin suurlähetystöjä vastaan ja kiristyshaittaohjelmahyökkäys Ruotsin valtion digitaalisten palvelujen tarjoajaa vastaan;
- Hakkeroituminen Microsoftin yritysjärjestelmiin Australian hallitukseen kohdistuneessa suurimmassa kyberhyökkäyksessä Hyökkäys kohdistui 65 Australian ministeriöön ja virastoon, joista anastettiin 2,5 miljoonaa asiakirjaa; ja
- Hakkeroituminen kiovalaisten asukkaiden webbikameroihin kerätäkseen tietoa kaupungin ilmapuolustusjärjestelmistä ennen ohjushyökkäyksen käynnistämistä Kiovaan.

Kansalaisulottuvuus

Kansalaisulottuvuus korostaa tiedon vaikutusta. Hyökkääjät voivat levittää systemaattisesti disinformaatiota kohdistettujen sosiaalisen median kampanjoiden avulla radikalisoidakseen yksilöitä, horjuttaakseen yhteiskuntia ja hallitakseen poliittista narratiivia.

Venäjän disinformaatio- ja propagandaekosysteemi sisältää viralisia viestintäkanavia, sosiaalisen median alustoja, sijaistoimijoita (proxy) ja anonyymejä alustoja väärien narratiivien luomiseksi ja vahvistamiseksi. Ekosysteemi koostuu viidestä pilarista: hallituksen virallinen viestintä, valtion rahoittama globaali viestintä, proxien käyttö, sosiaalisen median aseistaminen ja kyberavusteinen disinformaatio. Kreml hyödyntää näitä osana tiedon aseistamisstrategiaansa:[28] [29]

- Strategic Culture Foundation, Venäjän ulkomaantiedustelupalvelun (SVR) johtama Venäjälle rekisteröity verkkolehti;
- Global Research, kanadalainen verkkosivusto, joka on osa Venäjän disinformaatio- ja propagandaekosysteemiä;
- New Eastern Outlook, Venäjän tiedeakatemian itämaisen tutkimuksen instituutin pseudoakateeminen julkaisu, joka edistää disinformaatiota ja propagandaa keskittyen ensisijaisesti Lähi-itään, Aasiaan ja Afrikkaan;
- News Front, Krimillä sijaitseva disinformaatio- ja propagandajärjestö, joka tarjoaa ”vaihtoehtoisen tiedonlähteen” länsimaiselle yleisölle;
- SouthFront, Venäjälle rekisteröity monikielinen disinformaatiosivusto, joka keskittyy sotilaallisiin ja turvallisuuskysymyksiin;
- Katehon, Moskovassa sijaitseva ajatushautomo, joka keskittyy lännenvastaiseen disinformaatioon ja propagandaan; ja
- Geopolitica.ru, alusta venäläisille ultranationalisteille, joka levittää disinformaatiota ja propagandaa länsimaiselle yleisölle.

Taloudellinen ulottuvuus

Ilman määrätietoisia toimia globaali rahoitusjärjestelmä tulee entistä haavoittuvammaksi. Innovaatioiden, kilpailun ja haitallisten teknologioiden ohjatessa yhä enemmän digitaalista kehitystä, järjestelmän suojaaminen on välttämätöntä. Vaikka monet uhkatekijät ovat taloudellisesti motivoituneita, valtion tukemat hyökkääjät tekevät myös yhä enemmän häiritseviä ja tuhoisia hyökkäyksiä rahoitusjärjestelmiä vastaan.

Kyberturvallisuus on olennainen osa talouden ja rahoitusmarkkinoiden vakauden ylläpitämistä. Venäjä pyrkii vaikuttamaan Euroopan politiikkaan sekä suoraan että välillisesti, ja on käyttänyt energiaa ulkopolitiikan välineenä. Kriittiseen infrastruktuuriin ja talousjärjestelmiin kohdistuvat kyberoperaatiot voivat horjuttaa talouden ja rahoituksen vakautta. Iso-Britannian kansanedustajana Rishi Sunak analysoi mahdollisia Venäjän hybridihyökkäyksiä joulukuussa 2017 sanoen: ”Merenalaisen kaapeli-infrastruktuurin sabotointi on eksistentiaalinen uhka Isolle-Britannialle. Seurauksena olisi kaupankäynnin vahingoittuminen ja hallitusten välisen viestinnän häiriintyminen, mikä saattaa johtaa taloudelliseen sekasortoon ja kansalaislevottomuuksiin.”[30] [31]

Globaalin rahoitusjärjestelmän tehokas suojaaminen on ensisijaisesti organisatorinen haaste. Vaikka puolustuksen vahvistamiseen ja säännösten kiristämiseen tähtäävät toimenpiteet ovat merkittäviä, ne eivät yksin riitä vastaamaan kasvaviin uhkiin. Rahoituspalvelutoimialalla on yleensä tarvittavat resurssit ja tekniset valmiudet, toisin kuin monilla muilla aloilla. Keskeinen haaste on kyberturvallisuuden koordinointi hallitusten, rahoitusviranomaisten ja teollisuuden välillä sekä olemassa olevien resurssien tehokas hyödyntäminen.[32]

Tekninen ulottuvuus

Hyökkäysvektori on menetelmä, jonka avulla hyökkääjä voi saada luvaton pääsy tietokoneeseen, verkkoon tai IT/OT-infrastruktuuriin infektoidakseen järjestelmän ja toteuttaakseen suunnitellun operaation kohteessa. Hyökkäysvektorit käyttävät hyväkseen järjestelmän haavoittuvuuksia.[33]

Joulukuun 2021 ja maaliskuun 2022 välisenä aikana Yhdysvaltain CYBERCOMin joukot tekivät yhteistyötä Ukrainan hallituksen kanssa kyberpuolustusoperaatioissa Ukrainan kyberjoukkojen kanssa. Tämä yhteistyö oli osa laajempaa toimintakokonaisuutta, jonka tarkoituksena oli parantaa kyberkestävyyttä kriittisissä kansallisissa verkoissa. Tiimit toteuttivat uhkien etsimisoperaation Ukrainassa sekä tarjosivat analyysi- ja neuvontatukea teknisesti edistyneillä menetelmillä. He toteuttivat myös kriittisiin verkkoihin puolustuksellisia toimenpiteitä ja tunnistivat 90 haitallista koodia, jotka oli luotu häiritsemään tai lamauttamaan Ukrainan infrastruktuuria. Ryhmät saivat myös tietoa vastustajien taktiikoista, tekniikoista, menettelytavoista, suunnitelmista, kyvyistä ja työkaluista.[34]

Ukrainaan kohdistuvia Venäjän kyberuhkatoimia ovat toteuttaneet useat Venäjän kolmeen tärkeimpään turvallisuuspalveluun liittyvät toimijat: Venäjän turvallisuuspalvelu (FSB), ulkomaantiedustelupalvelu (SVR) ja asevoimien sotilastiedustelu (GRU). Nämä kybertoimijat ovat osallistuneet erilaisiin kyberoperaatioihin Ukrainaa vastaan, mukaan lukien häiritsevät ja tuhoavat toimet.

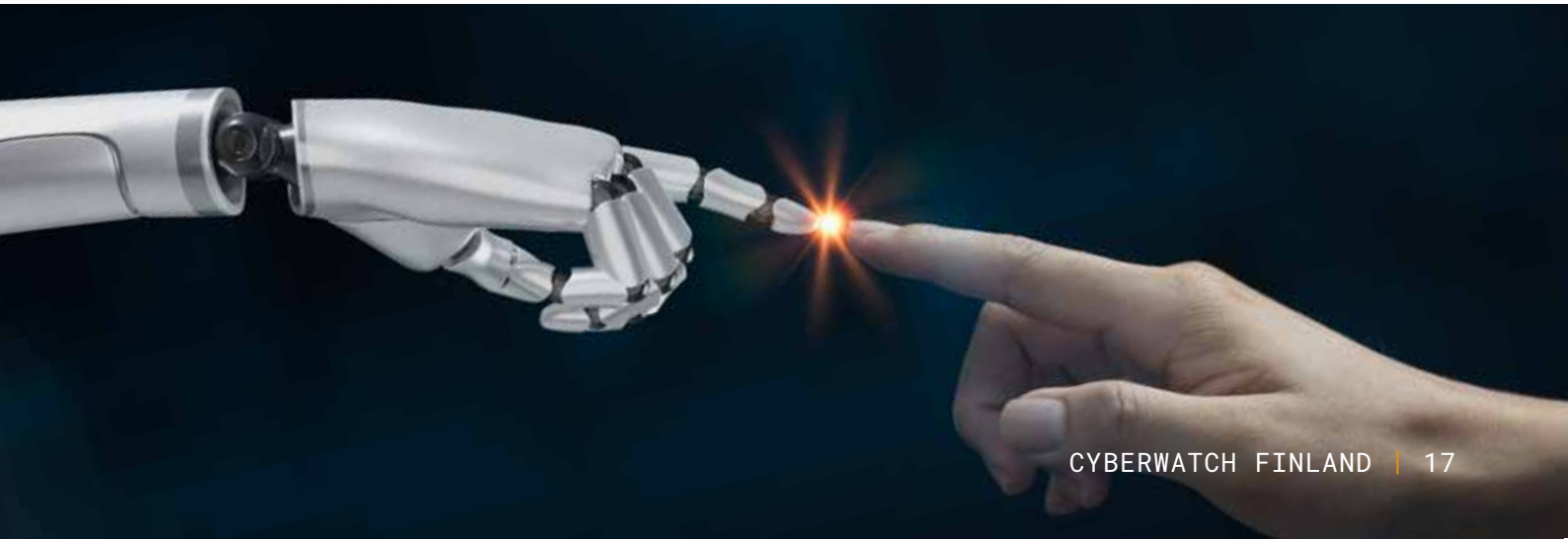
Kansainvälisen rikostuomioistuimen (ICC) syyttäjät tutkivat Venäjän kyberhyökkäyksiä Ukrainan siviili-infrastruktuuriin mahdollisina sotarikoksina. ICC:n syyttäjät työskentelevät ukrainalaisten ryhmien kanssa tutkiakseen hyökkäyksiä, jotka vaikuttivat sähkö- ja vesihuoltoon sekä yhteyksiin hätäkeskuksiin tai mobiilidatapalveluihin, jotka välittävät ilmahyökkäysvaroituksia.[35]

KOHTI KOGNITIIVISTA SODANKÄYNTIÄ

Hybridiuhkien tarkoituksena on hyödyntää valtion haavoittuvuuksia ja usein heikentää demokraattisia perusarvoja ja vapauksia. Digitaalinen kybermaailma voidaan jakaa edellä kuvattuun kuuteen vuorovaikutuksessa olevaan ulottuvuuteen, joissa jokaisen ytimessä on ihminen. Näissä ulottuvuuksissa ihmiset toimivat eri rooleissa, kuten poliitikkoina, päätöksentekijöinä, operaattoreina, sotilaina, systeemisuunnittelijoina ja kansalaisina. Kognitiivinen ylivoima ja kognitiivinen sodankäynti läpäisevät kaikki nämä ulottuvuudet, mikä osoittaa siirtymistä puhtaasti kineettisistä lähestymistavoista aivan uuteen vaikuttamisen suuntaan.

Internet ja sosiaalinen media ovat nykyään merkittäviä kognitiivisen sodankäynnin välineitä, jotka voidaan kohdistaa avainhenkilöihin, tiettyihin ihmisryhmiin ja suureen yleisöön. Sosiaalisen median alustoista on tullut keskeisiä foorumeita, joissa pyritään vaikuttamaan ja manipuloimaan suuren yleisön käsityksiä, mielipiteitä ja käyttäytymistä. Tekoäly voi muuttaa kognitiivisen sodankäynnin toimintatapoja mahdollistamalla kehittyneempiä ja tehokkaampia toimintastrategioita.

Kansakuntien tulisi käsitellä hybridivaikutusta erityisesti kybertoimintaympäristössä. Valtioiden olisi varmistettava, että kybertoimintaympäristössä ja kansallisessa politiikassa toteutettavat toimet tukevat kokonaisvaltaista ja järjestelmällistä lähestymistapaa kyberturvallisuuteen ja kyberpuolustukseen. Niiden tulisi edistää kansallista, alueellista ja maailmanlaajuista kyberturvallisuutta koskevaa vuoropuhelua, yhteistyötä ja tiedonvaihtoa. Yhteiskunnan kriisinsietokyvyn vahvistaminen hybridiuhkia ja kognitiivisia sodankäyntioperaatioita vastaan vaatii yhteistyötä kaikkien asiaankuuluvien kansalaisjärjestöjen, yksityisen sektorin, akateemisten yhteisöjen ja kansalaisjärjestöjen välillä. Lisäksi tarvitaan laajaa ja monitieteistä tutkimusta ja koulutusta kybertoimintaympäristössä ja kognitiivisessa ympäristössä.



VIITTEET

[1] Martti Lehto and Gerhard Henselmann, 'Non-kinetic Warfare: The new game changer in the battle space', 15th International Conference on Cyber Warfare and Security, 2020, Old Dominion University, Norfolk, Virginia, USA, 316–325.

[2] Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla, 'Cognitive warfare: An attack on truth and thought', NATO and Johns Hopkins University report, Fall 2020.

[3] EU parliament, 'Insights, Understanding the EU's approach to cyber diplomacy and cyber defence', European Union, May 28, 2020, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651937.

[4] Annegret Bendiek and Matthias C. Kettemann, 'Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy', SWP comment, no. 16, February 24, 2021, https://www.swp-berlin.org/10.18449/2021C16/.

[5] Cyber Risk GmbH, 'The Cyber Diplomacy Toolbox', https://www.cyber-diplomacy-toolbox.com/.

[6] NATO Cyber Defence, Factsheet, April 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.

[7] NATO, 'Cyber defence', last updated: 14 September, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm.'

[8] Julia Voo, Irfan Hemani, and Daniel Cassidy, 'National Cyber Power Index 2022, Harvard Kennedy School, Belfer Center Report, September 2022, https://www.belfercenter.org/publication/national-cyber-power-index-2022.

[9] Chris Jaikaran, 'Cybersecurity: Deterrence Policy', 18 January, 2022, https://crsreports.congress.gov/product/pdf/R/R47011.

[10] Martti Lehto, 'Cyber-attacks Against Critical Infrastructure', in Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M Lehto and P Neittaanmäki (Springer 2022), 3–42, ISBN: 978-3-030-91293-2.

[11] Anne Gardenier, Rinie van Est, and Lambèr Royakkers, 'Technological Citizenship in Times of Digitization: An Integrative Framework', Digital Society, Volume 3, Issue 2: 21 (2024), https://doi.org/10.1007/s44206-024-00106-1.

[12] EU, 'Europe's Digital Decade: Digital targets for 2030', https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

[13] European Commission, 'Second report on the State of the Digital Decade calls for strengthened collective action to propel the EU's digital transformation', 02 July, 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3602.

[14] Steve Morgan, 'Cybercrime to Cost the World $10.5 Trillion Annually by 2025' (Special Report, 13 November, 2020), Cybercrime Magazine, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[15] ENISA, 'Cybersecurity as an Economic Enabler', March 2016, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler.

[16] Martti Lehto, 'Cyber-attacks Against Critical Infrastructure', in Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M. Lehto and P. Neittaanmäki (Springer 2022), 3-42, ISBN: 978-3-030-91293-2.

[17] NATO, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

[18] Arsalan Bilal, 'Russia's hybrid war against the West', NATO Review, 26 April, 2024, https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html.

[19] Martti J. Kari, 'Russian Strategic Culture in Cyberspace', JYU Dissertations 122, 11 October, 2019.

[20] Alexander Stubb, 'Comprehensive Security in the 21st century: The Finnish model', 08 May, 2024, https://www.presidentti.fi/en/speech-by-president-of-the-republic-of-finland-alexander-stubb-at-hertie-school-in-berlin-on-8-may-2024/.

[21] Arsalan Bilal, 'Hybrid Warfare: New Threats, Complexity, and "Trust" as the Antidote', NATO Review, 30 November, 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[22] Stéphane Duguin and Pavlina Pavlova, 'The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict', EU Directorate-General for External Policies Policy Department, Workshop September 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

[23] NATO, 'Speech by NATO Secretary General Jens Stoltenberg at event hosted by the NATO Association of Canada and the Canadian NATO Parliamentary Association', 19 June, 2024, https://www.nato.int/cps/en/natohq/opinions_226837.htm.

[24] ODNI, 'Annual Threat Assessment of the U.S. Intelligence Community', 05 February, 2024, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[25] Stéphane Duguin and Pavlina Pavlova, 'The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict', EU Directorate-General for External Policies Policy Department, Workshop September 2023, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf.

[26] CyberPeace Institute, https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline.

[27] CSIS, 'Significant Cyber Incidents', https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[28] DoS, 'GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem', August 2020.

[29] Government of Canada, 'Russia's use of disinformation and information manipulation', 28 February, 2024, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng.

[30] NATO STRATCOM COE, 'Russia's Strategy in Cyberspace', June 2021.

[31] Helmi Pillai, 'Protecting Europe's critical infrastructure from Russian hybrid threats' (Centre for European Reform, Policy Brief, 25 April, 2023), https://mailings.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid#FN-25.

[32] Tim Maurer and Arthur Nelson, 'The Global Cyber Threat' (IMF report, Spring 2021), https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

[33] Martti Lehto, 'Cyber-attacks against Critical Infrastructure', in Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M. Lehto and P. Neittaanmäki (Springer 2022), 3-42, ISBN: 978-3-030-91293-2.

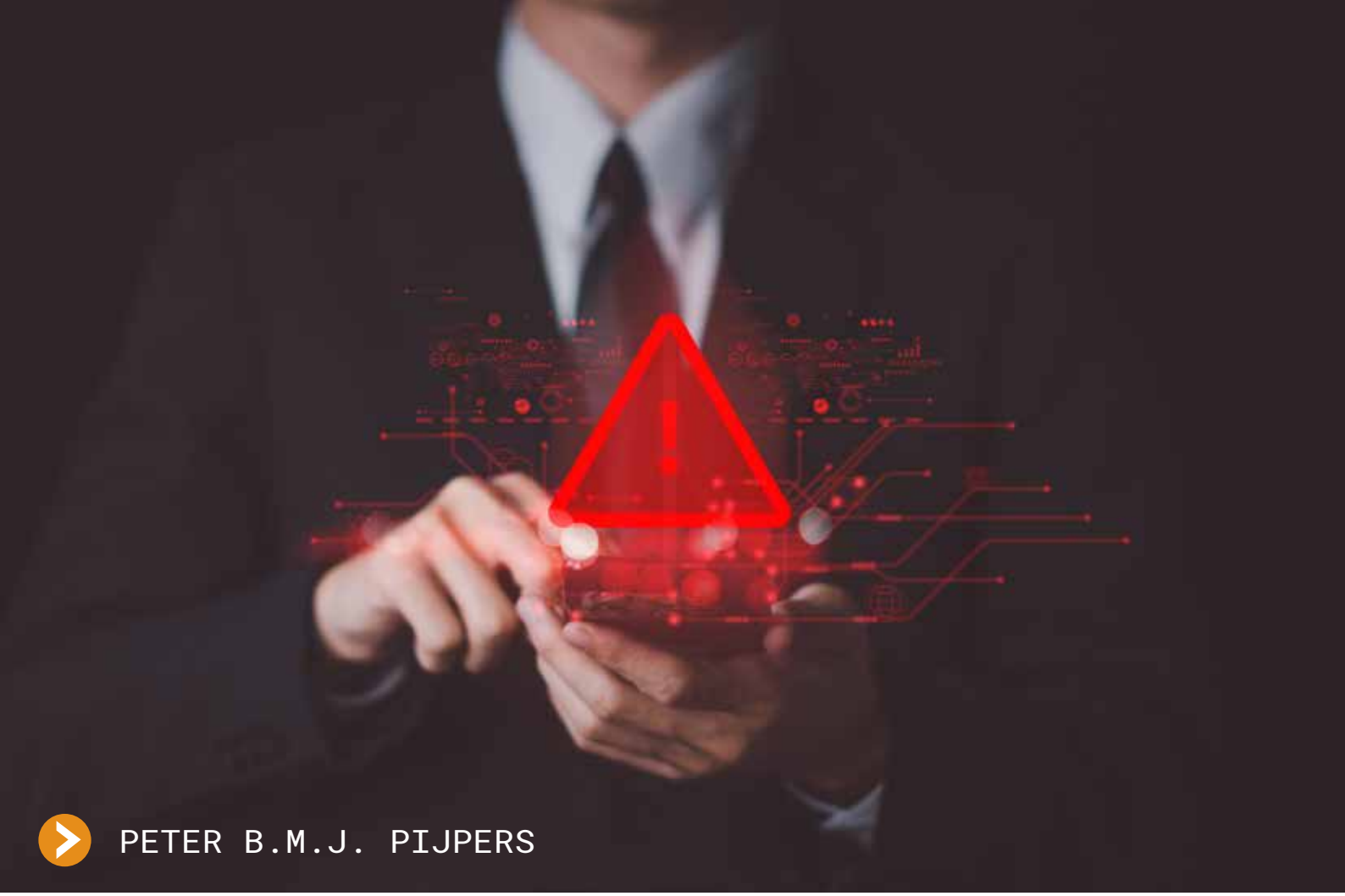
[34] Cyber National Mission Force, 'Before the Invasion: Hunt Forward Operations in Ukraine', 28 November, 2022, https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/.

