Strategisen kyberturvallisuuden erikoisjulkaisu

Cyberwatch Finland

MAGAZINE 3/2023

ÄLYKÄSTÄ KYBER-TURVALLISUUTTA

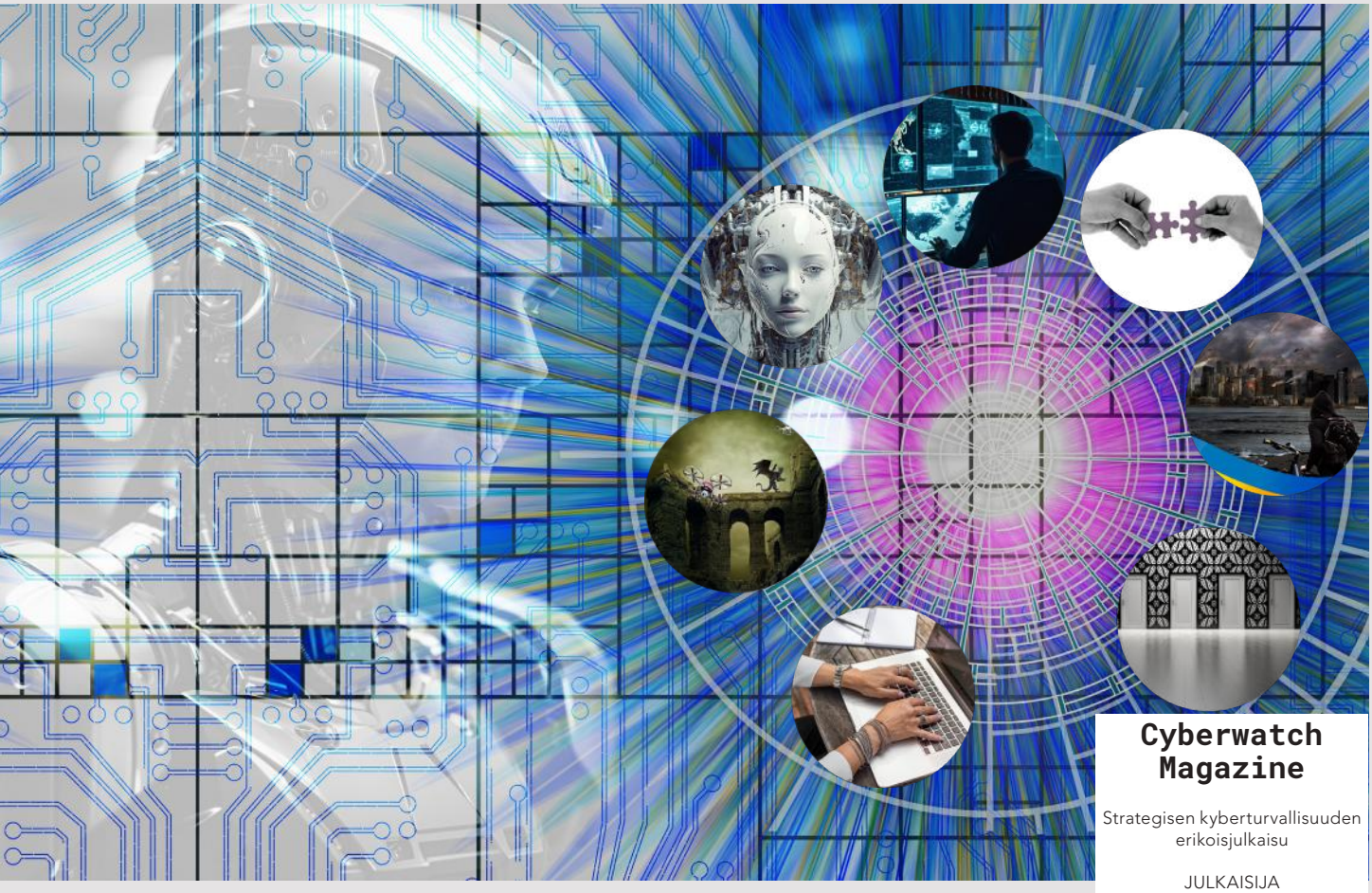
TEKOÄLY JA RIKOLLISUUS

NELJÄ SKENAARIOTA KYBERASEIDEN JA NIIDEN PELOTEVAIKUTUKSEN KÄYTTÖÖN

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

SISÄLLYS

3/2023



Cyberwatch Magazine

Strategisen kyberturvallisuuden erikoisjulkaisu

JULKAISIJA
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

TOIMITUS
Päätoimittaja
Aapo Cederberg
aapo@cyberwatchfinland.fi

Toimitussihteeri
Elina Turunen
elina@cyberwatchfinland.fi

ULKOASU JA TAITTO
Elina Turunen
elina@cyberwatchfinland.fi

KUVITUS
Unsplash
Pixabay
Shutterstock

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

PAINO
Scanseri Oy, Helsinki

NYT TARVITAAN ÄLYKÄSTÄ KYBERTURVALLISUUTTA!

// Aapo Cederberg

Globaali turvallisuustilanne on entistä epävakaampi ja huolestuttavampi. Yllätyksiä ja ennalta arvaamattomia kriisejä syntyy koko ajan. Tuntuu, ettei kukaan ole turvassa kriisien heijastusvaikutuksilta. Digitalisaatio liittyy kehittyneissä yhteiskunnissa kaikkiin elämän osa-alueisiin ja ennen kaikkea kriittisten palveluiden ja infrastruktuurin toimivuuteen. Varmaankin siksi kyberhyökkäysten määrä kriittisiin kohteisiin on kaksinkertaistunut viimeisen vuoden aikana. Kohteiden valinta on entistä huolellisempaa, ja perustuu tehokkaaseen tiedusteluun ja haavoittuvuuksien analysointiin. Tiedustelutieto vaihtuu pimeässä verkossa valtiollisten toimijoiden ja kyberrikollisten välillä. On entistä vaikeampaa tietää, kuka on hyökkäysten tosiasiallinen toimeksiantaja. Tekninen attribuutio on vaikeaa ja hidasta. Poliittisen attribuution merkitys korostuu: hybridi- ja kyberoperaatiot liittyvät entistä selkeämmin poliittisiin päämääriin ja vaikuttamisoperaatioihin.

Kyberturvallisuuden järjestelyt noudattavat eri organisaatioissa pääosin saman tyyppisiä periaatteita ja ratkaisuja. Herää kysymys, riittääkö nykyinen taso? Kyberturvallisuuden ”kruunun jalokiviä” ovat uhkatiedustelu, ennaltaehkäisykyky ja kriisinsietokyky eli resilienssi. Tehokkaalla kyberturvallisuudella saavutetaan myös deterrenssi eli pelotevaikutus. Siksi hyökkäyksellisten kyberkyvykkyyksien kehittämiselle on kova kysyntä. Suurvallat kehittävät vastaiskukykyään ja kyberrikolliset konseptejaan ja rikollisia palveluitaan. Kyberhyökkäyksillä aiheutetaan globaalisti tarkasteltuna vuosittain kuuden triljoonan dollarin tappiot. Kyse on siis koko globaalin järjestelmämme kannalta kohtalon kysymyksestä.

Tulevaisuuden hyvinvointi edellyttää entistä ketterämpiä ja älykkäämpiä kyberturvallisuuspalveluita ja teknologioita. Teknologisia ratkaisuja voidaan kehittää tehokkaasti tekoälyn avulla. Kyberhyökkäysten torjunnassa korostuu kuitenkin ihmisten osuus ja inhimilliset tekijät. Siksi hyökkäysten estäminen ja ennaltaehkäisy edellyttävät parempaa tiedustelu- ja torjuntakykyä. Pimeän ja syvän verkon analyysien merkitys korostuu rikollisten ja valtiollisten toimijoiden hyökkäyssuunnitelmien ja -aikeiden ennakoinnissa. Tämäkään ei yksin riitä: vaan saatua dataa pitää pystyä analysoimaan ja tekemään sen perusteella oikeita johtopäätöksiä, jotta voidaan olla hyökkääjiä askeleen edellä. Vuodenvaihteessa voimaan astunut EU:n kyberturvallisuusdirektiivi (NIS2) edellyttää, että yhteiskunnan kannalta kriittiset toimijat toteuttavat ”asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet”. Tämäkin korostaa entistä älykkäämpien ja kustannustehokkaampien ratkaisujen kehittämistä. Nyt on juuri oikea aika panostaa älykkääseen kyberturvallisuuteen ja uusien ratkaisujen innovointiin. Tehdään se yhdessä. ■

AAPO CEDERBERG
- Toimitusjohtaja ja perustaja
- **Cyberwatch Finland**

NELJÄ SKENAARIOTA KYBERASEIDEN JA NIIDEN PELOTEVAIKUTUKSEN KÄYTTÖÖN

// Max Stucki ja Tuomo Kuosa

Kyberaseet ovat haittaohjelmia, esimerkiksi viruksia ja vakoiluohjelmia, joilla yritetään vahingoittaa vastapuolen kriittistä infrastruktuuria. Kyberaseilla voi olla merkittävä pelotevaikutus, jolloin offensiiviset kybervalmiudet luovat kostotoimien uhan, joka saa hyökkääjät luopumaan aikeistaan. Samoin vahva kyberpuolustus tekee iskuista vähemmän houkuttelevia. Tulevaisuudessa massiivinen kyberkilpavarustelu voi luoda hauraan kauhun tasapainon suurvaltojen välille. Myös laajamittainen kybersodankäynti on mahdollista. Toisaalta voi myös käydä niin, että joko kyberturvallisuuden kehittyminen taikka vajavaiset investoinnit kyberaseisiin tekevät kyberoperaatioista vähemmän houkuttelevia.

TAUSTAA

Kyberase tarkoittaa käytännössä haittaohjelmistoa kuten virusta, troijalaista, vakoiluohjelmaa tai muuta korruptoivaa koodia, jota voidaan käyttää kyberhyökkäyksessä. Ne tekevät hallaa vastapuolen tietokoneverkoille ja järjestelmille, vahingoittavat tai kaatavat digitaalisia infrastruktuureja, yrittävät saada haltuun arvokasta tietoa tai saavuttaa jonkin muun, usein poliittisen tai sotilaallisen, tavoitteen. Tällaisten aseiden käyttö osittain korvaa sotilaallisen voiman sekä fyysisen sabotaasin tai vakoilun tarpeet.

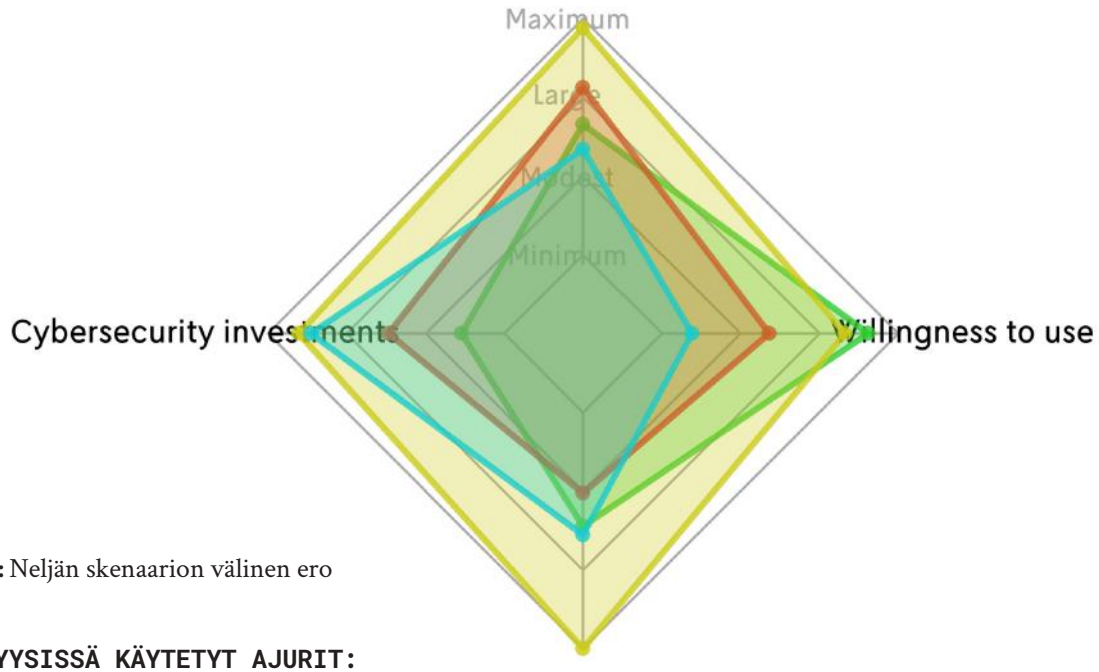
Kyberaseistusta voidaan ajatella ikään kuin hakkerointina, mutta on ehkä parempi puhua erilaisten haittaohjelmistojen ja haktivistiryhmien toimien yhdistelmästä, joka voidaan valjastaa samanaikaisesti yhteishyökkäykseen valtioiden välisissä konflikteissa, joissa niillä voidaan saavuttaa suurempaa vaikutusta kuin yksittäisillä haittaohjelmilla. Vastustajien tietokantojen hyväksikäyttö ja vahingoittaminen lukeutuvat kyberaseiden käytön päätavoitteisiin. Kenties tunnetuin esimerkki kyberaseiden käytöstä tähän mennessä on Iranin ydinohjelman sabotoinnissa käytetty Stuxnet-haittaohjelma.

Kyberaseiden pelotevaikutuksella viitataan siihen uhkakuvaan, joka syntyy vahvan kyberaseistuksen myötä. Mittavan kybervarustelun valtiot voivat sen avulla pelotella mahdollisia hyökkääjiä luopumaan aikeistaan. Kyberaseiden pelotevaikutusta on kuitenkin pidetty ongelmallisena käsitteenä, jota ei voida suoraan verrata esimerkiksi totuttuun ydinaseilla pelotteluun, sillä kyberkostouhka voi olla suhteellisen merkityksetön, mikäli hyökkääjää ei pystytä tunnistamaan. Näin ollen syyksilukemisen ongelmat sekä digitaalisen puolustuksen uskottavuus, kuten muun muassa kyberaseiden käytön hyötyjen mitätöiminen järjestelmien turvaamisella, lukeutuvat ongelmakohtiin, jotka pitää ratkaista ennen kuin kyberaseiden pelotevaikutus varsinaisesti astuu voimaan.

Pian sen jälkeen, kun Venäjä aloitti hyökkäyksensä Ukrainaan alkuvuodesta 2022, presidentti Bidenille väitetysti tarjottiin mahdollisuutta iskeä Venäjän internetyhteyksiin, sähköverkkoihin, rautateihin sekä muuhun valtiolle tärkeään ohjelmistoon kyberaseiden avulla. Yhdysvaltojen tiedetään kehittäneen tällaisia aseita jo vuosia, mutta valtionjohto päätti kuitenkin olla käyttämättä niitä. Mahdollisena syynä saattoi olla, että pelotevaikutuksesta ei haluttu vielä luopua. Koko arsenaalin valjastaminen tähän konfliktiin olisi nimittäin pitkälti mitätöinyt sen tehokkuuden tulevaisuudessa, sillä kyberaseet yleensä muuttuvat tehottomiksi käytön jälkeen, koska vastapuoli havahtuu omien järjestelmiensä haavoittuvuuteen ja korjaa ne.

NELJÄ SKENAARIOTA

Keskeiset toimijat: USA, Kiina, Venäjä, Israel, Iso-Britannia, hakkeriryhmät.



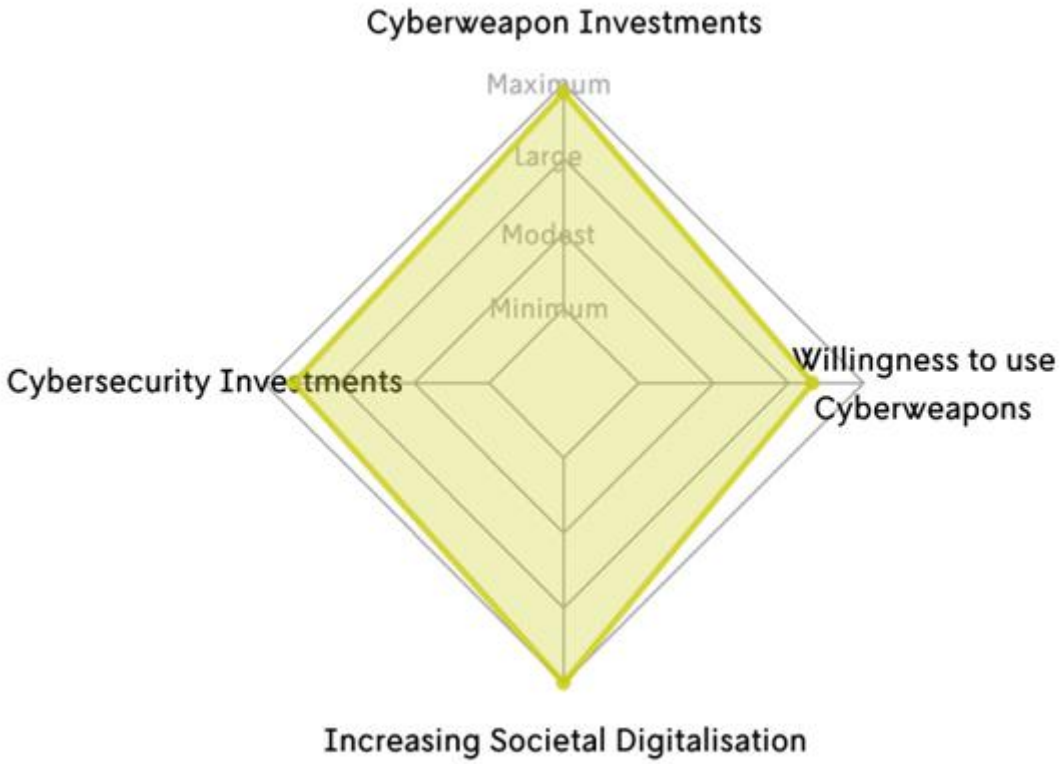
Kuva: Neljän skenaarion välinen ero

ANALYYSISSÄ KÄYTETYT AJURIT:

- Sijoitukset kyberaseisiin (Cyberweapon investments)
- Halukkuus käyttää kyberaseita (Willingness to use cyberweapons)
- Lisääntyvä yhteiskunnan digitalisaatio (Increasing societal digitalisation)
- Sijoitukset kyberturvallisuuteen (Cybersecurity investments)

SKENAARIO 1: KYBERASEIDEN KILPAVARUSTELU

Lisääntyvä riippuvuus digitaalisista palveluista on tehnyt kyberaseista merkittävän työkalun kansainvälisessä valtapolitiikassa, mikä on saanut maat myös investoimaan kyberturvallisuuteen. Maailma on lukittautunut kybervarustelukilpailuun, jossa talousblokit kehittävät omia kyberaseita ja valmistautuvat mahdolliseen valtavaan virtuaaliseen iskuun.



Kuva: Kunkin ajurin rooli tässä skenaariossa

Kyberaseista on tulossa merkittävä väline kansainvälisessä voimapolitiikassa. Koska yhteiskunnat ovat tulleet täysin riippuvaisiksi digitaalisista palveluista, vastapuolen kriittisiin järjestelmiin iskeminen on nyt houkutteleva tapa tuottaa vahinkoa. Valtavat sijoitukset kybervalmiuksiin lisäävät myös investointeja kyberturvallisuuteen. Vaikka kyberkeinoja käytetään usein ennen kuin voidaan puhua tosiasiallisesta sodasta, suurvaltojen välille on kehittymässä hauras "molemminpuolisen varman kybertuhon" tasapaino. Useimmat valtiot ovat valmiina käyttämään joitain kybertoimia, mutta täysimittaista kyberiskua toisen maan lamauttamiseksi ei ole vielä tehty. Maailma ja erityisesti kyberaseistuksen jakavat taloudelliset blokit ovat lukittuneita kilpavarusteluun, jossa kaikki yrittävät valmistautua potentiaaliseen laajaan kyberhyökkäykseen, jota ei toivottavasti tulla näkemään.

KEHITYSPOLKU SKENAARIOSSA 1:

2025: Digitaalinen infrastruktuuri on nyt yleisesti ensisijainen kohde kyberoperaatioille. Voimakkaampia ja kyvykkäämpiä kyberkeinoja kehitetään vastapuolen vahingoittamiseksi ja oman selustan turvaamiseksi.

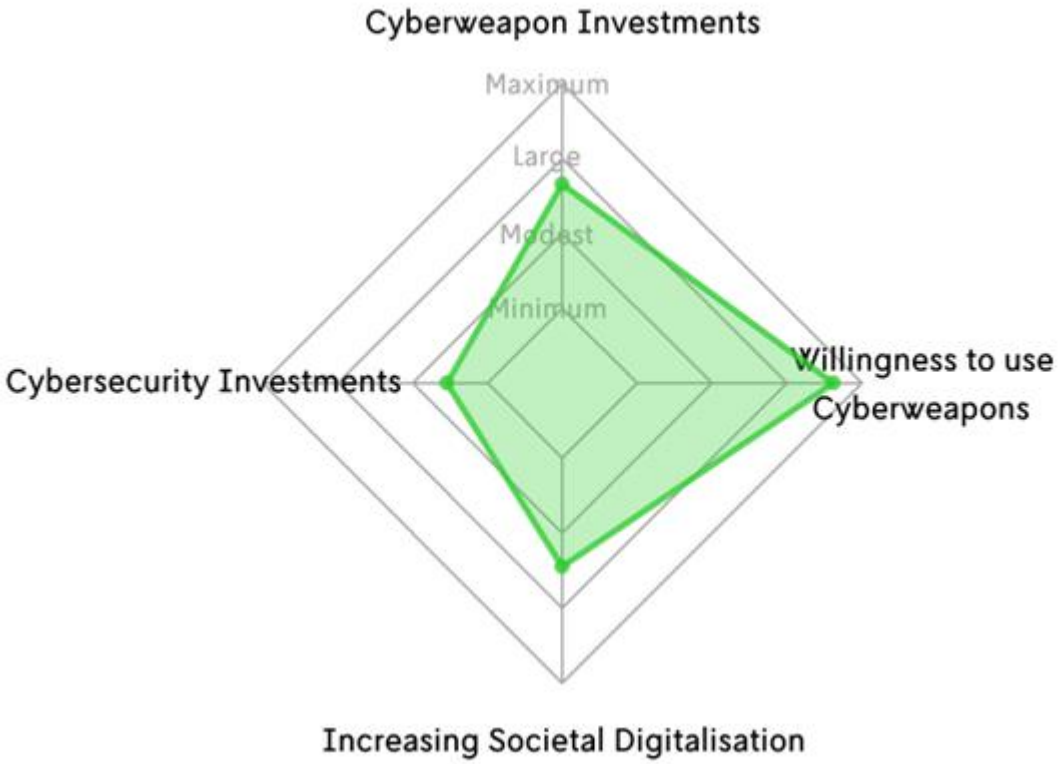
2027: Kyberturvallisuuden investoinnit kasvavat merkittävästi, kun hyökkäykset julkisiin ja yksityisiin kohteisiin lisääntyvät. Hyökkäysten takana ovat todennäköisesti toiset valtiot, jotka käyttävät rikollisia hakkeriryhmiä välikäsinä.

2028: Edistyneiden kyberaseiden kehittäminen on alati kalliimpaa, sillä turvallisuusjärjestelmät ovat myös koko ajan varmempia.

2030: Yhdysvallat julistaa pystyvänsä lamaannuttamaan Kiinan tärkeät järjestelmät ilman fyysisiä operaatioita. Kiina väittää pystyvänsä yhtä laajoihin kostotoimiin. Venäjä ilmoittaa, että tarpeeksi laajamittaiset kyberhyökkäykset sen infrastruktuuria kohtaan tullaan kostamaan ydinaseilla.

SKENAARIO 2: HEIKKO KYBERTURVALLISUUS JOHTAA LISÄÄNTYVÄÄN KYBERASEIDEN KÄYTTÖÖN

Vaikka kyberaseissa ja kyberturvallisuudessa on edistytty jonkin verran, ne eivät vastaa odotettua potentiaalia valtioiden välisessä sodankäynnissä. Heikon kyberturvallisuuden vuoksi kyberaseet ovat kuitenkin edelleen houkutteleva vaihtoehto rikollisille ja terroristiryhmille.



Kuva: Kunkin ajurin rooli tässä skenaariossa

Sekä kyberaseissa että kyberturvallisuudessa on nähty jonkin verran kehitystä. Tästä huolimatta kyberaseet eivät ole vielä odotetun kaltainen mullistava tekijä valtioiden välisessä sodankäynnissä. Osittain tämä johtuu siitä, että maat varmistavat sisäisten toimintojensa jatkuvuuden digitaalisten järjestelmien kaatumisen varalta tai eivät yhdistä sisäisiä toimintojaan lainkaan internetiin. Mahdollisten kohteiden määrä on näin huomattavasti pienempi. Silti puutteelliset kyberturvallisuustoimenpiteet tekevät kyberhyökkäyksistä houkuttelevia rikollis- ja terroristiryhmille, jotka pystyvät aiheuttamaan niillä jonkinlaista vahinkoa etenkin yksityisellä sektorilla. Kyberaseita ei voida käyttää todellisen pelotevaikutuksen rakentamiseen ulkoisia uhkatekijöitä vastaan. Sen sijaan ne ovat lähinnä poliitikkojen puheissa esiintyvä pelote, jolla ei ole vielä todellista voimaa takanaan.

KEHITYSPOLKU SKENAARIOSSA 2:

2025: Kyberhyökkäykset yleistyvät maailmassa, jossa voimapolitiikka vallitsee ja oman toiminnan salaaminen on yhä helpompaa.

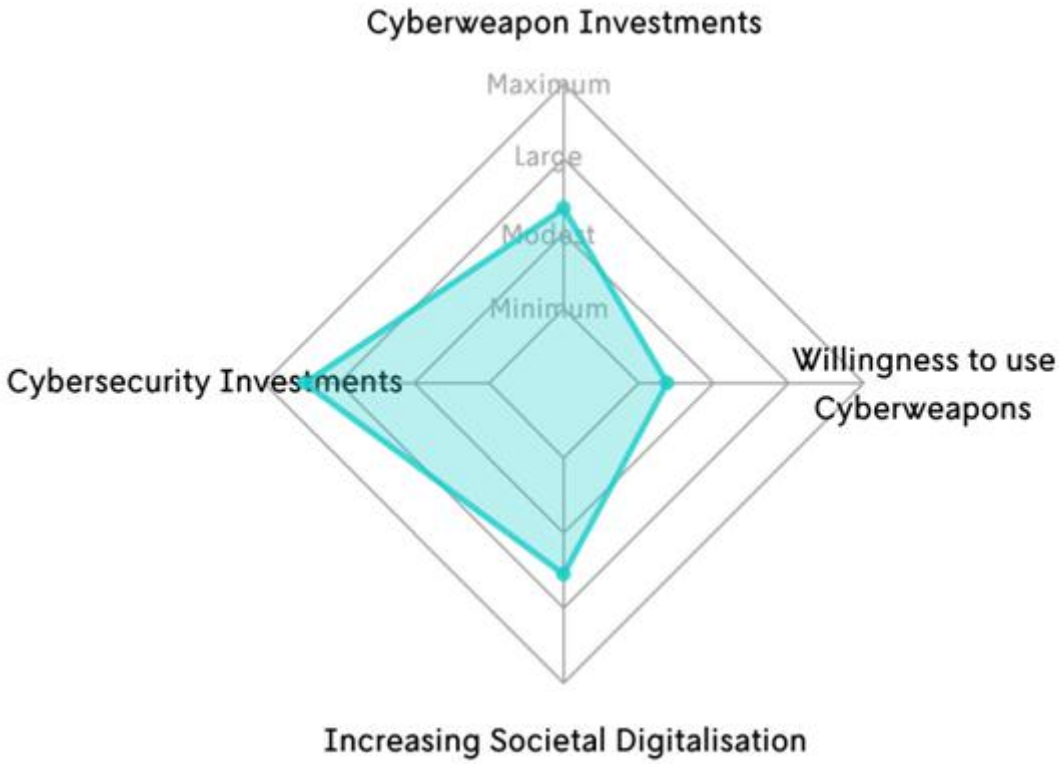
2028: Kyberhyökkäykset ovat entistä voimakkaampia ja pidempikestoisia. Kyberturvallisuus ei pysy kehityksen tahdissa. Taloudelliset kustannukset ovat valtavia.

2030: Valtiot sijoittavat lisää verkosta erillään toimivaan tärkeään infrastruktuuriin ja käyttävät digitaalisten järjestelmien rinnalla epätavallisia vaihtoehtoisia järjestelmiä.