[35] Anthony Deutsch, Stephanie van den Berg and James Pearson, 'ICC probes cyberattacks in Ukraine as possible war crimes', 14 June, 2024, https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/.

KIRJOITTAJA:

Sotatieteiden tohtori Martti Lehto, eversti evp. työskentelee tutkimusjohtajana Jyväskylän yliopiston informaatioteknologian tiedekunnassa. Hänen tutkimusalueitaan ovat kyberturvallisuus ja kybersodankäynti. Hän palveli 30 vuotta Ilmavoimissa C4ISR-järjestelmien kehitystehtävissä. Hän on myös Maanpuolustuskorkeakoulun ilma- ja kybersodankäynnin dosentti. Hänellä on yli 220 julkaisua, tutkimusraporttia ja artikkelia kyberpolitiikasta, kybersodankäynnistä, kyberturvallisuuskoulutuksesta ja kriittisen infrastruktuurin suojaamisesta. Tämän artikkelin näkemykset ovat kirjoittajan näkemyksiä, eivätkä ne edusta Jyväskylän yliopiston näkemyksiä.

MARTTI LEHTO



PETER B.M.J. PIJPERS

Lainsäädäntö kognitiivisen sodankäynnin työkaluna

Tiivistelmä:
Vaikka vastustajan tahdon alistaminen on ollut sodankäynnin huippu Sun Tzusta lähtien, nykyinen kognitiivisen sodankäynnin käsite on saanut vetovoimaa mahdollisuudella vaikuttaa vastustajaan suoraan kyberavaruuden ja sosiaalisen median kautta. Kyberavaruuden kautta tapahtuva vaikuttamisoperaatio sisältää yleisen mielipiteen horjuttamista, manipuloivaa psykologista sodankäyntiä ja lakisodankäyntiä. Lain käyttö vallan välineenä ihmismieleen ja kognitioon vaikuttamiseksi on mahdollista, koska käynnissä on oikeudellisia kiistoja siitä, miten (kansainvälistä) oikeutta sovelletaan kyberavaruuteen. Valtiot voivat poimia rusinat pullasta, tai jopa käyttää hyväkseen kansainvälisen oikeuden tulkintojen eroja ajaakseen tai puolustaakseen kansallisia etujaan kognitiivisen sodankäynnin keinona.

Tutkimuskysymys:
Voivatko valtiot käyttää oikeudellista epäselvyyttä välineenä edistääkseen kansallisia etujaan?

Johtopäätökset:
Kyberavaruus on antanut uutta voimaa vihamielisille vaikuttamisoperaatioille. Kognitiivinen vaikuttaminen, tai jopa sodankäynti, käyttää digitaalisia keinoja yhteiskunnan täyttämiseen paitsi narratiiveilla ja propagandalla, myös hyödyntämällä kansainvälisen oikeuden erilaisia tulkintoja. Näitä kyberavaruuteen sovellattavia oikeudellisia tulkintoja käytetään vastustajan päihittämiseksi ja kansallisten etujen edistämiseksi.

Jatkotoimenpiteet:
Lainsäädännöllä pyritään vaikuttamaan kohdeyleisöjen kognitioon. Tämän ratkaisemiseksi valtioiden on ensin lisättävä tietoisuutta kognitiivisesta vaikuttamisesta ja yhdenmukaistettava Naton/EU:n kanta näihin hyökkäyksiin. On tunnustettava, että teknologinen kehitys on nopeampaa kuin lainsäädäntökyky. Länsimaissa tulisi olla tietoisia siitä, että lakia käytetään vallan välineenä. Tulevat lait eivät saa vahvistaa autoritaarisia käytäntöjä, mutta ne eivät myöskään saa korostaa länsimaista valta-asemaa.

Tahtoon vaikuttaminen: johdanto

Toukokuussa 2024 Saksan ulkoministeri Annalena Baerbock syytti Saksan sosiaalidemokraattiseen puolueeseen (SPD) kohdistuneesta kyberhyökkäyksestä APT 28:aa, joka on Venäjän sotilastiedustelupalvelun GRU:n alainen uhkatoimija. [1] Hyökkäys, luultavasti tietojenkalasteluhyökkäys, oli osa laajempaa hyökkäyskampanjaa, joka kohdistettiin kesäkuussa 2024 pidettyihin Euroopan parlamentin (EU) vaaleihin. Myös Naton Pohjois-Atlantin neuvosto ilmaisi huolensa Baltian maihin, Puolaan ja Isoon-Britanniaan kohdistuneista kyberhyökkäyksistä.

Vaalit ovat demokratioille epävarmaa aikaa. Ne ovat saumoja, joissa yhteiskunta siirtyy vaaleilla valituilta lainsäätäjiltä toiselle. Kaikissa järjestelmissä, olipa kyse sotilasoperaatioista tai lämmitysjärjestelmän hitsaamisesta, saumat ovat haavoittuvia. Liberaalit demokratiat ovat haavoittuvampia kuin autoritääriset valtiot, koska demokraattisessa järjestelmässä on enemmän saumoja, toisin kuin autoritäärisissä joissa valtaa ei useinkaan ole aidosti jaettu, puhumattakaan vallanvaihdosta.

Kansan tahtoon vaikuttaminen vaalien kautta oli pitkään osa kaksinapaisen kylmän sodan maailmaa. Neuvostoliiton aktiiviset toimenpiteet ja Amerikan poliittinen sodankäynti kattoivat vaaleihin puuttumisen. Näin suostuteltiin tai manipuloitiin ulkomaisen yleisön ja poliittisten johtajien tietoisuutta valitsemaan tai perustamaan hallituksen Neuvostoliiton tai Yhdysvaltojen etujen mukaisesti.

Vaikka vastustajan tahdon alistaminen on ollut sodankäynnin tavoite Sun Tzusta lähtien, kognitiivisen sodankäynnin käsite on saanut vetovoimaa kyberavaruuden kasvun ja mahdollisen suoran sosiaalisen median vaikuttamisen kautta. Kyberavaruus on ihmisen tekemä ulottuvuus, joka on lisännyt kolme kerrosta olemassa olevaan tietoympäristöön: itse laitteisto; virtuaalinen persoona, jota käytämme kommunikoimaan verkossa; ja tiedot ja protokollat, jotka mahdollistavat viestinnän. [2] Nämä lisäkerrokset tarjoavat uusia saumoja, joita valtiolliset ja valtiosta riippumattomat toimijat haluavat suojella tai käyttää vuorovaikutuksessa muiden kanssa.

Kybertoimintaympäristön ilmaantuminen on mahdollistanut kolme kybertoimintaan liittyvää toimintatapaa: digitaalisen tiedustelutiedon keräämisen (vakoilun) skannaamalla tai kopioimalla virtuaalisiin tietovarastoihin rajoittuvia tietoja; digitaaliset vaikuttamisoperaatiot; [3] ja digitaalisen vastustajan heikentämisen. [4] Jälkimmäisellä tarkoitetaan kyberhyökkäyksiä, jotka ovat virtuaalisen ulottuvuuden toimintoja, jotka heikentävät kyberavaruutta binäärikoodilla, muokkaavat tai manipuloivat tietoja ja heikentävät tai tuhoavat laitteistoja tai protokollia, mikä johtaa virtuaalisiin ja/tai fyysisiin vaikutuksiin kyberavaruudessa. Digitaalisissa vaikuttamisoperaatioissa kyberavaruutta käytetään vektorina ryhmien tai yleisöjen (inhimilliseen) kognitiiviseen ulottuvuuteen käyttämällä sisältöä, sanoja, meemejä ja kuvamateriaalia ”aseina”. [5] Lukuun ottamatta suuria valtion tukemia operaatioita, josta aiempi esimerkki on Stuxnet, useimmilla Ukrainassa ja Gazassa havaituilla kyberhyökkäyksillä on ollut rajallinen vaikutus. Sitä vastoin valtiotason vaikuttamisoperaatioilla, mukaan lukien Venäjän vaalivaikuttamisella Yhdysvaltain vuoden 2016 presidentinvaaleihin, oli strategisia vaikutuksia. [6]

Kybertoimintaympäristöön liittyvien toimien lisäksi Ukrainan ja Gazan sodissa on syntynyt uusia toimijoita ja teknologioita. Valtiosta riippumattomat toimijat, kuten Anonymous, Microsoft ja Elon Musk, osallistuvat näihin konflikteihin joutumatta sotaa käyväksi osapuoleksi, ja tekoälyä on käytetty asejärjestelmien kohdentamisessa Gazan sodassa. [7] Nämä aiheet herättävät paitsi operatiivisia ja eettisiä myös oikeudellisia kysymyksiä – esimerkiksi valtiosta riippumattoman toimijan DDoS-hyökkäyksistä ja kansainvälisestä humanitaarisesta oikeudesta tai kansainvälisen humanitaarisen oikeuden 49 artiklan ensimmäisen liitteen kattavuutta kyberhyökkäyksistä. [8]

Valtioiden (kansainvälisen) oikeuden erilaisten tulkintojen käyttämistä tai hyödyntämistä voidaan käyttää jopa välineenä vaikuttamaan havaintoihin ja kognitioon. Tällainen ”lawfare”[9] voi olla väline, jolla vaikutetaan kohdeyleisöjen kognitioon kyberavaruuden kautta. Valtiot voivat poimia rusinat pullasta, tai käyttää vakuuttavasti hyväkseen kansainvälisen oikeuden tulkintojen eroja ajaakseen tai puolustaakseen kansallisia etujaan kognitiivisen sodankäynnin keinona.

Mitä kognitiivinen sodankäynti on?

Turvallisuuden tai armeijan näkökulmasta kognitiivinen alue on sodankäynnin huippu. Thukydidesin ja von Clausewitzin kaltaiset ajattelijat väittävät, että sodankäynnin ydin on vihollisen kukistaminen – sen varmistaminen, että vastapuoli (tahtoen tai tahtomattaan) vakuuttuu siitä, että sen pitäisi muuttaa käyttäytymistään ja toimia tahtomme mukaisesti.

Menneisyydessä kognitiiviseen alueeseen vaikuttivat fyysiset teot ja siten epäsuorasti armeijoiden tai pääkaupunkien tuhoamisen uhka. Kyberavaruuden syntymisen ja kognitiivisen psykologian lisääntyneen ymmäryksen myötä[10] nykypäivän kognitiivinen sodankäynti kohdistuu myös suoraan mieleen käyttämällä vaikutus- ja informaatio-operaatioita ja psykologista sodankäyntiä - siis sodankäyntiä ilman kineettisen voiman käyttöä. Kognitiivisia toimintoja voidaan soveltaa tietoiseen mieleemme vakuuttamiseen. Ne keskittyvät alitajuntamme hyödyntämiseen,[11] joka on käyttäytymisemme tärkein ajuri: ennakkoluuloihin; heuristiikkaan; intuitioon; ja tunteisiin.

Käsitteellisenä käsitteenä kognitiivista sodankäyntiä ei ole helppo määritellä. Cluzelin tutkimuspaperissa sitä verrataan yksilöiden mielien hakkerointiin ”jokaisen yhteiskunnan perustana olevan luottamuksen heikentämiseksi”, johon kuuluvat neurotieteiden ja tekno-

logian käyttö. [12] Hung ja Hung väittävät, että informaatiosodankäynti on kognitiivisen sodankäynnin osa,[13] ja vaikutusoperaatiot ovat vain informaatiosodankäynnin kyberelementtejä. Toiset väittävät päinvastoin ja toteavat, että ”kognitiivinen sodankäynti on absorboinut informaatiosodankäynnin”. [14] Molemmissa tapauksissa siirrytään median (tiedon) hallinnasta aivojen hallintaan (kognitio).

Naton ehdottama määritelmä on ”tarkoituksellinen, synkronoitu sotilaallinen ja ei-sotilaallinen toiminta, jonka tarkoituksena on vaikuttaa yleisön asenteisiin, käsityksiin ja käyttäytymiseen kognitiivisen paremmuuden saavuttamiseksi, ylläpitämiseksi ja suojelemiseksi”. [15] Muut kognitiivisen sodankäynnin määritelmät väittävät, että se on strategia, jossa keskitytään muuttamaan kohdeväestön ajattelua ja siten sen toimintaa. Vaihtoehtoisesti ajatellaan, että ”kognitiivisessa sodankäynnissä perimmäinen tavoite on muuttaa käsitystämme todellisuudesta ja harhauttaa aivoja päätöksenteekoon vaikuttamiseksi”. [16] Kaikissa kognitiivisen sodan määritelmissä ja kuvauksissa luottamus ja totuus ovat ensisijaisia kohteita. [17]

Kognitiivista sodankäyntiä kyberavaruudessa

Kyberavaruuden kasvun myötä yhteiskuntamme ovat digitalisoituneet. Samalla myös sodankäynti digitalisoituu. Kybertoiminnan mahdollisista ja todellisista vaikutuksista keskustellaan laajasti. Vaikka jotkut tutkijat väittävät, että kybersodankäynti vastaa tavallista sodankäyntiä, yleisempi näkemys on, että useimmat kyberoperaatiot eivät ylitä sodan kynnystä. Tämä tarkoittaa sitä että itse kybertekojen sijaan, kyberoperaatioiden luokittelussa on hyötyä niiden mahdollisten vaikutusten tutkimisesta. [18]

Tuore esimerkki laajamittaisesta kybertoiminnasta on Venäjän ja Ukrainan sota. Hyökkäyksen alettua helmikuussa 2022 on tehty yli 3 500 kyberhyökkäystä. [19] Eri toimijat, mukaan lukien valtiolliset, ovat ryhtyneet näihin hyökkäyksiin. Kuitenkin 95 prosenttia voidaan luokitella DDoS-operaatioiksi, turmelemisiksi tai hack&leak-operaatioiksi. Noin 90 prosenttia hyökkäyksistä ovat toteuttaneet valtiosta riippumattomat toimijat. Palvelunestohyökkäykset ja turmelemiset ovat Gartzken ja Lindsayn luokittelemia esteitä tai haittoja,[20] jotka eivät aiheuta ”kuolemaa ja tuhoa” eivätkä tue suoraan sotilaallista kampanjaa. Vaikka jotkin kyberhyökkäykset ovat tukeneet operatiivisen tason sotilaallisia tai diplomaattisia kampanjoita, joihin kuuluvat digitaalinen vakoilu tai vakavat wiper-kyberhyökkäykset, yhtäkään vakavaa strategista vaikutusta saavuttanutta hyökkäystä (eräänlaista kyber-Pearl Harbouria) ei ole rekisteröity.

Hyökkäysten määrästä huolimatta kybertoimintaympäristön vaikutus Venäjän ja Ukrainan sodassa näyttää marginaaliselta, mikä johtuu mahdollisesti Ukrainan vastustuksesta, sietokyvystä (jota tukevat yksityiset yritykset, kuten Microsoft) ja Venäjän puuttellisista kyvykkyyksistä. Joitakin merkittäviä poikkeuksia toki on. Osa kyberoperaatioista on palvellut tarkoitustaan. Ensinnäkin hyökkäyksen aattona Venäjä hyökkäsi Viasatin satelliitti-internetyhteyteen ja aiheutti sillä digitaalisen katkoksen Ukrainan joukoille. Toiseksi Ukrainan presidentin Zelenskyin strateginen verkkoviestintä ulkomaisten parlamenttien kanssa on johtanut diplomaattiseen tukeen sekä varojen, sotilasjärjestelmien ja ampumatarvikkeiden toimittamiseen.

Tuhoa tavoittelevien kyberhyökkäysten sijaan, digitaalisilla vaikuttamisoperaatioilla voi olla strategisia vaikutuksia. Vaikka vaikuttamisoperaatiot eivät välttämättä ole luonteeltaan pahantahtoisia, niiden tarkoituksena on vaikuttaa ihmisten tai ryhmien tietoiseen, tai mieluiten alitajuiseen ymmärtämiseen ja itsenäisiin päätöksentekoprosesseihin. Kognitiivinen sodankäynti kyberavaruuden vaikuttamisoperaatioiden avulla ei tähtää ihmisten tuhoamiseen, vaan kohdeyleisön ”uudelleenmuotoiluun” hyökkääjän arvoihin, moraaliin ja oikeustajuun sopivaksi. [21]

Krimin liittämisen jälkeen venäjämieliset valtiolliset ja valtiosta riippumattomat toimijat ovat toteuttaneet kyberpohjaisia propaganda- ja disinformaatiokampanjoita luodakseen informaatioympäristön, jossa on vastakkaisia näkemyksiä ja käsityksiä. [22] Venäjän ”informaatiovastakkainasettelun”[23] päätarkoitus on demoralisoida Ukrainan väestö ja lyödä kiilaa Ukrainan ja sen läntisten liittolaisten välille. Vaikuttamisoperaatioilla tavoitellaan myös venäläistä kotimaista yleisöä. Käytettyjä narratiiveja ovat länsimainen russofobia, Ukrainan ”denatsifikaatio ja demilitarisointi” sekä korruptio Ukrainan hallituksessa. [24] Ukraina hyödyntää samalla tavalla sosiaalista mediaa. Hyökkäyksen jälkeen presidentti Zelenskyi on puhunut väestölleen verkossa ja ylläpitänyt joukkojensa moraalia, mikä vaikuttaa positiivisesti sekä omien että vihollisen kognitiiviseen ulottuvuuteen. [25] Kansainvälinen tuki on Ukrainan elinehto ja siten sekä painopiste että Akilleen kantapää. [26]

Erityisesti ihmismielen manipulaatioita tavoittelevat vaikuttamisoperaatiot ovat luonnostaan petollisia. Ne hyödyntävät heuristiikkaa ja ennakkoluuloja, houkutellen kohdeyleisöä pois rationaalisesta päätöksentekoprosessista. Petty ja Cacioppo kutsuvat tätä perifeeriseksi reitiksi. [27] Perifeeristä reittiä käytetään käyttämällä sosiaalisesti jakavaa aihetta häiritsemään kohdeyleisöä, mikä heikentää heidän kykyään käsitellä saapuvia tietoja siihen liittyvän emotionaalisen tai provosoivan tunteen vuoksi. Hung ja Hung tekevät samanlaisen arvion väittäen, että kognitiivinen sodankäynti käyttää kahta ulottuvuutta: psykologisia tekniikoita (miten aivomme toimivat ja jotka perustuvat heuristiikkaan ja toistuvaan stimulaatioon); ja ulkoisentiedon kognitiivista käsittelyä. Ihmisiin vaikuttamiseksi ennakkokäsitysten ja saapuvien ärsykkeiden välillä on oltava kuilu (tai ”vapaa energia”), tai se on luotava. Kohdeyleisön keskuuteen on luotava epäilyksiä. Juuri tätä Venäjä hyödyntää omissa informaatio-operaatioissaan luodessaan vastaikkainasettelua. [28]

Länsimaiset demokratiat ovat alttiita kognitiivisen sodankäynnin vaikuttamisoperaatioille ja siten Venäjän informaatiovastakkainasettelulle, koska niiden avoimet yhteiskunnat perustuvat sanan- ja lehdistönvapauteen sekä äänestämisen ja valituksi tulemisen vapauteen. Laillisuus ja legitiimiys kulkevat käsi kädessä sen luottamuksen kanssa, joka ihmisillä on hallitukseen, tuomareihin ja perinteiseen (usein kirjoitettuun) mediaan. Länsimaiset demokratiat ovat vapaita keskustelemaan ja omaksumaan ulkoisia ärsykkeitä, luomaan uusia ideoita, innovoimaan, epäonnistumaan ja oppimaan. Tämä ei toteudu autoritaarisissa valtioissa, jotka yrittävät heikentää saapuvia (vieraita) ärsykkeitä, tietoa ja uusia ideoita varmistaakseen, että väestön käsitykset (tai aiemmat uskomukset) on linjassa (valtion valvoman) informaatioympäristön kanssa eikä vääristy (väärillä tai oikeilla) faktoilla, jotka muuttavat aiempaa uskomusta ja luovat epäilyksiä.

Kognitiivisen sodankäynnin lainsäädäntöä

Venäjä-esimerkin rinnalla Kiinan "kolme sodankäyntiä" -strategia on toinen esimerkki kognitiivisesta sodankäynnistä. Tämä oppi, josta vastuussa on pääasiassa Kiinan kommunistisen puolueen (KKP) United Front -työosasto[29] ja Kansan vapautusarmeija,[30] pyrkii säilyttämään KKP:n poliittisen vallan ja "hallitsemaan vallitsevaa keskustelua ja vaikuttamaan käsityksiin Kiinan etujen edistämiseksi". [31] Saapuvien ärsykkeiden tukahduttamiseksi ja hyvänlaatuisen kuvan levittämiseksi Kiinan kansantasavallasta kiinalaisdiasporat eivät saa ilmaista eriäviä mielipiteitä. Internetiä ja sosiaalista mediaa sensuroidaan usein kotimaassa. [32] Kolmen sodankäynnin oppi ei sisällä vain näkemyksiä joiden tavoite on vakuuttaa ja manipuloida kuulijaa, vaan myös oikeudellisia näkemyksiä, joilla kohdeyleisön asennetta ja siten käyttäytymistä voidaan muuttaa kotimaassa tai ulkomailla. [33]

Yleisen mielipiteeseen vaikuttava sodankäynti tai mediasota pyrkii muokkaamaan "kohdeyleisöjä massainformaatiokanavien tuottaman ja levittämän tiedon avulla", sekä perinteisesti (televisio, sanomalehti, elokuvat) että internetissä. [34] Yleisen mielipiteeseen vaikuttava sodankäynti (verkossa) tavoittelee yleisen mielipiteen muokkaamista ja johdonmukaisen viestin välittämistä kohdeyleisölle Kiinan kantoja suosivalla tavalla. [35]

Siinä missä mielipidesota keskittyy totuuden joidenkin puolien kehystämiseen tai korostamiseen ja toisten laiminlyömiseen, usein ripauksella huumoria, psykologinen sodankäynti on manipuloivampaa. Psykologiseen sodankäyntiin kuuluu tiedon käyttämistä vastustajan painostamiseen ja "vahingollisten tapojen ja ajattelutapojen luomiseen, sen puolustautumistahdon vähentämiseen ja ehkä jopa tappiomielialan ja antautumisen aikaansaamiseen". [36] Psykologisessa sodankäynnissä käytetään erilaisia tekniikoita, kuten pelottelua, uskontoa,[37] epäluulojen herättämistä, manipulointia ja petoksia. [38]

Mielenkiintoista on, että Kiinan kolmea sodankäyntiä voidaan soveltaa kaikissa konfliktivaiheissa (rauhasta sotaan) käyttämällä erilaisia oikeudellisia tulkintoja vaikuttaakseen muihin. Laillinen sodankäynti on suunniteltu "oikeuttamaan toimintatapa",[39] luomalla Kiinalle suotuisa normatiivinen ympäristö. Kiinan laillinen sodankäynti, jossa käsitellään länsimaisia keskusteluja lainsäädännöstä,[40] on ei-kineettisen sodankäynnin väline, joka tavoittelee vaikutusta toimijan käyttäytymiseen strategisten tavoitteiden saavuttamiseksi. Onnistunut oikeudellinen sodankäynti rajoittaa muiden liikkumisvapautta ja laajentaa samalla Kiinan toimintavapautta.[41]

Kolme sodankäyntiä ei ole KKP-spesifi politiikka. Sen tehokkuus on siinä, että se kattaa koko yhteiskunnan. Ulkomaiselle yleisölle se käyttää Kiinan mediamaisemaa niin, että eri lähteet ja versiot toistavat ja vahvistavat annettua viestiä. Näitä ovat mediakanavat (CGTN), kulttuuri-instituutit (Konfutse-instituutit), kiinalaiset vaihto-opiskelijat, [42] diasporayhteisöt, ajatushautomot ja Kiinan diplomaattiverkosto. [43]

Lainsäädäntö sodankäynnin välineenä

Kiinan oikeudellinen sodankäynti hyödyntää kansainvälisen oikeuden epäselvyyksiä, joka liittyy uuteen kehitykseen, mikä ei ole uutta. Ydinaseet ja lentokoneet otettiin käyttöön aseellisen konfliktin lakien (IHL) syntymisen jälkeen. Koska (kansainvälinen) oikeus perustuu kuitenkin periaatteisiin, kuten sotilaalliseen etuun, erotteluun, suhteellisuuteen ja välttämättömyyteen, eikä erityisiin tilanteisiin tai tekniikoihin, lakia sovelletaan edelleen. Käytännössä aloitetaan keskustelu siitä, miten olemassa olevaa kansainvälistä oikeutta sovelletaan uuteen kehitykseen – esimerkiksi YK:n hallitusten asiantuntijaryhmässä tai avoimessa työryhmässä. [44]

Koska kansainvälinen oikeus perustuu periaatteisiin, joista säännöt johdetaan, kansainvälisen oikeuden tarkoituksena on aina ollut tarjota oikeudellista liikkumavaraa, jotta yleisiä sääntöjä voidaan soveltaa tiettyyn tilanteeseen tai uuteen kehitykseen. [45] Toisaalta uusi kehitys voi aiheuttaa haasteita, mikä johtuu erityisesti (teknologisen) kehityksen nopeudesta, mukaan lukien tekoäly,[46] ihmisen parantaminen, miehittämättömät ilma-alukset ja kyberavaruus. Tämä parallaksi aiheuttaa epävarmuutta siitä, miten lakia sovelletaan. Kyberavaruudessa käydään keskustelua siitä, onko suvereniteetti – perinteisen kansainvälisen oikeuden oikeudellinen velvoite – sääntö (velvoite) ja periaate vai pelkkä oikeusperiaate; jälkimmäinen on Yhdistyneen kuningaskunnan kanta. Tämä ei ole semanttinen keskustelu, koska jos suvereniteetti on periaate – eikä siten velvoite – sitä ei voida rikkoa. Valtion vastuuta koskevissa artikloissa todetaan, että kansainvälisesti virheellinen toimi rikkoo primaarioikeussääntöä (velvoitetta), jonka voidaan katsoa johtuvan valtiosta. Jos suvereniteettia

loukkaa valtio, joka ei pidä sitä velvollisuutena, hyvitys tai vastatoimi voi rikkoa kansainvälistä oikeutta, jolloin riita voi kärjistyä konfliktiksi.

Toinen epäselvyyttä aiheuttava tekijä on se, onko kyberavaruus itsessään osa valtion aluetta ja siten sen lakien alainen. Monissa länsimaisissa näkemyksissä alue sisältää maaperän, aluemeren ja niiden yläpuolella olevan ilmapatsaan, ei avaruutta yleensä tai kyberavaruuden virtuaalisia aspekteja – nollia ja ykkösiä. [47] Tässä mielessä kyberavaruuden virtuaalinen ulottuvuus on rajaton. Monissa autoritaarisissa valtioissa kyberavaruuden kokonaisuus liittyy alueellisen koskemattomuuden valvontaan. Siksi Kiina väittää, että sillä on digitaalinen suvereniteetti kyberavaruudessa ”maaperällään”, kun taas länsimailla on vain alueellinen valvonta maaperänsä laitteistosta.

Lisäksi, vaikka länsimaat väittävät, että kansainvälinen oikeus korvaa kansallisen oikeuden, Venäjän perustuslaki väittää, että kansallisella lainsäädännöllä on etusija kansainväliseen oikeuteen nähden. Sitä vastoin Kiina käyttää kansainvälistä oikeutta korostaakseen vaatimuksiaan esimerkiksi Etelä-Kiinan merellä,[48] ja kiistää länsimaisen näkemyksen, jonka mukaan vain luonnolliset (ei keinotekoiset) saaret ovat osa aluevaatimusta.

Lopuksi totean, että yhteisessä kokeiluhankkeessa ei tehdä selvää eroa sodan ja rauhan välillä. Kolmen sodankäynnin perusteella nämä ”sodankäynnin” muodot alkavat ennen varsinaista sotilaallista sitoutumista, ja ne toteutetaan taistelukentän ja sen osallistujien muokkaamiseksi ja valmistelemiseksi. Kaikki nämä kolmen sodankäynnin muodot ovat sovellettavissa sodan ja rauhan kirjoon.

Miten vastata lain käyttöön sodan välineenä

Lain käyttö koginitioon ja havaintoihin vaikuttavana vallan välineenä on mahdollista jatkuvien oikeudellisten kiistojen vuoksi, ja valtioilla on erilaisia tulkintoja siitä, miten (kansainvälistä) oikeutta sovelletaan kyberympäristöön. Kognitiivisen sodankäynnin torjumiseksi on kriittistä ymmärtää hyökkääjän tavoitteet ja aikomus ennen vastatoimien käynnistämistä. Naton ja EU-maiden on lisättävä yleistä tietoisuutta mahdollisista ulkomaisesta kognitiivisen sodankäynnin keinoista, mukaan lukien lainsäädännön hyödyntäminen, ja yhdenmukaistettava kantoja liittoumissa. Lisäksi keskustelu uuden lainsäädännön tarpeellisuudesta on yhä tärkeä.

Ensinnäkin valtioiden, erityisesti liberaalien demokratioiden, on ymmärrettävä, että Kiinan ja Venäjän kognitiivisen sodankäynnin tavoitteet ja keinot eroavat toisistaan. Venäjän toiminnan tarkoituksena on kylvää hämmennystä levittämällä tietoa, joka on ristiriidassa olemassa olevan tiedon kanssa tai kumoaa sen. Esimerkki tästä on valheiden ketju, joka seurasi Venäjän MH17:n alasampumista. Venäjän kognitiiviset ja vaikuttamisoperaatiot voidaan nähdä vieraan valtion yleisöön vaikuttavana tylpänä välineenä, jonka tarkoituksena ei ole muuta kuin hämmentää, kylvää epäsopua ja heikentää luottamusta demokraattiseen perustaan. Vaikka Venäjä käyttää hyväkseen kansainvälisen oikeuden aukkoja, se haluaisi mieluummin laiminlyödä sen kokonaan.

Sitä vastoin Kiinan toimet ovat hienovaraisia ja niillä pyritään selvästi ylläpitämään tai parantamaan ulkomaisen yleisön hyväntahtoista kuvaa Kiinasta. Kiinan kansantasavalta vetoaa kansainväliseen oikeuteen, mutta kannattaa sen perusteiden uudelleenneuvotteluja, koska Kiinan mukaan nykyinen kansainvälinen oikeus heijastaa länsimaiden etuja. Venäjän tai Kiinan kognitiivisen toiminnan torjunnassa on otettava huomioon hyökkääjän tarkoitus. Pahin virhe olisi arvioida kognitiivista toimintaa länsimaisten standardien mukaisesti.

Tietoisuuden lisääminen on (yleensä) tehokas keino vastustaa kognitiivista sodankäyntiä. Yhdysvaltain kansalaiset eivät tienneet ulkomaisten toimijoiden sosiaalisen median kampanjoiden mahdollisista vaikutuksista vuoden 2016 presidentinvaalien alla - naiivius, joka oli jo suurelta osin kadonnut vuoden 2018 välivaaleihin mennessä. Koulutuksen saatavuus on ratkaisevan tärkeää, samoin kuin kouluille suunnatut ylimääräiset koulutusohjelmat avoimen ja vapaan (eli suodattamattoman) internetin eduista ja vaaroista, mikäli peruymmärryksen taso on jo saavutettu.

Tietoisuuden lisäämisen lisäksi koalitio voi estää tai rajoittaa ulkomaisen kognitiivisen sodankäynnin tehoa muodostamalla yhteisen kannan ja yhteisen blokin Naton ja EU:n jäsenvaltioiden kesken Japanin ja Australian kaltaisten kumppaneiden kanssa. Vastustajat käyttävät hyväkseen näiden liittoumien saumoja, varsinkin kun yhteistä perusaatetta ei ole. Tämä on tällä hetkellä nähtävissä Naton ja EU:n jäsenvaltioiden hauraissa ja vaihtelevissa linjauksissa Ukrainan sotaan, mikä on myös lisännyt kitkaa valtioiden välillä. [49]

Useimmat kansainväliset oikeustieteilijät väittävät, että nykyinen laki on riittävä. Lain soveltamista on kuitenkin tarkennettava, ja sitä varten tarvitaan enemmän valtioiden toimintaa ja oikeudellisia lausuntoja (opinio iuris). Vaarana on, että tämä on toiveajattelua. On mittava haaste sovittaa yhteen valtioiden eriävät mielipiteet – olivat ne sitten järkeviä oikeudellisia mielipitetä tai poliittisen pragmatismin heijastuksia. Jotkut valtiot ovat jo vakiinnuttaneet asemansa tai ovat nähneet edut, joita lain käyttäminen vallan välineenä esimerkiksi YK:n ja OEWG:n istunnoissa tarjoaa.

Lisäksi uusi kehitys (tekoäly, kvanttilaskenta) on aiempaa monimutkaisempaa, eikä kansainvälinen oikeus pysy enää uuden sen tahdissa. EU:n lainsäätäjät eivät edelleenkään pysty täysin ymmärtämään tekoälyn kaltaisen kehityksen mahdollisuuksia ja vaaroja. He näkevät kuitenkin aivan oikein lainsäädännön tarpeen. Tuloksena on lakeja, jotka heijastavat ennen kaikkea lainsäädäntöprosessin konsensuksen rakentamista, mutta jotka ovat sisällöltään moniselitteisiä, mikä puolestaan mahdollistaa itseä hyödyttävien lain kohtien poimimista tai sen tahallista väärintulkintaa ja siten lain käyttöä vallan välineenä. Kyseessä on siis varsinainen paholaisen dilemma.

VIITTEET

[1] APT means an advanced persistent threat (usually a state (financed) cyber actor); the GRU is the Russian military intelligence service. See Marcel Rosenbach and Christophe Schult, 'Baerbocks Digitaldetective decken russische Lügenkampagne auf', Der Spiegel, 26 January, 2024, https://archive.ph/2024.01.26-114242/https://www.spiegel.de/politik/deutschland/desinformation-aus-russland-auswaertiges-amt-deckt-pro-russische-kampagne-auf-a-765bb30e-8f76-4606-b7ab-8fb9287a6948.

[2] Peter B.M.J. Pijpers, 'Careful what You Wish for: Tackling Legal Uncertainty in Cyberspace', Nordic Journal of International Law Volume 92, Issue 3 (2023): 397–399.

[3] Andreas Krieg, Subversion: The Strategic Weaponization of Narratives, 2023.

[4] Peter B.M.J. Pijpers and Kraesten L. Arnold, 'Conquering the Invisible Battleground', Atlantisch Perspectief Volume 44, Issue 4 (2020): 11–14; Paul A.L. Ducheine, Peter B.M.J. Pijpers, and Kraesten L. Arnold, 'The "Next" War Should Have Been Fought in Cyberspace, Right?', in Beyond Ukraine, Debating the Future of War, eds Tim Sweijs and Jeff Michaels (Hurst Publishers, 2024); Paul A.L. Ducheine, Jelle van Haaster, and Richard van Harskamp, 'Manoeuvring and Generating Effects in the Information Environment', in Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis – NL ARMS 2017, ed. Paul A.L. Ducheine and Frans P.B. Osinga, 2017.

[5] Miranda Lupion, 'The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News', Journal of Slavic Military Studies, Volume 31, Issue 3 (2018): 329–330; Calder Walton, 'What's Old Is New Again: Cold War Lessons for Countering Disinformation', Texas National Security Review, Fall 2022.

[6] Ellen Nakashima, 'Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections', The Washington Post, 2018, https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html.

[7] Yuval Abraham, '"Lavender": The AI Machine Directing Israel's Bombing Spree in Gaza', +972 Magazine, April (2024), https://www.972mag.com/lavender-ai-israeli-army-gaza/.

[8] Article 49.1. of the 1977 Additional Protocol (1) to the Geneva Conventions states: '"Attacks" means acts of violence against the adversary, whether in offence or in defence.'

[9] Orde F. Kittrie, Lawfare: Law as a Weapon of War, (Oxford University Press, 2016), 4–8.

[10] Francois du Cluzel, 'Cognitive Warfare' (Innovation Hub, 2021), 12.

[11] Cornelus van der Klaauw, 'Cognitive Warfare', in: The Three Swords Volume 39 (2023), 99.

[12] Francois du Cluzel, 'Cognitive Warfare', 7.

[13] Tzu-chieh Hung and Tzu-wei Hung, 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', Journal of Global Security Studies Volume 7, Issue 4 (2020): 2–4.

[14] Russtrat, 'Cognitive Warfare: War of a New Generation', Institute of Russian Strategies, 24 December 2021, https://russtrat.ru/en/analytics_/24-december-2021-2228-7813.

[15] NATO Cognitive Warfare Concept, version of 17 April 2024, Supreme Allied Command Transformation.

[16] Cornelus van der Klaauw, 'Cognitive Warfare', 100.

[17] Alonso Bernal et al., 'Cognitive Warfare: An Attack on Truth and Thought', NATO & John Hopkins, 2020; Francois du Cluzel, 'Cognitive Warfare', (Innovation Hub, 2021), 8–9.

[18] Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed., (Cambridge University Press, 2017).

[19] CyberPeaceInstitute, 'Cyber Dimensions of the Armed Conflict in Ukraine' (2023), https://cyberconflicts.cyberpeaceinstitute.org.

[20] Jon Lindsay and Erik Gartzke, 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited', in The Power to Hurt: Coercion in Theory and in Practice, 2016, 179–203.

[21] Russtrat, 'Cognitive Warfare: War of a New Generation.'

[22] Todd C. Helmus et al., Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe (Rand Corporation, 2018), 7–25.

[23] Michelle Grisé et al., Russian and Ukrainian Perspectives on the Concept of Information Confrontation, Rand Research Report, 2022, 5–10.

[24] Tine Molendijk, 'Morale and Moral Injury among Russian and Ukrainian Combatants', in Reflections on the Russian-Ukrainian War, eds Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens, (Leiden University Press, 2024), 99–106.

[25] The story of a Ukrainian fighter pilot, 'the Ghost of Kyiv', went viral online. Another occurrence concerned the bold response of Ukrainian troops defending Snake Island after Russia's Black Sea Fleet flagship 'The Moskva' demanded their surrender or the attack on the Kerch bridge.

[26] Paul A.L. Ducheine, Peter B.M.J. Pijpers, and Kraesten L. Arnold, 'The "Next" War Should Have Been Fought in Cyberspace, Right?', 101–104.

[27] Richard E. Petty and John T. Cacioppo, 'The Elaboration Likelihood Model of Persuasion', Advances in Experimental Social Psychology 19 (1986): 126.

[28] T.S. Allen and A.J. Moore, 'Victory without Casualties: Russia's Information Operations' Parameters Volume 48, Issue 1 (2018): 60.

[29] Marcel Angliviel de la Beaumelle, 'The United Front Work Department: "Magic Weapon" at Home and Abroad', China Brief Volume 17, Issue 9 (2017).