2035: Hallitukset panostavat vaihtoehtoisiin, hitaampiin mutta varmempiin toissijaisiin järjestelmiin, joita käytetään kyberhyökkäysten tapahduttua. Tiettyjä kyberasevalmiuksia pidetään yllä, mutta niihin ei investoida merkittäviä summia.

SKENAARIO 3: SUURET INVESTOINNIT KYBERTURVALLISUUTEEN ESTÄVÄT KYBERASEIDEN KÄYTTÖÄ

Hallitukset ja yritykset investoivat raskaasti kyberturvallisuuteen, kun digitaalisten teknologioiden kehitys tuo mukanaan yhä edistyneempiä haittatoimintoja. Tehokkaampi kyberiskujen ennakointi ja mitätöinti, kansainvälinen yhteistyö ja aktiivinen kyberturvallisuuskulttuuri toimivat kyberturvallisuuden peruspilareina.



Kuva: Kunkin ajurin rooli tässä skenaariossa

Sekä yksityisellä että julkisella sektorilla sijoitetaan runsaasti kyberturvallisuuteen. Tärkeitä yhteiskunnallisia ja liiketoiminnallisia järjestelmiä suojataan ilkivaltaisten hyökkäysten varalta. Korkea suojaustaso saa kyberaseiden käytön näyttämään vähemmän houkuttelevalta. Riittämättömän tehokkuuden takia valtiot eivät ole valmiita sijoittamaan merkittävästi niiden hankintaan. Kyberturvallisuuden kehittämisessä keskeisessä asemassa on kyberkestävyys: vaikka kaikkia hyökkäyksiä ei voida torjua, järjestelmät itsessään kestävät iskut ja palautuvat toimintaan pikaisesti. Kybermaailman merkitys ei sinänsä pienene, mutta kriittisiä haavoittuvuuksia siellä ei ole tarjolla enää entiseen tapaan.

KEHITYSPOLKU SKENAARIOSSA 3:

2025: Kyberaseita käytetään usein, ja niistä on muodostumassa todellinen rasite hallituksille.

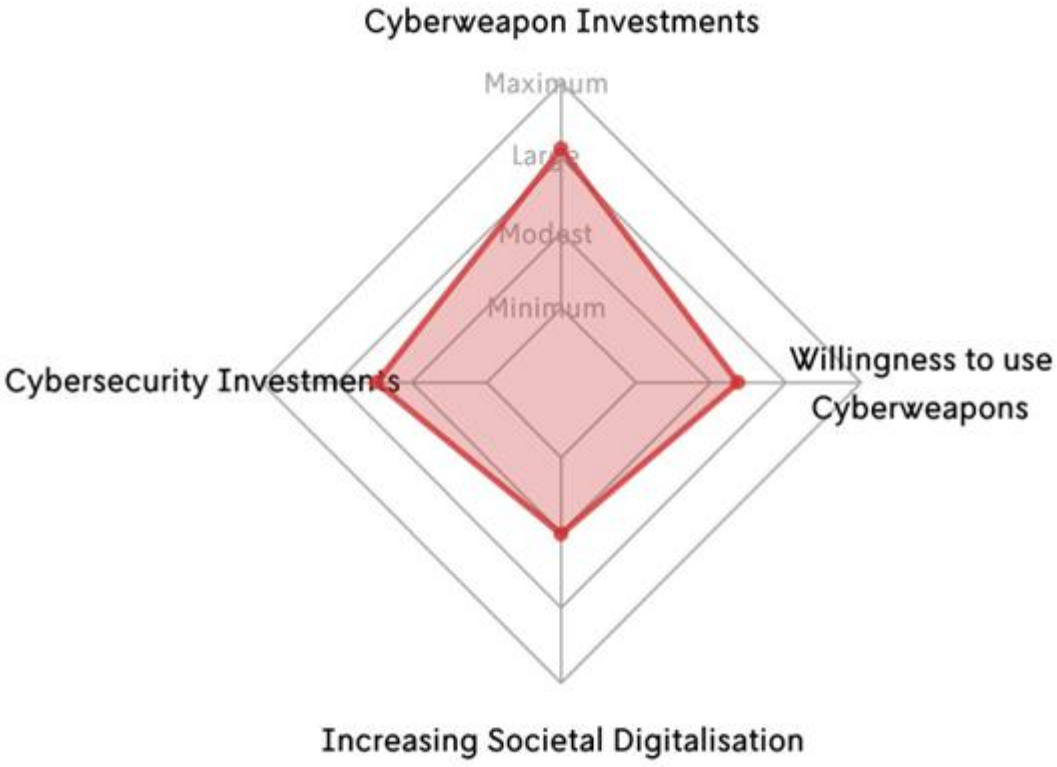
2028: Tekoälyn saralla saavutetaan läpimurto, ja yhdessä lohkoketjujen kanssa se parantaa kyberturvallisuutta huomattavasti.

2030: Järjestelmiin murtautumisen hintalappu on kohonnut sen tuottavuutta suuremmaksi. Ainoastaan valtioilla on varaa edistyksellisiin ja tehokkaisiin kyberhyökkäysarsenaaleihin.

2035: Kyberaseista on tullut lähes turhia kehittyneitä valtioita vastaan

SKENAARIO 4: KYBERASEIDEN MALTILLINEN KEHITYS

Kyberhyökkäys- ja puolustusvalmiuksiin sijoittaminen jatkuu, mutta kyberavaruuden turvallisuutta ympäröivä kohu tasoittuu. Vaikka kyberaseet normalisoidaan osaksi suurten kansainvälisten toimijoiden arsenaalia, kyberpelotteesta ei edelleenkään ole selvää käsitystä, eikä kyberhyökkäysten uhka ole kouriintuntuva.



Kuva: Kunkin ajurin rooli tässä skenaariossa

Kybervalmiudet sekä hyökkäys- että puolustussuuntaan paranevat sijoituksien ja kehitystyön myötä. Kybermaailmassa ei kuitenkaan enää kuhise samalla tavalla. Kyberaseet ja kyberturvallisuus ovat turvallisuushuolia siinä missä muutkin hallitusten ja yritysten kohtaamat uhat. Kyberaseista on monella tapaa tullut arkipäivää, ja oletus on, että kaikilla kansainvälisesti varteenotettavilla toimijoilla on niitä takataskussaan. Pelotevaikutuksen käsite ei ole silti selkeä. Kyberasearsenaalista on vaikea antaa todisteita, eikä iskujen tekijän selvittäminen ole aina helppoa, joten uhka vastaiskuista ei ole aina konkreettinen ongelma. Kukaan ei halua paljastaa korttejaan mitä tulee kyberaseisiin, jottei mahdollinen hämäysyritys paljastuisi.

KEHITYSPOLKU SKENAARIOSSA 4:

2025: Kyberaseista on tullut vakiintunut ja tärkeä osa useimpien asevoimien varustusta. Laajamittaista kyberaseiskua toisen valtion kriittisten järjestelmien lamaannuttamiseksi ei ole vielä kuitenkaan nähty.

2030: Kyberasearsenaalit yleistyvät ja kasvavat, mikä lisää kyberturvallisuuden kysyntää. Taloudelliset blokit tekevät mittavaa yhteistyötä sen kehittämisessä.

2035: Vaikka kaikki kehittyneet valtiot väittävät, että niillä on huomattavia kybervalmiuksia, on silti vielä epäselvää, voivatko ne koskaan vetää vertoja perinteisille keinoille aiheuttaa vahinkoa vastapuolen kriittiselle infrastruktuurille. ■

TUOMO KUOSA

- Futuristi, tohtori Tuomo Kuosa on yksi Futures Platformin perustajista ja toimii yhtiössä tutkimusjohtajana vetäen yhtiön monitieteistä tutkimustiimiä.
- **Futures Platform**

MAX STUCKI

- Max Stucki on toiminut strategisen ennakoinnin parissa usean vuoden ajan niin konsulttina kuin analyytikkona. Hän on auttanut useita julkisen ja yksityisen sektorin organisaatioita tutkimaan ja ymmärtämään tulevaisuutta.
- **Futures Platform**

SUOMEN KYBERTURVA-ALA TARJOAA RATKAISUJA EU:N DIGISTRATEGIAAN

// Peter Sund ja Risto Rajala

Kyberturvallisuus on yhä ajankohtaisempi aihe nopeasti digitalisoituvassa maailmassa. Kriittinen infrastruktuurimme, kuten logistiikka, sähköverkot ja vesihuolto sekä useimmat muut palvelut ovat riippuvaisia verkkoon tai toisiinsa liitetyistä tietojärjestelmistä. Samaan aikaan monet meistä omistavat ja käyttävät useita verkkolaitteita jatkuvasti ja luotamme niihin sekä jokapäiväisissä asioissamme että arkaluonteisimmissa ja tärkeimmässä henkilökohtaisen datan käsittelyssä.

Onneksi lainsäätäjämme kiinnittävät paljon huomiota digitaalisen toimintaympäristön turvallisuuteen. Meneillään olevan vaalikauden aikana Euroopan unioni (EU) on noudattanut kunnianhimoista ohjelmaa paremman digitaalisen elämän rakentamiseksi eurooppalaisille ja kyberturvallisuuden tason nostaminen on yksi sen kulmakivistä. EU käsittelee parhaillaan ja on jo hyväksynyt merkittäviä sääntelyaloitteita, joilla parannetaan merkittävästi kyberturvallisuutta kaikkialla Euroopassa. Vuoden 2022 lopulla hyväksytty NIS2-direktiivi asettaa uudistetut säännöt ja vastuut yrityksille ja muille yhteisöille, joita pidetään kriittisinä eurooppalaisten yhteiskuntien toimintojen kannalta. Kyberresilienssi-säädösehdotus on edennyt kolmikantaneuvotteluvaiheeseen, jossa Euroopan komissio, jäsenmaat ja Euroopan parlamentti hiovat viimeisiä yksityiskohtiaan. Kun kyberresilienssisäädös on hyväksytty, sillä otetaan käyttöön kattavat kyberturvallisuussäännöt kaikille verkkoon liitetyille laitteille ja ohjelmistoille. Yhdessä nämä kaksi aloitetta tekevät jokapäiväisestä elämästämme turvallisemman ja nostavat kyberturvallisuustoimenpiteiden riman verkottuneille yhteiskunnillemme sopivalle tasolle.

Kaikista EU:ssa tällä hetkellä toteutettavista hyvistä toimista huolimatta on myös lainsäädäntöehdotuksia, jotka ovat parhaimmillaankin haitallisia ja pahimmillaan uhkaavat suistaa raiteiltaan koko digistrategian sekä kyberturvallisuuden Euroopassa. Kybersolidaarisuussäädöstä koskevalla ehdotuksella on tärkeä tavoite tehostaa kyberpoikkeamien havaitsemista, analysointia ja niihin reagointia sekä tiedonvaihtoa jäsenmaissa. Valitettavasti lainsäädäntöehdotus on valmisteltu kiireessä ja ilman asianmukaisia vaikutustenarviointeja. Ehdotetut toimenpiteet vaikuttavat tehottomilta, vievät niukkoja resursseja muilta tarpeilta ja ovat oikeudellisesti kyseenalaisia. Myös markkinoiden vääristymisen riski on todellinen. Toivottavasti lainsäätäjät muuttavat ehdotusta ja tutkivat sen vaikutukset asianmukaisesti. Samaan aikaan kybersolidaarisuussäädöksen kanssa komissio julkaisi tiedonannon Cyber Skills Academy -akatemiasta, joka olisi periaatteessa verkkofoorumi, joka toimisi keskitettynä asiointipisteenä kyberturvallisuuskoulutustarjouksille, sertifioinneille, rahoitusmahdollisuuksille ja muille olemassa oleville aloitteille, joilla pyritään edistämään kyberturvallisuustaitoja. Vaikka Cyber Skills Academyn taustalla olevat aikomukset ovat järkeviä, tällaisen alustan perustamisen todelliset hyödyt ovat edelleen epäselviä. Jotta kyberturvallisuuden osaamisvajeeseen voidaan todella puuttua, nykyisiä ratkaisuja kyberturvallisuuskoulutuksen järjestämiseen on uudistettava, tehostettava ja laajennettava. Tämä on jäsenvaltioiden tehtävä. Samalla on tärkeää, että ei luoda tarpeettomia byrokraattisia rakenteita, jotka sulkisivat pois monia oppilaitoksia.

Vielä ongelmallisempi on ehdotus päästä päähän -salauksen (E2EE) heikentämisestä sähköisissä viestintäpalveluissa, jotta viranomaiset voisivat skannata yksityistä viestintää. Jos ehdotus hyväksytään, se loisi ennennäkemättömän valvontakoneiston, joka loukkaa perusoikeuksia. Tällainen ajatus liittyy tavoitteeseen ehkäistä ja torjua paremmin lasten seksuaalista hyväksikäyttöä, jota jokainen järkevä ihminen tietysti tukee, mutta ehdotettu tapa saavuttaa tämä tärkeä tavoite olisi erittäin ongelmallinen.

Ehdotukseen liittyviä oikeudellisia ja perustuslaillisia huolenaiheita on tuotu esiin monissa yhteyksissä, ja ehdotus on myös ristiriidassa kyberresilienssilakiehdotuksen kanssa. Salauksella on ratkaiseva rooli yksityisen ja turvallisen viestinnän tarjoamisessa, jota käyttäjät, mukaan lukien lapset, vaativat ja odottavat pitävänsä heidät turvassa verkossa. Jopa hyvää tarkoittavat pyrkimykset tarjota laillinen valvontaratkaisu päästä päähän -salausta hyödyntävälle viestinnälle heikentävät kriittisiä turvallisuusetuja tekemällä tällaisten palvelujen käyttäjistä alttiimpia haitallisille hyökkäyksille. Kaikenlaisten takaporttien tai luottamuksellisuuden rajoitusten luominen viranomaisille tarkoitetuille sähköisille viestintäpalveluille merkitsisi väistämättä sitä, että samoja takaportteja voitaisiin käyttää muihin hallinnon tarkoituksiin, jotka heikentäisivät merkittävästi digitaalista luottamusta. Samat takaportit olisivat myös rikollisten löydettävissä.

Jos päästä-päähän salausta heikennetään, eniten häviävässä asemassa ovat tavalliset Euroopan kansalaiset ja yritykset, joiden yksityisyyteen tunkeuduttaisiin ja joilta poistettaisiin pääsy turvallisiin viestintävälineisiin. Rikolliset ja muut pahantahtoiset toimijat puolestaan mitä todennäköisemmin löytäisivät muita keinoja viestiä salatusti. On tärkeää, että ne jäsenmaat, kuten Espanja, Unkari ja Kypros sekä muut, jotka tukevat päästä päähän salauksen heikentämistä tai ovat kantansa suhteen vielä epävarmoja, harkitsevat asiaa uudelleen ottaen huomioon elintärkeät kysymykset eurooppalaisten perusarvoista ja digitaalisen turvan toteutumisesta. Selkeä kannanotto päästä-päähän salauksen heikentämisen ehkäisemiseksi tulee sisällyttää lopulliseen säädökseen. Suomi on kiitettävästi yksi niistä jäsenmaista, kuten Viro, Saksa ja Itävalta, jotka ovat kyenneet näkemään myös aloitteen kielteiset seuraukset perusarvojen suojelemisessa. Suomen eduskunta on juuri ottanut kantaa edellyttämällä, että viranomaisten pakkokeinot eivät tosiasiallisesti johda päästä päähän -salauksen tai muiden vastaavien turvatoimien yleiseen heikkenemiseen tai purkamiseen tai käytön rajoittamiseen, ja siten viestinnän sekä siihen liittyvien palveluiden turvallisuus- ja kyberturvallisuustason heikkenemiseen.

Kun Euroopan kyberturvallisuusagenda on saatu valmiiksi, toivottavasti tavalla, joka on yhdenmukainen yksilöiden ja yritysten kannalta elintärkeiden perusoikeuksien ja digitaalisen turvallisuuden kanssa, se siirtyy täytäntöönpanovaiheeseen. Tämä vaihe on ratkaisevan tärkeä sen varmistamiseksi, että hyväksytyt asetukset palvelevat tarkoitustaan ja heijastavat niiden taustalla olevia poliittisia päätöksiä. On olennaisen tärkeää, että jäsenmaat aloittavat hyvissä ajoin akkreditointiprosessin tahoille, jotka pystyvät suorittamaan kolmannen osapuolen arviointeja tuotteille ja ohjelmistoille, joita pidetään kriittisinä kyberresilienssin kannalta. Asetusten onnistunut ja yhdenmukainen täytäntöönpano voi tarjota valtavia taloudellisia etuja, tietenkin paremman digitaalisen turvallisuuden tuomien hyötyjen joukossa, kun taas epäonnistuminen voi haitata vakavasti Euroopan teollisuuden kilpailukykyä. Samaan aikaan kaikkialla Euroopassa tarvitaan aitoja julkisen ja yksityisen sektorin kumppanuuksia sen varmistamiseksi, että kyberturvallisuuden tasoa nostetaan kaikissa yhteiskunnissa ja erityisesti yksityisellä sektorilla, jotka todellisuudessa omistavat suurimman osan tietojärjestelmistä ja kriittisestä infrastruktuurista.

Vaikka asianmukainen sääntely olisi käytössä, kyberturvallisuuden tasoa ei voida parantaa ilman uusimpia tuotteita, palveluja ja ratkaisuja. Tämä edellyttää merkittäviä EU:n tason toimia, joilla tuetaan uusien kyberturvallisuusteknologioiden kehittämistä ja käyttöönottoa. Onneksi suomalaisella kyberturva-alalla on paljon annettavaa uusien EU-säädösten toimeenpanoon ja valmiudet tarjota osaamistaan ympäri Eurooppaa sekä sen ulkopuolella. Suomalainen kyberturvallisuusala koostuu yrityksistä, joilla on erilaisia portfolioita maailmanluokan teknologioista ihmiskeskeisiin sovelluksiin, joiden avulla ihmiset voivat huolehtia omasta digitaalisesta turvallisuudestaan. ■

PETER SUND

- Kyberala ry:n (FISC ry) toimitusjohtaja
- **Teknologiateollisuus ry**

RISTO RAJALA

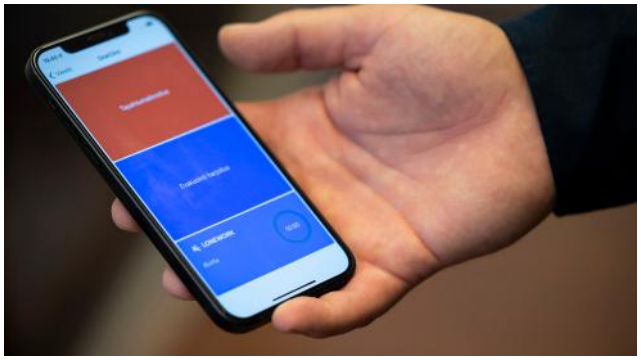
- Kyberala ry:n (FISC ry) neuvonantaja
- **Teknologiateollisuus ry**

JOKAINEN SEKUNTI MERKITSEE – VARAUTUMINEN JA KRIISIVIESTINTÄ KRIITTISENÄ OSANA KYBERTURVALLISUUTTA

// Kari Aho

Viimeistään kiristynyt kansainvälinen ilmapiiri on tehnyt selväksi, että elämme yhä epävarmemmassa ja uhkakuvien värittämässä maailmassa. Kyberhyökkäykset, järjestelmähäiriöt, sähkökatkokset ja fyysiset turvallisuusuhkat ovat vain muutamia esimerkkejä skenaarioista, jotka voivat aiheuttaa mittavia haittoja niin yksilöille kuin organisaatioille. Tilannetta mutkistaa entisestään se, että erilaiset kriisit voivat limittyä ja vaikuttaa toisiinsa. Näiden uhkakuvien kasvaessa ja monimutkaistuessa, jokainen menetetty sekunti voi olla kallis – ei ainoastaan taloudellisesti, vaan myös ihmishenkien ja yhteiskunnallisen vakauden kannalta. Tiukentuva sääntely tai toimintaympäristön asettamat vaatimukset myös osaltaan luovat painetta tarvittaville toimenpiteille. Tässä jatkuvasti muuttuvassa ympäristössä korostuvat erityisesti varautuminen ja oikea-aikainen viestintä.

Kansainvälisen tutkimusyhtiö Gartnerin vuonna 2021 julkaiseman tutkimuksen mukaan pelkkä IT-järjestelmähäiriö aiheuttaa keskimäärin yli 5 300 euron kustannukset jokaista häiriöminuuttia kohden. Kun lasketaan, mitä se tarkoittaa vain yhdessä tunnissa, niin summa nousee häkellyttävään 318 000 euroon. Tällaiset kustannukset voivat syntyä esimerkiksi teollisuuden tuotantolinjan seisahduksista, elintärkeiden laitteiden toimintahäiriöistä terveydenhuollossa tai laajemmissa organisaatioissa tilanteesta, jossa yleisesti käytetyt viestintäjärjestelmät, kuten sähköposti tai pikaviestinratkaisut, eivät ole saatavilla. Tämä estää työntekijöitä suorittamasta työtehtäviään vähintään osittain ja voi johtaa mittaviin tuotannon menetyksiin. Edellä mainittua täydentää IBM:n 2023 tekemä tutkimus, jonka mukaan keskimääräinen kustannus tietovuototapauksiin liittyen on 4.25 miljoonaa euroa, jossa on 15% kasvua kolmen vuoden takaiseen tilanteeseen verrattuna.



Olen Secapp Oy:n toimitusjohtaja, tietotekniikan tohtori, Kari Aho, ja pyrin avaamaan seuraavassa muutamia nostoja kyber- ja hybridiuhkin varautumiseen sekä kriisiviestinnän perusteisiin liittyen. Secappilla olemme jo yli kymmenen vuotta työskennelleet niin yksityisen sektorin, viranomaisten kuin julkishallinnon kanssa yhteistyössä varautumiseen, kriittiseen viestintään ja hälyttämiseen liittyvien asioiden parissa ja tuotamme niihin liittyvää SaaS-palvelua. Viime vuonna Secappilla lähetettiin yli 10 miljoonaa hälytystä erilaisiin poikkeustilanteisiin liittyen.

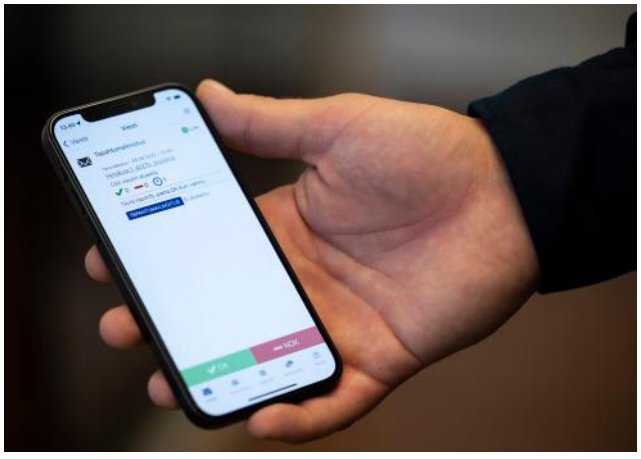
Kun puhutaan kyberturvallisuudesta ja mahdollisista kyberhyökkäyksistä, ajatuksemme kääntyvät usein teknisiin ratkaisuihin ja suojautumismekanismeihin, jotka ovat toki tärkeä osa kokonaisuutta. Kuitenkin vähintään yhtä tärkeässä roolissa on ihmisten varautuminen ja toimintavalmius: kuinka yksittäinen henkilö, organisaatio ja tarvittavat sidosryhmät toimivat, kun kriisitilanne ilmenee. Millaiset yleiset toimintaohjeet tilanteeseen liittyy? Miten ihmiset tavoitetaan ja tavoitettavuus varmistetaan kellonajasta riippumatta? Mitä varajärjestelyitä seurataan, kun normaalit toimintatavat tai järjestelmät eivät ole saatavilla? Kuka ottaa ohjat käsiinsä ja ohjaa toimintaa? Kenen vastuulla on viestiä tilanteesta muille sidosryhmille tai julkisuuteen? Milloin ja miten tietoa kerätään ja päivitetään? Ja kuka päättää tehtävät toimenpiteet ja sen, että poikkeustilanne on ohi ja normaaliin toimintaan voidaan palata?

Kuitenkin valitettava fakta on, että edelleen 51% prosenttia organisaatioista suunnittelee lisäävänsä investointeja varautumiseen, harjoitteluun, kouluttamiseen ja tarvittaviin työkaluihin vasta sen jälkeen, kun jokin uhkakuva on kertaalleen realisoitunut. Seuraavassa olisi kuitenkin lyhyt viiden kohdan muistilista, millaisia asioita teknisten työkalujen ja suojausmekanismien lisäksi olisi hyvä huomioida osana varautumista:

1 Kriisi- ja häiriötilanteissa tapahtuu helposti inhimillisiä virheitä ja unohduksia, joten suunnittele toimintaohjeet ja esimerkiksi viestintäryhmät eri tilanteita varten etukäteen. Näin varmistat, että kaikki olennaiset henkilöt saavat kriisitilanteessa oikeellisen tiedon oikea-aikaisesti ja osaavat toimia tilanteen vaatimalla tavalla.

2 Varmista ihmisten tavoitettavuus ja yhteistietojen ajantasaisuus riippumatta millaista viestintävälinettä tai -teknologiaa he käyttävät. Osalla on varmasti edelleen se vanha nokialainen siinä missä toisella viimeisin älylaite. Kotisohvalla ei välttämättä myöskään ole se päivystyspuhelin mukana, vaikka henkilö olisi tärkeää tavoittaa. Myöskään häiriötilanteissa ei voida aina luottaa, että kaikki teknologiat toimisivat, joten huomioi yhteystiedoissa ja -tavoissa myös mahdolliset varanumerot tai -yhteydenottotavat. Unohtamatta myöskään yhteystietojen turvallista käsittelyä niin, että ne eivät joudu kolmansien osapuolien saataville.

3 Viestinnän sisältö voi olla hyvin arkaluonteista ja sen joutuminen vääriin käsiin voi itsessään aiheuttaa esimerkiksi vaaratilanteita tai mainehaittaa. Tiedonkulun varmistaminen, tilannekuvan muodostaminen ja tilanteen dokumentointi ovat kuitenkin ensiarvoisen tärkeitä tilanteen ratkaisemiseksi. Varmista siis, missä tietosi sijaitsevat ja että niihin pääsevät käsiksi vain asiaankuuluvat henkilöt. Jos hallinta ei ole keskitettyä tai automatisoitua, niin helposti mukaan voi jäädä vaikkapa ex-työntekijä tai kääntäen siitä voi jäädä ulkopuolelle joku toiminnan kannalta olennainen henkilö.



4 Jokainen sekunti merkitsee kriisitilanteissa. Teknologian ei tulisi viedä noita arvokkaita sekunteja, vaan asioiden täytyy tapahtua yksinkertaisimmillaan automatisoidusti tai vähintään napin painalluksella. Tutki siis mahdollisuuksia, mitä prosesseja tai toimintatapoja olisi mahdollista automatisoida tai nopeuttaa, jotta avainhenkilöillä on aikaa keskittyä kriisitilanteessa itse tilanteen ratkaisemiseen esimerkiksi puhelimessa olemisen sijaan.

5 Muistuta sovituista toimintaohjeista toistuvasti, harjoittele ja kannusta ihmisiä antamaan kehitysideoita kriisitoiminnan parantamiseksi. Näin ollen toimintamallit pysyvät tuoreessa muistissa ja niitä viedään koko ajan kehittyneempään suuntaan.

Vaikka teknologia on keskeinen osa varautumista, ihmisten toiminta, kommunikaatio ja yhteistyö ovat vähintään yhtä tärkeitä. Organisaatioiden on ymmärrettävä sekä tekniset että inhimilliset näkökulmat, ja ne on koulutettava ja varustettava oikeilla työkaluilla ja protokollilla toimimaan tehokkaasti ja turvallisesti. Työkalujen näkökulmasta Secapp on esimerkki modernista ratkaisusta, joka auttaa kehittämään varautumista ja tuo tehokkaat työkalut nopeaan monikanavaiseen ihmisten tavoittamiseen. Onpa yksi asiakkaamme sanonut, että Secapp vähentää heillä jopa 90% tarvittavaa aikaa ihmisten tavoittamiseen. Voin sanoa olevani ylpeä siitä, miten Secapp auttaa tekemään maailmasta osaltaan turvallisemman paikan. Jokainen sekunti todella merkitsee. ■

KARI AHO

- Toimitusjohtaja ja perustaja.
- Secapp auttaa organisaatioita hallitsemaan kriisejä, pelastamaan ihmishenkiä ja turvaamaan päivittäistoimintoja.
- **Secapp**

TEKOÄLY JA RIKOLLISUUS

// Ismo Kallioniemi

Tekoälyjärjestelmien nopea kehitys ja laaja-alainen käyttöönotto eri toimialoilla on tuonut mukanaan uusia mahdollisuuksia, mutta samalla luonut yhteiskunnalle myös uusia haasteita. Eräs näistä haasteista on tekoälyn käyttö rikollisissa tarkoituksissa. Toisaalta, tekoälyjärjestelmiä voidaan hyödyntää myös erinäisiin rikostutkinnassa ja -torjunnassa.

Tässä kirjoituksessa tarkastellaan ensin yleisellä tasolla tekoälyjärjestelmien mahdollisia käyttökohteita rikosten toteuttamiseksi ja rikostorjunnassa. Tämän jälkeen kirjoituksessa käsitellään esimerkkinä yksityiskohtaisemmin väärennysrikollisuutta. Lopuksi kirjoituksessa esitetään näkemys kehityksen vaikutuksesta vallitsevaan oikeudelliseen tilanteeseen.

TEKOÄLYN KÄYTTÖ RIKOLLISIIN TARKOITUKSIIN

Vaikka tekoälyjärjestelmät ovat tavallaan yleiskäyttöistä teknologiaa, rikollisuuden puitteissa niille on joitakin ilmeisiä käyttökohteita. Näitä ovat muun muassa seuraavat:

1 Kalastelu (Phishing)-huijaukset: Tekoälyjärjestelmät voivat auttaa laatimaan uskottavampia kalasteluviestejä analysoimalla suuria määriä henkilökohtaisia tietoja ja räätälöimällä viestit tietyille kohteille, minkä myötä kalasteluviestit voivat olla aikaisempaa vakuuttavampia.

2 Syvävääreennökset (Deepfakes): Tekoälyn ohjaamat työkalut voivat luoda realistisia video- ja äänituotteita, mahdollisesti näyttäen tai saaden henkilöt näyttämään sanovan tai tekemään asioita, joita he eivät ole tehneet. Tätä voidaan käyttää kiristämiseen, disinformaatioon tai identiteettivarkauksiin.

3 Petolliset varainsiirrot: Koneoppiminen voi auttaa tunnistamaan kaavoja suurissa tietomäärissä, joita rikolliset saattavat puolestaan käyttää löytääkseen haavoittuvuuksia digitaalisissa varainsiirroissa tai optimoidakseen petollisten varainsiirtojen ajoituksen ja menetelmät niiden havaitsemisen vaikeuttamiseksi.

4 Ahdistelu ja vainoaminen: Tekoälyn ohjaamia kasvontunnistustyökaluja voidaan väärinkäyttää seuraamaan ja valvomaan henkilöitä ilman heidän tietämystään tai suostumustaan, mitä voidaan käyttää vainoamiseen tai muihin ahdistelun muotoihin.

5 Identiteettivarkaudet: Analysoimalla suuria määriä tietoja, tekoäly voi määrittää tehokkaimmat tavat tehdä identiteettivarkauksia.

6 Huumeiden ja muun laittoman aineiston jakelu: Tekoälyä voidaan käyttää analysoimaan rikoksentorjuntaviranomaisten toimintaa ja esimerkiksi arvioida, mitkä salakuljetusreitit ovat vaikeimmin havaittavissa.

7 Automatisoitu hakkerointi: Koneoppimisalgoritmeja voidaan käyttää uusien haavoittuvuuksien löytämiseen tai hyökkäysten automatisointiin, mikä mahdollistaa kyberhyökkäysten toteuttamisen aiempaa tehokkaammin.

8 Kyberkiusaaminen ja ahdistelu: Tekoälyjärjestelmät voivat luoda ja lähettää haitallisia viestejä tai sisältöä suurina määrinä, tehden kyberkiusaamiskampanjoista aiempaa laajempia ja vahingollisempia.

Toki tekoälyjärjestelmiä voidaan käyttää lukuisiin muihinkin rikollisiin tarkoituksiin, mutta edellä olevat esimerkit kuvaavat, miten tekoälyjärjestelmiä voidaan käyttää rikollisiin tarkoitusperiin.

TEKOÄLYN KÄYTTÖ RIKOSTORJUNNASSA

Tekoälyjärjestelmiä voidaan luonnollisesti käyttää myös rikostorjunnallisiin tarkoituksiin. Tällaisia tarkoituksia ovat esimerkiksi seuraavat:

1 Ennakoiva poliisitoiminta: Analysoimalla suuria tietomääriä tekoäly voi auttaa tunnistamaan potentiaalisia rikollisuuden keskittymiä tai aikoja, jolloin rikoksia on todennäköisesti tapahtumassa. Tämä mahdollistaa poliisin resurssien tehokkaamman kohdentamisen.

2 Kasvontunnistusjärjestelmät: Julkisissa tiloissa tai rajavalvonnassa käytettynä nämä järjestelmät voivat tunnistaa etsittyjä henkilöitä, kadonneita ihmisiä tai epäiltyjä reaaliajassa ja välittää tästä välittömästi tietoja viranomaisille.

3 Ampumisen havaitseminen: Tekoälyn ohjaamat järjestelmät, kuten SoundThinking (aiemmin ShotSpotter), voivat havaita ja paikantaa ampumiset reaaliajassa, auttaen poliisia reagoimaan nopeammin ampuma-aseisiin liittyviin tapahtumiin.

4 Petosten havaitseminen: Rahoituslaitokset käyttävät tekoälyjärjestelmiä havaitsemaan epätavallisia varainsiirtoja, jotka saattavat viitata petoksiin, rahanpesuun tai muihin talousrikoksiin.

5 Sosiaalisen median valvonta: Tekoälyä voidaan käyttää sosiaalisen median alustojen seurantaan erilaisten äärimmäisten käyttäytymistapojen tai laittomien toimintojen merkkien varalta.

6 Kyberturvallisuus: Tekoälyjärjestelmiä voidaan käyttää havaitsemaan kyberhyökkäysten, tunkeutumisten tai haittaohjelmatoiminnan tyypillisiä kaavoja ja käynnistämään vastatoimenpiteitä, kun epäilyttävää toiminta havaitaan.

7 Huumekaupan torjunta: Tekoälyjärjestelmät voivat analysoida kuljetusasiakirjoja ja muita vastaavia tietoja ennustaakseen ja tunnistaakseen mahdolliset huumeiden salakuljetusyritykset.

8 Videoiden ja muun aineiston analysointi: Tarkastettaessa suuria aineistomääriä, esimerkiksi valvontakameravideoita, tekoäly voi nopeasti havaita tietyt tapahtumat, esineet tai henkilöt, vähentäen huomattavasti inhimilliseen analysointiin tarvittavaa aikaa.

9 Äänentunnistus- ja profilointi: Hätäkeskuksissa tai muilla puhelinlinjoilla tekoäly voi analysoida ääniä tai lauseita havaitakseen mahdolliset poikkeavuudet, kuten toiminnan painostuksen alaisena.

10 Automatisoitu rikostutkinta: Tekoälytyökalut voivat nopeasti analysoida suuria määriä elektronista todistusaineistoa havaitakseen rikostutkinnan kannalta merkityksellisiä seikkoja.

Edellä käsiteltyjen esimerkkien kuvaamalla tavalla tekoälyjärjestelmille on ilmeisiä rikostorjunnallisia käyttökohteita. Toisaalta, kuvattujen tekniikoiden tekniikoiden lupaavuudesta huolimatta, niiden käyttämiseksi on toki huomioitava niiden käyttöön liittyvät rajoitteet erilaisten pakkokeinojen käyttämiseksi. Tämän kirjoituksen kaltaisessa yleisesityksessä tekoälyn rikostorjunnalliseen käyttöön liittyviä rajoituksia ei kuitenkaan voida tarkastella enemmin.

ESIMERKKINÄ VÄÄRENNYSRIKOLLISUUS

Lähtökohtaisesti tekoälyjärjestelmät ovat kykeneviä havaitsemaan periaatteessa missä tahansa aineistossa ilmenevät säännönmukaisuudet ja säännönmukaisuudet havaittuaan, toisintamaan niitä muutetussa muodossa kuitenkin alkuperäisen aineiston säännönmukaisuudet säilyttäen. Tämän johdosta tekoälyjärjestelmiä voidaan käyttää luomaan syvävääreennyksiksi kutsuttuja aineistoja, joissa esimerkiksi tietokoneen luoma autenttisen oloinen kuva henkilöstä esittää videolla sellaisen valheellisen sanallisen viestin, jonka väärennyksen tekijä sen tahtoo esittävän. Sama pätee tietenkin muihinkin säännönmukaisuuksiin, kuten vaikkapa ihmisen käsialaan ja sen ominaisuuksiin. Kuten rikostutkinnallisesta käsialavertailusta tiedetään, ihmisen käsialassa on lukuisia säännönmukai-suuksia, jotka tunnetaan muun muassa muotona, liikkeenä, suuntana ja tilankäyttönä, pyöreytenä, katkoina, aukkoina, riviväleinä ja vastaavina.

Hyvän esimerkin tekoälyjärjestelmän luomasta väärennöksestä tarjoaa aikoinaan The Wall Street Journalin artikkelissa ”Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case” käsitelty tapaus, jossa tekoälyjärjestlmä väärensi yhtiön toimitusjohtajan äänen, jota sittemmin hyödynnettiin perinteisen ”toimitusjohtapetoksen” välineenä siten, että yrityksen talousosastolle annettiin toimitusjohtajan äänellä virheellinen maksukehote. Tämän seurauksena yrityksen talousosasto erehdytettiin tekemään n. 200.000 euron maksusuoritus keksitylle alihankkijalle.

Toimitusjohtajapetosta koskevan esimerkin kuvaaman kaltaisia syvävääreennöksiä voidaan toki käyttää myös muihin kuin välittömiin taloudellisiin tarkoituksiin. Ilmeinen esimerkki olisi kannatuksen kannalta haitallinen syvävääreennös poliitikosta vaikkapa juuri ennen vaalipäivää, jolloin syvävääreennöksellä voitaisiin saavuttaa mahdollisesti suuriakin yhteiskunnallisia vaikutuksia.

OIKEUDELLINEN MERKITYS

Oikeudelliselta kannalta tekoälyjärjestelmien kautta toteutetut rikokset eivät lähtökohtaisesti ole ongelmallisia.

Vaikkapa tapon osalta lainsäädäntömme ei erottele sitä, kuinka tekijä surmaa uhrinsa. Oikeudellisesti sillä surmataanko rikoksen uhri teräasetta käyttäen vai ampumalla, ei ole merkitystä. Sama pätee siihen, onko petoksen erehdyttämistoimen kohteena ihminen vai tietojärjestelmä. Tältä osin laki on teknologianeutraali.

Lainsäädäntömme teknologianeutraaliudesta johtuen, tämän kirjoituksen alussa esimerkkeinä käsitellyt rikolliset tavat hyödyntää tekoälyjärjestelmiä eivät ole oikeudellinen ongelma. Tekoälyjärjestelmien vaikutus rikollisuuteen on enemmänkin tosiasiallinen, kuin oikeudellinen ongelma. Tekoälyjärjestelmät mahdollistavat useiden rikosten toteuttamisen aikaisemmasta poikkeavalla tavalla, mutta perusolemukseltaan rikokset säilyvät sellaisina kuin ne ovat aikaisemminkin olleet. Tässä suhteessa voimassa olevan lainsäädäntömme tarjoama oikeudellinen viitekehys on riittävä myös tekoälyjärjestelmillä toteutettujen rikosten sääntelemiseksi. ■

ISMO KALLIONIEMI

- ”Asianajaja Ismo Kallioniemi on tekoälyn oikeudellisiin kysymyksiin ja vaativiin oikeudenkäynteihin sekä niihin liittyviin selvityksiin erikoistunut asianajaja. Hän on tekoälyyn liittyviä oikeudellisia kysymyksiä käsittelevän “Tekoälyoikeus - Varallisuusoikeuden ja riskienhallinnan kysymyksiä”-kirjan kirjoittaja.”
- Asianajaja, osakas
- **Eversheds Asianajotoimisto Oy**

DROONIEN KASVAVA ROOLI NYKYAIKAISESSA SODANKÄYNNISSÄ JA UKRAINAN SODASSA

// Teemu Matilainen, Anton Hämelin ja Jaakko Vilander

TIIVISTELMÄ

Tämä artikkeli käsittelee lennokkien kasvavaa roolia ja niiden moninaisia vaikutuksia sodankäyntiin. Käsillä oleva tarkastelu on tehty Ukrainan sodan taustaa vasten, erityisesti 24. helmikuuta 2022 alkaen. Ukrainan sota on merkittävä esimerkki aseellisesta konfliktista, jossa miehittämättömät ilma-alukset (Unmanned Aerial Vehicles, jäljempänä droonit) on otettu strategiseen käyttöön, mikä painottaa niiden olennaista roolia nykyaikaisissa sotilaallisissa operaatioissa. Drooneja voidaan käyttää taistelukentällä monin eri tavoin, ja niiden vaikutus ylittää perinteisen sodankäynnin rajat ja rintamalinjat. Esimerkkeinä mainittakoon kriittiseen infrastruktuurin, kuten ukrainalaisiin viljavarastoihin, ja eritoten Moskovan keskustaan kohdistuneet iskut.

Mielestämme droonien tuottaman suorituskyvyn kehitys on olennaisessa määrin sidoksissa teknologiseen kehitykseen, erityisesti tekoälyn ja koneoppimisen saralla. Molemmat ovat yhä keskeisempiä drooniteknologian kehityksen kannalta. Droonien kykyjen kehittyessä ja kypsyessä myös niihin kohdistuvien vastatoimien ja -tekniikoiden jatkuva kehittely muodostaa merkittävän teknologisen innovaatio- ja tutkimusalan. Samanaikaisesti droonisodankäynnin ja elektronisen sodankäynnin (EW, Electronic Warfare) tulevaisuuden kyvyt saavat Ukrainassa tulikasteensa, mikä antaa viitteitä niiden kasvavasta roolista nykyaikaisessa sodankäynnissä. Täten Ukrainassa havaittava teknologinen dynamiikka toiminee kipinänä kehitykselle, joka tulee muovaamaan väistämättä myös tulevan sodan kuvaa.

Teknologista innostuksesta huolimatta muita, vähintään yhtä tärkeitä sotataidollisia näkökulmia ei tule jättää huomiotta. Droonisodankäyntiin liittyy nimittäin kriittisiä operatiivisia ja taktisia näkökulmia. Drooniteknologia on vasta alkutekijöissään, mutta mikäli se kyetään integroimaan osaksi muuta asevoiman käyttöä, voidaan sen avulla saavuttaa todellista ratkaisevaa vaikuttavuutta. Vaikka olemme saaneet osviittaa onnistuneesta droonisodankäynnin soveltamisesta perinteisempien joukkojen kanssa, niiden integrointi muuhun konventionaaliseen sodankäyntiin muodostaa edelleen suuren haasteen.

DROONIEN NOUSU

Vaikka Ukrainassa käytävä sota ei ole ensimmäinen kerta jolloin drooneja käytetään sodankäynnissä, ne eivät koskaan aikaisemmin ole näytelleet yhtä merkittävää roolia kuin nyt. Tämän vuoksi droonien käyttö Ukrainassa edustaa jyrkähköä muutosta sodan kuvassa. Drooneja ei ole käytetty myöskään koskaan aiemmin näin laajasti osana aseellista selkkausta. Esimerkiksi Royal United Services Institute arvioi, että Ukraina menettää noin 10 000 droonia kuukaudessa, mikä jo itsessään on merkki droonien laajamittaisesta käytöstä. Koska ilmapuolustus on molemmin puolin keskittynyt pääsääntöisesti miehitettyjen ilma-alusten torjuntaan, on miehittämättömistä järjestelmistä tullut erityisen tehokkaita. (Franke 2023, Hambling 2023).

Ukrainan sodan osapuolten lisäksi myös esimerkiksi terroristiryhmä Isis kannattajien ovat kyenneet hyödyntämään drooneja tehokkaasti osana epätavanomaisen sodankäyntinsä brutaaleja taktiikoita. Vuonna 2014, Isisin ottaessa hallintaansa Irakin suurimman kaupungin, Mosulin, se teki historiaa ensimmäisenä aseistettuja drooneja taistelussa käyttävänä terroristiorganisaationa. Räjähteillä varustetuilla drooneilla hyökättiin irakilaisia ja kaupunkia puolustavan koalition joukkoja vastaan. Iskut johtivat sekä haavoittumisiin että rintamakarkuruuteen Irakin armeijassa. Toisin sanoen drooneilla oli ilmeisiä, sekä fyysisiä että psyykkisiä seurauksia.

Isis sovelsi alun perin halpoja kaupallisia drooneja sotilaallisiin tarkoituksiin, kuten tiedusteluun ja valvontaa, mutta kehittivät niitä myöhemmin hyökkäysoperaatioihin varustamalla ne improvisoiduilla räjähteillä. Halpojen kaupallisten droonien käyttö oli pakon sanelemaa, koska siihen aikaan lähinnä suurempien valtioiden asevoimilla oli varaa tiedusteluun, valvontaan ja maalitiedusteluun (ISTAR) tarkoitettuihin aseistettuihin drooneihin. Edullisten ja muokattujen droonien käyttö Isisin sotilaallisiin tarkoituksiin johti oivalluksiin myös muiden toimijoiden keskuudessa. Näin monet sotilaalliset ja ei-sotilaalliset, valtiolliset ja ei-valtiolliset väkivaltaiset toimijat ovat alkaneet harkita tämän teollisuuden avaamia mahdollisuuksia.

Isisin kalifaatin nousun jälkeen maailman katse kiinnittyi Ukrainaan, etenkin Itä-Ukrainan Donbassiin, jossa oli käynnistynyt toinen sota. Eräs tuonaikainen innovoija oli Aerorozvidka-niminen yksikkö, joka rakentui vapaaehtoisten ja innokkaiden tietotekniikan asiantuntijoiden varaan. Ryhmä aloitti niin ikään alun perin työnsä ostamalla halpoja kaupallisia drooneja ja kehittämällä niistä sotilaallisiin tarkoituksiin sopivia. Kahden vuoden päästä, vuonna 2016, Aerorozvidka onnistui kehittämään oman räjähteitä pudottavan miehittämättömän ilma-aluksen nimeltä R18. Aerorozvidka valmistaa edelleen kyseistä droonia useita kappaleita päivässä ja jakaa ne Ukrainan asevoimien eri yksiköille (Haxhimustafa 2023). Näistä lähtökohdista syntyi Ukrainan kukoistava drooniteollisuus. Kohta vuosikymmenen käynnissä olleen sodan aikana Ukraina on tuonut suuren joukon eri lennokki- ja droonijärjestelmiä tositoimiin (ks. taulukko 1). Ukrainan tasangot näyttävät samalla toimivan sekä puolustajan että hyökkääjän drooniteknologian testikenttänä, joskin Ukraina on tähän mennessä osoittanut olevansa kilpailussa etumatkalla.

Lähteet sivulla 28

TAULUKKO 1 LUETTELO TODENNÄKÖISESTI UKRAINASSA KÄYTETYISTÄ LENNOKEISTA (TÄYDENNETTY JA VIIMEISTELTY CHAVEZ 2023, S. 8 PERUSTEELLA)

Class	Role	Russia	Ukraine
Military	Combat (UCAV)	Forpost-R Kronstadt Orion "Inokhodets" STC Orlan-10 and -30 Qods Mohajer-6 (IRN) Lastochka-M (lit. Swallow)	A1-CM Furia (lit. Fury) UA Dynamics Punisher Baykar Bayraktar TB2 (TUR)
	Reconnaissance	ZALA 421-series ENICS Eleron-3(SV) Granat-series Izhmash Tachyon Zastava	Ukrspecsystems Shark UAV DEVIRO Leleka-100, "Stork" Tupolev 143 (USSR) Skyeton ACS-3 Baykar Bayraktar Mini (TUR) AeroVironment RQ-20 Puma (US) SYPAQ Corvo PPDS (AUS)[1]
	Combat (dropping)		Ukrspecsystems PD-1 and -2 Aerorozvidka R18
	Combat (loitering)	ZALA Lancet-3(M) ZALA KUB HESA Shaheed-136 (IRN)	Bober (lit. Beaver) AeroVironment Switchblade 600 (US) AeroVironment Switchblade 300 (US) Aevex Phoenix Ghost (US) RAM II (based on Leleka) WB Electronics Warmate (POL)
Commercial	Various	DJI Mavic (CHN)	DJI Mavic (CHN) DJI Matrice M30T (CHN) Various "dronations"

1) "Pahvidrooni" jota on käytetty myös taistelutehtävissä

Maanviljelystä ja muusta raskaasta teollisuudesta tunnettu Ukraina ei ehkä ole itsestään selvä ympäristö drooni-innovaatioille. Sodan synnyttämä pakottava tarve on kuitenkin tehnyt maasta jonkinlaisen kärkikastin tuotekehityslaboratorion, joka houkuttelee tunnettuja yrityksiä myöntämään rahoitusta. Kuten Ukrainan varapääministeri Mykhailo Fedorov sanoi haastattelussa Ukrainan pääkaupungin, Kiovan toimistossaan: "Tämä on 24/7 teknologiakilpailu. Haasteena on se, että jokaisen kategorian jokaista tuotetta on muokattava päivittäin, jotta saisimme etumatkaa." Reilut 200 ukrainalaista droonien tuotantoon osallistunutta yritystä tekeekin nyt tiivistä yhteistyötä asevoimien etulinjan yksiköiden kanssa droonien kehittämiseksi, jotta niillä voitaisiin entistä tehokkaammin vakoilla ja vaikuttaa viholliseen (Hudson & Khudov 2023).

DROONIT JA NIIDEN KÄYTTÖKATEGORIAT

Drooneille löytyy monenlaista käyttöä, mutta niiden käyttö voidaan tiivistää kolmeen pääkategoriaan: kuljetus, tiedustelu ja valvonta (ISR) sekä vaikuttaminen. Sotilaskäytössä kuljetusdrooneilla kuljetetaan suhteellisen helposti kriittistä materiaalia, kuten verensiirtotarvikkeita, polttoainetta tai paristoja etäälläkin sijaitseviin paikkoihin. Koska autonomisuus on aikaisempaa huomattavasti tavallisempi piirre myös kaupallisissa laitteissa, droonit tarjoavat ei-massamaiselle täsmälogistiikalle matalariskisen ja suhteellisen helpon vaihtoehdon. Selvä epäkohta tällä hetkellä on järjestelmien vaatimaton hyötykuorma, toimintamatka ja nopeus. Kuljetusvälineenä droonien täytyy pystyä palaamaan tukikohtaan, ja silloin ihanteellinen ratkaisu on pyöriväsiipinen malli. Tämä mahdollistaa pystysuoran lentoon lähdön ja laskeutumisen (VTOL) melkein miltä tahansa alustalta, mutta samanaikaisesti se tuo mukanaan muotoiluun liittyviä rajoituksia, jotka hankaloittavat yllä mainittujen ominaisuuksien parantamista.

Valvonta ja tiedustelu ovat tavallisimpia droonien käyttöaloja. Kaikissa drooneissa on useammalla spektrillä toimivia valokuva-, video- tai muuta tietoa kerääviä sensoreita, joiden avulla joukkojen on mahdollista paikallistaa vihollisen tukikohtia, seurata joukkojen liikehdintää ja koordinoida tulenkäyttöä. Drooneissa voi olla myös signaalitiedustelusensoreita (SIGINT), erityisesti elektronisen tiedustelun sensoreita (ELINT). Yhtenä esimerkkinä joidenkin droonien tiedetään olevan varustettuja IMEI/IMSI-sieppareilla (International Mobile Equipment/Subscriber Identity), joilla voidaan matkia mobiilitukiasemaa tiedustelutarkoituksessa. Droonin hyödyt tiedustelukäytössä piilevät yksinkertaisesti siinä, että sensorin korkeus on suoraan verrannollinen sen radiohorisonttiin. Koska drooni voi viedä hyötykuormansa hyvin korkealle, kasvattaa tämä signaalitiedustelulaitteistosta saatavaa hyötyä. Sama koskee optisia sensoreita. Siten droonit tarjoavat joukoille mahdollisuuden seurata taistelukenttää kirjaimellisesti lintuperspektiivistä.

ISR-droonien käyttö on erityisen tuloksekasta Ukrainan tasankojen tapaisilla alueilla, missä kasvillisuus tai maantieteelliset esteet pienentävät suoraa näköyhteyttä verrattain vähemmän kuin muissa toimintaympäristöissä. Venäjän sota Ukrainassa onkin osoittanut, että droonit voivat olla erityisen arvokkaita tilanteissa, joissa taistelu tapahtuu juoksuhaudassa. ISR-näkökulma drooni sodankäynnissä ei kuitenkaan rajoitu pelkästään reaaliaikaisen tilannetiedon keräämiseen. Droonit voivat myös dokumentoida hyökkäyksiä, esimerkiksi vaurioarvioita tehtäessä tai informaatio-operaatioita tuettaessa. Lisäksi Ukraina on kehittänyt laiteohjelmistoja tehostaakseen tykistön paikantamiskykyä, maalinvalaisua, tiedustelua ja johtamista. Ukrainan polytekninen kehittämisohjelma on edistynyt, mutta ei kuitenkaan riittävästi täyttääkseen valtion tarpeita (Haxhimustafa 2023).

TAISTELUDROONIEN VIISI ALALAJIA

Kineettiseen vaikuttamiseen tarkoitetuissa drooneissa on kaksi keskeistä ominaisuutta: lentoaika ja uudelleenkäyttö[2]. Vaanivilla drooneilla on tarpeeksi kestävyyttä, jotta ne voivat leijailla taistelukentän yläpuolella seuraten kohteita, kun taas toiset vaikuttamiseen tarkoitetut droonit mahdollistavat vain välittömät etsi ja tuhoa -tyyppiset tehtävät. Itsemurhadroonit tuhoutuvat tavallisesti käytön jälkeen, kun taas toiset käyttävät erillistä pudotettavaa tai laukaistavaa räjähdeosaa ja sopivat siten uudelleen käytettäväksi. Vaanivat järjestelmät ovat usein sotilaskäyttöön tarkoitettuja, toisin kuin itsemurhadroonit, jotka yhä suuremmassa määrin ovat kaupallisia – joskin jako ei ole yksinomaan näin karkea. Nämä kaksi termiä eivät sulje toisiaan pois, ja vaikka niillä tarkoitetaan eri asioita, niitä käytetään paikoin synonyymeinä. Tästä nousee kolmas tärkeä kategorisoiva ominaisuus, eli kuluttajakäyttö. Tällä tarkoitetaan, onko drooni tarkoitettu erityisesti sotilaskäyttöön vai onko kyseessä kaupallinen, niin sanottu kaksoiskäyttötuote, jota voidaan siviilikäytön lisäksi soveltaa sotilaskäyttöön.

Tässä tapauksessa käytämme uudelleenkäyttöä, kestävyyttä ja kuluttajakäyttoä kineettiseen vaikuttamiseen tarkoitettujen droonien luokittelemiseksi viiteen (joskin osin päällekkäiseen ja ei-tyhjentävään) kategoriaan. Nämä ovat miehittämättömät taisteluilma-alukset (UCAV, Unmanned Combat Aerial Vehicle), vaanivat droonit (loitering drone), sotilaskäyttöiset ilmaräjähteet (Aerial Explosive Charges , AEC*), muunnellut kaupalliset droonit, joissa on ulkoinen räjähde (Modified Commercial Drones with an External Ordnance (MCD-EO*) sekä muunnellut kaupalliset droonit, joissa on itsetuhoutumismekanismi, toisin sanoen lentävät improvisoidut räjähteet (Improvised Explosive Devices, ABIEDs). Kategorisoinnissa aiemmin mainittuja käytetään yleisemmin strategisen ja operatiivisen tason tehtävissä ja tulenkäytössä, kun taas myöhempien käyttöympäristöt ovat taktisia tai pitkälti jopa taisteluteknisiä. Droonien kategorisointi sekä niiden käyttöperiaatteiden ja suorituskykyjen luokittelu saattaa edesauttaa sotilashenkilöstöä esimerkiksi uhka-arvioita tehtäessä.

[2]Lisäksi koko ja toimintakorkeus ovat muuttujia jotka tarjoavat mahdollisuuksia droonien luokkitteluun
* Nämä eivät ole aiemmin käytettyjä luokkitelutapoja, mutta ovat hyödyllisiä analysoidessa erilaisia drooneja.

TAULUKKO 2 LENNOKKIEN LUOKITTELU PERUSTUEN UUDELLEENKÄYTTÖÖMAHDOLLISUUTEEN, KESTÄVYYTEEN JA KULUTTAJAKÄYTTÖÖN.