[30] But not solely: the ministry of State Security, the Taiwan Affairs office and the Central Committee of the Party (international liaisons, propaganda and the United Front work department) are involved, to name only a few.

[31] Pieter Zhao, 'Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy', The Strategy Bridge, August (2023), https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology.

[32] Alina Polyakova and Chris Meserole, 'Exporting Digital Authoritarianism: The Russian and Chinese Models', Policy Brief, Democracy and Disorder Series, 2019, 1–22, 2–6.

[33] Albert Zhang, 'Gaming Public Opinion Influence Operations', ASPI Policy Brief no. 71 (2023).

[34] Dean Cheng, Cyber Dragon: Inside China's Information Warfare and Cyber Operations, Praeger, 2017, 51–53; Peter Mattis, 'China's 'Three Warfares' in Perspective', in War on the Rocks, 2023.

[35] See e.g.: CGTN Official, 'Samarland, Listed by UNESCO as a World Heritage Site', X (Twitter), 2023, https://twitter.com/cgtnofficial/status/1707625764412440805?s=43&t=7eecH6cep1ONZNAMcRFBlw.

[36] Deng Cheng, Cyber Dragon: Inside China's Information Warfare and Cyber Operations, 44–45.

[37] Tzu-chieh Hung and Tzu-wei Hung, 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', 4.

[38] Paul Charon and Jean-Baptiste Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', IRSEM, 49–51; Nadine Yousif, 'MP Michael Chong Urges US–Canada Cooperation on China Interference', BBC News, 2023, https://www.bbc.com/news/world-us-canada-66791749.

[39] Emilio Iasiello, 'China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities', Journal of Strategic Security Volume 9, Issue 2 (2016): 56.

[40] Aurel Sari, 'Hybrid Threats and the Law: Concepts, Trends and Implications', 2020, 10–12.; Bret Austin White, 'Reordering the Law for a China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace', Journal of National Security Law & Policy Volume 11, Issue 2 (2021): 435–88.

[41] Charon and Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', 51–55.

[42] Pieter Zhao, 'Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy', The Strategy Bridge, August (2023), https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology.

[43] Rush Doshi and Robert D. Williams, 'Is China Interfering in American Politics?', Lawfare, October (2018).

[44] United Nations General Assembly, 'Final Substantive Report', Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.

[45] See e.g. the so-called Martens Clause in the preamble of the 1899 Hague Convention of the Law and Customs of War on Land.

[46] Todd C. Helmus, 'Artificial Intelligence, Deepfakes, and Disinformation: A Primer', Rand Perspective, July (2022); Adrian Agenjo, 'Lavender Unveiled: The Oblivion of Human Dignity in Israel's War Policy on Gaza', Opinio Juris, April (2024): 1–5, http://opiniojuris.org/2024/04/12/lavender-unveiled-the-oblivion-of-human-dignity-in-israels-war-policy-on-gaza/.

[47] Michael N. Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations', International Review of the Red Cross (Cambridge University Press, 1 April 2019).

[48] National Institute for South China Sea Studies, 'A Legal Critique of the Award of the Arbitral Tribunal in the Matter of the South China Sea Arbitration', Asian Yearbook of International Law 24 (2020).

[49] Vladimir Soldatkin and Anita Komuves, 'Hungary's Orban talks Ukraine peace with Putin, stirring EU outcry', Reuters, https://www.reuters.com/world/europe/hungarys-orban-says-no-position-negotiate-between-ukraine-russia-2024-07-05/.

KIRJOITTAJA:

Tohtori Peter B.M.J. Pijpers on kyberoperaatioiden apulaisprofessori Alankomaiden puolustusakatemiassa, tutkija Amsterdamin yliopiston kansainvälisen oikeuden keskuksessa ja ulkomaalainen tutkija Etelä-Floridan yliopiston globaalissa ja kansallisessa turvallisuusinstituutissa. Pijpers on julkaissut kyberavaruuden vaikuttamisoperaatioiden oikeudellisista ja kognitiivisista ulottuvuuksista sekä siitä, miten asevoimat voivat liikkua informaatioympäristössä. Katso lisäksi Orcid ID 0000-0001-9863-5618. Kirjoittajaan voi ottaa yhteyttä osoitteeseen b.m.j.pijpers@uva.nl. Tämän artikkelin näkemykset ovat kirjoittajan omia, eivätkä edusta Alankomaiden puolustusakatemian näkemyksiä.

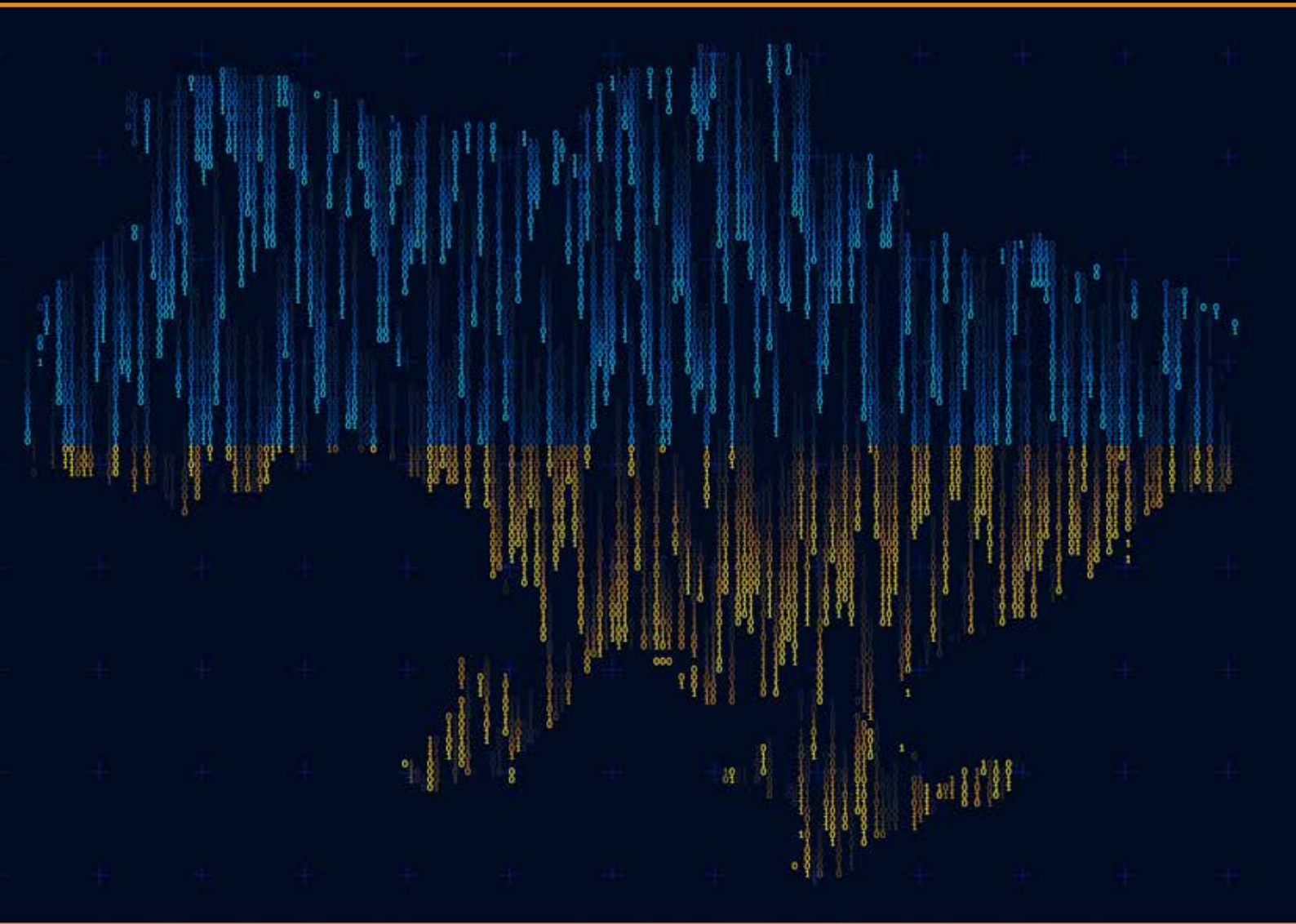
PETER B.M.J. PIJPERS

Cyberwatch Finland

VIIKKOKATSAUS

9/2025

Erikoiskatsaus Ukrainan sodasta



Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Alkusanat

Ukrainan sodan laajamittaisen hyökkäyksen alkamisesta tuli maanantaina kuluneeksi kolme vuotta. Vuosipäivän muistamiseksi Cyberwatch Finland julkaisee viikkokatsauksen teemakatsauksen Ukrainan sodan kyberulottuvuudesta. Laajamittaisen hyökkäyksen alkuvaiheessa Ukrainan sotaa kommentoitiin maailman ensimmäisenä rajoittamattomana kybersotana, ja kyberkomponenttiin suhtauduttiin uteliaasti ja sen varaan laskettiin paljon. Sittemmin käsitys kybervälineen käyttötarkoituksista on tarkentunut, ja kybersota on kehittynyt. Kybersodalla on ollut laaja vaikutus eurooppalaiseen ja länsimaiseen turvallisuusympäristöön. Mitä hyökkäyksen neljäs vuosi tai mahdolliset rauhanneuvottelut tarkoittavat kyberympäristössä, ei vielä tiedetä, mutta valistuneita arvioita voidaan kuitenkin esittää.

Kybersodan kehittyminen

Ukrainan kybersodan taustoitusta tulee hakea kauempaa, kuin laajamittaisen hyökkäyksen aloittamisesta helmikuussa 2022. Sodan voidaan laskea alkaneen jo vuoden 2014 Krimin valtauksesta ja Itä-Ukrainan tapahtumista. Vuodet 2014–2022 petasivat laajamittaista hyökkäystä myös kybermaailmassa. Esimerkiksi verkossa levitettävän dis- ja misinformaation sekä muut kognitiivisen sodankäynnin muodot näkyivät niin Ukrainassa, Euroopassa kuin Venäjällä.

Vuosina 2014–2022 Ukraina kohtasi kyberhyökkäyksiä, joista yksi merkittävimmistä oli maan sähköverkkoon kohdistunut kyberhyökkäys vuonna 2015, joka jätti yli 200 000 asukasta ilman sähköä useiden tuntien ajaksi. Sähköverkkoon hyökättiin uudestaan kyberhyökkäyksellä vuonna 2016, jolloin pääkaupungissa Kiovassa, keskellä talvipakkasia, jälleen sadat tuhannet jäivät ilman sähköä. Tämän hyökkäyksen vaikutukset saatiin kuitenkin rajattua vain noin tuntiin. Vuonna 2017 Ukrainaa riivasivat Petya-kiristyshaittaohjelmahyökkäykset, jotka muun muassa CIA ja Ukrainan viranomaiset ovat myöhemmin yhdistäneet Venäjälle. Aikaa ennen laajamittaista hyökkäystä käytettiin Ukrainan kriittisiin järjestelmiin soluttautumiseen myöhempää käyttötarkoitusta varten. Tammikuussa 2022 Ukrainaan kohdistui kyberhyökkäyksiä, joilla todennäköisesti tähdättiin pelotteluun ja informaatiovaikutukseen, ja näin pedattiin helmikuun lopun laajamittaista kineettistä hyökkäystä.

Laajamittaisen hyökkäyksen jälkeistä Venäjän kybertoimintaa on tyypillisesti kuvattu kolmivaiheiseksi. Näistä ensimmäisessä Venäjä laukaisi nopeasti aiemmin saamansa jalansijat ukrainalaisissa järjestelmissä. Tähän lukeutuvat kriittiseen infrastruktuuriin ja viestintään vaikuttaneet kyberhyökkäykset, joita ovat muun muassa Viasat-satelliittien hakkeroiminen sekä tuhoamistarkoituksessa wiper-haittaohjelmilla tehdyt hyökkäykset ukrainalaisiin organisaatioihin. Kyberhyökkäyksillä ei kuitenkaan onnistuttu tuhoamaan järjestelmiä tai kriittistä infrastruktuuria pysyvästi. Varsin pian Venäjä huomasi, että on todennäköisesti helpompaa ja nopeampaa tuhota infrastruktuuria perinteisen kineettisen vaikuttamisen avulla, joten kyberhyökkäyksissä siirryttiin Venäjän puolelta enemmän kybertiedusteluun ja tiedon varastamiseen. Tavoitteena on ollut muun muassa kerätä tietoa fyysisten iskujen aiheuttamista tuhoista sekä muista strategisista kohteista. Kolmannessa vaiheessa muotona on ollut jonkinlainen näiden kompromissi, jossa iskuja tehdään tarkemmin ja harkitummin.

Ukrainan kybertoiminnassa ei sen sijaan ole erotettavissa yhtä selkeästi eri vaiheita. Laajamittaista hyökkäystä edeltävältä ajalta on korostettu kansainvälisen yhteistyön, erityisesti joulukuussa 2021 alkaneen Yhdysvaltain Hunt Forward –operaation, merkitystä kyberpuolustuksen vahvistamisessa. Offensiivisen kybervoiman osalta Ukraina sai hyökkäyksen alussa mobilisoitua varsin paljon vapaaehtoisia oman kybertoimintansa tueksi ja muun muassa ohjeistusta palvelunestohyökkäyksien tekoon jaettiin laajalti. Vuosien aikana Ukrainan suorittamien kyberhyökkäysten määrä on jatkunut ja vapaaehtoisia on entistä tiukemmin sidottu osaksi armeijan rakenteita. Ukrainan näkyvämpiä kyberhyökkäyksiä Venäjälle ovat olleet valtion viranomaisiin ja erilaisiin rekistereihin tehdyt kyberhyökkäykset. Samanaikaisesti Ukrainan kyberpuolustusta on pyritty vahvistamaan kansainvälisen tuen avulla.

Ehkä yllättävintä on, että toistaiseksi Ukrainan kybersodassa ei ole havaittu käänteentekeviä yksittäisiä edistysaskeleita kybersodan kehittymisessä, kuten laajamittaisen hyökkäyksen ensivaiheessa ajateltiin. Näihin lukeutuivat esimerkiksi odotukset uusista hyökkäystavoista, haittaohjelmista tai muista kyberinnovaatioista. Mahdollista tosin on, että merkittävimmät innovaatiot pidetään salaisuuksina, ja niiden leviämistä pyritään estämään. Ennen laajamittaista hyökkäystä ja vielä sen alkaessa kyberympäristön roolin ajateltiin olevan huomattavan erilainen kuin miksi se todellisuudessa muodostui. Venäjä ei saanut Ukrainaa polvilleen kyberkeinoin ja kyberaseiden tuhovoima osoittautui oletettua pienemäksi. Kyberaseella voidaan sodankäynnissä nähdä olevan vain kiineettistä operointia tukeva rooli.

Ukrainan kyber-rintaman nykytilanne

Tällä hetkellä käynnissä olevat Ukrainan sodan kyberoperaatiot voidaan karkeasti jakaa kolmeen kategoriaan. Ukrainan ja Venäjän keskinäisiin, toistensa järjestelmiin tekemiin iskuihin, Venäjän operaatioihin Ukrainaa tukeviin maihin kohteisiin sekä informaatioympäristön operaatioihin. Kuten mainittua ensimmäisen kategorian hyökkäykset olivat aktiivisimmillaan sodan ensimmäisen vuoden aikana Venäjän laukaistessa valmistelemiaan aseita ja hyödynnettyä saavutettuja jalansijoja. Sittemmin näkyvät ja julkisuuteen päätyvät venäläiset hyökkäykset ovat olleet verrattain harvemmassa niiden keskittyessä salassa toteutettavaan tiedonhankintaan.

Tällä hetkellä useammin näkeekin uutisia Ukrainan toteuttamista iskuista venäläisiin kohteisiin. Viimeisin esimerkki on tammikuun lopulla venäläistä öljyjätti Gazpromia vastaan tehty hyökkäys, jossa ukrainalaiset ainakin väitetysti onnistuivat lamauttamaan yhtiön verkkopalvelut muutaman päivän ajaksi. Tapaus kuvaa hyvin siitä, miksi Ukraina hyökkäyksiä toteuttaa. Niiden tavoitteena on tehdä sota näkyväksi ja tuntuvaksi tavallisille venäläisille, vaikuttamalla käytössä oleviin palveluihin ja nakertamalla valtamedian narratiiveja siitä, miten hyvin erikoisoperaatio sujuu.

Toinen tavoite on oman ja liittolaisten taisteluhengen ylläpitäminen onnistumisista raportoimalla ja muistuttamalla, että kamppailu jatkuu kaikilla rintamilla. Tästäkin hengennostatuksesta tammikuun isku on oiva näyte, sillä se toteutettiin historiallisen vuoden 1918 Krutyn taistelun muistopäivänä. Krutyn taistelu on Ukrainassa tunnettu symbolinen tapahtuma, jossa ukrainalaisista kadeteista koottu joukko puolusti onnistuneesti Kiovaa kymmenkertaista venäläistä ylivoimaa vastaan. Samankaltaista henkeä yritetään nyt herätellä kyberhyökkäysten myötä. Vaikka Gazpromille iskusta ei todellisuudessa koitunut todennäköisesti kovinkaan merkittäviä tappioita tai haittavaikutuksia, on Ukrainan iskujen tavoitteet usein muualla kuin suoraan venäläisten yritysten toimintaan vaikuttamisessa. Merkittävä osa kyberresursseista ohjautuu todennäköisesti vakoilu- ja tiedonhankintaoperaatioilta suojautumiseen, mutta tässä tapahtuvat onnistumiset (tai epäonnistumiset) jäävät usein julkisuudelta piiloon.

Venäjän toteuttamista kyberoperaatiosta viime aikoina eniten huomiota ovat saaneet Ukrainan liittolaisiin tai tukijoihin kohdistuneet iskut. Näitä ovat sekä matalan tason palvelunestohyökkäykset, joita eri haktivistiryhmät toteuttavat päivittäin, että korkeamman tason APT-ryhmien operaatiot. Jälkimmäiset vaihtelevat toteutustavaltaan ja kohteiltaan, mutta selkeä muutos on tapahtunut sodan aikana siinä, kuinka suuri määrä operaatioista ohjautuu Ukrainaan ja kuinka paljon sen ulkopuolelle. Sodan ensimmäisen vuoden aikana Venäjän APT-ryhmien huomio vaikutti olevan lähes yksinomaan Ukrainassa, mutta vuoden 2023 ja etenkin 2024 aikana länsimaat valikoituivat kohteeksi useasti. Konkreettinen havainto tästä saatiin huhtikuussa 2024, kun Ukrainan sodan aikana kehitetystä edistyneestä Kapeka-nimisestä haittaohjelmasta saatiin havaintoja ympäri Eurooppaa. Syitä siihen miksi kohteet ovat valikoituneet Ukrainan ulkopuolelta, ovat se, että Ukrainassa Venäjän on mahdollista käyttää suorempia aseita, kuin piilossa toteutettuja kyberoperaatioita ja se, että tavoiteltua tuhovaikutusta ei Ukrainassa saavutettu laajalla kyberkampanjalla.

Näkyvä Ukrainan sodan kyberilmiö on ollut kamppailu informaatioympäristössä. Tämä on jatkunut samankaltaisena käytännössä koko sodan ajan molempien osapuolten pyrkien vakuuttamaan omaa puoltaan menestyksestä, sekä vaikuttamaan puolueettomissa maissa vallitseviin narratiiveihin tuottamalla omia tavoitteita palvelevia uutisia ja valeuutisia. Laajamittaisen hyökkäyksen alkuvaiheessa varsinkin Ukrainan strateginen viesti oli voimakkaampi, ja käänsi yleisen mielipiteen länsimaissa sen puolelle. Venäjällä taas on ollut omaa yleisöään muun muassa Latinalaisessa Amerikassa sekä Afrikassa. Vuosien varrella Ukrainan viesti on heikentynyt, mikä näkyy Euroopassa kipuiluna Ukrainaan annettavan avun suhteen ja Venäjää ymmärtävien mielipiteiden kasvuna esimerkiksi Saksassa.