	UCAV	Loitering drone	AEC	MCD-EO	MCD (ABIED)
Reusability	Reusable	Non-reusable	Non-reusable	Reusable	Non-reusable
Endurance	Long to medium	Long to medium	Short	Medium to short	Medium to short
Consumer-use	Non-consumer	Non-consumer	Non-consumer	Consumer	Consumer
	Strategic				Tactical

MIEHITTÄMÄTTÖMÄT TAISTELUILMA-ALUKSET

UCAV-drooni, joka tunnetaan myös taistelulennokkina, arkikielellä usein lyhennettynä muotoon lennokki tai drooni, on miehittämätön ilma-alus, jota käytetään 1) tiedusteluun, valvontaan ja maalitiedusteluun, mutta myös 2) taistelutehtävissä kineettiseen vaikuttamiseen. Taistelulennokissa on olemuksellisesti asejärjestelmiä, kuten ohjus, esimerkiksi panssarintorjuntaohjus, ja/tai ulkoisiin ripustimiin kiinnitettyjä pommeja. Tällaisia lennokkeja ohjaa reaaliajassa tavallisesti ihminen, mutta niissä voi olla myös kyky autonomiseen käyttöön. Poiketen valvontaa ja tiedustelua suorittavista miehittämättömistä ilma-aluksista taistelulennokkeja käytetään sekä lennokki-iskuihin että taistelukentän tiedustelutehtäviin.

Koska lennättäjä ohjaa tämäntyyppistä ilma-alusta ohjauslaitteella erillisestä lennättämispaikasta tarvittaessa vaikka satelliittiyhteydellä, ilma-aluksessa ei tarvita lentäjälle välttämättömiä ohjausjärjestelmiä, ja näin ollen miehittämätön ilma-alus on miehitettyä ilma-alusta kevyempi ja pienempi. Tämä vähentää myös tarvetta huomioida inhimillisiä tarpeita kuten väsymystä, nälkää tai kuumuutta. Useilla mailla on käytössään kotimaisia taistelulennokkeja, ja sitäkin useampi maa on tuonut markkinoille tai kehittävät parhaillaan sellaisia. Huomattavia tuottajamaita ovat Yhdysvallat, Turkki, Israel ja Kiina.

Erityisesti Turkki tavoittelee suurvallan asemaa miehittämättömien järjestelmien tuottajana ja on haastamassa tässä ominaisuudessa Kiinaa, joka tuottaa tällä hetkellä eniten lennokkeja maailmassa. Teknologisesti hienostuneet taistelulennokit, kuten MAM-L-pienoisohjuksilla varustettu turkkilainen Baykar Bayraktar TB2, ovat nousseet kansakunnan laajaan tietoisuuteen viimeistään Ukrainan sodan aikana. Bayraktar TB2 on kuitenkin osoittanut kyvykkyytensä jo huomattavasti ennen Ukrainan sotaa, muun muassa Syyriassa tehdyissä operaatioissa, missä se tuhosi kenties vastoin yleisiä odotuksia Pantsir-S1- ja 9K330 Tor -ilmapuolustusjärjestelmiä sekä Vuoristo-Karabahissa, jossa sen avulla hävitettiin valtavia määriä armenialaisia panssarivaunuja, panssaroituja ajoneuvoja sekä tykkejä. (Cannon 2022)

Lähteet sivulla 28

Bayraktar on kuitenkin saavuttanut rajansa Ukrainassa. Siinä missä droonit vastasivat yli 70 prosentista Armenian raskaan kaluston menetyksistä Vuoristo-Karabahin sodassa 2020, josta Bayraktar TB2:n osuus oli jopa 63,4 prosenttiyksikköä, Ukrainassa Bayraktar TB2 on vastannut vain alle prosentista Venäjän raskaan kaluston tappioista. Täten järjestelmän rooli on kutistunut ISR-lennokin tasolle sodan jatkuessa. Tämä johtuu todennäköisesti Venäjän huomattavista lennokintorjuntakyvyistä (Nersisyan & Moore 2023). Lisäksi vain pieni prosenttiosuus Bayraktarin tuhoamasta kalustosta on ollut taistelupanssarivaunuja, jotka ovat osoittautuneet sitkeiksi drooneja vastaan. (Oryx 2022a)

Venäjän tärkeimmät taistelulennokkimallit ovat Orion sekä Forpost-R, joka on lisensoitu kopio Israelin Aerospace Industriesin (IAI) valmistamasta Searcher-lennokista. Yleisesti voidaan sanoa, että taistelulennokeihin liittyvä kehitystyö Venäjällä on pysähtynyt, sillä maassa on perinteisesti keskitytty taisteluhelikoptereiden käyttöön ja kehittämisen. Venäläisellekin liukuhihnalle ilmestyy kuitenkin jatkuvasti uusia droonimalleja, etenkin Ukrainan sodan myötä. (Oryx 2022c). Ottaen huomioon Venäjän viimeaikaiset vastoinkäymiset esimerkiksi korkean teknologian ohjusten ja lentokoneiden kehitystyössä, ei kuitenkaan kannata pidättää hengitystä odottaessa Venäjältä joukoittain uusia ja operatiiviseen käyttöön tarkoitettuja taistelulennokkeja.

VAANIVAT LENNOKIT

Vaaniva lennokki on ilma-ase, jossa on sisäänrakennettu panos (taistelukärki) ja joka voi vaania (odottaa passiivisena) maalialueen läheisyydessä, kunnes maali on paikannettu. Vaaniva lennokki hyökkää maalia kohti törmäämällä siihen. Vaanivien lennokkien avulla voidaan lyhentää reaktioaikaa maaleihin, jotka ovat näkyvissä vain ajoittain, sen sijaan, että lähelle maalialuetta sijoitettaisiin arvokkaita laukaisualustoja. Kyseiset lennokit antavat myös mahdollisuuden valikoida maaleja, koska iskua voidaan muuttaa lennon aikana tai se voidaan keskeyttää kokonaan.

Vaanivat lennokit asemoituvat risteilyohjusten ja taistelulennokkien välimaastosta. Vaanivilla lennokeilla on yhteisiä ominaisuuksia molempien kanssa, paikaten myös kummankin puutteita. Risteilyohjuksista ne eroavat siinä, että ne on tarkoitettu vaanimaan maalialueen läheisyydessä suhteellisen kauan ja taistelulennokeista siten, että vaanivan lennokin on tarkoitus tuhoutua hyökkäyksessä sisäänrakennettua taistelukärkeä hyödyntäen. Siten vaanivat järjestelmät ovat tavallaan ei-perinteisiä pitkän kantaman aseita. Kun niiden käyttöä arvioidaan Ukrainan sodan lukumäärien valossa, on itse asiassa mahdollista, että Venäjän kaukovaikuttamisen painopiste on siirtynyt risteilyohjuksista pitkän kantaman omaaviin vaaniviin lennokkeihin.

Iranilaisvalmisteinen Shahed-136 on näistä pitkän kantaman vaanivista aseista ylivoimaisesti suosituin. Se voi tunkeutua oletettavasti satojen kilometrien syvyyteen ja vaania selustassa vielä määrätyn ajan. Shahed-järjestelmät sisältävät myös huomattavan määrän räjähdysainetta. Lisäksi ne voivat valaista oman maalinsa, lentää maalia kohti ja räjähtää maaliin osuttaessa pitkälti ohjuksen tavoin (Business Insider 2023). Varsinaisen uhan muodostaa kuitenkin sen valtavan pitkä toimintamatka, jonka kerrotaan olevan yli 1 000 kilometriä. Syyskuusta 2022 lähtien Moskovan joukot ovatkin käyttäneet näitä edullisten risteilyohjusten tavoin terrorisoidakseen kaupunkeja joka puolella Ukrainaa. Usein niillä on hyökätty maan energiaverkostoihin tai siviili-infrastruktuuriin.

Keskipitkän kantaman drooneista Venäjän vaaniva lennokki Lancet-3M on niin ikään osoittautunut hyvin tehokkaaksi Ukrainassa (Nersisyan & Moore 2023). Sen 40 kilometrin pituisen toimintamatkan ansiosta on ollut mahdollista lamauttaa ja tuhota erityyppistä pitkälle kehittynyttä länsimaista kalustoa, kaukana Ukrainan rintamalla – joskin tässäkään tapauksessa ei ole kyetty tuhoamaan kovin suuressa määrin ukrainalaisia panssarivaunuja. Lennokin dokumentoitu ja vahvistettu osumatarkkuus on lähteiden (Oryxin) mukaan ollut 73,4 %, mikä tarkoittaa 113 osumaa ja 41 harhaiskua.

Vastaavasti myös Ukraina on niittänyt menestystä omien vaanivien järjestelmiensä kanssa. Näistä kenties huomattavin saavutus on ollut vaikuttaminen viiteen hävittäjään, kahteen Pantsir-S1-ilmatorjuntajärjestelmään sekä S-300-ilmatorjuntaohjusjärjestelmän tutkiin Kurskin lentokentällä (Shahskova 2023). Ottaen huomioon, että iskussa käytetty SYPAQ Corvo maksaa noin 3 500 Yhdysvaltain dollaria ja että hävittäjät arvioidaan kymmenien miljoonien arvoisiksi, isku on osoitus resurssien äärimmäisen taloudellisesta ja tehokkaasta käytöstä. Vaanivien järjestelmien opportunistisemmastakin taloudellisesta hyötykäytöstä on viitteitä, sillä eräässä tapauksessa ukrainalainen lennokki oli lähellä osua venäläiseen Ka-52-taisteluhelikopteriin kesken lennon.

Vaikka AEC-järjestelmät eivät ole varsinaisia vaanivia drooneja, edustavat ne silti omaa rajattua osa-aluettaan droonien kirjossa. AEC:t, kuten vasta markkinoille tullut Insta Steel Eagle, erovat vaanivista lennokeista siinä, että ne perustuvat suunnattuun räjähdys- ja sirpalevaikutukseen. Ne muistuttavat näin ollen jalkaväkimiinoja tai -panoksia, sen sijaan että törmäisivät kohteeseen ja räjähtäisivät osuessaan. Lisäksi niiden toimintamatka on

varsin vaatimaton. Toimintamatkaan liittyvien varjopuolten vuoksi AEC:n kyvyt saadaan parhaiten käyttöön käyttämällä niitä joukkueen tai komppanian puolustustaistelussa ja ensi kädessä vihollisen elävää voimaa vastaan.

KAUPALLISET MUUNNELLUT DROONIT

Asevoimat ovat jo jonkin aikaa käyttäneet erilaisia kaupallisia tai kuluttajakäyttöön tarkoitettuja, vaihtelevalla itseohjautuvuudella varustettuja drooneja. Pienehköt ohjelmalliset muutokset droonien perusjärjestelmiin (toisin sanoen käyttöjärjestelmiin) mahdollistavat sen, että niillä voidaan pudottaa erilaisia räjähteitä. Tämä kehitys on ollut erityisen tunnusomaista Ukrainassa. Kranaatteja pudottavat nelikopterit (quadcopters) ovat itse asiassa kenties kaikkein kuvaavampaa aineistoa Ukrainassa käytävästä sodasta. Teknologian kehittyessä Ukrainan sodan molemmat osapuolet ovat alkaneet ottaa käyttöön tuhansia kaupallisia kilpadrooneja, joissa on joko ulkoinen ammus (MCD-EO) tai omatekoiset taistelukärjet (ABIED).

Ulkoisella ammuksella varustettu MCD on tavallisesti nelikopteri, koska se pystyy pudottamaan räjähteen lähes pystysuoraan alaspäin, mikä helpottaa tähtäämistä. Niiden alhainen lentokorkeus ja nopeus tekevät niistä kuitenkin alttiita maaleja jopa käsiaseiden tulelle. Tämä on tilanne etenkin suuren hyötykuorman omaavilla malleilla. Ammus voi parhaimmassa tapauksessa painaa useita kiloja. Sama koskee ABIED-malleja. Joissakin tapauksissa ukrainalaiset ovat liittäneet drooneihin jopa 7,5 kilogramman räjähdysainemäärällä varustettuja PM-62-panssarimiinoja, jotka räjäytetään heitinkranaattien iskusytyttimillä.

ABIED-drooni sen sijaan on alun perin kaupallinen versio itsetuhoutuvasta droonista. Toisin sanoen drooni itsessään toimii taistelukärkenä, joka ohjataan suoraan maaliin. ABIED:t hyötyvät siksi suuremmasta nopeudestaan, eikä niiden tarvitse jäädä leijumaan. Tämän tuloksena ABIED-aseessa tulisi mieluiten olla kiinteät siivet. Järjestelmän asevaikutus perustuu tavallisesti painevaikutukseen ja sirpaloitumiseen, mutta niissä voi myös olla suunnattu vaikutus kohteesta riippuen. Suunnattu vaikutus pienentää hyötykuorman painoa, aiheuttaen suuremman vaikutuksen kohteeseen pienemmällä räjähdemäärällä. ABIED on kuitenkin maassakin ollessaan vaarallinen. On tärkeää, ettei koskaan lähesty alas pudotettua ABIED-asetta. Ne ovat erittäin vaarallisia, ellei niitä käsitellä oikein.

MCD-drooneissa on tiettyjä heikkoja puolia. Ensinnäkin niiden vaimean räjähdysvoiman ja olemattoman panssarinläpäisykyvyn vuoksi niiden pääasiallinen käyttötarkoitus on elävä voima sekä tietyin varauksin ei-panssaroidut kohteet. Lisäksi niiden sensoreiden laatu saattaa vaihdella. Parhaimmillaan jotkut droonit voivat olla varustettuja lämpö- tai pimeäkameralla, joiden avulla ne voivat operoida huonossakin valaistuksessa. Vallitsevat olosuhteet rajoittavat kuitenkin usein kaupallisten droonien käyttöä. Viimeisenä asiana niiden turvattomuus elektronisen tiedustelun, elektronisen vaikuttamisen tai kyberturvallisuuden näkökulmasta tekevät monista drooneista käyttökelvottomia kansallisvaltiotasoista vastustajaa vastaan.

Puolisotilaalliset joukot, rikollisjoukot ja erilaiset terroristiorganisaatiot käyttävät kuitenkin usein kaupallisia, muunneltuja ja omatekoisia asejärjestelmiä sisältäviä drooneja – valitettavan usein tappavalla tehokkuudella. Tämän tapaiset rikolliset käyttävät tyypillisesti drooneja staattisiin kohteisiin, kuten tukikohtiin, joukkojen lähtöalueisiin tai -asemiin sekä kiinteisiin fasiliteetteihin. Kaupalliset droonit ovat kuitenkin tulleet kiinteästi mukaan myös tavanomaiseen sodankäyntiin. Ukrainassa käytävän sodan erityispiirteisiin kuuluvat kaupallisten droonien runsas käyttö niin taistelu- kuin tiedustelutarkoituksiin. Lisäksi uusi trendi Ukrainassa on ollut FPV (First Person View) -droonien mukaantuonti. Niissä kameran tuottama kuva välittyy suoraan operaattorille silmälasien tavoin kasvoille puettavan näyttöpäätteen kautta. (Nersisyan & Moore 2023).

DROONIEN KÄYTÖN TOISSIJAINEN VAIKUTUS

Droonien käyttö ei kuitenkaan rajoitu pelkästään välittömään vaikutukseen. On viitteitä siitä, että droonit, yhdistettyinä niin kutsuttuun parviälyyn, ovat kuormittaneet Venäjän ilmavalvontaa ja rajoittaneet sen kykyä havaita esimerkiksi pitkän kantaman ohjuksia tai lennokkeja. Potentiaalisiin tapauksiin luetaan muun muassa ohjusristeilijä Moskvan upottaminen 2022 ja isku Venäjän merivoimien tukikohtaan Sevastopolissa 2023. Drooneja voitaisiin myös käyttää valemaalien tavoin arvokkaimpien resurssien, kuten tavanomaisten hävittäjien, suojelemiseksi.

Droonien kyky uhata vihollisen selustaa ilmasta, sitoo myös elintärkeitä ilmapuolustuskykyjä alueelta, joka vastaa vihollisen lennokkikaluston enimmäistoimintamatkaa. Lisäksi suuri joukko matalamalla lentäviä ja alemmalla tutkapoikkipinta-alalla varustettuna drooneja, yhdistettynä tavanomaisen ilma-aluskaluston käyttöön, pakottaa vastustajan valvomaan yhä laajempaa ilmatilan osaa. Täten Ukrainan kyky uhata Moskovaa lennokeilla eturintamasta aina Kremliin asti on itsessään voimatekijä, joka pakottaa Venäjän hajaanuuttamaan ilmapuolustuksen kykyjään suuremmalle ilmatilan osalle sekä maantieteelliselle alueelle. Tästä seuraa, että

Lähteet sivulla 28

esimerkiksi arvokas lentokalusto on sijoitettava kauemmaksi eturintamalta, jotta se välttyisi joutumasta Ukrainan lennokkiarmadan tähtäimiin.

Se tosiasia, että useat lennokit pystyvät lävistämään suojakerroksia ja vaikuttamaan Moskvan kaltaiseen kohteeseen on todiste sekä lennokkien tehokkuudesta että Venäjän ilmapuolustuksen heikkoudesta. Suureksi osaksi S-400-järjestelmästä riippuvaisen Venäjän sisämaan ilmapuolustuksen haittapuoli on, että se on luotu vastaamaan ulkopuolelta suuntautuvaan ydinhyökkäykseen. Näin Venäjän ilmapuolustukseen jää aukkoja, jotka ovat pienempien, maan rajojen sisäpuolelta tai rajan läheisyydestä laukaistujen lennokkien mentäviä. Valtava näytös Ukrainan lennokkikyvystä oli sen samanaikainen isku useampaan kohteeseen, mukaan lukien Pihkovaan ja Moskovaan, elokuussa 2023. Isku vaurioitti ainakin neljää Iljushin-76-kuljetuskonetta (Jeskanen 2023). Mutta vaikka Ukraina on niittänyt merkittävää taktista menestystä, pelkät drooni-iskut eivät sellaisenaan riitä varmistamaan strategista voittoa.

Vaikka drooni olisikin mahdollista paikallistaa, siihen vaikuttaminen on aivan toinen asia. Alkeellisten lennokkien tuhoaminen ohjusjärjestelmillä on tuskin kustannustehokasta, koska siihen käytettävät ohjukset voivat olla huomattavan paljon arvokkaampia kuin itse maali. Tästä johtuen kineettisten tai sirpaloituvien ammusten käyttö on taloudellisesta näkökulmasta kannattavampaa. Esimerkkinä tällaisesta voisi olla ajoneuvoasenteisen Slinger 160-lennokintorjuntajärjestelmän toimittaminen Ukrainaan. Järjestelmän tutka löytää jopa 35 senttimetrin kokoiset kohteet yli kilometrin etäisyydeltä ja sen 30 millimetrin konetykki takaa tulen vaikuttavuuden (Perttula 2023). Ukrainan sodan alkuvaiheiden jälkeen markkinoille tulleet SHORAD (Short Range Air Defense) -järjestelmät ovat myös sodan edetessä onnistuneet eliminoimaan enenevissä määrin drooneja (Kallberg 2022).

Ukraina on myös hankkinut useita Shahed Hunter -nimellä tunnettua lennokintorjuntajärjestelmiä. Nimi viittaa Venäjän käyttämiin iranilaisvalmisteisiin lennokeihin. Shahed Hunter vaikuttaa häiritsemällä tutka- ja komentosignaalia, ja voi havaita vihollisen lennokin jopa 40 kilometrin etäisyydeltä kohteesta. Se kaappaa vihollisen droonit hyödyntäen omia pienoisdrooneja sekä niiden laukaisemaa raskasta verkkoa. Verkko vangitsee kohdedroonin ja laukaisee laskuvarjon, joka hiljentää sen vauhtia ja mahdollistaa pehmeän laskeutumisen niin turvallisesti ettei se räjähdä tai vaurioidu. Shahed Hunter-järjestelmiä käytetään jo Ukrainassa esimerkiksi kriittisten infran, kuten energialaitosten suojana. (United24 2023; Business Insider 2023).

Kustannustehokkaimmat aseet drooneja vastaan ovat kuitenkin ei-kineettiset aseet. Yksi mahdollinen vaihtoehto voisi olla suunnatun energian aseet (DEW, Directed-Energy Weapons). Näiden aseiden ideana on suunnata määritettyyn maaliin tarvittava määrä energiaa, kuten laser-, mikroaalto- tai hiukkassäteilyä, sen vahingoittamiseksi. DEW-aseilla vaikuttaminen voi siten olla edullisempaa ja välittömämpää, mikä helpottaa maalin määritystä ja vaikutuksen saavuttamista. Tällainen tuote on esimerkiksi Raytheon 50 kW High Energy Laser (HEL), jolla on kerrottu olevan kyky tehdä muut ilmassa liikkuvat kohteet, kuten droonit vaarattomiksi (Osborn, 2023). DEW-teknologia on kuitenkin vasta kehitysvaiheessa. Elektronisen sodan kyvykkyydet, joita Venäjän asevoimilla on suhteellisen paljon, ovat sitä vastoin näyttäneet kykynsä vastata droonien muodostamaan kasvavaan ilmauhkaan.

ELEKTRONINEN SODANKÄYNTI DROONEJA VASTAAN

Elektroninen sodankäynti (EW) viittaa tiedusteluun ja järjestelmien häiritsemiseen sähkömagneettisen säteilyn avulla sekä niiden vastatoimiin. Käytännössä kaikki joukot käyttävät nykyään, kaluston tasosta tai sotilasjoukon taktiikasta riippumatta, komentojärjestelmiä ja asejärjestelmiä, joista purkautuu jonkinlaista sähkömagneettista säteilyä. Tästä syystä elektronisen sodankäynnin joukot ovat nykyaikaisen sodankäynnin leimallinen ja erottamaton osa. Elektroninen tiedustelu ja valvonta paljastavat vihollisjoukot ja asejärjestelmät sekä maalla, merellä että ilmassa (The Finnish Defence Forces 2022).

Vaikka useimmat droonien sensorit ovat passiivisia, droonit itsessään edellyttävät aktiivista yhteyttä operaattoriin, jotta niitä voitaisiin käyttää reaaliajassa. Tämä asettaa sekä droonit että maa-asemat alttiiksi elektroniselle tiedustelulle. Tällaisessa tilanteessa henkilöstöön kohdistuvaan uhkaan voidaan vaikuttaa erottamalla käyttöliittymä, siis operaattori, säteilevästä antennista. Elektronista sodankäyntiä voidaan myös käyttää droonin kommunikointi-, navigaatio- ja ohjausjärjestelmien häirintään. Droonit toimivat eri signaalien, mukaan lukien radiotaajuuksien, GNSS-paikannuksen ja muiden langattomien teknologioiden varassa. Erilaisilla elektronisen sodankäynnin tekniikoilla voidaan häiritä näitä signaaleja, mikä vaikeuttaa tai tekee droonille mahdottomaksi ottaa vastaan komentoja, säilyttää ohjattavuus tai navigoida tarkasti. (Noreika 2023; Kallberg 2022)

Häirintä on aina ollut ongelmana erityisesti nelikoptereita käytettäessä, koska kuluttajakäyttöön tarkoitettujen droonien lennättäjät käyttävät tunnettuja, lakiin perustuvia taajuuksia. Tässä tapauksessa häirintää suorittavan ei tarvitse tehdä muuta kuin kohdistaa riittävän kovaa melua, eli haittalähetettä, lennättäjän käyttämälle taajuudelle. Tästä seuraa, että droonin hallintasignaali hukkuu niin sanottuun staattiseen lumimyrskyyn ja lakkaa vastaamasta. Sodan kehittyessä esimerkiksi Venäjä on

ottanut käyttöön yhä tehokkaampia ja hienostuneempia häirintälaitteita häiritäkseen tykistötulta ohjaavia drooneja ja pudottaakseen pommeja juoksuhautoihin (Hambling 2023). Perinteinen tapa suojautua häirinnältä on ollut taajuushyppely. Tällöin häiritsijän tulee kasvattaa häirittävää taajuusaluetta, jotta se ylittäisi hyötysignaalin.

Sodan aikana osapuolet ovat myös alkaneet käyttää hyväksi tekoälyyn (AI) perustuvia ratkaisuja. Tekoälyyn perustuvat ohjelmistot voivat esimerkiksi vakauttaa droonia elektronisesta häirinnästä riippumatta ja pitää sen lukittuna etukäteen määriteltyyn kohteeseen, vaikka kohde liikkuisi. Tätä voidaan pitää varteenotettavana parannuksena verrattuna nykyisiin drooneihin, jotka seuraavat liikkuessaan tiettyjä koordinaatteja. Tekoälyyn perustuvat ohjelmistot merkitsisivät päivitystä erityisesti Ukrainan edullisille mutta samalla häirinnälle alttiille FPV-drooneille. Jos drooni menettää yhteyden lennättäjäänsä ja kohde on lukittu, tekoäly ottaa droonin ohjaukseensa. Droonin sensorit voivat tunnistaa kohteen fyysiset piirteet ja säätää droonien lentoreitin sitä mukaa, kun kohdetta lähestytään. Tästä huolimatta tarvitaan edelleen inhimillinen päätöksentekijä, jotta voidaan tehdä päätös siitä, mihin kohteeseen isketään. (Hudson & Khudov 2023)

Tekoäly näyttelee jo nyt avainroolia lisättäessä miehittämättömien järjestelmien autonomiaa koneoppimisen ja massadatan avulla. Autonomia parantaa droonien toiminnallisuuksia, mikä kasvattaa tähystyksen ja ilmaiskujen tarkkuutta. Tekoälyn ohjaamat droonit eivät kuitenkaan ole yhtään paremmat kuin ne algoritmit joiden perusteella ne toimivat tai niille syötetyt datamassat, joten jää nähtäväksi, jääkö niiden kasvanut arvo lyhyellä aikavälillä vain taktiselle tasolle (Rogers & Kunertova 2022, s. 8). Autonomiset droonit mahdollistavat myös parviälyn hyödyntämisen, joskin alkeellisen sellaisen. Tämä tarkoittaa sitä, että häirintää suorittavien järjestelmien pitäisi levittyä laajalle alueelle tehokkaan torjunnan aikaansaamiseksi. Täten häirintälaitteet eivät sellaisenaan pysty yksin poistamaan edullisten, mahdollisesti parvelevien autonomisten järjestelmien ja pienten droonien muodostamaa uhkaa (Kunertova 2022, s. 4).

DROONISODAT

Innovaatiot droonien käytössä Ukrainana sodan aikana antavat ymmärtää että, aseistettujen droonien julkisuuskuvaan olisi tulossa uusia ulottuvuuksia. Droonien pääasiassa kaupallinen alkuperä ja yksityisen sektorin mukaantulo ovat kaksi varsin merkittävää tekijää, jotka muovaavat drooneista käytävää keskustelua. Vapaaehtoiset toimijat ja erilaiset rahoituskampanjat ovat niin ikään tehostaneet siviilien osallistumista sotilaalliseen ja väkivaltaiseen toimintaan, joka on perinteisesti ollut valtion monopolin hallitsemaa. Sekä Venäjän että Ukrainan joukot ovat saaneet osan lennokkikyvyistään paikallisväestöön kuuluvilta lennokkiharrastajilta. Rahaa hävittäjien hankintaan keräävät hyväntekeväisyyskampanjat kuten esimerkiksi Ukraina Prytula Foundation ja Come Back Alive, jotka voivat olla suoraan yhteydessä aseteollisuuteen. Tämä yksityisen sektorin tuki normalisoi osittain droonien käytön räjähteiden kuljetukseen. (Kunertova 2022 s. 3).

Edellä mainittu kuvastaa käynnissä olevaa muutosta, jossa väestö tuottaa asevoimille teknologiseen kärkikastiin kuuluvaa täydentävää materiaalia eikä päinvastoin. Drooni on nyt yksi monien laitteiden joukossa (siinä missä älypuhelimet, ajoneuvot, tietokoneet jne.), joita kansalainen voi lahjoittaa sotaa käyvän kansakunnan käyttöön. Voi vain arvailla minkälaisia mahdollisuuksia tämä luo maille, joilla on laajat reservijoukot, kuten Suomi ja Israel.

Tätä tarkoitusta varten Ukraina on muun muassa toimeenpannut Army of Drones -ohjelman, jonka tavoitteena on optimoida Kiovan tiedustelu- ja taisteludroonien käyttöä tasapainottamaan Venäjän ilma- ja tykistöaseiden etulyöntiasemaa. Ohjelma on auttanut yksityisiä yrityksiä kouluttamaan jo yli 10 000 lennättäjää kuluneen vuoden aikana ja tavoitteena on kouluttaa vielä toiset 10 000 seuraavan kuuden kuukauden aikana. Heinäkuussa 2022 Ukrainian World Congress (UWC) ja Ukrainan digitaalisesta siirtymästä vastaava ministeriö allekirjoittivat yhteistyömuistion tukeakseen Army of Drones -projektin UNITED24-joukkorahoitusta. Ohjelmaan sisältyy lennokkien hankinta, toimittaminen, ylläpito ja korvaaminen sekä lennättäjien kouluttaminen (Ukrainian World Congress 2022). Ukrainan presidentti Zelenskyi sanoi 5. toukokuuta 2023, UNITED24-projektin vuosipäivänä pitämässään puheessa, että rahoitusprojekti oli jo tuottanut yli 330 miljoonaa Yhdysvaltain dollaria yli sadasta maasta (United24 2023; Business Insider 2023).

Ikään kuin alleviivatakseen nykyistä droonisodankäynnin aikaansaamaa muutosta, Ukrainan taivaalla ja ilmasodankäynnissä koittaa uusi aika: drooni vastaan drooni -kamppailut, joissa erilaiset järjestelmät ovat taistelussa toisiaan vastaan. Tällaisissa 2000-luvun kaartotaisteluissa ei käytetä luoteja, ohjuksia tai pommeja, vaan enenevässä määrin ei-kineettisiä vaikuttamisen menetelmiä sekä puhdasta törmäystekniikkaa. Tiedustelevia harrastajatason nelikoptereita törmää toisiinsa armottomassa ilmassa tapahtuvassa härkätaistelussa. Toisissa kohtaamisissa pitkälle kehittyneet ilma-alukset käyttävät edistynyttä tutkaa – jota tukee tekoäly ja viimeisimmät lentokone-elektroniikan saavutukset - laukaistakseen vihollisen drooneja sieppaavia verkkoja. (Sherman 2023).

Lähteet sivulla 28

YHTEENVETO

Viime vuosina Ukrainasta on tullut tärkeä maa droonien kehityksen ja valmistuksen kannalta. Kumppanuusohjelmat sekä yksityisen ja julkisen sektorin tehokas yhteistyö ovat johtaneet lennokkien kehittelyyn tai uusiokäyttöön sotilaallista tarkoitusta varten. Sodan synnyttämä innovaatiopaine, ukrainalaisten kekseliäisyys ja mahdollisuudet tehdä yhteistyötä monien asiantuntijoiden kanssa ovat auttaneet luomaan hyvän perustan kotimaiselle puolustusteollisuudelle. Tulevaisuudessa Ukrainan lennokkiteollisuus tulee todennäköisesti olemaan vakavasti otettava kansainvälinen toimija, joka pystyy viemään taistelussa testattuja järjestelmiä muihin maihin (Franke 2023).

Asia, joka askarruttaa sotilasalan asiantuntijoita ja suunnittelualan sotilaita on, kuinka tehokasta droonisodankäynti todellisuudessa on. Tällä hetkellä kysymys jää todennäköisesti ratkaisematta. Vaikka dataa, jopa avointa dataa onnistuneista lennokki-iskuista on runsaasti saatavilla, ei ole esimerkiksi luotettavaa tai tarkkaa tietoa siitä, mikä on onnistuneiden drooni-iskujen määrä suhteessa suunniteltuihin drooni-iskuihin. Droonien tehokkuus vaikuttaisi kuitenkin olevan täysin tilannesidonnaista. Siihen vaikuttavat monet välilliset tekijät, kuten joukon kokoonpano ja joukkorakenne, konfliktin luonne, maasto ja osapuolten käytettävissä olevat resurssit. Esimerkiksi Ukrainan sodan erityispiirteet, kuten korkea teknologia verrattuna Vuoristo-Karabahiin, voivat selittää sotien väliset erot (Cannon 2023).

Ukrainan sota kuitenkin todistaa, että drooneista on tullut näkymättömämpiä, nopeampia, pienempiä, kuolettavampia ja helppokäyttöisempiä ja että käyttäjäkunta on suurempi. Niitä myös käytetään yhä nerokkaammin tavoin. Sota on osoittanut, että drooneilla voidaan

vaikuttaa eri tavoin riippuen käytettävästä alustasta ja sen hyötykuormasta. Siinä missä isoilla ohjusta kuljettavilla drooneilla voi olla merkittäviäkin vaikutuksia, erityisesti ilmaherruustilanteissa, pienet droonit ovat osoittautuneet kriittisiksi kun kyse on jalkaväen, johtamisen ja tykistön maalinosoituksen tilannetietoisuudesta. Lisäksi ilmasta pudotettavien ammusten käyttö merkitsee haastavaa ja vähemmän helposti puolustettavissa olevaa tapaa kuljettaa räjähteistä koostuvaa hyötykuormaa (Kunertova 2022, s. 2).

Sodan synnyttämä innovaatiopaine tulee myös näyttämään, mitä teknologian kehityksen avulla voidaan saavuttaa droonioperaatioden avulla tulevina vuosina. Joka tapauksessa on selvää, että elektroninen sodankäynti ja droonisodankäynti näyttelevät ja tulevat näyttelemään yhä suurempaa roolia nykyaikaisessa sodankäynnissä – kuten Ukraina on todistanut. On täysin mahdollista, että drooni ja elektronisen sodankäynnin kyvyt synnyttävät uuden kissa ja hiiri -leikin, joka muistuttaa panssareiden ja panssarintorjunta-aseiden välistä klassista kaksinkamppailua. Käynnissä oleva sota Ukrainassa on nopeuttanut ja tulee edelleen nopeuttamaan näiden kahden aspektin kehitystyötä ja siten osaltaan muovaamaan tulevaisuuden sotia. Sodan kuvaa ei tule kuitenkaan muuttamaan mikään yksi droonien kategoria. Erityyppisiä drooneja syntyy jatkuvasti, ja tämän seurauksena tulevaisuuden sodissa tullaan todennäköisesti näkemään järjestelmiä, jotka vaihtelevat kaupallisista pienoisdrooneista täysin autonomisiin hävittäjiin.

Droonisodankäynti on kuitenkin yhä suurelta osin lapsenkengissä. Vaikka droonit tuovat mukanaan etuja erilaisiin nykyaikaisiin aseellisiin konflikteihin, on aivan eri asia muuttaa teknologista tai jopa taktista kekseliäisyyttä käytännön operatiiviseksi menestykseksi. Ukrainan voiton avain piilee edelleen hyökkäystaisteluun kykenevissä taistelupanssarivaunuissa, ei drooneissa. Vaikka ilmoilla on viitteitä lennokkien ja maavoiman onnistuneesta yhdistämisestä esimerkiksi Vuoristo-Karabahissa, on kuitenkin pitkälti ratkaisematon kysymys, kuinka droonit integroidaan puolustushaarat ja aselajit yhdistävään liikesodankäyntiin – erityisesti jos ei ole ilmaherruutta. Näin ollen droonit myötävaikuttavat sodankäynnin kehittymiseen, ei niinkään sodankäynnin vallankumoukseen. Lennokit voivat kuitenkin tuoda merkittävää hyötyä, jos niillä onnistutaan tehokkaasti tukemaan liikesodankäyntiin kykeneviä joukkoja. Näin menetellen lennokit voivat tuottaa tärkeää lähi-ilmatukea (Close Air Support, CAS), valvontaa tai tiedustelua eri muodoissa. Tältä osin lennokit edustavat eräänlaista maavoimien ilmailun uutta tulemista.

”Uusi maavoimien ilmailu” ei kuitenkaan ole ainoa mittasuhteita ja näkökulmia lennokkisodankäynnin kehitystasoon luova havainto. Itse asiassa lennokkien käyttö Ukrainassa muistuttaa monessa suhteessa lentokoneiden mukaantuloa sodankäyntiin ensimmäisen maailmansodan aikana. Niitä käytetään ensisijaisesti tiedustelutoimintaan, aivan kuten kaksitasokoneita käytettiin 1900-luvun alussa. Vaikuttamisen kannalta niiden käyttö rajoittuu perustehtäviin, kuten iskusytyttimillä varustettujen kranaattien pudottamiseen, samoin kuin suuressa sodassa. Jopa alkuperäiset itsemurha- eli kamikaze-koneet olivat saman aikakauden tuotteita, vaikkakin ne otettiin käyttöön vasta toisen maailmansodan aikana. Maailmansotien ajan koneet muistuttavat drooneja myös psykologisten vaikutusten osalta. Ukrainan aroilla syöksypommittajien kauhua herättävä ulvonta on vain vaihtunut kaupallisten nelikoptereiden pahaenteiseen kehräykseen.■

TEEMU MATILAINEN, ANTON HÄMELIN, JAAKKO VILANDER

Artikkelin kirjoittajilla on vuosien kokemus turvallisuusalan eri tehtävistä ja rooleista. He ovat toimineet Suomen lisäksi myös kansainvälisissä tehtävissä.

LÄHTEET

Ali Haxhimustafa 2023. From ISIS to Ukraine: The Evolution of Drones' Use On The Battlefield. Published 31.7.2023. https://www.thedefencehorizon.org/amp/evolution-drones-ukraine-isis.

Alius Noreika 2023, Ukraine is Seeking Electronic Warfare Equipment to Counter Lancet Drones. Technilogy org. Published 3.7.2023. https://www.technology.org/2023/07/03/ukraine-electronic-warfare-to-counter-lancet-drones/.

Business Insider 2023. A Ukrainian donation drive built an 'Army of Drones' and picked up an unusual system called a 'Shahed Hunter' for Kyiv's forces. Published 11.5.2023. https://www.businessinsider.com/ukraine-army-of-drones-shahed-hunters-donation-push-2023- 5?r=US&IR=T.

Brendon J. Cannon 2022. Turkey's rise as a drone power: trial by fire. Defense and Security Analysis, pp. 1–20. DOI: 10.1080/14751798.2022.2068562

David Hambling 2023, New Report: Ukraine Drone Losses Are '10,000 Per Month'. Forbes. Published 22.5.2023. https://www.forbes.com/sites/davidhambling/2023/05/22/ukraine-drones-losses-are-10000-per-month/.

Dominika Kunertova 2022. The Ukraine Drone Effect on European Militaries. Center for Security Studies (CSS). Published 2022. https://css.ethz.ch/content/dam/ethz/special/interest/gess/cis/center-for-securities-studies/pdfs/PP10-15_2022-EN.pdf.

Jan Kallberg. Drones Will not LiberateUkraine – but Tanks Will. Center for European Policy Analysis (CEPA). https://cepa.org/drones-will-not-liberate-ukraine-but-tanks-will/.

James Rogers & Dominika Kunertova 2022. The Vulnerabilities of the Drone Age Established Threats and Emerging Issues out to 2035. Center for war studies. Published 2022. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO_VDA_Policy_Report.pdf.

Jason Sherman 2023. Drone-on-Drone Combat in Ukraine Marks a New Era of Aerial Warfare. Scientific American. Published 3.4.2023. https://www.scientificamerican.com/article/drone-on-drone-combat-in-ukraine-marks-a-new-era-of-aerial-warfare/.

Jenni Jeskanen 1.9.2023. Venäjän ilma-torjunta "ei pysty selviämään tehtävistään edes hyvällä tasolla", sanoo sotilas-asiantuntija. Ulkomaat, Helsingin Sanomat. https://www.hs.fi/ulkomaat/art-2000009820525.html.

John Hudson and Kostiantyn Khudov 2023. The war in Ukraine is spurring a revolution in drone warfare using AI. The Washington post. Published 26.6.2023. https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/.

Kerry Chávez 2023. Learning on the Fly: Drones in the Russian-Ukrainian War. Arms Control Today, January-February. https://www.armscontrol.org/act/2023-01/features/learning-fly-drones-russian-ukrainian-war.

Kris Osborne 28.8.2023. Laser-Armed, Drone Killing Strykers Bring Army New Attack Tactics. Warrior Maven, Center for Military Modernization. https://warriormaven.com/land/laser-armed-drone-killing-strykers-bring-army-new-attack-tactics.

Leonid Nersisyan & Cerwyn Moore 2023. Comparing Russo-Ukrainian war and Second Karabakh war: performance and failures. In Pentti Forsström (ed.). Russia's war on Ukraine – Strategic and operational designs and implementation, p. 78-86. Department of Warfare, National Defence University. Tampere: Punamusta. (Unpublished)

Maryna Shashkova 27.8.2023. Kyiv Claims 5 Russian Fighter Jets Hit in Drone Attack on Kursk Airfield. Kyiv Post. https://www.kyivpost.com/post/20973.

Oryx 25.3.2022a. Defending Ukraine - Listing Russian Military Equipment Destroyed By Bayraktar TB2s. Oryx Spioenkop. https://www.oryxspioenkop.com/2022/02/defending-ukraine-listing-russian-army.html.

Oryx 25.11.2022b. Hit or Miss: The Russian Loitering Munition Kill List. Oryx Spioenkop. https://www.oryxspioenkop.com/2022/11/hit-or-miss-russian-loitering-munition.html.

Oryx 7.4.2022c. Nascent Capabilities: Russian Armed Drones Over Ukraine. Oryx Spioenkop. https://www.oryxspioenkop.com/2022/04/nascent-capabilities-russian-armed.html

The Finnish Defence forces 2022. Elektroninen sodankäynti suojaa, paljastaa ja hyökkää keihään kärjessä. Published 5.5.2022. https://maavoimat.fi/-/elektroninen-sodankaynti-suojaa-paljastaa-ja-hyokkaa-keihaan-karjessa-.

Ukrainian World Congress 2022. UWC IS PARTNERING WITH THE UKRAINIAN MINISTRY OF DIGITAL TRANSFORMATION TO BUILD AN ARMY OF DRONES FOR UKRAINE. Published 2022. https://www.ukrainianworldcongress.org/united24/.

Ulrike Franke 2023. Drones in Ukraine and beyond: Everything you need to know. The European Council on Foreign Relations (ECFR). Published 11.8.2023. https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/.

United24 2023. 'SHAHED HUNTER': FIRST ANTI-DRONE SYSTEMS NOW INSTALLED AT CRITICAL INFRASTRUCTURE FACILITIES. Published 27.01.2023. https://u24.gov.ua/news/shahed_hunters_defenders.

Pentti Perttula 8.9.2023. Tämä ilmatorjuntatykki osuu drooniin yhdellä laukauksella. Verkkouutiset. https://www.verkkouutiset.fi/a/tama-ilmatorjuntatykki-osuu-drooniin-yhdella-laukauksella/?ref=rns_tw#1e9.

Cyberwatch Finland

YRITYKSEN HENKILÖSTÖN KYBEROSAAMINEN KEHITTYY CYBER MASTER -KURSSEILLA

// Pertti Kuokkanen

Viimeisen kahden vuoden aikana yhteistoiminnassa MIF:n kanssa on koulutettu yli 120 kyberosaajaa yrityksiin ja julkishallinnon organisaatioihin. Koulutus on tullut tarpeeseen ja sen on todettu vastaavan siihen haasteeseen, mitä nykyinen toimintaympäristön jatkuva muutos on vaatinut. Koulutusmuotona on ollut yli vuoden kestävät erikoisammattitutkinnot.

KYBERTOIMINTAYMPÄRISTÖN KIIHTYVÄ MUUTOS ASETTAA HAASTEITA OSAAMISELLE

Toimintaympäristön muutos haastaa yritykset ja julkishallinnon organisaatiot niin toiminnallisesti kuin muodollisesti kehittämään henkilöstönsä osaamista. Erilaisiin kyberturvallisuuden uhkatekijöihin vastaaminen, toiminnan jatkuvuuden hallinta ja yhteiskunnan sääntely synnyttävät uusia tarpeita ja vaatimuksia ydintoiminnan turvalliselle toteuttamiselle ja siten myös henkilöstön kouluttamiselle.

Verkostomaisen digitalisaation laajentuessa, palvelujen ja tavaroiden ostajat tulevat yhä voimakkaammin ilmaisemaan huolensa siitä, lisääkö yhteistyö yrityksen tai palveluorganisaation kanssa heidän kyberriskiään. Tämän lisäksi taloudellinen huolenaihe liittyy mahdollisiin suuriin vahinkoihin, jotka voivat johtua tietoverkkovirheistä. Rikolliset kohdistavat yhä useammin toimintansa suuria yrityksiä vastaan pienempien kumppanien kautta. Toimitusketjujen tarkastelu on nousemassa merkittäväksi riskien hallinnan osatekijäksi.

Yhteiskunnan ohjauksessa esimerkiksi EU:n CER- ja NIS2-direktiivit tuovat uusia velvoitteita yrityksien ja organisaatioiden toiminnalle. CER-direktiivi määrittää yhdenmukaiset vähimmäisvaatimukset, joilla voidaan turvata keskeisten palvelujen tarjonta EU:n sisämarkkinoilla ja parantaa kriittisten toimijoiden häiriönsietokykyä. Se korostaa riskiperusteista lähestymistapaa toimintavarmuuden takaamiseksi monenlaisia uhkia vastaan: luonnonuhat, terrori-iskut, sisäpiiriuhat tai sabotaasi, joilla kaikilla voi olla kyberturvallisuus tai muu siihen liittyvä osatekijä. NIS2-direktiivi tavoitteena on parantaa kyberturvallisuuden perustasoa EU:n alueella ja varmistaa kriittisten toimijoiden jatkuvuus. Se sisältää vaatimuksia mm. toimintaperiaatteille, tapausten käsittelyprosesseille, toimitusketjujen turvallisuudelle sekä kyberhygienian peruskäytännöille ja kyberturvallisuuskoulutukselle.

Osaamisen näkökulmasta yrityksien ja organisaatioiden on määritettävä henkilöstönsä kyberosaamisen pätevyysvaatimukset, varmistettava niiden saavutettavuus soveltuvan koulutuksen, harjoittelun tai kokemuksen perusteella sekä hankittava vaadittava pätevyys ja arvioitava tehtyjen toimenpiteiden vaikuttavuutta. Tästä kaikesta on säilytettävä asianmukaista dokumentoitua tietoa näyttönä pätevyydestä. Käytännön eri keinoja pätevyyden saamiseksi voivat olla esimerkiksi nykyisten työntekijöiden kouluttaminen, mentorointi, siirtäminen toisiin tehtäviin tai pätevien henkilöiden palkkaaminen tai vuokraaminen.

YRITYKSEN KOULUTUSOHJELMAT VASTAAMAAN VAATIMUKSIA

Ajantasainen koulutusohjelma varmistaa säännöllisen tietojen ja taitojen ylläpidon ja ottaa huomioon muuttuvan toimintaympäristön asettamat vaatimukset. Koulutuksen tasoa tulee arvioida säännöllisillä harjoituksilla tai testeillä.

Yrityksen kyberosaamisen tilaa voi alustavasti hahmotella vastaamalla esimerkiksi seuraaviin yksinkertaisiin kysymyksiin:

- Saavatko yrityksen uudet työntekijät riittävän perehdytyskoulutuksen yrityksen digitalisaatioon ja sen turvallisuuteen?
- Onko yrityksellä säännöllinen koulutus- ja harjoitusohjelma, jolla heidän tietoja ja taitoja päivitetään viimeaikaisista uhkista ja suuntauksista (tilanneymmärryksen kehittyminen)?
- Täyttääkö henkilöstömme osaaminen NIS2-direktiivin vaatimukset?

Osaamisen rakentaminen ja sen ajantasainen toteuttaminen perustuu yrityksen tai organisaation toiminnallisiin tavoitteisiin. Koulutuksen järjestämiseen liittyen on hyvä läpikäydä huolellisesti esimerkiksi seuraava varmistettavien asioiden lista:

- Yrityksen tavoitteiden saavuttamiseen ja riskien hallitsemiseen tarvittavat taidot on määritetty.
- Työtehtävien vaatimat valmiudet ja osaamistasot on määritetty koulutussuunnittelun pohjaksi.
- Työntekijöille on annettava osaaminen sietokyvystä oman työtehtävän mukaisesti.
- Koulutusohjelma varmistaa säännöllisen tietojen ja taitojen ylläpidon ottaen huomioon muuttuvan toimintaympäristön asettamat vaatimukset.
- Koulutusohjelma sisältää yrityksen jatkuvuuden toimintamallit, sekä teknologioiden käytön ja poikkeustilanteiden hallinnan toimintamallit.
- Koulutuksen taso arvioidaan säännöllisillä harjoituksilla tai testeillä.
- Yrityksen johto ymmärtää osaamisen kehittämisen osaksi kybervastuullisuutta.

> **Koko ala on todella mielenkiintoinen ja aion jatkaa oman tietämyksen parantamista ja kehitystä. Verkkohaavoittuvuus ja tietovuodot on aina ajankohtaisia työelämässä ja näitä olisi hyvä käydä läpi vuosittain.**

Opiskelijan palaute keväällä 2023 päättyneeltä kurssilta.

CYBER MASTER – KOULUTUS KEHITTÄÄ KYBEROSAAMISTA.

Cyber Master –koulutuksen tavoitteena on laajentaa ymmärrystä kyberturvallisuuden moniulotteisista uhkista ja keinoista, jotta voidaan turvata organisaation toimintaa ja hallita mahdollisia eteen tulevia häiriötilanteita. Koulutus on jaettu kahdelle eri tasolle seuraavasti:

1. Tuotekehitystyön erikoisammattitutkinto / Cyber Master on tarkoitettu henkilöille, joilla on mahdollisuus kehittää organisaation kyberturvaa ja viedä ideoita eteenpäin sovellettavaksi käytännön tasolle. Koulutus on tarkoitettu ensisijaisesti suunnittelijoille ja palvelumuotoilijoille.

2. Johtamisen ja yritysjohtamisen erikoisammattitutkinto / Cyber Master on tarkoitettu henkilöille, joilla on mahdollisuus päättää ja/tai kehittää organisaation kyberturvaa ja viedä ideoita eteenpäin sovellettavaksi. Koulutus on tarkoitettu ensisijaisesti organisaation johtoryhmässä toimiville henkilöille.

Kyberturvallisuus rakentuu kyvystä ymmärtää, tunnistaa ja lisätä yrityksen tai organisaation kyberturvallisuutta ja henkilöstön osaamista. Ohjelman aikana kehitetään ja rakennetaan yrityksen kykyä ja kestävyyttä kohdata kyberturvallisuuden kasvat haasteet toimintaympäristön analyysin, riskienhallinnan ja jatkuvuuden suunnittelun toimenpitein.

Kyberturvallisuus on paljon enemmän kuin turvaamista ja suojaamista; se on havainnointia, ennakointia, kykyä reagointiin ja oikea-aikaista viestintää kyberoperaatioiden ennaltaehkäisemiseksi. Kyberturvallisuuden kehitystyönä kasvatetaan koko yrityksen ennakoivaa kykyä sietää poikkeus- ja häiriötekijöitä sekä hallita kriisitilanteita. Koulutusohjelman avulla koulutuksen opit viedään suoraan käytäntöön. Koulutuksen lopputuloksen jalkauttaminen viimeistään kurssin lopussa ja myös sen jälkeen on erittäin tärkeää yrityksen kyberkulttuurin rakentamisen näkökulmasta. Tässä yhteydessä opiskelijan mentorin rooli korostuu merkittävästi. Kurssin kehittämispanos kohdistuu suoraan yrityksen tai organisaation toimintaan. Koulutuksen aikana opiskelija suorittaa erikoisammattitutkinnon.

OPETUSKOKONAISUUDET

Kurssi on rakennettu sisällöllisesti neljän työpajan periaatteelle seuraavasti:

Työpaja 1: Opettaa tarvittavat käsitteet ja antaa perusteet niille toimenpiteille, joilla kurssilainen kykenee selvittämään oman organisaation nykytilan, toimintavalmiuden ja jatkuvan parantamisen kyvyn sekä luomaan pohjaa kehittämistyölle. Tuloksena syntyy toimintaympäristöanalyysi.
Työpaja 2: Tavoitteena on kehittää omia tietoturvataitoja ja selvittää organisaation kyky havaita, estää, hillitä ja reagoida muuttuviin kyberuhkiin, sekä laatia organisaation/vastuualueen kyberriskianalyysi.
Työpaja 3: Organisaation kyberturvallisuusstrategian/toimintamallin rakenne ja luonnos - visio ja kehittämistoimet. Kyberturvallisuuden ja kehittämisen edellyttämät jatkotoimet organisaation tavoitteiden ja vision pohjalta. Liittymäpinnat organisaation liiketoimintastrategiaan ja varautumissuunnitelmaan.
Työpaja 4: Operatiivisen tason suunnitelma kiireellisimmistä toimenpiteistä kyberturvallisuuden parantamiseksi. Näillä toimenpiteillä luodaan edellytykset strategian toimeenpanolle ja ne ovat osa jatkuvuuden hallinnan toimenpiteitä. Sisältää myös viestinnän, kyberhygienian ja jatkuvan parantamisen osiot.

Jokainen työpaja koostuu 2–3 opetusjaksosta, joissa annetaan perusteet valittuihin aihealueisiin, itseopiskelumateriaalia sekä harjoitustehtäviä. Tehtävät tehdään yrityksen tai organisaation omassa toimintaympäristössä. Näillä töillä pyritään maksimoimaan niin opiskelijan kuin yrityksen saama hyöty. Osa jaksoista toteutetaan lähipäivinä ja osa etäopetuksena.

Tämä koulutusohjelma on myös räätälöitävissä lyhyemmiksi yritys- tai organisaatiokohtaisiksi ohjelmiksi. Ohjelman modulaarinen rakenne ja sisältö voidaan muokata asiakkaan tarpeita vastaavaksi ja laajuudelta sopivaksi.

> **Ylipäätään tuotekehitystyön tarve tietoturvassa ja yleisessä käytössä. Osata tuotteistaa tarpeet johtoryhmälle hyvin, jotta avautuu kukkaron nyörit tärkeisiin asioihin!**

Opiskelijan palaute keväällä 2023 päättyneeltä kurssilta.

OSAAMISEN TAVOITTEENA JOUSTAVA JA KEHITTYVÄ KYBERKULTTUURI

On yrityksen etu, että yrityksessä on ja kehittyy hyvä kyberkulttuuri koostuen digitalisaatioon liitetyistä toimintatavoista, työmoraalista, yhteisistä säännöistä ja ehdoista sekä työntekijöiden välisistä vuorovaikutustavoista. Vain osaamisen kehittämisen ja jalkauttamisen keinoin voidaan päästä tähän tavoitteeseen.

Arvoisa lukija, kun olet jo näin pitkälle päässyt, niin kysy vielä itseltäsi:

- Onko varmistettu, että työntekijät kokevat voivansa vaikuttaa yrityksen digitalisaatioon, kyberturvallisuuteen ja että heillä on mahdollisuus tuoda esiin näihin liittyviä epäkohtia?
- Ovatko hallitus ja johtoryhmä (jäsenet) sitoutuneet kyberturvallisuutta koskeviin päätöksiin, noudattavatko itse niitä ja tuovatko he esiin tehottomia käytäntöjä yhteistyössä työntekijöiden kanssa?
- Toimiiko johto vastuullisesti ja järjestääkö työntekijöille asianmukaisen kyberkoulutuksen?
- Onko varmistettu, että organisaatiossa puhutaan avoimesti ja myönteisesti henkilöstölle siitä, miksi kyberturvallisuus on tärkeää?

Jos olosi on tämän jälkeen vielä epävarma, niin varmista seuraavat asiat:

- Yrityksen hyvä turvallisuuskulttuuri koostuu digitalisaatioon liitetyistä toimintatavoista, työmoraalista, yhteisistä säännöistä ja ehdoista sekä työntekijöiden välisistä vuorovaikutustavoista.
- Digitalisaation ja kyberturvallisuuden tuomat muutokset on käsitelty hyvässä hengessä, käsittäen yhteiset tavoitteet, työtehtävät ja vastuualueet, sekä pelisäännöt ja toimintatavat.
- Yrityksen henkilöstö
  - tietää, miten ja kenelle epäkohdista tai poikkeamista voi raportoida. He myös kokevat olevansa kannustettuja raportointiin.
  - ei pelkää negatiivisia seurauksia raportoidessaan epäkohdista tai poikkeamista.
  - kokee voivansa kyseenalaistaa toimintamalleja rakentavalla tavalla, hyödynnetään henkilöstön kyvyt, taidot ja luovuus.
  - kokee, että näkemyksiä hyödynnetään aidosti kyberturvallisuuskäytäntöjen suunnittelussa ja muutoksessa.
  - ymmärtää kyberturvallisuuden tärkeyden ja merkityksen organisaatiolle. Otetaan huomioon oppiva ja kehittyvä työyhteisö, kannustetaan aktiivisuuteen ja sujuvaan yhteistyöhön.
- Epäonnistumisten sijaan raportoinnissa ja sisäisessä viestinnässä keskitytään onnistumisiin (kerrotaan esimerkiksi moniko raportoi tietojenkalastelusähköposteista, eikä sitä moniko lankesi niihin).
- Annetaan aikaa sosiaaliselle kanssakäymiselle.