Vuoden 2025 aikana merkittävin aihe, josta osapuolet eri narratiiveja levittävät on ollut Yhdysvalloissa tapahtunut vallan vaihdos ja sen vaikutus konfliktin tulevaisuuteen. Venäläismedioissa Trumpin valtaannousu on nähty positiivisena ja Ukrainan sodankäyntikykyyn merkittävästi vaikuttavana tekijänä. Esimerkiksi venäläisen Argumenty i fakty (Аргументы и Факты) –lehden otsikoissa Trumpin kerrotaan kynivän Ukrainan puhtaaksi ja antavan lausuntoja, joissa syyttää Zelenskyä taitamattomaksi diplomaatiksi, jonka huonojen neuvottelutaitojen syytä koko sota alunperin on. Ukrainan valtionmediassa Ukrinformissa puolestaan Trump mainitaan hyvin harvoin ja uutisissa korostetaan muiden kuin Yhdysvaltojen tarjoaman avun roolia sekä yritetään kiinnittää huomio sodan aktiivisiin tapahtumiin ja Ukrainan rintamavoittoihin kansainvälisen tilanteen sijaan. Molempien osapuolten media on yhä täynnä lähes päivittäisiä uutisia menestyksestä rintamalla, kummankin todennäköisesti liioitellessa menestystään.

Vaikutus laajempaan eurooppalaiseen kyberympäristöön

Ukrainan sodalla on ollut merkittävä vaikutus eurooppalaiseen ja kansainväliseen kyberympäristöön. Näkyvin vaikutus on ollut venäjämielisten vapaaehtoisten haktivistien suorittamilla kyberiskulla Eurooppaan. Tyypillisimmillään iskut ovat olleet palvelunestohyökkäyksiä tai hajautettuja palvelunestohyökkäyksiä. Myös verkkosivujen turmelemista epäasiallisella sisällöllä on nähty. Haktivistikampanjat saivat varsin suurta huomiota laajamittaisen hyökkäyssodan alkuvaiheessa, mutta sittemmin siihen on totuttu ja hyökkäysten tietty "harmittomuus" on tunnistettu.

Sen sijaan laajempaa merkitystä on ollut hybridivaikuttamisella, jota on erityisesti kriittisen infrastruktuurin osalta tehty myös kyberkeinoin. Suomessa ja Euroopassa kriittisen infrastruktuurin alan yritykset, kuten sähköverkoista vastaava Fingrid ja useat teleoperaattorit ovat raportoineet yrityksistä murtautua järjestelmiin päivittäisten palvelunestohyökkäyksien lisäksi. Toistaiseksi suojaus on toiminut, eikä valtavia kyberkatastrofeja ole nähty. Mahdollista on, että Venäjän tuhotessa Ukrainan kriittistä infrastruktuuria ohjuksin ja muiden perinteisten aseiden muodossa, on kyberaseet kriittistä infrastruktuuria vastaan säästetty länsimaita varten. Hybridivaikuttamiseen liittyvät fyysiset sabotoinnit, joita on nähty Itämeren alueella muun muassa tietoliikennekaapeleiden katkeamisen muodossa.

Samalla kybervakoilun arvioidaan kasvaneen Euroopassa. Venäläisten matkustusrajoitteet, diplomaattien karkotukset ja muut venäläisten liikkuvuutta Euroopassa kaventaneet keinot ovat pakottaneet Venäjän siirtymään aiempaa enemmän kohti verkkotiedustelua. Vaikka valtiotason operaatioista harvoin puhutaan avoimesti edes niiden paljastuessa, on sodan aikana joitakin venäläisten APT-ryhmien toteuttamia kyberoperaatioita eurooppalaisiin kohteisiin päätynyt julkisuuteen. Venäjä ei ole ainoa sitä harjoittava maa, vaan toimintaa toteuttaa esimerkiksi Kiina ja Pohjois-Korea. Erityisen kiinnostuksen kohteina ovat olleet puolustusteollisuuden yritykset.

Lopuksi

Ukrainan sota on selvästi siirtymässä uuteen vaiheeseen mahdollisten rauhanneuvotteluiden myötä. Kirjoitushetkellä on vaikea sanoa mihin suuntaan kehitys on kulkemassa. On olemassa erilaisia näkemyksiä kiihdyttääkö vai vähentääkö mahdollinen aselepo ja rauha kyberhyökkäyksiä. On epätodennäköistä, että missään skenaariossa kyberhyökkäyksen lakkaisivat kokonaan. Se mihin suuntaan kyberrintama kehittyy, on monen tekijän summa ja lähitulevaisuuden ennakointi on vaikeaa. Rauhanneuvottelut tai aselepo voivat vähentää näkyvien operaatioiden määrä, ja tarjota osapuolille hengähdystauon, mutta toisaalta varsinkin Venäjän provokaatiot ja aselevon testaaminen ovat todennäköisiä. Myös mahdollisen rauhan tai aselevon ehdot todennäköisesti vaikuttavat siihen kuinka halukkaita osapuolet ovat näyttäviin kyberoperaatioihin.

Tällä hetkellä on tärkeää seurata Ukrainan mahdollisten rauhanneuvotteluiden etenemistä ja niiden vaikutusta kyberympäristöön. Riippuen siitä, mitä seuraavat kuukaudet tuovat tulleessaan, voi Venäjältä vapautua lisää kyberkapasiteettia länsimaiden vastaan tehtäviin operaatioihin. Lisäksi on syytä huomioida, että todennäköisesti parhaat opit Ukrainan kybersodasta, torjutuista hyökkäyksistä ja tehokkaista iskukeinoista ovat toistaiseksi pelkästään sodan osapuolten tiedossa. Tällä hetkellä operatiivista tietoa parhaista toimintatavoista varjellaan, jotta tietoisuus omista kyvyistä tai siitä, miten paljon toisen toiminnasta voidaan havaita, ei valuisi viholliselle. Jos ja kun rauha syntyy, on mahdollista, että nämä opit päätyvät laajempaan tietoisuuden, joko sodassa kovettuneiden venäläishakkerien länsimaihin suuntautuvissa operaatioissa tai tärkeinä oppeina siitä, miten Ukraina on hyökkäykset onnistunut torjumaan.

Ukrainan kybersodan tapahtumia

Viasat satelliittiverkko KA-SAT

AJANKOHTA: 24.2.2022
KUVAUS: Ukrainan sodan laajamittaisen hyökkäyksen ensimmäinen kyberhyökkäys ja kybersodan "lähtölaukaus". Tunteja ennen maahyökkäyksen alkamista venäläiset hakkerit toteuttivat tietoja tuhoavan wiper-iskun satelliittipalveluntarjoaja Viasatin KA-SAT satelliittiverkkoon. Tarkemmin kohteena oli järjestelmän Italiassa sijaitseva maa-asema, ja tavoitteena oli häiritä Ukrainan viranomaisten käyttämiä viestiyhteyksiä. Tekijäksi on epäilty Venäjän sotilastiedustelun GRU:n alaisia hakkeriryhmiä.
VAIKUTUS: Hyökkäys lamaannutti lähes kaikki Viasatin yhteyksiä käyttäneet modeemit Euroopassa, ja esimerkiksi saksalainen energiayhtiö menetti hallinnan tuhansiin tuulivoimaloihin ja kymmennet tuhannet yksityiset käyttäjät kärsivät internet-katkoksista. Vaikutus Ukrainan viranomaiskommunikointiin oli kuitenkin todennäköisesti toivottua huomattavasti pienempi.

Vulkan files tietovuoto

AJANKOHTA: 24.02.2022
KUVAUS: Laajamittaisen hyökkäyksen ensimmäisinä päivinä tapahtunut venäläisen NTC Vulkan –nimisen yhtiön tietovuoto. Kyseessä on keskisuuri venäläinen tietoturvatalo, jonka perustajat omaavat taustan Venäjän asevoimissa. Tietovuoto tapahtui yhtiön sisältäpäin, kun sotaa vastustava työntekijä luovutti saksalaismedian haltuun tuhansia yhtiön sisäisiä dokumentteja, jotka paljastivat yhteyksiä venäläisiin valtiollisiin hakkeriryhmiin ja tietoja näiden operaatioista.
VAIKUTUS: Länsimaisten tiedustelupalveluiden haltuun päätyi runsaasti tietoa venäläisten APT-ryhmien tekniikoista ja taktiikoista sekä siitä, miten iskuja valmistellaan ja suunnitellaan. Yrityksellä paljastui olevan yhteyksiä sekä turvallisuuspalvelu GRU:n että ulkomaantiedustelu SVR:n alaisiin hakkeriryhmiin. Yritys oli toiminut alihankkijana ja työkalujen kehittäjinä edellä mainituille.

KyivStar

AJANKOHTA: Joulukuu 2023, isku tapahtui 12.12. Vaikutukset jatkuivat viikkoja.
KUVAUS: Yksi merkittävimmistä ja julkisuudessa eniten esillä olleista Venäjän kyberoperaatioista Ukrainaan. Kohteena oli yksi maan suurimmista teleoperaattoreista Kyivstar ja toteuttajana GRU:n alainen Sandworm. Arvioiden mukaan järjestelmiin oli tunkeuduttu jo kuukausia aiemmin. Toteutustapana oli wiper-isku eli tavoitteena vain tuhota dataa ja estää järjestelmien toiminta.
VAIKUTUS: Tuhannet teleoperaattorin palvelimet ja tietojärjestelmät pyyhkityyivät kokonaan ja noin 24 miljoona käyttäjää menettivät puhelinverkkoyhteyden päivien ajaksi. Tämä johti siihen, että käyttäjät eivät muun muassa saaneet valtion lähettämiä varoituksia ilmahyökkäyksistä tai ohjusiskuista alueellaan. Kyivstar kärsi useiden miljoonien edestä taloudellisia tappioita, mutta jätti silti tammikuun laskut perimättä asiakkailtaan pahoitteluna toimintakatkoksesta. Tiedossa ei ole, että hyökkäys olisi merkittävästi vaikuttanut Ukrainan asevoimiin tai niiden kommunikaatioon.

Venäläisten haktivistiryhmien iskut ympäri Eurooppaa

AJANKOHTA: Laajamittaisen hyökkäyksen alkamishetkestä tähän päivään.
KUVAUS: Useat venäläiset haktivistryhmät kuten Noname057(16) ja Killnet ovat toteuttaneet päivittäisiä kyberhyökkäyksiä eurooppalaisia kohteita vastaan. Iskut ovat pääosin olleet palvelunestohyökkäyksiä, mutta joukossa on ollut myös verkkosivujen tärvelemistä ja joskus jopa tietomurtoja. Suurin osa hyökkäyksistä aiheuttaa kuitenkin vain hyvin pienen tai ohimenevän haitan uhreilleen ja niiden päätarkoituksena ei olekaan varsinaisesti aiheuttaa vahinkoa, vaan saada aihetta Telegram-kanavilla reposteluun. Toinen tavoite, johon alkuvaiheessa päästiin hyvin, on epävarmuuden ja pelon aiheuttaminen kohdeyhteiskunnassa. Vaikka palvelunestohyökkäyksistä uutisoitiin sensaatiomaisesti ja ne saattoivat aiheuttaa hämmennystä, ne pian tunnistettiin verrattain harmittomiksi ja tämä vaikutus heikkeni.
VAIKUTUS: Haktivistien operaatioilla ei ole ollut pitkäaikaisia tai merkittäviä vaikutuksia. Hetkellisiä katkoksia kohteena olevien verkkosivujen saatavuudessa ne voivat aiheuttaa, mutta näissä kyse voi olla myös siitä, että palvelun omistaja itse rajoittaa ulkomailta tulevaa liikennettä.

Avaruusmeteorologian tutkimuskeskus “Planeta”

AJANKOHTA: 24.1.2024
KUVAUS: Ukrainan tiedustelupalvelu GUR ilmoitti toteuttaneensa tietomurron venäläistä avaruusmeteorologian tutkimuskeskusta vastaan. Raportissaan GUR ilmoitti iskun toteuttajaksi BO Team –nimisen hakkeriryhmän, joka koostuu ukrainalaisista vapaaehtoisista.
VAIKUTUKSET: Ukrainan raporttien mukaan kymmenien miljoonien edestä tiedostoja ja jopa fyysistä laitteistoa tuhoutui iskun seurauksena. Venäläiset lähteet puolestaan kielsivät sen onnistumisen kokonaisuudessaan. Tutkimuskeskus hallitsee kymmeniä satelliitteja, joten tavoitteena on voinut olla vaikuttaa Venäjän asevoimien tai viranomaisten kommunikaatiojärjestelmiin, mutta luonnollisesti myös tämän vaikutuksen venäläislähteet ovat kiistäneet.

LÄHTEET:

Cyberwatch Finland, julkaisut 2022–2025

https://kyivindependent.com/ukrainian-military-intelligence-disrupts-gazproms-digital-services/

https://www.ukrinform.net/

https://aif.ru/politics/world/zelenskiy-dovyol-trampa-kak-prohodyat-peregovory-mezhdu-ssha-i-rossiey

https://www.securityweek.com/kapeka-a-new-backdoor-in-sandworms-arsenal-of-aggression/

https://www.thesign.media/blog/cyberattack-on-viasat-satellites-eu-accuses-russia

https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat

https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html

https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

https://therecord.media/ukrainian-hackers-hit-russian-scientific-center

https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report

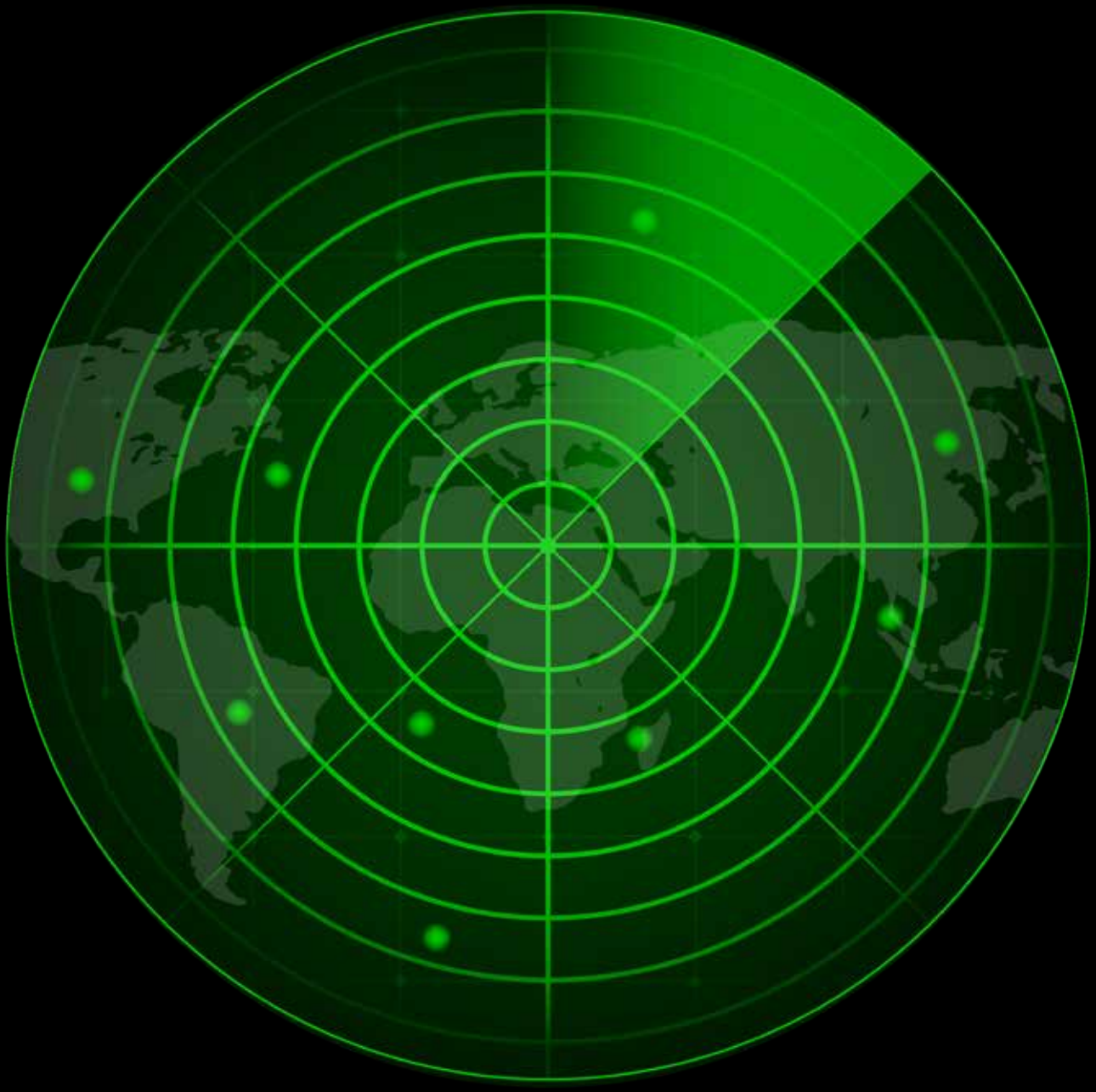
https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf

https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64622&embedded=true&a=bi

https://www.withsecure.com/en/whats-new/pressroom/withsecure-uncovers-kapeka-a-new-malware-with-links-to-russian-nation-state-threat-group-sandworm

Intohimona kyberturvallisempi maailma

Cyberwatch Finland



KUUKAUSIKATSAUS

MAALISKUU/2025

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

SISÄLTÖ:

Tässä katsauksessa

Tässä kuukausikatsauksessa tarkastelemme edellisen kuukauden merkittävimpiä kybermaailman ilmiöitä ja sidomme ne laajempiin kokonaisuuksiin. Katsaus jakautuu kolmeen tarkastelukulmaan: kuukauden merkittävämpiin kybermaailman tapahtumiin, ilmiöihin, joita haluamme erityisesti korostaa sekä kokonaisuuksiin, joiden kehitystä kannattaa seurata.

Helmikuun osalta nostamme esiin muutokset venäläisten APT-ryhmien kohteissa, Münchenin turvallisuuskonferenssin kybernäkökulmat sekä oppeja Yhdysvalloissa puhuttaneen Doge-viraston toimista kyberturvallisuuden kannalta. Seurattavia aiheita ovat avoimen lähdekoodien projektien tulevaisuus sekä näkökulmat julkisen ja yksityisen sektorin kyberyhteistyöhön, josta esimerkkinä on Puolan ja Googlen välinen yhteistyö, joka edelleen syventyi helmikuussa.

1 TAPAHTUMIA KYBERMAISEMASSA

Historiasta on tunnettu sanonta, että joskus viikoissa tapahtuu enemmän asioita kuin vuosikymmenissä. Kun tarkastellaan helmikuun ja alkuvuoden 2025 tapahtumia, ei voida välttyä analogialta. Pelkästään helmikuun aikana globaalisti on tapahtunut paljon: Yhdysvalloissa Trump aloitti merkittävät muutostyöt maan hallinnossa, ja näillä on ollut selkeä vaikutus myös kybertoimintaympäristöön. Oli Trumpista tai hänen politiikastaan mitä mieltä tahansa, on kiistatonta, että valtaannousun aiheuttamat muutokset tuntuvat globaalisti monella eri toimintakentällä ja niissä riittää analysoitavaa historian sekä politiikan tutkijoille vielä pitkäksi aikaa. Samaan aikaan helmikuussa Ukrainan sota saavutti kolmannen vuosipäivänsä ja tapahtumaa tuntui leimaavaan aselevosta käytävä keskustelu, jossa itse Ukraina ei kuitenkaan ollut koko aikaa osallisena. Neuvotteluja käytiin Yhdysvaltojen ja Venäjän välillä, sekä myös Münchenin turvallisuuskonferenssissa. Euroopan maat ovat puhuneet kovaan ääneen Ukrainan tuen jatkamisen tärkeydestä. Voikin siis liioittelematta sanoa, että tällä hetkellä eletään merkittäviä hetkiä, jotka voivat muodostaa pohjan eurooppalaiselle turvallisuusympäristölle vuosiksi eteenpäin.