Jos tehtävien läpikäynnin tuloksena syntyi toiminnallisia poikkeamia, niin kehitä yrityksesi tai organisaatiosi kyberosaamista kaikilla tasoilla ja kaikissa tehtävärooleissa. Tarvittaessa ole yhteydessä, me järjestämme asiaan koulutusta ja tuemme sinua. ■

Kysy lisää koulutuksista:
myynti@cyberwatchfinland.fi
Puhelin:
Ake +358 45 343 6500

Ehkä yksi oleellinen koulutuksen kautta tullut oivallus on, kuinka johto asiat näkevät ja kuinka näkemyksiin voidaan vaikuttaa ja kehitystarinat-päivänä asiasta tuli myös hyvää keskustelua sekä lisää näkemystä.

Opiskelijan palaute keväällä 2023 päättyneeltä kurssilta.

PERTTI KUOKKANEN

- Vanhempi neuvonantaja, pääkouluttaja
- Eversti evp.
- Valtiotieteen tohtori
- **Cyberwatch Oy**

UKRAINAN SODASSA ON KYSYMYS MYÖS INFORMAATIOTILAN JA KYBERULOTTUVUUDEN HERRUUDESTA

// Josef Schroefl ja Soenke Marahrens

TAUSTAA

Aamulla 24. helmikuuta 2022[1] Venäjän aloittama hyökkäys Ukrainaa vastaan herätti meidät yhtäkkiä todellisuuteen, jota on vaikea ymmärtää. Siitä lähtien erityisesti suuremmat länsimaat ovat joutuneet hylkäämään sen itsepetoksen, jota he ovat siihen asti viljelleet. Venäjän presidentti on aina kiistänyt murhat, myrkytykset ja monet länsimaiseen arvojärjestelmäämme kohdistuneet hyökkäykset, jolloin hän on käyttänyt "totuutta" katalana hämäysstrategianaan. Venäjän "totuus" aina johdonmukaisesti viestinyt saman sisällön: Venäjä on aina syytön kaikkeen, josta länsi sitä syyttää. Putinin tehtävänä on ollut ainoastaan pyrkimys pelastaa Venäjä ja venäläiset länsimaiselta tuholta, koska länsi haluaa tuhota Venäjän.

Venäjän hyökkäystä Ukrainaan ei pysty ymmärtämään ilman Putinin historian tulkintaa. Hänen mielestään Venäjä on joutunut puolustautumaan lännen vihollisuuksia vastaan jo yli 1000 vuoden ajan ja on sitä kautta muodostunut vahvaksi valtioksi - viimeksi toisessa maailmansodassa. Putin syyttää länttä siitä, että se on haastanut Venäjän suurvalta-aseman vuodesta 1990[2] lähtien.

Tavoitteidensa saavuttamiseksi Putin on aktivoinut vanhat KGB:n aikaiset menetelmät. "Vanhoja" Neuvostoliiton työkaluja olivat mm.:

- Dis- ja misinformaatio: Valeuutisia on levitettävä kaikilla mahdollisilla kanavilla. Viime vuosina Kreml on rakentanut omaa mediateollisuutta RT:n ja Sputnikin kanssa vaikuttaakseen mielipideilmastoon ulkomailla. Neuvostoliiton ja nykyisen venäläisen disinformaation erikoisuus on todellisten tai historiallisten tapahtumien uudelleenkirjoittaminen.
- Sabotaasi: Tavoitteena on hämmentää vihollista ja horjuttaa väestön luottamusta hallituksensa kykyyn taata elämän perustarpeet. Valtiolliset toimijat tekevät tiivistä yhteistyötä järjestäytyneen rikollisuuden kanssa, mikä on Venäjän sodankäynnin tunnettu ominaisuus[3].

Toisin kuin neuvostoaikana, Putinin käytössä on kuitenkin uusia "digitaalisia kiihdyttäjiä" Internetin ja sosiaalisten verkostojen muodossa. Tämä tarkoittaa sitä, että tänä aikana venäläiset käyvät yhä intensiivisempää kyber- ja informaatiosotaa, mukaan lukien psykologisen ja ideologisen materiaalin systemaattinen jakelu. Tämä on luonteeltaan provosoivaa, osittain totuudenmukaista, osittain valheellista tietoa, joihin yhdistettynä hyökkäykset kriittistä infrastruktuuria kohtaan voivat aiheuttaa massapsykoosia, epätoivoa ja tuhon tunnelmaa sekä heikentää luottamusta hallitukseen ja asevoimiin.

KYBER- JA INFORMAATIOSODAN KESKINÄISRIIPPUVUUS

Kybersota on toisaalta sotilaallinen konflikti virtuaalitilassa, kyberavaruudessa ja sen ympärillä, ja se sisältää kaikki tietoturvatoimenpiteet sekä kaikki toimet suvereniteettia vaarantavien kyberhyökkäysten torjumiseksi. Suvereniteetin vaarantamista voivat olla kyberhyökkäykset sotilaallisiin ICT-järjestelmiin sekä kriittiseen infrastruktuuriin ja/tai perusoikeudellisiin instituutioihin.

Toisaalta kybersodalla tarkoitetaan informaatioajan huipputeknologisia sodan muotoja, jotka perustuvat lähes kaikkien siviili- ja sotilasalueiden laajaan tietokoneistamiseen, digitalisointiin ja verkostoitumiseen. Tämä tarkoittaa, että taistelua oikeasta tiedosta - mukaan lukien informaatiosota - käydään pääasiassa kyberavaruudessa. Informaatiosodan ilmenemismuodot tunnetaan syvävääränöksinä, dis- ja misinformaatio-operaatioina sekä psykologisina operaatioina (PsyOps). Kaikkea tätä voidaan häiritä sähkömagneettisen spektrin avulla, kuten esimerkiksi hyökkäämällä satelliittijärjestelmiin.

Kyberulottuvuus tarjoaa myös puolustusvaihtoehtoja eli väärää ja/tai dis- ja misinformaatiota voidaan torjua Internetin avulla. Yhdysvaltain CyberCommandin johtaja kenraali Nakasone erinomaisesti osoitti, miten tämä onnistui viime vuoden Yhdysvaltain vaaleissa, kymmeniä sosiaalisen median tilejä suljettiin sotilaallisen Computer Network Attacks:n[4] avulla.

Sama näkyy myös tämänhetkisessä sodassa Ukrainassa: Molemmat osapuolet käyttävät yleisiä kyberhyökkäyksiä, kuten kiristyshaittaohjelmia, palvelunestohyökkäyksiä, kryptosovelluksia, haittaohjelmia, nollapäivähaavoittuvuuksia, tietokoneviruksia sekä SCADA-hyökkäyksiä keinoina vaikuttaa viholliseen ja vahinkojen aiheuttamiseen tai hyökkäysten torjuntaan.

Ymmärtääkseen miten Venäjän kansalaiset näkevät maailman, on osattava kieltä ja katsottava Venäjän televisiota. Kremlin kontrolli läpäisee Venäjän television kaikki osat. Päiväsaikaan ei ole enää nähtävissä saippuasarjoja, vaan kovaa syvälle painautuvaa propagandaa Venäjän roolista maailmassa, liberaalin mutta heikon lännen muodostamasta uhasta ja Ukrainan "vapauttamisesta" natseista. Käytetty retoriikka on kovaa: "Banderan eliitti on likvidoitava; heitä ei voi uudelleen kouluttaa. Heitä tukeneen yhteiskunnallisen sakan on koettava sodan kauhut, otettava oppia ja maksettava syyllisyydestään.[5]" Tämä oli ja on edelleen yksi Venäjän tärkeimmistä viesteistä ja palvelee sen narratiivia "uhanalaisista arvoista".

Samaa retoriikkaa käytetään myös, kun halutaan kritisoida muitakin edistyksellisiä länsimaisia arvoja, kuten naisten oikeuksia, etnisiä ja uskonnollisia vähemmistöjä tai LGBTQ-yhteisöä. Kremlin-myönteisten

disinformaatiokanavien mukaan länsimaat tuhoavat perusarvot rappion, feminismin ja liiallisen poliittisen korrektiuden kautta. Venäjä taas näyttäytyy Kremlin viestinnässä säädyllisyyden ja moraalin vartijana[6].

Venäjä on yrittänyt rajoittaa Ukrainan kyberulottuvuutta tuhoamalla heidän palvelin- ja mobiiliyhteyksiään, kuten 3G/4G-verkoa, häiritsemällä heidän kansallisia komento- ja ohjausjärjestelmiään sekä pyrkimällä vaikuttamaan siihen, ettei Ukraina pysty vastaamaan venäläiseen dis- ja misinformaatioon.

Yksi Venäjän propagandatoiminnan päätarkoituksista onkin "dehumanisoida" eli epäinhimillistää toinen osapuoli. Kohdennetut vaikuttamiskeinot ovat osa psykologista sodankäyntiä. Nämä narratiivit[7] määrittävät, miten ja mitä lännen pitäisi ajatella kriisistä/sodasta ja miten tätä tulisi tuomita. Monet ovat yhtä mieltä siitä, että sodassa Ukrainan kanssa, Venäjä, haastaa sodan sääntöjä uusilla ja odottamattomilla tavoilla[8].

”Kyberulottuvuus” on uusi taistelukenttä ja sen keinot, kuten informaatio-operaatiot, voivat olla yhtä kovia voimia kuin sotilaalliset keinot. Tästä ei kuitenkaan Nato ja EU sekä niiden jäsenmaat ole täysin samaa mieltä. Onko kyse yhdestä uudesta sodan ulottuvuudesta vai onko parempi tarkastella näitä taistelukenttiä erillisinä[9].

Kuitenkin on selvää, että sähkömagneettinen spektri, informaatio- ja kyberulottuvuus sijaitsevat informaatioympäristön fyysisten ulottuvuuksien sisällä, ja niitä voidaan käyttää sodankäynnin yhtenä ulottuvuutena, jotka ovat vastaavia ja samanlaisia kuin maa-, ilma-, meri- ja avaruusulottuvuudet.

Näitä ulottuvuuksia voidaan pitää samanarvoisina. Hyökkäykset informaatio- tai sähkömagneettiseen ulottuvuuteen eivät voi onnistua yhtä hyvin ilman kyberulottuvuuden käyttöä[10]. Tämän yhteyden voi myös tiivistää vertauskuvaan: se on kuin kierreputki, jossa vesi virtaa. Kierteet ovat sähkömagneettinen spektri, putki on kyberympäristö ja vesi edustaa siinä virtaavaa tietoa[11]. Sähkömagneettista spektriä ei näin ollen voida täysin erottaa kyber- ja informaatioulottuvuudesta.

ELEKTRONINEN SODANKÄYNTI

Käynnissä on näkymätön taistelu radiotaajuuksien herruudesta. Molemmat osapuolet yrittävät estää vastustajan radio- ja tutkajärjestelmiä toimimasta. Etu on kuitenkin ollut Ukrainalla, koska se on muun muassa tehnyt kyberhyökkäyksillä toimintakyvyttömäksi venäläisiä drooneja, jotka ovat esiintyneet venäläisinä hävittäjinä vääriä tunnisteita käyttäen. Joissakin tapauksissa ukrainalaiset ovat jopa pystyneet ottamaan droonit hallintaansa[12].

Mutta miksi ja miten sähkömagneettinen spektri ja Internet Ukrainassa ovat edelleen toiminnassa - eikä Venäjä ole tuhonnut niitä?

Ensinnäkin - Starlink, yhdysvaltalaisamerikkalaisen liikemiehen Elon Muskin yritys, joka tarjoaa Internet-yhteyden satelliittiverkkonsa kautta, on ollut hyödyllinen. Ukrainalla on tällä hetkellä käytössä useita tuhansia Starlink-päätelaitteita paikallisen matkapuhelinverkon tukemiseksi ja ylläpitämiseksi. Elon Musk esitti äskettäin julkisesti ajatuksen järjestelmän sammuttamisesta. Hän julkaisi Twitterissä myös rauhansuunnitelman, joka on varmasti otettu ilolla vastaan Moskovassa. Rauhansuunnitelmassa Musk ehdotti, että Krimin pitäisi pysyä Venäjällä (Muskin mukaan siirto oli alun perinkin Hrustsovin vika) ja, että Donbassin kansan pitäisi äänestää, kuuluvatko he mieluummin Venäjään vai Ukrainaan. Joitakin päiviä myöhemmin Musk pyörsi puheensa ja Starlink-satelliittiverkko toimii edelleen Muskin rahoittamana[13].

Toiseksi hyökkäyspäivänä (24. helmikuuta) kolme kauan suunniteltua keskeistä päätöstä astui voimaan:

1. Ukrainan telealan sääntelyviranomainen (NKRZI) oli myöntänyt ukrainalaisille operaattoreille lisää 3G- ja 4G-taajuusalueita. Taajuuksien lisääntyminen merkitsi sitä, että koko maa hyötyi tästä lisäkapasiteetista, erityisesti ensimmäisen pakolaissaallon aikana.
2. Ukrainan matkapuhelinoperaattorit ja teleyhtiöt päättivät olla jäädyttämättä käyttäjien liittymiä, vaikka niiden saldo loppuisi. Tämä tarkoitti, että kaikki sotilaat (mutta myös pakolaiset ja väestö ylipäätään) ovat pystyneet kommunikoimaan, esimerkiksi perheidensä kanssa.
3. Kaikki ukrainalaiset matkapuhelinoperaattorit ja NKRZI keskeyttivät Venäjältä ja Valko-Venäjältä saapuvat verkkovierailut. Tämä tarkoitti sitä, että Venäjän ja Valko-Venäjän matkaviestinverkkoja ei voitu enää käyttää verkkovierailuihin.

Nämä ovat keskeisiä syitä, miksi Venäjä ei ole pystynyt lamauttamaan Ukrainan matkapuhelinverkkoa ja internetiä hakkeroinnilla tai pommituksilla. Toisaalta myös venäläiset sotilaat tarvitsevat sitä viestintäänsä! Älypuhelimia löytyy kaikilta sotilailta. Mutta matkapuhelimet pingaavat signaaleja lähimpään radiomastoon, jolloin sekä Ukraina että Venäjä voivat seurata vihollisjoukkojen liikkeitä. Tässä tapauksessa Ukrainalla on etulyöntiasema, koska se omistaa alueen, jolla tämä radioliikenne tapahtuu, ja sillä on keinot analysoida saatua dataa[14].

On tärkeää mainita, millä sodankäynnin alueella Venäjä onnistui, ainakin aluksi. Nimittäin elektronisen sodankäynnin alalla. Euroopan turvallisuus- ja yhteistyöjärjestö Etyj havaitsi ja raportoi jo vuoden 2020 lopulla, että elektronisen sodankäynnin järjestelmien

Lähteet sivulla 39

käyttöönotto Venäjän miehittämässä Donbassissa lisääntyi merkittävästi. Kesti maaliskuun 2022 puoliväliin asti, ennen kuin Venäjän armeija sai valmistelunsa päätökseen ja alkoi erittäin onnistuneesti häiritä ukrainalaisten droonien toimintaa. Erityisesti sodan alussa Ukraina toivoi, että droonit antaisivat heille edun tiedustelussa, jotta he voisivat käyttää omaa tykistöään paremmin Venäjän paljon suurempaa arsenaalia vastaan[15].

Kaiken tämän lisäksi Nato on toimittanut Ukrainan asevoimille droonihäirintälaitteita. Häirintälaitteet ovat osa kattavaa Naton tukipakettia, minkä on vahvistanut pääsihteeri Jens Stoltenberg 25. marraskuuta lehdistötilaisuudessa Brysselissä. Häirintälaitteiden tarkoituksena on erityisesti auttaa Ukrainaa torjumaan kamikaze-lennokkien hyökkäyksiä. Laitteet ovat yleensä sähkömagneettisia lähettimiä, jotka häiritsevät droonien navigointi- tai viestintäjärjestelmiä, mutta niitä voidaan käyttää myös häiritsemään venäläisten panssarivaunujen ja/tai tykistön komento- ja valvontajärjestelmiä[16].

INFORMAATIOTILAN HALLINTA

Vladimir Putinin trolleista, kyberrikollisista ja kybersotureista koostuva informaatioarmeija on osoittanut tuhovoimansa jo vuosia. Heidän kyberhyökkäyksensä ovat häirinneet lukemattomia vaaleja ja kansanäänestyksiä, joista tunnetuimpina esimerkkeinä ovat brexit ja Yhdysvaltojen vuoden 2016 vaalit[17]. He hakkeroivat länsimaisia tietokonejärjestelmiä, levittivät viruksia, kuten NotPetya vuonna 2017, joka oli yksi historian vaikuttavimmista kyberhyökkäyksistä. Lisäksi he hyökkäsivät länsimaista kriittistä infrastruktuuria vastaan, josta esimerkkeinä ovat SolarWinds -isku vuonna 2020 ja Colonial Pipeline -isku vuonna 2021[18].

Tarkastellessa Putinin kunnianhimoista erikoisoperaatiota, informaatioarmeija vaikuttaa epäonnistuneen kaikilla rintamilla. Tavoitteena on ollut levittää väärää tietoa, manipuloida Ukrainan yhteiskuntaa ja horjuttaa maata sodan aikana. Narratiivi Venäjästä itäisenä johtajana, joka taistelee natseja vastaan Ukrainassa ja suojelee kaikkia etnisiä venäläisiä, ei ole kuitenkaan menestynyt. Ukraina hallitsee toistaiseksi taistelua länsimaalaisten sydämistä. Venäjän on hyvin vaikea enää muuttaa tätä asetelmaa.

Länsimaat uskovat siihen, että Ukraina on selvästi voittamassa "informaatiosodan". Monissa Afrikan valtioissa, Intiassa, Pakistanissa tai Kiinassa, sosiaalisessa mediassa venäläiset disinformaatiotoimijat onnistuvat uskottavasti kohdentamaan narratiivinsa ja meeminsä[19]. Venäjän propaganda lankeaa hedelmälliseen maaperään, koska se ammentaa näiden maiden kielteisistä kulttuurikokemuksista. Tällainen lähestymistapa voi kuitenkin kääntyä myös päinvastaiseksi, mikä kävi ilmi syyskuussa 2022 Shanghain yhteistyöjärjestön (SCO) huippukokouksessa Samarkandissa, jossa monet alueen maat pitävät nyt Kiinaa, ei Venäjää, auttavana kätenä ja apuna kehitykselle[20].

Venäjän ja Euroopan äärioikeistolaisen propagandan uskottavuus on heikentynyt ja toimintaedellytykset huonontuneet sosiaalisessa mediassa, kuten Facebookissa, Twitterissä ja Instagramissa. Sodan puhkeamisen jälkeen siellä on yritetty levittää salaliittokertomuksia, jotka oikeuttavat Venäjän hyökkäyksen. Yleisin näistä oli, että Putinin täytyi hyökätä kaivaakseen esiin salaiset biolaboratoriot Ukrainassa, jonne salaisia kemiallisen ja biologisen sodankäynnin aineita tuotettiin CIA:n toimesta[21]. Kaikki tämä näyttää epäuskottavalta, ja tällaisten valeuutisten leviäminen on enemmän ja vähemmän epäonnistunut.

Venäjä pyrkii suojaamaan oman maansa informaatiotilaa. Venäjän duuma hyväksyi lain, joka mahdollistaa jopa 15 vuoden vankeusrangaistuksen "väärien tietojen" julkaisemisesta Venäjän valtion toimista. Duuman kolmannessa käsittelyssään hyväksymässä laissa määrätään vankeusrangaistuksia ja sakkoja ihmisille, jotka "tietoisesti levittävät väärää tietoa" Venäjän valtion virastojen toimista "Venäjän alueen ulkopuolella"[22].

Venäjä levitti Euroopan väestöstä syyskuussa 2022 valeuutista, joissa ilmiannettiin naapureita poliisille, jos he lämmittävät asuntonsa yli 19 asteeseen. Tämä ei ollut uskottava, koska kukaan ei uskonut, että länsimainen media ja valtion viranomaiset reagoisivat välittömästi sosiaalisessa mediassa[23]. Myös äskettäin käynnistetty disinformaatiokampanja, jossa puolustusministeri Shoigu toimi nokkamiehenä, epäonnistui. Shoigu soitti kuuden kuukauden tauon jälkeen kollegoilleen Yhdysvalloissa, Isossa-Britanniassa ja Ranskassa syyttäen Kiovaa halusta räjäyttää radioaktiivinen, "likainen pommi" esittämättä minkäänlaisia todisteita. Yhdysvallat, Ranska ja Iso-Britannia kutsuivat väitettä "likaisesta pommista" selvästi vääräksi ja maiden ulkoministerien yhteisessä lausunnossa muistutettiin, ettei Ukrainalla ole ydinaseita ja, tämä oli liian kömpelö yritys hankkia tekosyitä eskalaatiolle[24].

KYBERTOIMINTAYMPÄRISTÖ

Sota kyberympäristössä oli alkanut kauan ennen kuin ensimmäiset Venäjän joukot ylittivät Ukrainan rajan. Vuodesta 2014 lähtien Ukrainassa on rekisteröity yli 5 000 kyberhyökkäystä valtion instituutioita ja kriittistä infrastruktuuria vastaan[25].

Vuoden 2021 puolivälin jälkeen hakkerit ottivat kohteekseen digitaalisia palveluntarjoajia, logistiikkapalvelujen tarjoajia ja toimitusketjuja Ukrainassa sekä ulkomailla, saadakseen pääsyn paitsi Ukrainan myös Naton jäsenmaiden järjestelmiin. Kun vuoden 2022 alussa kaikki diplomaattiset yritykset konfliktin liennyttämiseksi

epäonnistuivat ja Venäjän armeija jatkoi joukkojensa sijoittamista Ukrainan rajalle, kyberhyökkäykset voimistuivat nopeasti. Hakkerit käyttivät Ukrainan instituutioita vastaan esimerkiksi ns. pyyhkijähaittaohjelmia, jotka tuhoavat kiintolevyjä ja dataa[26].

Pian hyökkäyksen jälkeen pankkien ja ministeriöiden verkkosivustoille hyökättiin uudelleen seuraavassa hyökkäysaallossa. Samaan aikaan tuhannet laajakaistan käyttäjät Euroopassa menettivät Internet-yhteytensä amerikkalaisen satelliittioperaattorin Viasatin modeemeihin kohdistuneessa hyökkäyksessä. Kaikkien näiden hyökkäysten yhteisenä tavoitteena oli sulkea Ukrainan viranomaisten ja erityisesti armeijan komento- ja valvontajärjestelmät[27].

Ukraina on laajentanut ja parantanut valmiuksiaan viime vuosina. Joidenkin länsimaiden, kuten USA:n Israelin, Liettuan, Alankomaiden, Puolan, Viron, Romanian ja Kroatian, tuella, jotka lähettävät kyberturvallisuusasiantuntijoita auttamaan Ukrainaa kyberuhkien torjumisessa[28].

Ukraina sai tukea myös ei-valtiollisilta toimijoilta:

- Anonymous-kollektiivi alkoi tukea Ukrainaa välittömästi fyysisen hyökkäyksen alettua. YourAnonNewsin johdolla Twitterissä nousi trendaaviksi yksi merkittävä Anon-tili toisensa jälkeen[29]. Aloituslahjana Venäjän puolustusministeriön verkkosivusto hakkeroitiin ja palvelimelle piilotetut tietueet julkaistiin.

- Toisaalta taas pahamaineinen "Killnet-jengi" lupasi tukea Moskovalle ja uhkasi kostotoimilla. Anonymous kirjoitti Twitterissä 21. toukokuuta, että "kollektiivi on virallisesti kybersodassa Killnetiä vastaan". Pian sen jälkeen, kun Anonymous julisti kybersodan ja kaatoi Killnetin verkkosivuston.

- Tähän mennessä noin 45 hakkeriryhmää on aktivoitunut Ukrainan hyväksi. Useimmat heistä liittyvät löyhästi Anonymousiin. Kaikki ryhmät toteuttavat kiristysohjelmia, psyopseja, hakkerointia ja vuotoja, palvelunestohyökkäyksiä ja turmelemiskampanjoita Moskovaa vastaan[30].

- Ukrainan digitaalisen muutoksen ministeri Mykhailo Federov perusti helmikuun 2022 lopulla Telegramissa toimivan ukrainalaisen vapaaehtoisen "IT-armeijan". Tällä hetkellä noin 300 000 vapaaehtoista hakkeria eri puolilta maailmaa tukee Ukrainaa hyökkäämällä esimerkiksi venäläistä mediaa, valtiollista radiotoimintaa, yrityksiä vastaan[31].

Venäjä on yrittänyt saada Ukrainan polvilleen kyberulottuvuudessa. Venäjän hyökkäykset ovat aiheuttaneet jonkin verran vahinkoa, mutta toistaiseksi eivät mitään dramaattista. Lisäksi on toteutettu palvelunestohyökkäyksiä, joissa eurooppalaiset ja yhdysvaltalaiset verkkosivustot ylikuormitetaan tarkoituksellisesti tietoliikenteellä. Samoin toteutetaan kybervandalismia, jossa verkkosivustoja kaapattiin ja niiden sisältöä muokattiin[32]. Joitakin näistä koordinoitiin myös kineettisten hyökkäysten kanssa. Esimerkiksi iskettiin matkapuhelinoperaattoreihin alueilla, joita tulitettiin samanaikaisesti Venäjän tykistöllä tai oli aiemmin isketty kriittiseen infrastruktuuriin[33]. Kuitenkaan Ukrainan tietoliikenneverkkoja ei ole pystytty lamauttamaan kuin hetkellisesti. Venäläiset hakkerit ovat iskeneet myös Ukrainan ulkopuolella. Huomionarvoista on hyökkäykset hallitusten palvelimiin Liettuassa (toukokuussa), Italiassa (kesäkuussa), Montenegrossa (elokuussa), Saksassa (syyskuussa), Bulgariassa ja Puolassa (molemmat lokakuussa)[34].

Venäläiset eliittihakkerit, joilla on tarttuvia nimiä, kuten "Fancy Bear", "Snake", "Sandworm" tai "Killnet", ovat toistaiseksi pystyneet aiheuttamaan suhteellisen vähän vahinkoa. Siihen lienee monia syitä, eikä vain Ukrainan hyvä valmistautuminen näihin hyökkäyksiin. Monet asiantuntijat ovat tarkkailleet Venäjän hyökkäyksiä ja tehneet sen johtopäätöksen, että "lukuun ottamatta satelliittihakkerointia sodan alussa, kaikki hyökkäykset ovat olleet puhtaasti opportunistisia. Niitä ei ole huolella harkittu tai hyvin suunniteltu." Näyttää siltä, että Venäjän verkkosota toteutetaan ja käydään samalla tavalla kuin fyysiselläkin taistelukentällä: raa'alla voimalla, eikä niinkään hienovaraisuutta hyödyntäen[35].

MIKSI VENÄLÄINEN "KYBER-PEARL HARBOR" ON EDELLEEN TOTEUTTAMATTA?

Yksi sodan suurimmista yllätyksistä tähän mennessä on täysimittaisen kybersodan puuttuminen. Miksi Venäjä ei ole vielä mobilisoinut kaikkia kyber- ja informaatiosodankäynnin mahdollisuuksiaan sodassa Ukrainaa vastaan? Miksi "Cyber Armageddon[36]"tai "Cyber Pearl-Harbor[37]"ei ole toteutunut? Tähän on kolme mahdollista selitystä[38]:

Aika -hypoteesi:
Suuremman vahingon aikaansaamiseksi hyökkääjien olisi pystyttävä oleskelemaan pitkään länsimaisten yritysten ja viranomaisten hyvin suojatuissa verkoissa räjäyttääkseen "virtuaalipomminsa". Länsimaidenkin voimakkaat ja hyvin koulutetut kyberarmeijat tarvitsisivat vähintään vuoden tällaisten ohjelmien valmisteluun ja olisivat alttiita vakoilulle tuona aikana. Venäjän hakkereilla saattoi olla paljon vähemmän aikaa. Näin ollen kyber- ja informaatiosoturit eivät ole saaneet

Lähteet sivulla 39

tarvittavaa mandaattia Kremliltä, koska sotilaallinen varustautuminen muilla aloilla (maalla, merellä ja ilmassa) on tarvinnut kaiken Venäjän valtion johdon huomion.

Valmius -hypoteesi:
Kiova on ottanut opikseen vuodesta 2014 ja on paremmin valmistautunut, osittain myös länsimaiden ja ei-valtiollisten toimijoiden avun ansiosta. Esimerkiksi Microsoft on auttanut Ukrainaa ottamalla haltuunsa Internet-verkkotunnuksia venäläiseltä hakkeriryhmä Strontiumilta (joka on sidoksissa Killnetiin) ja ohjaamalla hyökkäykset niin kutsuttuihin "valemaaleihin[39]".

Epävarmuus -hypoteesi:
Tämä ratkaisu on epämiellyttävin ja vaarallisin. Massiivinen kyberhyökkäys ei todellisuudessa ole mahdoton - venäläisillä kyber- ja informaatiosotureilla oli tarpeeksi aikaa ja tukea Moskovasta valmistellakseen sekä toteuttaakseen laajamittaisen hyökkäyksen. Virus on jo verkoissamme, mutta emme tiedä siitä ja Putin vain odottaa, milloin on sopiva hetki laukaista se.

Riippumatta siitä, mikä hypoteesi voisi olla oikea, Ukrainasta saadut opetukset edellyttävät EU:lta ja Natolta koordinoitua ja kattavaa strategiaa kyberpuolustuksen vahvistamiseksi kaikkia kybertuho-, vakoilu- ja vaikutusoperaatioita vastaan.

JOHTOPÄÄTÖKSET JA SUOSITUKSET

Krimin liittämisen jälkeen vuonna 2014 uskottiin, että Venäjä oli luonut uuden modernin sodankäynnin muodon. Ampumatta laukaustakaan, Putinin joukot ottivat haltuunsa Ukrainan niemimaan, jota pidettiin hybridisodankäynnin uutena kultastandardina - sodassa, jossa tankit eivät ole keskipisteenä, vaan disinformaatio, kyberhyökkäykset, sabotaasi ja erikoisjoukot. Kukaan Natossa ja/tai EU:ssa ei ollut uskonut Moskovan pystyvän tällaiseen operaatioon, kaikki olivat yllättyneitä. On ilmeistä, että venäläiset eivät ole sotataidollisesti niin pitkällä kuin oletettiin. Ukrainan kansan maanpuolustustahdon aliarviointi ja omien kykyjen yliarviointi johtivat siihen, että hybridihyökkäyksestä Ukrainaan tuli hybridisota, joka riistäytyi käsistä ja on nyt muuttunut varsin perinteiseksi sodaksi.

Myös tässä sodassa, kyber- ja informaatioulottuvuudessa, sähkömagneettisen spektrin käyttö on edelleen yksi taistelukentän tärkeimmistä osista, kyse ei ole vain puhtaasta propagandasta tai yksittäisistä kyberiskuista.

Länsi on todennäköisesti valmistautunut pitkittyneeseen, enimmäkseen matalan intensiteetin sotaan. Putin kokee pakotteiden asettamisen jo lähes sodanjulistuksena. Venäjälle vastatoimien väline voisi olla kyber- ja disinformaatio-operaatiot. Kesäkuussa 2023 julkaistussa raportissaan Microsoft varoitti Venäjän sotilaallisen hyökkäyksen kyberoperaatioiden lisääntymisestä Euroopan kriittisiä infrastruktuureja vastaan.[40] Odotettavissa on myös kyberhyökkäyksiä toimijoilta, kuten "Cadet Blizzard", jotka ovat liittyneet Venäjän GRU:hun. Helmikuussa 2023 alkaneet hyökkäykset kohdistuivat valtion virastoihin ja IT-palveluntarjoajiin Ukrainassa. Siksi lännen yhteisiä toimia kyberresilienssin parantamiseksi sekä kansallisella, EU:n että Naton tasolla, on kiireellisesti tehostettava.

Kyberuhkaympäristö kehittyy nopeasti. Siksi Euroopan ja Yhdysvaltojen on nyt valmistauduttava jatkuviin harmaan alueen konflikteihin. Vain ennakoinnin, riskien vähentämisen ja luovuuden avulla kyberavaruuden voimatasapainoa voidaan muuttaa kokonaisen, turvallisen ja vapaan globaalin internetin puolustajien hyväksi.

Se, joka voittaa kyberulottuvuudessa, päättää, mitä ihmiset ja yhteiskunnat uskovat ja miltä heidän mielestään totuus näyttää. Koska se, joka häviää taistelun tiedosta, menettää myös hetken toimia ja mahdollisuuden voittaa fyysinen sota. Tällä hetkellä näyttää siltä, että Venäjä ei ole suosikki voittamaan tätä sotaa - ei edes informaatio- ja kyberulottuvuudessa. ■

DR. JOSEF SCHRÖFL

- Kandidaatin tutkinto tietotekniikassa ja maisterin tutkinto kansainvälisistä suhteista Delawaren yliopistosta. Tohtorin tutkinto kansainvälisestä politiikasta Wienin yliopistosta.
- Strategiasta ja puolustuksesta vastaava apulaisjohtaja.
- **Hybrid CoE Helsinki/Suomi**

SOENKE MARAHRENS

- Tietojenkäsittelytieteen tutkinto sekä maisterin tutkinnot Royal Military Collegesta, Kanadasta ja Federal Armed Forces -yliopistosta, Hampurista.
- Johtaja, strategia ja puolustus, johtaa hybridisodankäynnin tutkimushaaraa.
- **Hybrid CoE Helsinki/Suomi**

LÄHTEET :

1. Similar articles and its content has been published by the author already in several magazines in 2023 (TDHJ, ÖMZ, Hybrid CoE flash findings, CyberWatch Magazine, etc.). This essay is a continuation of the events in the Ukraine war.
2. See also: Angela Stent: “Putin's World : Russia Against the West and with the Rest”, 2020, Twelve, US, p12-25
3. Like described from James O. Finckenauer and Yuri A.Voronin in “The Threat of Russian Organized Crime”, NCJ 187085 from June 2001
4. https://www.c4isrnet.com/cyber/2021/03/25/us-military-conducted-2-dozen-cyber-operations-to-head-off-2020-election-meddling/ (Unless otherwise indicated, all links were last accessed on 08.01.2022)
5. https://www.watson.ch/international/russland/444993013-nachrichtenagentur-des-kremls-ruft-zur-vernichtung-der-ukraine-auf
6. according to the task force of the European External Action Service “EUvsDisInfo”, https://euvsdisinfo.eu/report/russia-fights-the-collective-west-not-just-ukraine
7. The author understands “Narratives” as overall messages that are spread and constantly repeated in the form of individual texts, images and videos by fake accounts in social networks or on supposed news portals. Individual reports always contribute to a message, a narrative. Some of these narratives have been used for many years, combined or altered according to current events and settings.
8. https://www.cyberscoop.com/russia-ukraine-cyberwar-nato-geneva-microsoft/
9. Germany f.e. sees it together (https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum). GB and the the US not (https://www.cybercom.mil/, https://www.ncsc.gov.uk/)
10. Therefore I mostly agree with Stefan Libicki´s essay from 1995: “Is there an elephant? Seven forms in search of a function: Command-and-control warfare, Intelligence-based warfare, Electronic warfare, Psychological warfare, Hacker warfare, Information warfare, Cyberwarfare” (https://apps.dtic.mil/sti/pdfs/ADA367662.pdf)
11. See also Nicolas Mazzucchi “AI-based technologies in hybrid conflict: The future of influence operations”, Hybrid CoE Paper 14, June 2022.
12. https://www.nzz.ch/international/der-elektronische-krieg-in-der-ukraine-unsichtbar-aber-wichtig-ld.1688611?
13. https://kurier.at/politik/ausland/elon-musk-ukraine-russland-putin/402186138
14. https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/
15. https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/
16. https://orf.at/stories/3295244/ The Russian army has been increasingly attacking ukainian critical infrastructure with kamikaze drones since October 2022, using mainly Iranian-made aircraft Shahed-136. It has a triangular wing and is equipped with a warhead. The drone is usually launched from trucks and crashes towards its target at high speed, but can be interfered by electromagnetic attacks.
17. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections
18. https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/
19. https://carnegieendowment.org/sada/87353
20. https://www.politico.eu/article/russia-disinformation-africa-europe-sergey-lavrov/
21. https://www.bbc.com/news/60711705
22. https://www.independent.co.uk/news/world/europe/ukraine-war-latest-russia-law-b2028440.html
23. Neue Zürcher Zeitung (intern. Edt.), Donnerstag 15.September 2022, p6
24. https://orf.at/stories/3291109/
25. https://www.databreaches.net/security-service-of-ukraine-identified-fsb-hackers-who-carried-out-more-than-5000-cyberattacks-on-state-bodies-of-ukraine/
26. https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat
27. SonntagsZeitung, Samstag 9 April 2022, S. 17
28. https://carnegieendowment.org/2022/06/16/ukraine-war-shows-how-nature-of-power-is-changing-pub-87339
29. The largest accounts have over 15 million followers: (https://www.derstandard.at/story/2000134361378/anonymous-sind-zurueck-wie-der-cyberkrieg-gegen-russland-ablaeuft
30. https://orf.at/stories/3256364/
31. https://t.me/itarmyofukraine2022
32. https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/
33. https://www.ohchr.org/en/press-briefing-notes/2022/10/ukraine-attack-civilians-and-infrastructure
34. https://orf.at/stories/3284892/ as well as https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland
35. See the interview with Marina Krotofil: https://securityboulevard.com/2022/08/bsidestlv-2022-marina-krotofils-kinetic-and-cyberwarfare-twins-siblings-or-distant-relatives-or-why-bombs-speak-louder-than-electronic-bits/
36. Or cyber apocalypse: Implies that critical infrastructure within one or more countries is continuously bombarded with ransomware and other attacks so that every civilian service is either dramatically slowed or shut down.
37. The term was coined in 2012 by U.S. Defense Secretary Leon E. Panetta and aims to relate the intensity and potential devastation of a major cyber-attack with the 1941 attack on Pearl Harbor, a surprise military attack by the Japanese Navy against the U.S.
38. Thank You Stephanie Carvin for sharing Your article: “How to Explain the Failure of Russia’s Information Operations in Ukraine?” from March 2022 (https://www.cigionline.org/articles/how-to-explain-the-failure-of-russias-information-operations-in-ukraine/). Your thoughts inspired me for that conclusion.
39. https://www.csoonline.com/de/a/microsoft-uebernimmt-domains-von-russischen-hackern,3673868
40. https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/

KUUKAUSIKATSAUS LOKAKUU/2023

// Cyberwatchin analyysitiimi

SISÄLLYS:

TÄSSÄ KATSAUKSESSA

Kansainvälisen kyberympäristön osalta syyskuussa korostui EU-komission puheenjohtaja Ursula von der Leyenin puheenvuoro EU:n roolista digitalisaation edistämisessä muun muassa sääntelyä kehittämällä. Myös Vuoristo-Karabahin alueen konflikti oli esillä kyberoperaatioiden näkökulmasta, kun niiden rooli on tullut yhä keskeisemmäksi konfliktin molempien osapuolten työkalupakissa. Kansainvälinen rikostuomioistuin ICC ilmoitti myös syyskuussa alkavansa tutkimaan kyberympäristössä tapahtuvia rikoksia sotarikoksina.

Kyberrikollisuuden osalta pinnalla oli YK:n kyberrikoksia koskevan konferenssin tulevaisuuden tavoitteet entistä paremman globaalin kyberrikossääntelyn kehittämiselle. Tämän lisäksi esillä oli lisääntynyt teknologisten häiriötilanteiden raportoiminen kyberhyökkäyksenä, ilman tarkempia perusteita, mikä kertoo tulkintatapojen muutoksesta ja kyberuhan muodostamasta yhteiskunnallisesta pelosta. Teknologisten laitteiden ja sovellusten kehityksessä esille nousivat kehittyneet ja ilmaiseksi saatavilla olevat tietojen palauttamistyökalut kiristyshaittaohjelmien uhreille. Lisäksi teknologian suhteen puhutti myös web3-teknologioiden kehitys sekä laskusuhdanteen vaikutus IT- ja kyberturvallisuusyrityksiin.

Katsauksessa tarkastelemme edellisen kuukauden keskeisiä aiheita, sitoen ne laajempaan kokonaisuuteen. Katsauksemme jakautuu kolmeen tarkastelukulmaan: jatkuviin seurannan kohteisiin, joista valitsemme kulloinkin merkittävimmät käsiteltäviksi; ilmiöihin, joita haluamme erityisesti edellisestä kuukaudesta korostaa sekä ilmiöihin, joiden kehitystä kannattaa seurata. Kuukausikatsauksen liitteenä toimitetaan kuukauden merkittävimpiä kyberhyökkäyksiä ja aktiivisia uhkatoimijoita käsittelevä uhkaseurantaraportti.

Tässä katsauksessa käsittelemme sitä, miten perinteisestä maailmasta tutut rikokset omaksutaan yhä nopeammin kybertoimintaympäristössä, ja miten fyysinen maailma ja kyberulottuvuus sekoittuvat yhä tiiviimmin toisiinsa. Tämän lisäksi tarkastelemme, kuinka kansainvälinen yhteistyö kybertoimintaympäristössä on kehittynyt viime kuukausien aikana ja mitä positiivista yhteistyöstä voi seurata huolimatta merkittävistä haasteita. Syyskuun tapahtumista kannattaa erityisesti seurata, mihin suuntaan Ranskan suhtautuminen sosiaalisen median ja internetin valvontaan kehittyy. Toinen tärkeä seurattava ilmiö on, miten turvallisuusviranomaiset ovat yhä enemmän kyberhyökkäysten kohteina, Viimeisimpinä esimerkkeinä ovat olleet kyberhyökkäyksiin Iso-Britannian poliisitoimia kohtaan. Pohdinnan arvoista on myös se, onko ukrainalainen kyberrikollisuus loppunut Ukrainan sodan alettua.

1. TAPAHTUMIA KYBERMAISEMASSA

1.1. Kansainvälinen kyberympäristö

Poliittiset puheet, kansainväliset konfliktit ja kansainvälinen rikostuomioistuin ovat olleet pinnalla viime aikoina. Kuukauden mielenkiintoisin poliittinen ulostulo oli EU-komission puheenjohtaja Ursula von der Leyenin pitämä Unionin tila -puhe, joka oli yksi seuratuimpia poliittisia puheenvuoroja maailmassa. Puhe pidetään kerran vuodessa ja se määrittelee unionin tulevaisuuden suuntaviivoja, kertoo unionin tahtotilasta ja kertaa mennyttä EU:n näkökulmasta. Tämän vuotisessa puheessa digitalisaatiolle ja tekoälylle oli omistettu oma osuutensa. Puhe heijasteli EU:n tavoitetta olla edelläkävijä digitaalisessa toimintaympäristössä. Von Der Leyen korosti muun muassa EU:n pioneeriasemaa kansalaisten digitaalisten oikeuksien saralla, ja kehui, kuinka EU-sääntely tekee digiympäristöstä turvallisemman. Mainituksi tulivat myös tekoäly ja sen tuomat uhat sekä mahdollisuudet. Vaikka teemoja puheessa usein lähestyttiin sääntelyn näkökulmasta, voidaan puhe tulkita osana EU:n laajempaa tavoitetta kohti digitaalista suvereniteettia. Digi- ja tekoälyasiat ovat tällä hetkellä pinnalla ja unionilla on ääneen lausuttu pyrkimys edistää niitä myös tulevaisuudessa. Tämä on merkittävää, jotta EU pystyisi säilyttämään asemansa muuttuvassa maailmassa suurvaltojen, kuten Kiinan ja Yhdysvaltojen, keskellä.

Syyskuun 19. päivä Vuoristo-Karabahissa uudelleen leimahtanut kriisi on merkittävä myös kybernäkökulmasta. Konflikti on Armenian ja Azerbaidzhanin välinen ja sitä seurasi välitön kyberhyökkäysten määrän kasvu molemmissa maissa. Jo aiemminkin konflikti on kytenyt verkkoulottuvuudessa, sillä kyberiskuja on vuosien varrella nähty puolin ja toisin. Valtioilla on niin ikään ollut pääsy kehittyneimpiin kybertyökaluihin – esimerkiksi Amnesty International on huomauttanut Pegasus- ja Predator-vakoiluohjelmistojen käytöistä kummassakin maassa. Kriisi osoittaa jälleen sen, että kyberulottuvuudella on oma roolinsa eri typpisissä konflikteissa.

Kansainvälinen rikostuomioistuin ICC ilmoitti syyskuussa alkavansa tarkastelemaan kyberympäristössä tapahtuvia rikoksia mahdollisina sotarikoksina. Tämä perustuisi niin kutsuttuun Rooman perussääntöön, jonka mukaan rikostuomioistuimella on oikeus tutkia ja tuomita sotarikoksia, rikoksia ihmisyyttä vastaan ja joukkotuhoon liittyviä rikoksia. On kuitenkin epäselvää, miten valtiolliset kyberhyökkäykset sopivat tähän kehykseen tai kuinka valtioiden voidaan osoittaa olevan näiden takana. Usein valtiot käyttävät käsikassaroinaan rikollisia hakkerijengejä tai pystyvät aina naamioimaan ja kiistämään toimintansa. Ilmoitus on kuitenkin askel oikeaan suuntaan ja viestii siitä, että myös kyberympäristöön suhtaudutaan vakavasti ja rikolliset pyritään saattamaan vastuuseen toimistaan. ICC ei myöskään itse ole välttynyt kyberhyökkäyksiltä, sillä syyskuussa se joutui myös itse kyberhyökkäyksen kohteeksi. Isku ei kuitenkaan välttämättä liity juuri tähän ilmoitukseen, vaan taustalla voi vaikuttaa esimerkiksi muut tuomioistuimen työn alla olevat tutkinnat.

1.2. Kyberrikollisuus

Syyskuussa merkittävimpien kyberrikollisuuteen liittyvien tapahtumien joukkoon kuuluivat yhtäältä YK:n ja ICC:n pyrkimykset kyberrikollisten ja kybersotarikollisten vastaisissa toimissa ja toisaalat uutiset jatkuvasti monipuolistuvista ja kehittyvistä kyberrikollisuuden muodoista. YK päätti syyskuun alussa viidennen kyberrikoksia koskevaan lainsäädäntöön keskittyvän työryhmän konferenssin, jonka tavoitteena on ensi vuoden alussa muodostaa työpaperi, joka voisi toimia pohjana tulevaisuuden globaalille kyberrikoksia koskeville säädöksille. Samoin syyskuussa kansainvälisen rikostuomioistuimen pääsyyttäjä ilmoitti tavoitteista aloittaa kyberympäristössä tapahtuvien sotarikosten tutkinta ja syyttäminen. Molemmat tapahtumista kertovat samaa tarinaa siitä, miten kyberoperaatiot haastavat olemassa olevaa lainsäädäntöä ja niiden käsitteleminen on varsin hankalaa nykyisten säädösten puitteissa. Kyberrikokset ovat luonteeltaan lähes aina kansainvälisiä, ja toteuttajan tunnistaminen sekä etenkin syyllisyyden todistaminen ovat merkittäviä haasteita niissäkin tilanteissa, joissa tekijää ja uhria koskisi sama lainsäädäntö. Nykyinen säädöskenttä on pitkälti kykenemätön vastaamaan tähän problematiikkaan, ja vaikka on hyvä, että työtä lakien yhtenäistämiseksi globaalilla tasolla tehdään, matka on yhä pitkä ja useita haasteita edessä.

Itse kyberrikollisuuteen liittyvissä ilmiöissä korostuivat tavat, miten kyberympäristö jatkuvasti näyttelee entistä merkittävämpää roolia rikoksissa, jotka eivät varsinaisesti sovi ilmiön ”puhtaaseen” määritelmään. Käytännössä nämä ovat rikoksia, joissa kyberympäristö näyttelee jonkinlaista osaa toiminnassa, mutta eivät tapahdu yksinomaan kyberympäristössä, vaan rikkovat rajan fyysisen maailman ja kyberrikosten välillä. Kyse voi olla pienen mittakaavan rikoksista, jossa digitaaliset latteet tukevat perinteisempinä tunnettuja rikoksen muotoja, tai toisaalta laajojen kansainvälisten rikollisorganisaatioiden toiminnasta, jossa esimerkiksi vapaudenriisto yhdistyy kyberrikoksiin. Rajat näiden kahden pitkään toisistaan erillisiksi käsitettyjen rikosmaailmojen välillä vaikuttavat hämärtyvän, kun toiminnan mahdollisuudet kasvavat ja samalla hyödyt tulevat entistä konkreettisemmin esille. Tätä kehitystä käsitellään tarkemmin myöhemmin tässä katsauksessa.

Sen lisäksi, että kyberrikollisuus kehittyy, tuntuu myös, että suhtautuminen siihen on muuttunut huomattavasti jo yksin viimeisten kuukausienkin aikana. Pelkästään lainvalvonnan eteen tehtävän työn lisäksi tästä kertoo jatkuvasti kasvava viranomaishuomio, politiikan keskittyminen kybermaailmaan ja se, miten vakavasti tapahtuneisiin rikoksiin suhtaudutaan ja kuinka suurta pelkoa kyberuhat herättävät. Kyberympäristö tuntuu edelleen monelle vieraalta toimintakentältä ja jossain määrin tuntemattomalta uhalta. Maailmalta tuleva uutisointi tuhoisista kyberhyökkäyksistä onkin aiheuttanut ilmiön, jossa missä tahansa häiriötilanteessa tai toimintakatkoksessa ensimmäinen epäily ja pahin pelko on kyberhyökkäyksen kohteeksi joutuminen. Koska näistä viestiminen on myös tärkeää, on viime aikoina saatu useitakin esimerkkejä tapauksista, joissa teknisen häiriön kokenut taho on jopa ehtinyt raportoida joutuneensa kyberhyökkäyksen kohteeksi ennen kuin vian todellinen syy on selvinnyt. Sekä pelon lietsomisen välttämiseksi että oman julkisuuskuvan ylläpitämiseksi olisi kuitenkin tärkeää ensin varmistua tapahtuman luonteesta ennen ulkoista viestintää. Vaikka on hyvä, että kyberhyökkäyksiin suhtaudutaan vakavasti ja niihin liittyvä viestintä on avointa ja nopeaa, ei pahimman sattuessa kannata kiirehtiä turhaan. Tilanteessa tulee pyrkiä rauhallisuuteen, jotta voidaan tarkasti arvioida vahingon laajuus sekä luonne ja mitoittaa jatkotoimenpiteet näiden mukaan.

Lähteet sivulla 50

1.3. Teknologia

Teknologisen tilanteen osalta syyskuussa saatiin hyviä uutisia työkaluista ja ratkaisuista, joita kyberuhkien kohteeksi joutuneilla on käytettävissään. Kyse on ilmaiseksi saatavilla olevista kiristyshaittaohjelmien uhreille kehitetyistä tietojen palauttamistyökaluista, joiden kohdalla sekä määrä että laatu ovat huomattavasti kasvaneet viime aikoina. Verkosta löytyy avoimesti ja täysin veloituksetta saatavilla olevia työkaluja, joilla useiden eri kiristyshaittaohjelmien salaamat tiedostot voidaan palauttaa. Syyskuun aikana tämä työkalujen jo valmiiksi laajahko kirjo sai joukkoonsa lisäyksen, kun Key Group -hakkeriryhmän käyttämään haittaohjelmaan julkaistiin python-koodikielellä kirjoitettu komentosarja. Julkaistun komentosarjan avulla haittaohjelman tekemä salaus on mahdollista purkaa ja palauttaa alkuperäiset tiedostonimet. Kyseessä on sikäli harvinainen uutinen, että useammin törmätään uusiin teknolgoisiin tapoihin, joita rikolliset toiminnassaan hyödyntävät, kuin ratkaisuihin, joilla uhkaan voidaan vastata tai uhrien kärsimiä vahinkoja rajoittaa. Positiivisesta uutisesta huolimatta on pidettävä mielessä, että rikolliset ovat jo osittain muokanneet toimintaansa tämänlainen kehitys mielessään. Kiristyshyökkäyksissä yhä harvemmin ollaan riippuvaisia pelkästään datan salauksen pitävyydestä, vaan usein samalla uhataan myös esimerkiksi datan vuotamisella ulospäin tai sen avoimella julkaisulla.

Teknisen kybersuojauksen suhteen ei tule unohtaa kaikkein tärkeintä toimenpidettä eli asianmukaista järjestelmien päivittämistä. Syyskuussa tämä vaatimus jälleen korostui, kun uutisoitiin jatkuvasti kasvavasta nopeudesta, jolla rikolliset hyödyntävät joko itse havaitsemiaan tai avoimesti julkaistuja haavoittuvuuksia. Samoin järjestelmien päivittämisen merkitys tuli esiin myös, kun uutisoitiin suosituista ja tehokkaista hyökkäysmuodoista, esimerkiksi web-skimmauksesta, jotka täysin perustuvat huonosti suojattuihin järjestelmiin. Vaikka kyse ei olekaan teknologian saralla uudesta tilanteesta, jossa turvallissuspäivitysten asentaminen ja tietoisuus omia järjestelmiä koskevista haavoittuvuuksista on kriittistä, ei samaa ohjetta voida toistaa liikaa.

Tulevaisuuden suhteen teknologian saralla puhutti syyskuussa sekä potentiaalisesti kasvava web3-teknologioiden rooli että laskusuhdanteen ja taantuman mahdollinen vaikutus IT- ja kyberturvallisuusalan rahoitukseen. Web3 ja siihen liittyvät teknologiat ovat olleet kartalla jo pitkään ja niiden nimeen vannovat ovat odottaneet ja ennustaneet koko internettiin pohjautuvan infrastruktuurin radikaalia uudelleenjärjestämistä. Tämä ei kuitenkaan vielä lähitulevaisuudessa vaikuta todennäköiseltä. Vaikka esimerkiksi lohkoketjut tai niihin pohjautuvat varmennejärjestelmät kehittyvät ja löytävät jatkuvasti uusia hyödyntämiskohteita, on mahdollista, että käsite Web3 uutena internetin ajanjaksona jää vielä tulevaisuuden visioksi. Monet näitä teknologioita hyödyntävät ja markkinoivat yritykset ovat kuitenkin löytäneet jonkin verran rahoitusta, mikä ei nykypäivän taloustilanteessa ole enää läheskään niin itsestään selvää kuin informaatioteknologioihin keskittyvien yritysten kohdalla on saatettu tottua. Etenkin kyberturvallisuutta tarjoavien toimijoiden määrän räjähdysmäinen kasvu on johtanut siihen, että vaikka asia on jatkuvasti yhä tärkeämpi ja enemmän huomiota saava, ei kaikille uusille toimijoille yksinkertaisesti löydy omaa markkinarakoa. Projekteista käytävän kilpailun voittaminen on yhä hankalampaa ja riskinä on että, kuten niin monella muullakin toimintakentällä, isot toimijat jyräävät pienemmät alleen tukahduttaen innovaatiota ja vähentäen kuluttajilla valittavissa olevien vaihtoehtojen määrää.

2. VALOKEILASSA

2.1. Perinteistä rikollisuutta helpompaa toteuttaa kyberulottuvuudessa

Perinteisestä maailmasta tutut rikokset omaksutaan nopeasti myös kybertoimintaympäristössä, jossa teknologia toimii rikoksen tekovälineenä tai jollakin muotoa rikoksen välittäjänä. Aiemmin ihmisiin ja yksilöihin kohdistuvat rikokset ovat nyt teknologian myötä entisestään monipuolistuneet ja tulleet yhä helpommin toteutettaviksi. Kyberrikollisuus ja perinteinen rikollisuus yhdistyvätkin koko ajan enemmän toisiinsa ja niitä alkaa olla varsin hankala erottaa toisistaan. Esimerkiksi digitaalisiin alustoihin perustuvat huijaukset ovat vain yksi toiminnan muoto muun rikollisen toiminnan joukossa. Kyberrikoksia on pitkään ajateltu tekevän vain niihin erikoistuneet rikolliset mutta nyt niitä on entistä helpompaa toteuttaa ilman, että rikollinen omaisi erityistä teknistä osaamista.

Tästä yhtenä esimerkkinä ihmiskaupan ja kyberrikosten yhdistyminen. YK:n raportin mukaan ilmoitukset kyberrikoksiin liittyvästä ihmiskaupasta ovat jatkuvasti lisääntyneet. Ihmiskauppatapauksissa uhrilta riistetään väkivalloin vapaus, kyky pitää yhteyttä kotiin sekä läheisiin, ja pakotetaan uhrit lopulta tekemään kyberrikoksia sortajansa nimiin ilman, että he itse hyötyisivät rikoksesta mitenkään. Useimmiten kyberrikokset, joissa hyödynnetään ihmiskaupan uhreja, ovat eri tasoisia krypto- tai romanssihuijauksia mutta myös uhkapelaamiseen liittyvät petokset ovat yleistyneet. Huijausta tekevän osapuolen ei välttämättä tarvitse osata muuta kuin tuottaa uskottavan kuuloisia viestejä, sillä rikoksiin käytettävät huijaussivustot ja työkalut ovat nykyisin kehittyneitä, helppokäyttöisiä ja pitkälle automatisoituja. Tämänkaltainen toiminnan muoto on nousussa etenkin Kaakkois-Aasiassa eikä se ole sitä harjoittavien rikollisorganisaatioiden ainoa toiminnan muoto tai tulonlähde vaan yksi rikoksentekotapa muiden joukossa. On siis hyvä ymmärtää se, että kyberrikollisetkaan eivät automaattisesti ole aina pahantekijöitä vaan kyberrikoksen tekijäkin saattaa olla itse rikoksen uhri.