Kaikella tällä on välitön vaikutus myös kybertoimintaympäristöön. Kansainvälinen politiikka vaikuttaa sekä valtiolliseen APT-toimintaan että siitä irralliseen kyberrikollisuuteen. Esimerkiksi Venäjään sidoksissa olevien hakkeriryhmien toimintaan vaikuttaa olennaisesti se, halutaanko välejä lännen kanssa liennyttää vai kärjistää. Samanaikaisesti muutokset Yhdysvaltojen hallinnossa vaikuttavat kyberturvallisuuteen, ja huolta on ilmaistu muun muassa siitä, missä määrin leikkaukset hallinnon kyberturva-asiantuntijoista tulevat vaikuttamaan kykyyn torjua tai analysoida ulkoisia uhkia. Tämä voi johtaa siihen, että kyberosaaminen kasvavissa määrin siirtyy yksityisille toimijoille, erityisesti kansainvälisille teknologiayhtiöille.

Suurien muutosten keskellä ei tule unohtaa, että kyberturvallisuus nojaa silti käytössä oleviin teknologioihin ja niiden hyödyntämiseen. Kuukauden aikana eniten huomiota herätti tammikuun lopulla kuin tyhjästä ilmaantunut kiinalainen DeepSeek-tekoäly, joka vaikutti pystyneen tehostamaan tekoälysovellusten tuotantoa moninkertaisesti länsimaisiin kilpailijoihin verrattuna. Vaikka kaikkien väitteiden paikkansa pitävyyttä ei voidakaan todentaa on silti selvää, että tällä hetkellä eletään jonkinlaista tekoälyn kulta-aikaa. Uusia sovelluskohteita keksitään jatkuvasti samaan aikaan, kun niiden kehittämiseen vaadittavat resurssit muuttuvat aina vain halvemmaksi. Esimerkkinä Elon Muskin xAI startup julkaisi uuden Grok-3 tekoälyn, joka vaikuttaa lyövän aiemmat sovellukset selvästi suorituskyvyssä. Tekoälyn potentiaalista on tähän mennessä hyödynnetty vasta murto-osa. Google Labsin johtaja totesi esimerkiksi helmikuussa verkkolehti Wiredille, että vaikka uusien suorituskykyjen kehittäminen lopetettaisiin nyt kuin seinään, on hyödyntämättömiä innovaatioita varastossa sen verran, että niistä riittäisi tuotteiksi muutettavaa suorituskykyä seuraavaksi 5–10 vuodeksi. Lausunnossa on todennäköisesti jonkin verran ”Lapin lisää”, mutta jonkinlaista indikaatiota se antaa siitä, miten tekoälyn teho kasvaa tällä hetkellä nopeammin kuin mitä sille ehditään keksimään hyödyntämiskohteita.

2 VALOKEILASSA

2.1 Venäläisen APT-ryhmän kohdevalikoima muuttunut

Microsoft julkaisi helmikuussa raportin koskien venäläisen muun muassa nimillä Sandworm, APT44 ja Seashell Blizzard tunnetun hakkeriryhmän alaryhmää, jonka toimintaa se oli seurannut ja analysoinut useamman vuoden ajalta. Paitsi, että ryhmän iskujen maantieteelliset kohteet ovat muuttuneet Ukrainan sodan aikana (ensin vain Ukraina, sitten tämän liittolaiset ja vuoden 2024 aikana erityisesti englantia puhuvat länsimaat), on myös itse operaatioissa havaittu kehitystä, jota voidaan pitää APT-ryhmälle poikkeuksellisena. Yleensä puhuttaessa valtiollisesti tuetuista APT-ryhmistä, mieleen nousevat hyvin suunnitellut ja pitkään valmistellut hyökkäykset, joiden kohteet ovat tarkkaan valikoituja. Microsoftin raportin mukaan ryhmän toiminnassa on kuitenkin tapahtunut muutos hyökkäysten kohteiden valinnassa.

Microsoftin raportissa puhutaan ”spray and pray” -toimintamuodosta, jolla kuvataan suhteellisen satunnaista kohdevalikointia ja yleisesti tiedossa olevien haavoittuvuuksien hyödyntämistä. Sandworm ryhmän on havaittu skannaavan laajalla otannalla valitun kohdemaan organisaatioiden ulkoista verkko-omaisuutta julkisesti saatavilla olevilla työkaluilla (tai näihin verrattavilla ratkaisuilla), ja valikoivan kohteensa yksinkertaisesti sen perusteella minne hyökkäyksen toteuttaminen on helppoa. Vasta järjestelmiin murtautumisen jälkeen tarkastellaan sitä, minkälainen organisaatio varsinaisesti on kyseessä, ja onko siihen tehdyllä hyökkäyksellä tai varastettavissa olevalla tiedolla strategista hyötyä. Hyödylliseksi todetuissa kohteissa operaatio on jatkunut syvemmälle järjestelmiin tunkeutumisella ja arvokkaan tiedon varastamisella. Microsoftin raportissa ei eritellä mihin kohteisiin ryhmän on havaittu näin tunkeutuneen, ja millaisissa hyökkäys on ikään kuin jätetty kesken vähäisen merkityksen vuoksi. Todennäköisesti kohteet, joissa hyökkäystä on jatkettu, ovat sellaisia, jotka eivät muuten olisi nousseet uhkatoimijoiden listoille, mutta ovat osa esimerkiksi kriittisten toimijoiden tai valtion virastojen alihankintaketjuja. Kyseessä voi olla esimerkiksi alihankkija, alihankkijan alihankkija tai jollekin ketjun osalle IT-palveluita tuottava yritys, jota ei kenties muuten olisi tunnistettu osaksi ketjua tai mahdolliseksi vektoriksi kriittisiin tietoihin.

Kyberpuolustajien on huomioitava muutos toimintatavoissa, koska muutos vaikuttaa merkittävästi siihen, mitkä yritykset tai organisaatiot ovat riskissä joutua APT-ryhmän operaation kohteeksi. Jatkossa jokaisen organisaation tulee huomioida uhka toiminnassaan. Erityisasemassa ovat kriittisten organisaatioiden alihankkijat, jotka todennäköisesti ovat ensimmäisiä skannauksen kohteita tämänkaltaisissa iskukampanjoissa. Uhkaa voi huomattavasti pienentää helpoilla, mutta jonkin verran panostusta vaativilla toimilla. Oman ulkoisen infrastruktuurin hallinta ja aktiivinen haavoittuvuuksien päivittäminen pienentävät merkittävästi riskiä hyökkäyksen kohteeksi joutumiselle. Samaa skannausta, jota nyt myös APT-ryhmät harrastavat voi tehdä itse ja sen avulla voidaan tunnistaa aukot ennen kuin niitä päästään hyödyntämään. Sen lisäksi, että tämän avulla estetään yleisimmät hyökkäystavat (joita myös Sandworm oli käyttänyt), antaa se kuvan mahdolliselle skannaajalle kyberturvaan vakavasti suhtautuvasta ja suojauksesta hyvin huolehtivasta organisaatiosta, jonka järjestelmistä ei todennäköisesti siten muitakaan aukkoja löydy.

Vaikka hyökkäyskampanjassa hyökkäystä ei yleensä ollut jatkettu, jos kohde todettiin “arvottomaksi”, ei tähänkään voi tuudittautua. APT-ryhmien toimintaan on viimeisten vuosien aikana useasti yhdistynyt taloudellinen motiivi ja vaikka strategista arvoa ei kohteella olisikaan, voidaan siltä silti esimerkiksi vaatia lunnaita. Kiinalaisten APT-ryhmien hakkereiden on jopa epäilty toteuttavan tämänkaltaisia ransomwareiskuja ”sivubisneksenä” kohteisiin, joihin on onnistuttu tunkeutumaan, mutta joiden tiedoilla ei ole strategista arvoa valtiolle. Onnistunutta tunkeutumista ei myöskään aina tarvitse hyödyntää itse, vaan se voidaan esimerkiksi myydä, jolloin rahalliseksi hyödyksi muuttaminen on melko vaivatonta. Oli kyse sitten kriittisestä toimijasta, sen alihankkijasta tai täysin tästä ketjusta irrallisesta organisaatiosta, APT-iskujen todennäköisyys vaikuttaa olevan nousemassa ja uhkaan vastaaminen vaatii reagointia.

2.2 Münchenin turvallisuuskonferenssin terveisiä

Helmikuun 14.-16. järjestettiin perinteinen Münchenin kansainvälinen turvallisuuskonferenssi. Konferenssi koostui korkean tason tapaamisista, puheista, paneeleista sekä turvallisuusalan asiantuntijoiden kohtaamisista. Myös kyber- ja teknologiaturvallisuudesta puhuttiin ja keskusteltiin runsaasti, vaikka päähuomion tapahtumassa sai Ukrainan sota, mahdolliset tulevat neuvottelut ja rauhansuunnitelmat. Turvallisuuskonferenssissa on perinteisesti keskitytty strategisen tason kysymyksiin.

Tapahtumassa kuultiin useita puheenvuoroja ja paneelikeskusteluja, jotka joko suoraan tai epäsuoraan käsittelivät kyberturvallisuutta. Erityisesti tekoäly tuntui puhuttavan useissa yhteyksissä. Esimerkiksi tekoälyä suoraan käsittelevässä paneelikeskustelussa "Ai Just Can't Get Enough: Disinformation, Ai, and Democracy" huomiota kiinnitettiin teknologian nopean muutoksen mukanaan tuomista haasteista sekä uusista riskeistä. Paneelissa pohdittiin demokratian hidasta päätöksentekoprosessia ja sitä, kuinka tulisi samaan aikaan kannustaa innovoimaan, mutta myös yhtälailla säätelemään teknologiaa ja sen tuomia riskejä. Erityisesti EU on paininut sen kanssa, mikä on tarpeellista sääntelyä ja mikä taas rajoittaa liiaksi innovointia ja kehitystä. Yhdysvaltojen näkökulma on ollut "Bisnes edellä" -mentaliteetti. Yhtiöiden on annettu innovoida ja luoda talouskasvua ja regulaatiota on pohdittu myöhemmin. Ehkä EU:n tulee harkita tarkemmin omaa lähestymistapaansa. Dilemmana on, kuinka antaa yhtiöiden innovoida tarpeeksi ja kasvaa tarpeeksi ilman, että puututaan tai asetetaan liiaksi vaatimuksia teknologialle ja sen käytölle, samalla kuitenkin estäen uusien teknologioiden laittomat käyttökohteet.

Muissa aihetta sivunneissa paneeleissa, todettiin muun muassa tekoälyn itsessään olevan hyvin antidemokraattinen teknologia. Tekoäly keskittää valtaa tekoälyn haltijoille, sen avulla on helppo harjoittaa massavalvontaa, ja lisäksi se on hyvin manipulatiivinen ja hallusinoiva. Tekoäly sopiikin täydellisesti autoritääristen valtioiden työkalupakkiin. Monissa keskusteluissa puhuttiin tekoälyn reguloinnista ja siitä, kuinka tekoälyllä voidaan saada paljon aikaan, niin hyvässä kuin pahassa. Monet tahot varoittivat sotaa käyvän Venäjän kasvavista tekoälyn hyödyntämisen kyvykkyyksistä, esimerkiksi disinformaation levittämisessä sekä kyberhyökkäyksien toteuttamisessa. Lisäksi tekoälyn yhteyttä kyberrikollisuuteen pohdittiin ja sitä, tuleeko tekoäly massiivisesti lisäämään kyberrikollisuuden toteuttamia iskuja. On jo nähty viitteitä siitä, että tekoälyllä voidaan tuottaa haittaohjelmia ja toteuttaa sen avulla laajoja hyökkäyksiä.

Teknologiakilpailu oli myös esillä. Esimerkiksi "All Bits Are Off: The Risks of Racing for Tech Dominance" -paneelissa keskusteltiin teknologiakilpailusta, nykyisestä tilanteesta sekä ylipäätään tarpeesta käsittää tilanne kilpailuna. Näkökulmina olivat muun muassa lännen, Kiinan ja Venäjän välinen vastakkainasettelu, sekä erilaiset lähestymistavat kilpailun voittamiseksi. Huomiona oli länsimaiden useita vuosikymmeniä jatkunut itsestään selvä asema teknologian edelläkävijänä, joka viimeisten vuosien aikana on ollut muutoksessa. Pohdintaa paneelissa oli siitä, onko voittava strategia vastata kilpailuun sanktioilla ja tiukoilla tulleilla vai keskittymällä tiukasti omaan innovointiin ja teknologiakehitykseen.

Konferenssissa kuultiin puheenvuoroja myös siitä, että seuraava depatti tullaan käymään teknologian pakottamisesta taipumaan demokraattiseen ympäristöön, huomioon ottaen yksityisyyden ja ihmisoikeudet, tai demokraattisen poliittisen järjestelmän ja vapaan maailman on taipumisesta teknologian mukana enemmän kohti autokratiaa. Esimerkkinä mainittiin, että tilanne on jo huonontunut siinä mielessä, että monet yhtiöt harjoittavat sovelluskäyttäjiensä mikroprofilointia, mikä mahdollistaa vaikuttamisen heidän ajatteluunsa. Teknologia ei enää välttämättä palvele yksilöä, vaan yksilöt palvelevat teknologiaa ja näitä teknologioita hallitsevia yhtiöitä. Demokraattisen maailman tulisikin huolehtia siitä, että ihmisillä olisi aidosti mahdollisuus päättää omasta datastaan ja omien tietojensa käytöstä - siitä mihin dataa luovuttaa ja mihin ei, sekä mitä kerätyllä datalla tehdään ja mitä ei. Tekoäly voi lisäksi toimia myös hyödyllisenä lisäsuorituskykynä ja esimerkiksi paneelikeskustelussa tulevaisuuden tiedustelukeinoista se mainittiin mahdollisena työkaluna, jonka avulla pienten valtioiden tiedustelupalvelujen on mahdollista tuottaa arvokasta tietoa ilman suuria resursseja.

Kokonaisuudessaan Munchenin turvallisuuskonferenssissa nousi esille monia tärkeitä kyber- ja teknologiaturvallisuuteen liittyviä asioita sekä toi asiantuntijoita ja päätöksentekijöitä yhteen pohtimaan ajankohtaisia aiheita. Asiasta lisää voi käydä lukemassa ja kuuntelemassa konferenssin verkkosivuilta: https://security-conference.org/en/msc-2025/

2.3 Doge aiheutti turhia kyberriskejä

Yhdysvalloissa presidentti Donald Trumpin nimittämä uusi virasto Doge (Department of Government Efficiency) on aiheuttanut laajaa tyrmistystä muun muassa irtisanomisten ja muiden toimenpiteiden takia. Doge on perustettu presidentin asetuksella, ja sen lainsäädännöllinen asema ja toimivaltuudet ovat sanalla sanoen epäselviä. Poikkeukselliset toimet ovat kyberturvallisuuden näkökulmasta aiheuttaneet merkittäviä ja turhia riskejä. Vaikka toistaiseksi ei voida osoittaa arkaluontoisia tietoja vuotaneen uhkatoimijoiden käsiin, tarjoaa Dogen viime aikaisten toimien tarkastelu hyvän muistutuksen perustason tietoturva- ja kyberturvallisuuskäytäntöjen merkityksestä.

Dogen tarjoama ensimmäinen oppitunti liittyy siihen, kenelle ja millä perusteilla pääsyjä kriittisiin tietojärjestelmiin annetaan. Yhdysvaltain virastojen arkaluontoisiin ja salattuihin asiakirjoihin ja järjestelmiin päässeille dogelaisille ei ilmeisesti oltu tehty taustaselvityksiä, ja pääsyjä tietojärjestelmiin on saatu mm. painostamalla ja lomauttamalla turvallisuushenkilökuntaa. Otsikoissa on ollut myös tapaus, jossa Dogen työntekijä oli vahingossa saanut oikeuden koodiin, joka hallitsi liittovaltion veronpalautusten, sosiaaliturvamaksujen ja muiden maksamista. Dogelaisille annetut laajat pääsyoikeudet rikkovat periaatetta, jonka mukaan pääsy tulisi antaa vain materiaaliin, jonka käsittelyyn on perusteltu ja aito tarve. Tapaus korostaakin identiteetin ja pääsynhallinnan merkitystä oman ja asiakkaiden tiedon turvaamisessa. **Toinen riski** koskee organisaation kyberturvallisuuskoulutuksen ja pelisääntöjen läpikäymistä, ja limittäytyy edelliseen huomioon taustaselvitysten puutteesta. Ei ole tietoa onko henkilöillä koulutusta tai tietotaitoa esimerkiksi kyberturvallisuuden tai tietosuojan perusasioista. Huolettomat toimintatavat ja koulutuksen puute ovat selkeitä riskitekijöitä, jotka jokaisen organisaation tulisi tunnistaa.

Kolmas riski koskee yleistä sekaannusta, jota tapahtumat ovat aiheuttaneet. Dogelaisten toimien valvonta on ilmeisen puutteellista, minkä lisäksi toimia on tehty kiireessä. Kiire, kokonaisuudenhallinnan puute sekä riittämättömät valvontatoimet tarjoavat uhkatoimijoille houkuttelevan ikkunan väärinkäytöksille, kuten tiedon varastamiselle tai järjestelmiin soluttautumiselle, sillä kaaoksen keskellä tietoturvaloukkaukset voivat jäädä huomaamatta. Tavallisissa organisaatiossa tämä voi näkyä kriisitilanteissa, organisaatiorakenteen muutoksissa tai muissa tilanteissa, joissa vaaditaan äkillistä reagointia. Muutoksia tulisi kuitenkin välttää tekemästä turvallisuuden kustannuksella.

Organisaatiosta riippumatta Dogen aiheuttama kaaos tarjoaa hyvän oppitunnin kyberturvallisuuden perusasioista. Identiteetin- ja pääsynhallinta, henkilöstön koulutus ja kokonaisuudenhallinta muodostavat pohjan kokonaisvaltaisen kyberturvallisuuden rakentamiselle.

3 SEURAA NÄITÄ

3.1 Ovatko avoimen lähdekoodin projektit kriisissä?

Avoimen lähdekoodin projektit ovat keskeisiä internetin infrastruktuurin ja nykyaikaisten verkkopalveluiden osia. Avoimen lähdekoodin projekteja on olemassa valtava määrä, ja ne kattavat suuren osan internetin tärkeistä osa-alueista. Monet avoimen koodin projektit toimivat pohjina käyttöjärjestelmien eri toiminallisuuksissa ja niitä lainataan paljon myös sovelluskehityksessä. Esimerkiksi viime vuonna esiin noussut XZ utils-projektin aukko olisi jakeluun päätyessään vaikuttanut käytännössä kaikkiin Linux-käyttöjärjestelmän laitteisiin, eli miljooniin tietokoneisiin ja palvelimiin ympäri maailman.

Jo pitkään eri avointen lähdekoodien projektit ovat kohdanneet haasteita ja ongelmia. Usein projektit ovat rahoitukseltaan ja resursoinneiltaan hyvin pieniä, ja perustuvat lähes yksinomaan vapaaehtoisten palkattomaan työpanokseen, mikä vaikeuttaa projektien kehitystä ja ylläpitoa. Tästä asetelmasta juontuvat useat muut avointen lähdekoodien projektien ongelmat. Kehittäjien motivaatio ja sitoutuminen on usein koetuksella, kun oman leipätyön ohella pyrkimyksenä on ylläpitää ja kehittää projekteja, joissa ei ole rahoitusta tai joissa ei välttämättä ole mukana muita tekijöitä tai vain muutama muu apukäsi. Projektien ylläpito ja esimerkiksi tuotteen turvallisuudesta vastaaminen olemattomilla resursseilla voi olla haasteellista. Viitteitä siitä, että näiden projektien sekaan on pyritty ujuttumaan ulkopuolisen hyökkäyksen mahdollistavaa sisältöä, on viime vuosien aikana saatu kasvavia määriä, ja aiheellisesti huolta herättää vapaaehtoisten kehittäjien kyvyt ja resurssit suojata projektit näiltä pyrkimyksiltä. Projektin alkuperäiset kehittäjät saattavat myös menettää kiinnostuksen ja siirtyä uusiin haasteisiin, jolloin vaarana on, että projektien ylläpito lakkaa täysin.

Avointen lähdekoodien projektit ovat yhteisöllistä toimintaa. Alan asiantuntijat ja kiinnostuneet koodarit sekä tuotteiden loppukäyttäjät usein yhdessä ylläpitävät, kehittävät, kommentoivat ja käyttävät avoimen lähdekoodin sovellutuksia ja projekteja. Tämä luo myös haasteita. Yhteisön sisälle saattaa muodos-

»

»

tua erilaisia ristiriitoja tai konflikteja, jotka vaikeuttavat projektin kehitystyötä ja ylläpitoa. Tästä saatiin esimerkki helmikuun alkupuolella, kun Rust for Linux (R4L) projektin avainhenkilöiden välille syntyi erimielisyyksiä ja suoranaista riitaa. Seurauksena osa kehittäjistä päätyi jättämään projektin.

Tulevaisuuden uhkana avoimien lähdekoodien projekteille on ikääntyvä kehittäjäyhteisö. Nuorempi sukupolvi ei entiseen malliin sitoudu yhteisen hyvän ylläpitoon ilman selkeää ja motivoivaa palkkiota työstä. Tähän on esitetty erilaisia resursointiratkaisuita, joissa projektien sovellutuksia hyödyntävät tahot lähtisivät sponsoroimaan aktiivisesti näitä kehitys- ja ylläpitotöitä, jolloin kehittäjille voitaisiin maksaa palkkiota. Tilastojen mukaan yli 60 % avoimen lähdekoodin kehittäjistä ei nykyisellään saa työstään palkkaa vaan tekee työtä harrastuneisuuden ja yhteisen hyvän innoittamana oman työnsä ohessa.

Monet organisaatiot hyödyntävät IT-järjestelmissään avoimen lähdekoodin projekteja, kuten Linux -käyttöjärjestelmää tai erilaisia verkkopalvelimia sekä relaatiotietokantojen hallintajärjestelmiä. Mikäli avointen lähdekoodien projektien kehittäjämäärät jatkavat vähenemistään, luo se monenlaisia turvallisuusriskejä ylläpidon ja kehittämisen ongelmien kautta. Organisaatiot voivat myös itse olla aktiivisia ja tarjoutua sponsoroimaan hyödyntämiään projekteja sekä luomaan aktiivista keskustelua sekä positiivista yhteisöllisyyttä avoimen lähdekoodin kehitystyön ympärille.

3.2 Puola luottaa Googleen, julkisen ja yksityisen sektorin kyberyhteistyö tarjoaa mahdollisuuksia

Puola ja Google allekirjoittivat helmikuussa uuden muistion (memorandum) digitaalisesta yhteistyöstä ja investoinneista. Taustalla vaikuttaa pitkäaikainen yhteistyö, jonka yhtenä alkuna voidaan pitää vuotta 2014, jolloin Google perusti oman start up –kampuksensa maahan. Vuosien varrella yhteistyö on kehittynyt ja esimerkiksi vuonna 2022 Google ilmoitti investoivansa 700 miljoonaa dollaria Puolaan. Tuoreen yhteistyön tavoitteena ovat miljardi-investoinnit. Googlen omien arvioiden mukaan investoinnit voivat nostaa Puolan bruttokansantuotetta jopa kahdeksalla prosentilla. Tavoitteena mainitaan tekoälyratkaisujen käyttöönotto puolalaisissa yrityksissä ja organisaatioissa, erityisesti energia-alalla ja kyberturvallisuudessa. Muistio pitää sisällään myös kohdan Googlen osallistumisesta puolalaisten digitaalisten taitojen kehittämiseen.

Yhteistyön taustalla vaikuttavat molempia osapuolia hyödyttävät tavoitteet ja aiemmat positiiviset kokemukset. Googlen kanssa tehtävä yhteistyö on Puolalle taloudellisesti merkittävää ja on historiallisesti tukenut IT-alan, mukaan lukien kyberturvallisuuden, kehityksessä ja ekosysteemin muodostumisessa. Tuore muistio lupaa tukea kyberturvallisuuteen ja energiasektorille, mikä on strategisesti merkittävää Puolan ollessa yksi suosituimmista venäläisten hakkereiden kohteista. Google on samalla yksi merkittävimmistä yrityksistä tietoturvan ja tekoälyn saralla. Puolalle voi olla hyötyä tästä osaamisesta ja yhteistyöstä.

Puolassa on panostettu erityisesti työvoiman saatavuuteen ja maa mielellään markkinoi itseään Itä-Euroopan digialan osaamisen ja koulutuksen keskuksena. Tällä hetkellä Puolassa arvioidaan olevan 400 000 IT-alan työntekijää. Kansallisessa digistrategiassa vuosille 2025–2035 tavoitteeksi on otettu muun muassa uuden supertietokoneen rakentaminen, “tekoälytehtaan” rakentaminen sekä investointien ohjaaminen kyberturvallisuuteen ja tekoälyyn. Näin on muodostunut IT-alan yrityksille, kuten Googlelle suotuisa toimintaympäristö. Googlelle houkuttimena toimii myös suhteessa edullisemmat työvoimakustannukset sekä toimintaympäristö, joka mahdollistaa uusien oppien ammentamisen esimerkiksi venäläisistä kyberhyökkäyksistä.

Vaikka julkisen ja yksityisen sektorin yhteistyö on parhaimmillaan molemmille osapuolille hedelmällistä, ja Suomenkin kokonaisturvallisuuden mallissa alan yritysten ja viranomaisten välistä yhteistyötä korostetaan, ei yhteistyö ole täysin riskitön. Kansallisen turvallisuuden kannalta voi olla haitallista, mikäli kyberpuolustuksessa keskeisesti aletaan nojaamaan liikaa ulkomaalaisiin voittoa tavoitteleviin yrityksiin. Toisaalta tilanne on jo pitkään ollut se, että kyberturvallisuuden merkittävin osaaminen on yksityisellä puolella. Kyseessä on hankala dilemma - miten yhteistyö saadaan pysymään tasapainossa ja kansallisen turvallisuuden osalta kestävällä tolalla. Yhteistyö internetin suuryritysten kanssa takaa todennäköisesti pääsyn tuoreimpaan teknologiaan ja moderneimpiin toimintatapoihin. Samanaikaisesti olisi tärkeä panostaa omaan kansalliseen suorituskykyyn säilyttämällä kyvykkyyksiä viranomaispuolella sekä esimerkiksi kansallisiin startupeihin sekä koulutukseen panostamalla.

LÄHTEET:

Tapahtumia kybermaisemassa

Cyberwatchin viikkokatsaukset helmikuu 2025

https://www.bbc.com/news/articles/cm292319gr2o

https://www.theguardian.com/technology/2025/feb/18/elon-musk-grok-3-ai-chatbot

https://commission.europa.eu/news/eu-reaffirms-unwavering-support-ukraine-anniversary-invasion-2025-02-24_en

Venäläisen APT-ryhmän kohdevalikoima muuttunut

https://thehackernews.com/2025/02/microsoft-uncovers-sandworm-subgroups.html

https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-emperor-dragonfly-ransomware-attack

Munchenin turvallisuuskonferenssin terveisiä

https://securityconference.org/en/msc-2025/

https://therecord.media/munich-cyber-security-and-security-conference-2025

Doge aiheuttaa turhia kyberriskejä

https://therecord.media/treasury-fully-aware-of-risks-posed-by-doge-access-to-database https://www.washingtonpost.com/business/2025/02/25/elon-musk-doge-data-privacy-security/

https://www.hs.fi/maailma/art-2000011017558.html

Ovatko avoimen lähdekoodin projektit kriisissä?

https://www.theregister.com/2025/02/16/open_source_maintainers_state_of_open/?td=rt-3a

https://explore.tidelift.com/2024-tidelift-survey/2024-tidelift-state-of-the-open-source-maintainer-report

https://www.theregister.com/2025/02/13/ashai_linux_head_quits/

https://www.theregister.com/2025/02/07/linus_torvalds_rust_driver/

https://lkml.org/lkml/2025/2/6/1292

https://www.linuxfoundation.org/blog/open-source-maintainers-what-they-need-and-how-to-support-them

https://www.techzine.eu/news/security/118829/vigilance-required-to-counter-infiltration-attempts-of-open-source-projects/

Puola luottaa Googleen, julkisen ja yksityisen sektorin kyberyhteistyö tarjoaa mahdollisuuksia

https://www.gov.pl/web/primeminister/google-invests-billions-in-polands-digital-future

https://blog.google/around-the-globe/google-europe/increasing-googles-investment-in-poland/

https://www.securityweek.com/google-hub-in-poland-to-develop-ai-use-in-energy-and-cybersecurity-sectors/

UHKATIEDUSTELUSEURANTA

Cyberwatch Finland julkaisee uhkatiedusteluseurannan, johon on koottu viimeisen kuukauden ajalta merkittävimpiä kyberhyökkäyksiä sekä tietoa aktiivisimmista ja nousevista uhkatoimijoista ympäri maailmaa. Cyberwatchin analyytikot seuraavat paitsi pintaverkossa, myös syvässä ja pimeässä verkossa tapahtuvaa toimintaa. Lähteenä on lisäksi kansainvälisten tietoturvatoimijoiden julkaisuja sekä laaja suomalaisen ja kansainvälisen mediakentän seuranta.

Merkittävimpiä kyberiskuja ja -kampanjoita

SIGNAL KALASTELUKAMPANJAN KOHTEENA

AJANKOHTA: Operaatio havaittiin helmikuun puolessa välissä 2025
KUVAUS: Venäjän hallintoon kytköksissä olevat hakkerit ovat hyödyntäneet Signal-viestintäsovelluksen "Linked devices" -ominaisuutta kalastelu-hyökkäyksissä muun muassa Ukrainan asevoimien edustajiin. Kalastelun kohteena oleville lähetettiin saastutettuja QR-koodilinkkejä naamioituna ryhmäkutsuiksi. Lisäksi Venäjän sotilastiedustelupalvelu GRU:n Sandworm-ryhmän (APT44) on todettu hyödyntäneen samaista "Linked devices" -ominaisuutta taistelukentältä takavarikoitujen puhelinten Signal-tilien haltuun ottamiseksi.
TEKIJÄ: UNC5792 & UNC4221 & APT44
MOTIIVI: Sota
VAIKUTUKSET: Signal paikkasi uudessa sovelluspäivityksessään havaitut ongelmat, ja toistaiseksi niiden on todettu estäneen kyseisen hyökkäystekniikan jatkokäytön. Tapaus korostaa viestintäsovellusten haavoittuvuutta.

TANSKAN KIINTEISTÖOMISTAJIEN TIETOJEN VUOTO

AJANKOHTA: Helmikuu 2025
KUVAUS: Tanskan kiinteistöomistajien tietokanta vuodettiin verkkoon. Tietokanta sisälsi 3,5 miljoonan ihmisen tietoja, mm. nimiä, osoitteita, syntymäaikoja sekä organisaatiotietoja.
TEKIJÄ: Tuntematon
MOTIIVI: Tuntematon
VAIKUTUKSET: 3,5 miljoonan ihmisen tietoja päätyi verkkoon. Näitä tietoja voidaan hyödyntää tulevissa rikollisissa toimissa, kuten identiteettivarkauden tukena. Tapaus on esimerkki, kuinka paljon tietoja ja kuinka suuri vaikuttavuus voi olla yhteen tietokantaan tehdyssä tietomurrossa.

KRYPTOVÄLITTÄJÄ BYBIT HYÖKKÄYKSEN KOHTEENA

AJANKOHTA: 21.2.2025
KUVAUS: Kryptovaluuttavälittäjä ByBit koki kyberhyökkäyksen, jonka tekijäksi epäillään pohjoiskorealaisia hakkereita. Hyökkäys kohdistui yhtiön sisäiseen siirtoprosessiin, jossa siirrettiin Ethereumia Offline-varastosta Online-käyttövarastoon. Varastetut kryptovaluutat siirrettiin aluksi kryptolompakoihin, jotka tunnistettiin Lazarus-ryhmän aiemmin käyttämiksi lompakoiksi. Hyökkääjä oli julkaissut tämän jälkeen omia kryptokolikoitaan, joiden kautta se pesi varastettuja kryptovaluuttoja. Hyökkääjä oli lisäksi siirtänyt osan kryptoista erilaisiin crypto-mixereihin, jotka sekoittavat kryptovaluutat muiden palvelua käyttävien valuuttojen kanssa. Tällöin niiden seuraaminen ja jäljittäminen on lähes mahdotonta.
TEKIJÄ: Lazarus (Pohjois-Korean APT38)
MOTIIVI: Taloudellinen
VAIKUTUKSET: ByBit menetti hyökkäyksessä noin 1,5 miljardin USD arvosta Ethereum-kryptovaluuttaa. Toistaiseksi ei ole tiedossa, saadaanko mitään palautettua yhtiön haltuun. ByBit yhtiö tekee todennäköisesti iskun seurauksena valtavia tappioita, mutta vakuuttaa kaikkien asiakkaidensa varojen olevan edelleen turvassa ja kantavansa itse vastuun tapahtuneesta. Tapaus on esimerkki Pohjois-Korean harjoittamasta rikollisesta toiminnasta taloutensa sekä ydinohjelmansa rahoittamiseksi.

Aktiivisimpia sekä nousevia uhkatoimijoita

CLOP

KUVAUS: Ensikertaa vuonna 2019 havaittu venäjää puhuva Ransomware-as-a-Service (RaaS) -toimija. Kohdistaa hyökkäyksensä pääosin terveyden, finanssialan, median, teollisuuden sekä koulutuksen sektoreille. Hyökkäysten kohteena länsimaat, etenkin Yhdysvallat.
VIIME AIKOJEN TOIMINTA: Ryhmä on ollut alkaneen vuoden 2025 ylivoimaisesti aktiivisin lunnashaittaohjelmatoimija. Ryhmän tuotteilla on tehty alkuvuoden aikana yli tuhat lunnashaittaohjelmahyökkäystä, luvun kasvaessa päivittäin.
TOIMINTATAVAT JA TAKTIIKAT: Clop hyödyntää toiminnassaan erityisesti kohdennettua tietojenkalastelua sekä haavoittuvuuksia sovelluksissa ja erilaisissa järjestelmissä. Sen hyökkäysten on todettu keskeytyneen sen jälkeen, kun uhrin on todettu puhuvan venäjää tai muuta entisen Neuvostoliiton alueen kieltä. Clop toteuttaa hyökkäyksensä nelinkertaista kiristysmenetelmää. Se varastaa ja salaa uhrin tietokannat. Se uhkaa uhria DDoS -hyökkäyksillä, mikäli lunnaita ei makseta ja lisäksi ottaa yhteyttä uhrin asiakkaisiin ja työntekijöihin uhaten julkaista heidän yksityisiä tietojaan, ellei lunnaita makseta.

LUMMA STEALER

KUVAUS: Ainakin vuodesta 2022 aktiivisena ollut Malware-as-a-Service (MaaS) -toimija venäjänkielisillä foorumeilla. Haittaohjelman kehittäjänä uskotaan olevan "Shamel" -uhkatoimija, joka myy haittaohjelmaa Telegramissa, sekä pimeän verkon myyntialustoilla.
VIIME AIKOJEN TOIMINTA: Lumma julkaisee viikoittain keräämiään lokitietoja (Lumma Malware Logs), jotka pitävät sisällään esimerkiksi kirjautumistietoja, evästeitä sekä kryptolompakkotietoja. Ensisijaisesti se käy näillä tiedoilla kauppaa pimeän verkon eri alustoilla, mutta julkaisee osan tiedoista myös ilmaiseksi. Lopulta nämä julkaistut tiedot päätyvät useille muille pimeän verkon koontilistoille, jotka jäävät kiertämään osana isompia "Credential Stuffing" -yhdistelmälistoja. Näitä listoja voivat hyödyntää lukemattomat eri kyberuhkatoimijat erilaisissa rikollisissa toimissaan.
TOIMINTATAVAT JA TAKTIIKAT: Viime aikoina Lumma on hyödyntänyt erityisesti väärennettyjä CAPTCHA-vahvistussivuja, joilla käyttäjä huijataan suorittamaan haitallisia PowerShell-komentoja. Erilaisten piraattisovellusten on todettu myös sisältäneen Lumma-haittaohjelman. Näitä sovelluksia on mainostettu muun muassa Telegramissa sekä Youtuben videoilla.

STORM-2139

KUVAUS: Microsoft tunnisti ja nimesi helmikuussa kansainvälisen kyberrikollisryhmän Storm-2139:n jäseniä. Mukana rikollisryhmän toiminnassa havaittiin olevan muun muassa Iranin, Iso-Britannian, Kiinan sekä Vietnamin kansalaisia.
VIIME AIKOJEN TOIMINTA: Storm-2139 on aktiivisesti pyrkinyt rikkomaan eri palveluntarjoajien tekoälysovellusten sääntöjä luomalla omia teknisiä työkaluja, joilla sääntöjä on pystytty kiertämään. Tarkoituksena on ollut tekoälyn väärinkäyttö ja hyödyntäminen kyberrikollisuudessa, muun muassa syvävääreennöksissä. Ryhmän toiminta osoittaa uusien teknologioiden soveltuvuuden kyberrikollisuuteen sekä sen kansainvälisen ja rajat ylittävän luonteen.
TOIMINTATAVAT JA TAKTIIKAT: Storm-2139 jakautuu kolmeen tasoon: Kehittäjiin, toimittajiin sekä käyttäjiin. Kehittäjät kehittävät työkaluja, joilla pystyvät väärinkäyttämään erilaisia tekoälysovelluksia. Toimittajat muokkaavat kehittäjien työkaluista tiettyihin tekoälysovelluksiin soveltuvia työkaluja, joita käyttäjät sitten hyödyntävät laittomiin kyberrikollisiin toimiin. Usein lopputuotteina on esimerkiksi seksuaalista materiaalia julkisuuden henkilöistä.

Cyberwatch Finland

Missiomme:

KYBERTURVALLISUUDESTA BISNESMAHDOLLISUUS

**Cyberwatch Finland palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä niiden kyberturvallisuuskulttuuria.
Tiukentuva sääntely parantaa kaikkien kyberturvallisuutta, mutta vähimmäisvaatimusten noudattaminen ei riitä yhä kiristyvässä kilpailussa. Korkeatasoinen kyberturvallisuuskulttuuri on kilpailuetu ja luo uusia liiketoimintamahdollisuuksia.**

Laaja-alainen osaaminen, kokemus ja näiden uniikki yhdistelmä on vahvuutemme

Asiantuntijatiimimme koostuu strategisen kyberturvallisuuden monipuolisesta osaamisesta, jota täydentää laaja-alainen kokemus johtamisesta, kokonaisturvallisuudesta ja toiminnasta kansainvälisessä yritysympäristössä. Asiantuntijoillamme on kyky tulkita ja esittää monimutkaisia kybermaailman ilmiöitä ja kehityskulkuja helposti ymmärrettävässä muodossa. Käytämme työssämme hyväksi kehittyneitä teknisiä alustoja ja analytiikkatyökaluja.

Autamme asiakasta pysymään ajan tasalla ja kehittämään kyberturvallisuuskulttuuria johdonmukaisesti. Samalla rakennamme yhdessä kestävämpää ja turvallisempaa maailmaa.

Aapo Cederberg, Cyberwatch Finlandin toimitusjohtaja ja perustaja

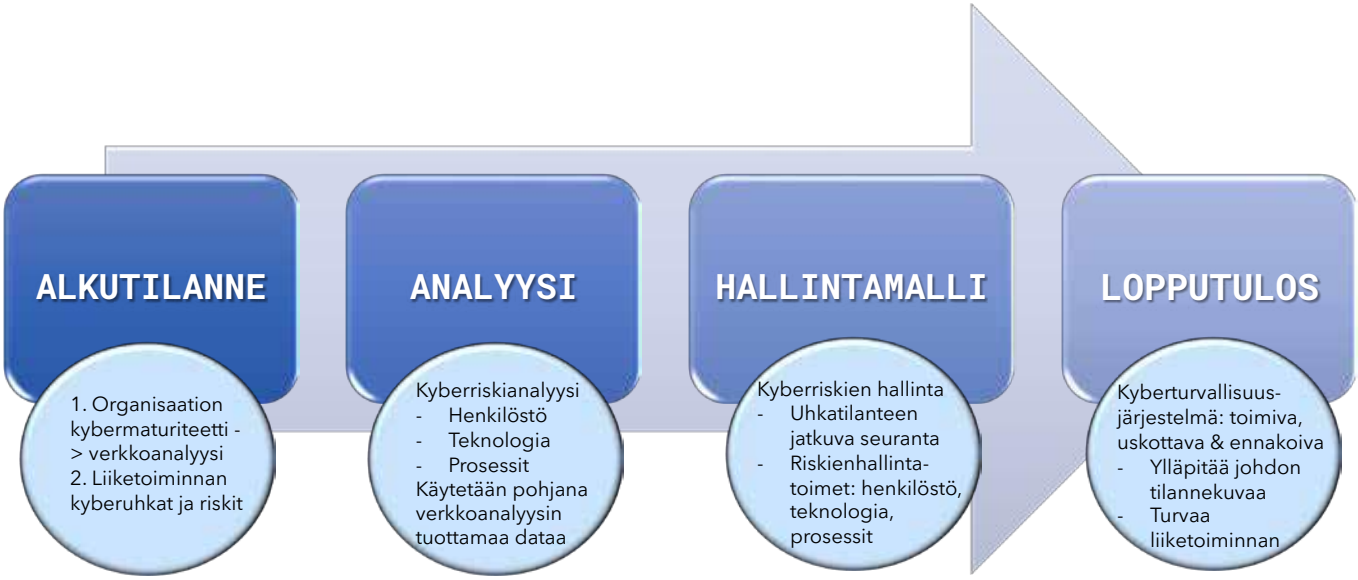
Cyberwatch Finland on strategisen kyberturvallisuuden asiantuntijatalo, joka palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä valmiuksia suojata ja puolustaa niiden merkittävimpiä toimintoja.

Kyberriskienhallintamalli

Kyberturvallisuus tulee yhä enemmän ottaa huomioon ennakoiden liiketoimintasuunnitelman eri vaiheissa. Kokonaisvaltaisessa kyberturvallisuuden riskienhallintasuunnitelmassa laaditaan selkeä tiekartta siitä, miten kyberturvallisuusuhkat huomioidaan entistä paremmin ja miten lisääntyvä EU-regulaatio sekä kansallisen lainsäädännön edellyttämät toimet käytännössä toteutetaan.
Suunnitelma kattaa kyberturvallisuuden neljä osatekijää, johtamisen, tekniset ratkaisut, henkilöstön osaamisen ja toimintaprosessit.

Kyberriskien hallintamallin prosessi koostuu neljästä vaiheesta:

1. Lähtötilanteen määrittelystä
2. Kyberriskianalyysista
3. Kyberriskien hallintamallista
4. Lopputuloksena toimivasta ja ennakoivasta kyberturvallisuusjärjestelmästä



Cyber Due Diligence

Cyberwatchin kyberturvallisuuden due diligence on prosessi, joka auttaa organisaatiotasi tunnistamaan ja arvioimaan kyberturvallisuuteen liittyviä riskejä, jotka voivat vaikuttaa esimerkiksi kaupalliseen sopimukseen, investointiin, rahoitusjärjestelyyn tai yrityskaupan ehtoihin. Cyber Due Diligence toimii myös sopimuspuolien kilpailutilanteissa välttämättömänä työkaluna.

Cyber Due Diligence- projektiin kuuluu yksityiskohtainen verkkoanalyysi ja auditointiprosessi, joka sisältää muun muassa:

- ✔ Kyberturvan ja tietoturvan nykytilan arvioinnin
- ✔ Kolmansien osapuolien kyberturvallisuuden tason tarkastelun
- ✔ Tietoturvaloukkausten ja mahdollisten kyberhyökkäysten historian tarkastelun
- ✔ Kyberturvallisuuskulttuurin tarkastelun
- ✔ Kyberhygienian tason arvioinnin ja kyberturvakoulutuksen järjestelyt
- ✔ Kyberturvallisuuden sääntelyyn ja vaatimuksiin vastaaminen
- ✔ Kyberturvan ja tietoturvariskien hallinnan
- ✔ Kyberturvallisuuskulttuurin integrointi yrityskaupan jälkeen (NIS2 yhteensopivuus sekä sisäisten politiikkojen yhteensopivuus)

Tilannekuvapalvelu

Cyberwatch seuraa jatkuvasti kyberturvallisuuden toimintaympäristöä keräämällä ja analysoimalla tietoa kybermaailman tapahtumista, ilmiöistä ja muutoksista. Tilannekuvaa tuotetaan ja ylläpidetään säännöllisesti ilmestyvillä tilannekatsauksilla.

VIIKKOKATSAUS

Viikkokatsauksessa esitellään kybertoimintaympäristön ajankohtaisia tapahtumia. Keskeistä viikkokatsauksessa on kyberilmiöiden ja trendien tunnistaminen ja niiden asettaminen asianmukaiseen viitekehykseen. Viikkokatsaukset toimivat pohjana kuukausikatsauksille sekä vuosiennusteille. Viikkokatsausten avulla saat ajantasaista kuvaa merkittävistä kybermaailman tapahtumista päätöksenteon tueksi. Viikkokatsaus ilmestyy 52 kertaa vuodessa suomeksi sekä englanniksi.

KUUKAUSIKATSAUS

Kuukausikatsauksessa tarkastellaan edellisen kuukauden merkittävimpiä kybermaailman tapahtumia, ilmiöitä, trendejä ja niiden keskinäisriippuvuuksia sitoen ne laajempaan kokonaisuuteen. Katsaus jakautuu kolmeen tarkastelukulmaan, joita ovat kuukauden merkittävimmät kybermaailman tapahtumat, erityisesti korostettavat ilmiöt sekä kokonaisuudet, joiden kehitystä on syytä seurata. Kuukausikatsauksen avulla saat syvempää ymmärrystä siitä, miten kybermaailman tapahtumat vaikuttavat yhteiskuntaan ja toimintaympäristöösi. Kuukausikatsaus ilmestyy 12 kertaa vuodessa suomeksi sekä englanniksi.

CYBERWATCH MAGAZINE

Cyberwatch magazine on digitaalinen ja painettu aikakauslehtemme, jossa sekä omat että verkostomme huippuasiantuntijat kirjoittavat kybermaailman ajankohtaisista tapahtumista, teknologian kehityksestä, lainsäädännön muutoksista sekä näiden vaikutuksista yhteiskuntaan, organisaatioihin ja yksittäisiin ihmisiin.

TEEMA- JA ERIKOISRAPORTIT

Tuotamme määrittelemästäsi teemasta, toimialasta tai kohdemarkkinasta erikoisraportteja ja katsauksia, kuten esimerkiksi uhkaraportteja, tulevaisuuskatsauksia ja -ennusteita, maa-analyyseja, toimintaympäristöanalyyseja tai muita erikoistajulkaisuja.

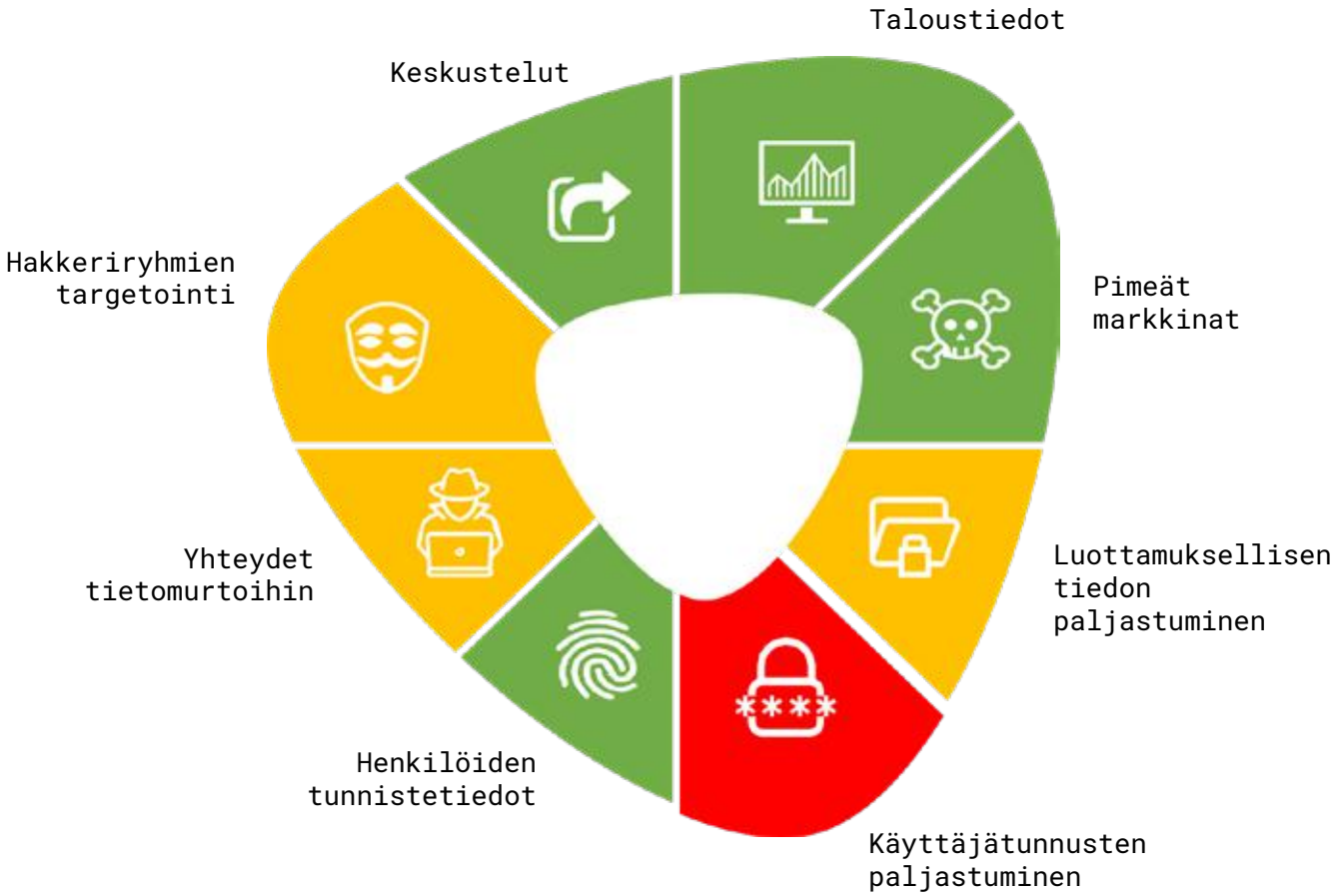
Verkkoanalyysi - darkSOC®

LÄHTÖTILANNEKARTOITUS

Verkkoanalyysin lähtötilannekartoituksen avulla selvitämme organisaatiosi profiilin ja altistumisen tason pimeässä ja syvässä verkossa. Analyysi paljastaa organisaatiosi kyberturvallisuuden puutteita, vuotaneita tietoja sekä muita mahdollisia ongelmakohtia. Verkkoanalyysi sisältää haavoittuvuuspinta-alan kartoituksen, jossa analysoidaan kohteen verkkoinfrastruktuurin rakennetta ja verkon kyberturvallisuuden tilaa.

Työkaluina käytämme sekä Cyber Intelligence Housen tietokantaa, että Badrap Oy:n palveluita. Dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa. Analyysin avulla saat näkemyksen siitä, miltä organisaatiosi näyttää kyberrikollisen silmin katsottuna.

Luokittelemme kyberaltistumiset kahdeksaan havaintokategoriaan ja jaamme havainnot vakavuuden perusteella kolmeen tasoon. Haavoittuvuuspinta-alan kartoituksessa muodostamme ulkopuolisen näkemyksen kyberturvallisuuden tasostanne. Keskeisimmät havainnot raportoidaan johdon yhteenvetoraportissa päätöksenteon tueksi. Raportti sisältää myös havaintojen yksityiskohtaisemman esittelyn sekä suositukset korjaavista toimista ja strategisen tason kehityskohteista.



MONITOROINTI

Lähtötilannekartoituksen pohjalta voidaan sopia syvän ja pimeän verkon monitoroinnista toimenpiteiden vaikuttavuuden selvittämiseksi ja uusien uhkien havaitsemiseksi. Monitoroinnissa havaittuja uusia löydöksiä tarkastellaan suhteessa aiempiin havaintoihin ja analysoidaan syitä havaintomäärien muutoksiin. Monitoroinnin tulokset raportoidaan sovituin väliajoin.

Säännöllinen monitorointi:
sovituin aikavälein toimitettava raportti, esimerkiksi kuukausittain, kvartaaleittain, puolivuosittain tai vuosittain.

Jatkuva monitorointi:
24/7 seuranta uusista havainnoista, joista tieto suoraan asiakkaalle sekä kuukausittainen raportointi.

VERKKOANALYYSI TOIMITUSKETJUILLE

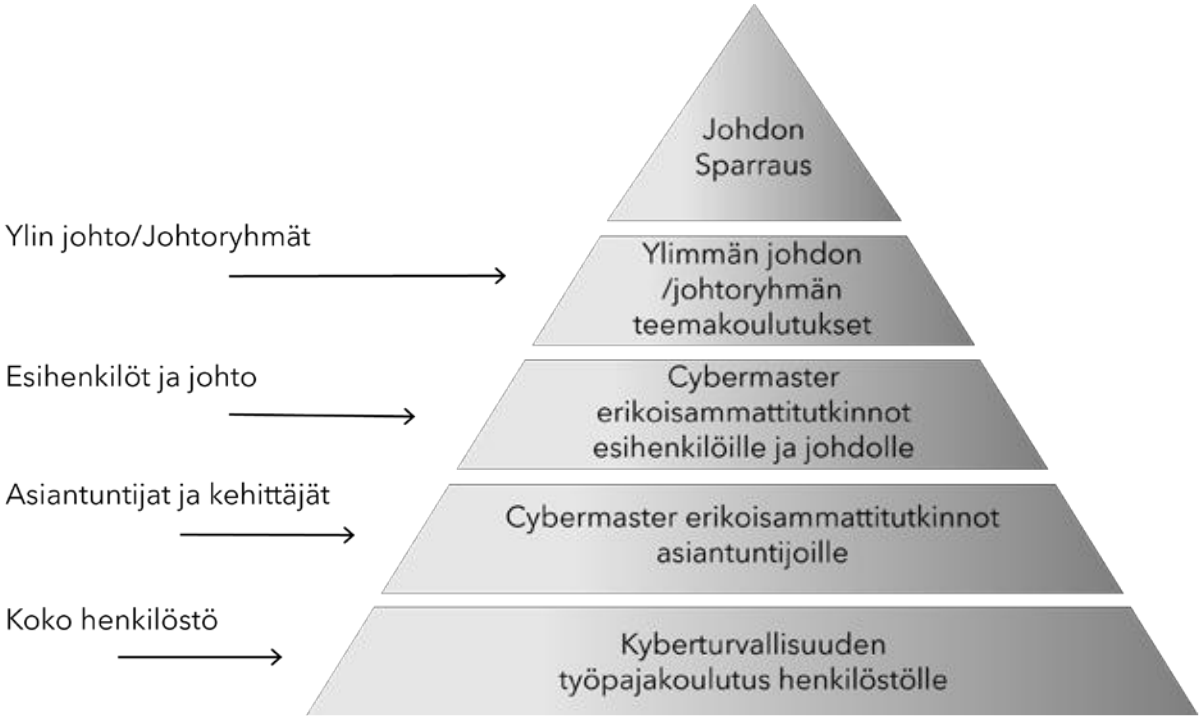
Analyysi voidaan tehdä valituille toimitusketjun organisaatioille (edellyttäen sopimusta). Havainnot jalkautetaan toimitusketjun organisaatioille, jotka vastaavat korjaavien toimenpiteiden suorittamisesta sekä raportoi tilaajalle, kun korjaavat toimenpiteet on tehty. Toimitusketjun kyberturvallisuuskäytäntöjen tarkastaminen lisää asiakasorganisaation omaa kyberkypsyyttä ja auttaa yritystä vastaamaan paremmin kyberturvallisuuslain vähimmäisvaatimuksiin. Mahdollistaa asiakkaalle esimerkiksi yritysostotilanteessa potentiaalisten yhteistyötahojen kybermaturiteettien selvittämisen ja riskiarvion tekemisen.

Powered by:

Koulutus ja osaamisen kehittäminen

MIF-KOULUTUSOHJELMAT

Tuotamme yhdessä Management Institute of Finlandin (MIF) kanssa Cyber Master erikoisammattitutkintokoulutusta. Tällä hetkellä koulutusohjelmissa voi suorittaa Cyber Master Basics sekä Cyber Master Extended -koulutuskokonaisuudet. Koulutusten tarkoituksena on syventää ymmärrystä kyberturvallisuuden uhista ja tarjota käytännön työkaluja suojaamaan organisaation toimintaa.



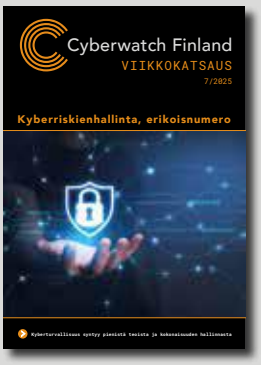
CYBERWATCH -KOULUTUSMODUULIT JA LUENNOT

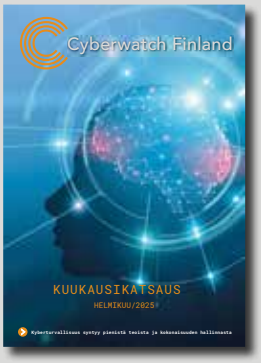
Toteutamme organisaatiollesi myös räätälöityjä koulutuskokonaisuuksia sekä luentoja, joiden avulla vahvistat kyberturvallisuuden osaamista ja valmistaudut kohtaamaan digitaalisen toimintaympäristömme muuttuvia haasteita.
Koulutustarjontamme koostuu moduulikokonaisuuksista sekä yksittäisistä luennoista, joista voit valita organisaatiollesi sen tilanteeseen tai toimintaan parhaiten soveltuvat osat. Koulutukset on mahdollista toteuttaa koulutuspäivinä, hybridikoulutuksina tai verkkokursseina. Koulutusten ja luentojen lisäksi voit tilata myös yritykselleesi skenaariotyöskentelyn, jonka avulla voit kerätä ja jäsentää tietoa, joka mahdollisimman kattavasti auttaa ymmärtämään tulevaa.

JOHDON NEUVONTAPALVELUT

Olemme kokenut ja luotettu neuvonantaja ja kyberturvallisuuden asiantuntija. Kyberkonsultoinnissa keskeistä on tuoda esille, mitä organisaation johdon tulee tietää kybermaailmasta, sen ajankohtaisista riskeistä ja niiden vaikutuksista.
Tuemme uhkien torjunnassa, kyberriskien hallinnassa ja toiminnan jatkuvuuden turvaamisessa. Autamme kehittämään kokonaisturvallisuuden, kyberturvallisuuden, sisäisen turvallisuuden asiakokonaisuuksia sekä kumppaniriskien hallintaa. Työskentelymetodeinamme ovat muun muassa teema-alustukset, muistiot, työpajat sekä skenaariotyöskentely.

JjulkaisujamME 2025





Ota yhteyttä

Cyberwatch Oy | Nuijamiestentie 5 C | 00400 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi

MESSUKESKUS
The real social media

FOR A BETTER DIGITAL FUTURE

Registration opens May 21st!

Politics, economy, reality and the future of cybersecurity.

Technology, digitalisation, and AI are transforming the global landscape at an unprecedented pace. While this shift creates vast opportunities, it also introduces new vulnerabilities affecting businesses and public administration. Cyber Security Nordic explores the critical role of cybersecurity, providing insights from both corporate and governmental perspectives. Connect with the entire Nordic cyber industry, discover the latest solutions, and experience the first-class programme.

SAFETY & COMPETITIVENESS | EUROPEAN SECURITY | TRUSTED DIGITALISATION & INFORMATION SECURITY | DEMOCRACY & DIGITAL POLICIES

CYBER SECURITY NORDIC

4–5 November 2025
Helsinki Expo and Convention Centre

cybersecuritynordic.com