Toinen esimerkki kyberulottuvuuden tulemisesta osaksi fyysisen maailman ongelmia, on lähisuhdeväkivallan uusi ulottuvuus digitaalinen lähisuhdeväkivalta. Digitaalinen lähisuhdeväkivalta tarkoittaa teknologian mahdollistamaa läheisiin kohdistuvaa häirintää, kiusaamista, pelottelua tai vainoamista. Sitä voi tapahtua pitkiäkin aikoja ja yleensä se vain pahenee ajan kuluessa. Digitaalinen lähisuhdeväkivalta voi ilmetä esimerkiksi toisen nettiselaimen sivuhistorian läpikäyntinä, luvattomana sähköpostien lukemisena, sosiaalisen median tilien toimintojen seuraamisena ja kontrollointina, intiimien kuvien jakamisena ilman lupaa, puhelimen sisällön säännöllisenä läpikäyntinä, käyttäjätunnusten ja salasanojen vaatimisena tai jopa erilaisten vakoilulaitteiden tai paikantimien asentamisena läheisen tavaroihin tai älylaitteisiin. Tämän kaltaisesta kontrolloimisesta ja kiusanteosta onkin teknologian kehittymisen ja sosiaalisen median alustojen myötä tullut yhä helpompaa toteuttaa. Se, missä sosiaalisen median palvelut ovat tarjonneet yksilöille entistä parempia vuorovaikuttamisen tapoja, ovat ne myös lisänneet joidenkin yksilöiden turvattomuuden tunnetta jo valmiiksi haastavassa elämäntilanteessa.

Lähteet sivulla 50

2.2. Kansainvälisellä kyberyhteistyöllä on potentiaalia hyvään

Kybermaailmassa tapahtuva yhteistyö on ollut jonkin verran tapetilla syyskuussa. Oli kyse sitten lainsäädännön yhtenäistämisestä tai eri valtioiden viranomaisten yhteistyöstä yksityisten turvallisuusyritysten kanssa, on selvää, että kyberturvallisuuteen liittyvä kansainvälinen yhteistyö on konkreettinen pyrkimys, jolla kyberuhkiin pyritään globaalilla tasolla vastaamaan. Kuten moneen kertaan todettua, haasteita tässä prosessissa on vielä paljon, eivätkä ne ole olankohautuksella ohitettavissa. On myös hyvä pitää mielessä ne potentiaaliset hyödyt, joita yhteistyön kehittämisellä voi olla.

Eräs kyberrikosten suosioon eniten vaikuttavista seikoista on matalan kiinnijäämisen riskin ohella erittäin pieni todennäköisyys joutua todellisuudessa vastuuseen teoista. Tähän syynä ovat niin haasteet todisteiden löytämisessä, kuin myös se, että rikokset toteutetaan usein toiselta puolen maailmaa kuin missä uhrit sijaitsevat. Näistä seikoista johtuen kyberrikosten tutkiminen vaatii huomattavaa teknologista kompetenssia ja kykyä panostaa resursseja tapausten selvittämiseen, sekä kansainvälistä yhteistyötä viranomaisten välillä pidätysten toteuttamiseksi ja rikoksilla saavutettujen hyötyjen takavarikoimiseksi. Vaikka paljon puhutaan siitä, miten vaikeaa tämän toteutuminen käytännössä on, saadaan jatkuvasti enemmän esimerkkejä onnistuneista tapauksista. Näissä usein eri valtioiden viranomaiset ovat yhteistyössä jonkin tietoturvatoimijan kanssa selvittäneet laajoja rikostapauksia johtaen pidätyksiin, laittomien palveluiden sulkemiseen ja varojen takavarikkoon. Tyypillisesti tässä yhtälössä yksityiset turvallisuustoimijat ovat tarjonneet esimerkiksi forensiikkakykyä ja viranomaisyhteistyötä on koordinoitu Interpolin tai muun globaalin organisaation toimesta.

Yksityisillä yrityksillä on usein asiakkaidensa kautta mahdollisuus analysoida ensikäden dataa rikoksen uhrien järjestelmistä, ja on erinomaista mainosta palveluille, mikäli niiden avulla kansainväliseen kyberrikollisuuteen voidaan puuttua.

Viime aikojen esimerkkinä onnistuneista viranomaisoperaatioista toimii pelkästään alkusyksyn ajalta Interpolin ja Afropolin johtama operaatio, jossa yli 25 Afrikan valtion viranomaisten yhteistyön avulla saatiin 14 henkilöä pidätettyä ja yli 20 000 verkkopalvelua suljettiin. Toisessa esimerkkioperaatiossa Kaakkois-Aasiasta käsin toiminut 16shop kalastelutyökaluja tarjoava alusta saatiin suljettua, jossa merkittävässä asemassa toimi Interpolin lisäksi yksityiset firmat, kuten Groub-IB, Palo Alto ja Trend Micro. Vielä viimeaikaisempana ja suomalaisia lähemmin koskettavana esimerkkinä toimii syyskuussa tapahtunut Suomen Tullin tekemä huumeiden myyntiin keskittyneen Piilopuoti-verkkosivuston sulkeminen Tor-verkosta. Tässä mukana toimi Suomen viranomaisten lisäksi poliisivoimia sekä Saksasta että Liettuasta.

Yhteistyö kybermaailmassa on siis mahdollista ja sillä voidaan saavuttaa myös tuloksia kyberrikollisuuteen vastaamisessa. Liikaa toiveita ei kannata kuitenkaan varata esimerkiksi YK:n kyberlainsäädännön edistämiseen pyrkivään prosessiin mutta on hyvä muistaa, että yhteistyö joka tapauksessa kehittyy jatkuvasti. Samoin sekä viranomaisten että yksityisten toimijoiden kyky vastata kyberrikollisuuden muodostamaan uhkaan edistyy koko ajan. Vaikka tuskin koskaan, tai ainakaan lähiaikoina, saadaan kaikkia maailman valtioita saman pöydän ääreen aidosti neuvottelemaan kyberrikollisuuden hillitsemisestä, ovat pienetkin edistysaskeleet silti arvokkaita.

3. NÄITÄ KANNATTAA SEURATA

3.1. Ranskan suunta puhuttaa edelleen

Ranskan suunta sisäisen ja verkkovalvonnan suhteen on puhuttanut Euroopassa pitkin vuotta. Keväinen tekoälyvalvontalaki ja presidentti Macronin kesäiset kommentit sosiaalisen median suitsemisesta herättivät laajaa vastusta ja huolta paitsi maan sisäisesti, myös Euroopan laajuisesti Ranskan suunnasta kohti valvontayhteiskuntaa. Panoksena on nähty olevan muun muassa kansalaisten oikeus yksityisyyteen ja vapaaseen internetiin. Syksyn sateiden myötä on paljastunut, että kritiikki ja vastustus eivät kuitenkaan ole vaikuttaneet maan hallituksen linjaan.

Viimeaikaisiin kehityskulkuihin lukeutuu Ranskan pikavauhtia ajama laki, jonka mukaan verkkoselainten kehittäjät joutuisivat estämään pääsyn tietyille, valtion määräämille sivustoille. Kriitikoiden mukaan tämä voi johtaa verkkosensuuriin, ja esimerkiksi verkkoselainjätti Mozzilla on aloittanut nimien keräämiseen vetoomukseen lakihankkeen pysäyttämiseksi. Euroopan unionin jättivaltiona Ranskan kehitys voi määrittää suuntaa myös Euroopassa sekä tarjota autoritäärisille valtioille ympäri maailman esimerkin sensuurille. Verkkoympäristö tuntuu olevan maassa muutenkin pinnalla, sillä esimerkiksi maan suuret sanomalehdet ilmoittivat estäneensä Open AI:n GPTBotin tietojenkeruun omilta verkkosivuiltaan. Taustalla vaikuttavat pääosin liiketoiminnalliset syyt, kuten haluttomuus jakaa tuotettua sisältöä ilmaiseksi taholle, jolta mitään ei saada vastineeksi. Lisäksi syyksi mainittiin haluttomuus tulla liitetyksi tekoälyn mahdollisesti luomaan väärään ja epätarkkaan sisältöön.

Laajaa kansainvälistä uutisointia saivat myös Ranskan aikeet kieltää iPhone 12 myynti. Tässä tapauksessa nähtävissä ei ollut varsinaista kyberturvallisuusnäkökulmaa, vaikka Apple onkin hiljattain ollut uutisissa ohjelmistoissaan olleiden kriittisten haavoittuvuuksien takia, jotka on sittemmin korjattu. Sen sijaan huolta on herättänyt laitteiden lähettämä elektromagneettinen säteily, joka ylittäisi raja-arvot. Viranomaisten aikeissa kieltää laitteen myynti, on kuitenkin jotain samaa, kuin lakiesitykseen verkkoselainten sensuurista. Loppujen lopuksi kaikki tiivistyy hankalaan rajanvetoon siitä, missä menee yksilöiden ja yritysten oikeuksien ja velvollisuuksien sekä valtion määräämän tai tarjoaman suojelun raja. Vaikka Ranskan toimien taustalla nähtäisiin olevan argumenttien mukaisesti turvallisemman verkkoympäristön luominen, voivat toimenpiteet kääntyä helposti alkuperäistä ideaa vastaan.

Lähteet sivulla 50

3.2. Turvallisuusviranomaiset yhä useammin kybervaikuttamisen kohteina

Elokuussa uutisoitiin, miten Iso-Britannian poliisiviranomaiset olivat joutuneet kyberhyökkäyksen kohteeksi. Hyökkäyksessä Suur-Lontoon poliisitoimen alihankkijaan kohdistui tietomurto, jonka seurauksena verkkoon vuosi poliisissa työskentelevien henkilöiden nimiä, valokuvia ja esimerkiksi tietoja henkilöiden asemasta poliisivoimissa. Tapahtunut vuoto koskettaa pahimmillaan kaikkia kyseisessä poliisitoimessa työskentelevää 47 000 henkilökunnan jäsentä, ja vaikuttaa esimerkiksi peiteroolissa työskentelevien viranomaisten turvallisuuteen. Nyt syyskuussa Manchesterin alueen poliisiviranomainen ilmoitti joutuneensa kiristyshaittaohjelmahyökkäyksen kohteeksi, jossa se oli niin ikään menettänyt poliisien henkilötietoja ja ID-tunnuksia. Näiden kahden hyökkäyksen välissä on aikaa alle kuukausi ja yhteistä näille oli myös se, että hyökkäykset toteutettiin jotakin poliisiviranomaisen alihankkijaa hyväksikäyttäen.

Näiden lisäksi heinäkuussa, vain muutamia kuukausia ennen Iso-Britanniaan kohdistuvia kyberhyökkäyksiä, Pohjois-Irlannin poliisi epähuomiossa kärsi tietovuodosta, jossa sen yli 10 000 viranomaisen ja henkilökuntaan kuuluvan tietoja vuosi verkkoon. Etenkin Pohjois-Irlannissa tilanne on edelleen hyvin tulenarka pitkään jatkuneiden etnisten konfliktien vuoksi, mikä on näkynyt etenkin poliisien tarpeena suojella yksityisyyttään entistäkin tarkemmin. Tapauksessa poliisiviranomainen oli vastannut sähköpostitse tietopyyntöön, johon oli epähuomiossa linkitetty viranomaisia ja henkilökuntaan kuuluvien henkilötietoja koskettava taulukko. Tämän tapauksen lisäksi Pohjois-Irlannin poliisitoimelta oli myös toisessa tietovuodossa varastettu dokumentteja, jotka sisälsivät muun muassa kentällä työskentelevien poliisien tietoja. Molempien tietovuotojen tiedot päätyivät myöhemmin pimeään verkkoon, ja Pohjois-Irlannin poliisi onkin pohtinut esimerkiksi Irlannin tasavaltalaisarmeijan (IRA) roolia molempiin sattuneisiin tapauksiin.

Näiden lisäksi Pohjois-Korean on raportoitu viime kuukausien aikana kohdistaneen kyberhyökkäyksiään muun muassa venäläistä ohjusvalmistajaa vastaan. Nyt viimeisin Microsoftin syyskuussa julkaisema raportti toteaa, että tämä ei ollut Pohjois-Korealta suinkaan ainutlaatuinen hyökkäys vaan se on kohdistanut hyökkäyksiään Venäjän hallintoa, armeijaa ja puolustusteknologiaa kohtaan useita kertoja vuoden alusta alkaen. Pohjois-Korealaisten kyberrikollisten tiedetään myös ulottaneen kyberhyökkäyksiään niin saksalaista, israelilaista, brasilialaista, tšekkiläistä, italialaista, norjalaista, puolalaista kuin suomalaistakin puolustusteollisuutta kohtaan. Microsoftin raportin mukaan 5 prosenttia Pohjois-Korean vakoiluaktiviteetista olisi viimeisen vuoden aikana kohdistunut juuri Suomen puolustusteknologiaa kohtaan. Kiina ja Iran ovat Pohjois-Korean ohessa tunnettuja siitä, että ne keskittävät valtiollisia kyberoperaatioitaan tällä hetkellä etenkin naapurimaidensa ja Yhdysvaltain hallinnon viranomaisia ja puolustusteknologiaa kohtaan.

Turvallisuusviranomaisista onkin tullut hyvin kiinnostava kybervaikuttamisen kohde, sillä samanaikaisesti iskulla saadaan helposti lamautettua merkittävä yhteiskunnallinen toimija, mutta samalla näillä rikoksilla kerätyt tiedot ovat äärimmäisen arvokkaita monelle perinteistäkin rikollisuutta harjoittavalle toimijalle, näin kasvattaen turvallisuusuhkaa niin kansallisesti kuin kansainvälisestikin. Turvallisuusviranomaisiin kohdistuvien kyberrikosten haitat voivatkin pian realisoitua entistä pahemmin todellisen maailman uhkakuvaksi etenkin sen uhreille, kun henkilötietojen vuotaminen mahdollistaa helpomman maalittamisen. Erityisesti peitetehtävissä ja salaisissa operaatioissa toimivien henkilöiden turvallisuus voi olla hyvin uhattu.

3.3. Unohtuiko ukrainalainen kyberrikollisuus?

Ukraina on aiemmin ollut tunnettu kehittyneestä ja korkean tason kyberrikollisuudestaan. Ennen sotaa sen nähtiin olevan maata riivaava ongelma ja esimerkiksi Naton Tallinnassa sijaitseva kyberpuolustuksen osaamiskeskus nosti aiheen esille vuonna 2018 raportissa, jossa kuvataan ukrainalaista kyberrikollisuutta ja pohditaan, onko Ukraina kyberrikollisten turvasatama. Esimerkkejä onnistuneista ukrainalaisten hakkereiden töistä löytyy monia, ja aikojen saatoissa hakkerit ovat useissa eri tapauksissa onnistuneet varastamaan kymmeniä miljoonia dollareita rahaa muun muassa yhdysvaltalaisilta pankkitileiltä. Ukraina on ollut kyberrikolliselle toiminnalle myös suotuisa kasvuympäristö verrattain matalan elintason ja palkkojen, korruption sekä toisaalta korkeakouluissa tarjotun laadukkaan IT-opetuksen myötä.

Sodan myötä ukrainalaisesta kyberrikollisuudesta on kuitenkin puhuttu verrattain vähän. Pääpainopiste on ollut sotaan liittyvien kyberoperaatioiden, niiden onnistumisten ja epäonnistumisten läpikäynnissä. Erityisesti Venäjän Eurooppaan kohdistamat kyberhyökkäykset ovat olleet pinnalla. Luonnollisesti sympatioiden ollessa laajasti Ukrainan puolella, ollaan aiheesta ja ongelmista kenties myös haluttu vaieta ja siten osoittaa tukea Ukrainan taistelussa hyökkäystä vastaan. Kyberrikollisuus tuskin on kuitenkaan kadonnut maasta, vaikka se eittämättä on muuttanut muotoaan. Esimerkiksi Google on raportoinut itäeurooppalaisten kyberrikollisjengien osittaisesta hajaantumisesta sodan ja poliittisten mielipiteiden takia. Aiemmin esimerkiksi venäläisten ja ukrainalaisten on ollut luonnollista tehdä yhteistyötä yhteisen kielen ja kulttuurin takia.

Pitkin vuotta on myös raportoitu onnistuneista kyberrikollisten pidätyksistä. Tässä mahdollisena selittävänä taustatekijänä voi olla tarve signaloida länsimaisille kumppaneille toiminnan tehokkuutta ja osoittaa, että ainakaan enää maa ei toimi turvasatamana rikollisuudelle. Keväällä maan kyberrikospoliisi ilmoitti pidättäneensä ukrainalaisten henkilötietoja venäläisille myyneen miehen. Kesällä taas Europol ilmoitti Saksan ja Ukrainan yhteistyöoperaatiosta, jossa huomattavan Doppelpaymer-kiristyshaittaohjelman taustatekijöitä onnistuttiin pidättämään. Vaikka pidätyksiä on tehty ja osa kyberrikollisista on todennäköisesti sodan myötä alkanut käyttämään taitojaan hyvään – esimerkiksi Ukrainan oman IT-armeijan riveissä - elää kyberrikollisuus ilmiönä varmasti yhä pinnan alla. Maahan virtaa jatkuvalla syötöllä kansainvälistä avustusrahaa, lahjoituksia tehdään useiden eri verkkoalustojen ja sivustojen kautta ja esimerkiksi kryptovaluuttojen muodossa. Olisikin poikkeuksellista, mikäli ainakin osa tästä avustuksesta ei päätyisi myös kyberrikollisten taskuun. On esimerkiksi uutisoitu tapauksista, joissa kalastelusivujen avulla, Ukrainalle tukea luvaten, on uhreilta onnistuttu huijaamaan rahaa.

Viime aikoina Ukrainan vastahyökkäyksen hitaan etenemisen myötä sotatoimista ja tilanteesta on alettu puhumaan mediassa kriittisempään sävyyn. Pikavoittoja ei enää odoteta ja asevoimien ja yhteiskunnan toimintaa on tarkasteltu kriittisesti myös vaikkapa korruption näkökulmasta. Ei olisikaan ihme, mikäli sodan kyberulottuvuudesta uutisoitaessa myös ukrainalainen kyberrikollisuus tekisi paluun uutisoitujen aiheiden listalle.

Lähteet sivulla 50

LÄHTEET

KANSAINVÄLINEN KYBERYMPÄRISTÖ:

Cyberwatch Finland 2023 Viikkokatsaus, viikko 38
Cyberwatch Finland 2023 Viikkokatsaus, viikko 39
https://ec.europa.eu/commission/presscorner/detail/en/speech_23_4426

KYBERRIKOLLISUUS:

Cyberwatch Finland 2023 Viikkokatsaus, viikko 36
Cyberwatch Finland 2023 Viikkokatsaus, viikko 37
Cyberwatch Finland 2023 Viikkokatsaus, viikko 38

TEKNOLOGIA:

Cyberwatch Finland 2023 Viikkokatsaus, viikko 37
Cyberwatch Finland 2023 Viikkokatsaus, viikko 38
Cyberwatch Finland 2023 Viikkokatsaus, viikko 39

PERINTEISTÄ RIKOLLISUUTTA HELPOMPAA TOTEUTTAA KYBERULOTTUVUUDESSA:

Cyberwatch Finland 2023 Viikkokatsaus, viikko 37
Cyberwatch Finland 2023 Viikkokatsaus, viikko 38

KANSAINVÄLISELLÄ KYBERYHTEISTYÖLLÄ ON POTENTIAALIA HYVÄÄN:

https://www.interpol.int/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation
https://tulli.fi/-/tulli-takavarikoi-piilopuoti-kauppapaikan-verkkopalvelimen-jalleen-merkittava-onnistuminen-anonyymissa-tor-verkossa
https://www.interpol.int/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation

RANSKAN SUUNTA PUHUTTAA EDELLEEN:

https://www.reuters.com/technology/why-has-france-banned-sales-apples-iphone-12-2023-09-13/ https://www.euractiv.com/section/artificial-intelligence/news/several-french-media-block-openais-gptbot-over-data-collection-concerns/
https://foundation.mozilla.org/en/campaigns/sign-our-petition-to-stop-france-from-forcing-browsers-like-mozillas-firefox-to-censor-websites/

TURVALLISUUSVIRANOMAISET YHÄ USEAMMIN KYBERVAIKUTTAMISEN KOHTEINA:

Cyberwatch Finland 2023 syyskuun kuukausikatsaus
https://www.securityweek.com/a-second-major-british-police-force-suffers-a-cyberattack-in-less-than-a-month/
https://www.securityweek.com/northern-irelands-top-police-officer-apologizes-for-industrial-scale-data-breach/
https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-target-russian-govt-defense-orgs/
https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/

UNOHTUIKO UKRAINALAINEN KYBERRIKOLLISUUS?:

https://www.ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf
https://www.zdnet.com/article/the-war-in-ukraine-has-shaken-up-the-cybercriminal-ecosystem-google-says/https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets
https://therecord.media/ukraine-arrests-man-for-selling-data-on-300-million-to-russians

UHKATIEDUSTELUSEURANTA

Cyberwatch Finland julkaisee uhkatiedusteluseurannan, jossa koottuna on viimeisen kuukauden ajalta merkittävimpiä kyberhyökkäyksiä sekä tietoa aktiivisimmista uhkatoimijoista ympäri maailman. 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 -KAMPANJOIA

KANSAINVÄLINEN RIKOSTUOMIOISTUIN, ICC

AJANKOHTA: 19.9.2023

KUVAUS: Kansainvälinen rikostuomioistuin ilmoitti joutuneensa kyberhyökkäyksen kohteeksi. Sotarikoksista syyttämisestä vastuussa oleva fyysisesti Hollannin Haagissa sijaitseva tuomioistuin on ollut viime aikoina uutisissa muutoinkin, kun se julkisesti syytti useita suuren profiilin venäläisiä poliitikkoja kansainvälisen oikeuden rikkomisesta. Esimerkiksi presidentti Vladimir Putinista annettiin pidätysmääräys keväällä 2023. Nyt tapahtuneesta kyberhyökkäyksestä tiedetään suhteellisen vähän, ja sen tutkinta on yhä käynnissä. Pahimmillaan on mahdollista, että joitain tuomioistuimen salatuista dokumenteista tai tietoa esimerkiksi käynnissä olevista tutkinnoista on vuotanut hakkereille.

TEKIJÄ: Ei varmaa tietoa, mutta epäilykset kohdistuvat Venäjään tai sen käyttämiin rikollisryhmiin.

MOTIIVI: Epäselvä, potentiaalisia tavoitteita salattujen dokumenttien anastaminen tai tuomioistuimen toiminnan häiritseminen hyökkäyksen informaatiovaikutushyödyn ohella.

VAIKUTUKSET: Tuomioistuin itse ei ole ilmoittanut esimerkiksi tietojen päätymisestä rikollisten haltuun tai muista kokemistaan haittavaikutuksista. Hollannin yleisradioyhtiö NOS:n mukaan salattuja tietoja olisi kuitenkin vuotanut, millä voi olla vaikutusta tuomioistuimen käynnissä oleviin tutkintoihin.

MERKITTÄVIMPIÄ KYBERISKUJA JA -KAMPANJOIA

MAROKON MAANJÄRISTYS

AJANKOHTA: Syyskuu

KUVAUS: Ranskankieliset verkkorikolliset kehittivät huijauksen, jolla huijasivat ihmisiä lahjoittamaan rahaa Marokon maanjäristyksen uhrien auttamiseen. Kyberrikolliset rekisteröivät käyttöönsä kaksi verkko-osoitetta, jolla he pyrkivät jäljittelemään humanitaarista apua tarjoavia avustusjärjestöjä, kuten tässä tapauksessa Ranskan Punaisen Ristin järjestöä. Usein humanitaariset kansalaisjärjestöt katastrofin satuttua aloittavat rahoituksien keräyksiä katastrofialueille. Tämä puolestaan houkuttelee verkkohuijareita keräämään varoja katastrofin nimissä, kuten tällä hetkellä kerätään Marokon maanjäristyksen nimissä rikollisesti rahalahjoituksia. Kyberrikolliset saattavat myös myydä valesivustoillaan tuotteita, joilla "kerätään varoja" katastrofin uhreille. Tällöin uhri saattaa rahojen lisäksi menettää myös pankkikorttitietonsa.

TEKIJÄ: Ei julkistettu

MOTIIVI: Taloudellinen

VAIKUTUKSET: Vaikutukset mittavimpia niille, jotka lahjoittavat valesivustojen kautta. Uhrit menettivät myös rahansiirtojen lisäksi omia henkilötietojaan sekä pankki- ja luottokorttitunnuksiaan. Aiheuttaa myös mainehaittaa niille organisaatioille, joita valhesivustot jäljittelevät.

TRAFICOM

AJANKOHTA: 18.09.2023 ja 07.09.2023

KUVAUS: Suomen liikenne ja viestintävirasto Traficom joutui syyskuun aikana kahteen kertaan palvelunestohyökkäyksen kohteeksi. Hyökkäykset ovat osa laajempia suomalaisiin viranomaisiin ja julkishallinnon kohteisiin kohdistuneita iskuaaltoja, joita venäjämieliset hakkeriryhmät toteuttavat usein tapanaan vastustaa Suomen viranomaisten tai poliittisten päättäjien ratkaisuja Venäjään liittyen. Syyskuussa saman hakkeriryhmän kohteita ovat olleet sen omien ilmoitusten mukaan esimerkiksi myös Helsingin päärautatieasema ja Saimaalla risteilyjä järjestävä yritys.

TEKIJÄ: Venäläinen hakkeriryhmä NoName057(16). Kyseinen ryhmä tekee päivittäin matalan tason palvelunestohyökkäyksiä venäjävastaisiksi kokemiaan toimijoita kohtaan ympäri maailman.

MOTIIVI: Informaatiovaikuttaminen ja pelon herättäminen suomalaisissa.

VAIKUTUKSET: Hyvin vähäiset. Jotkin Traficomin verkkopalvelut kärsivät hetkellisistä toimintahäiriöistä, mutta pitkäkestoista vaikutusta tai minkäänlaista tietovuotoa ei tapahtunut.

MGM RESORTS

AJANKOHTA: 11.9.-19.9.2023

KUVAUS: Hotelli ja kasinopalveluita tarjoava MGM Resorts joutui syyskuussa laajan kyberhyökkäyksen uhriksi. Hyökkäys vaikutti laajasti yhtiön toimintoihin ja vasta yhdeksän päivää iskun jälkeen yhtiö ilmoitti toimintojen olevan täysin palautettu. Yhtiö on joutunut myös aiemmin uhriksi, sillä vuonna 2019 yli 10 miljoonan asiakkaan tiedot vuosivat verkkoon.

TEKIJÄ: Kiristyshaittaohjelmia hyödyntävä ALPHV (tunnetaan myös nimellä BlackCat) -hakkeriryhmittymä otti vastuun teosta

MOTIIVI: Taloudellinen

VAIKUTUKSET: Vaikutukset ulottuivat yhtiön verkkosivuihin, varausjärjestelmään sekä kasinoiden pankkiautomaatteihin, pelikoneisiin ja luottokorttilaitteisiin. Ainakin 30 yhtiön omistuksessa olevaa hotellia ja kasinoa kärsi vaikutuksista.

AKTIIVISIMPIA TOIMIJOITA

SANDMAN

KUVAUS: Aiemmin tuntematon uhkatoimija, jonka kotimaasta tai koosta ei ole tietoa. Toimintatapaa on kuvattu edistyneeksi ja se on useissa lähteissä määritelty APT-ryhmittymäksi, mikä viittaisi valtion toimintaan taustalla.

VIIME AIKOJEN TOIMINTA: Kohteena ovat olleet erityisesti Lähi-idässä, Länsi-Euroopassa ja Etelä-Aasiassa toimivat televiestintää tarjoavat yritykset.

TOIMINTATAVAT JA TAKTIIKAT: Hyödyntää LuaDreamiksi nimettyä käyttäjän laitteelta tietoa varastavaa infostealer-haittaohjelmaa. Vakoilun avulla saatua tietoa voidaan hyödyntää esimerkiksi uusien kyberhyökkäysten suunnitteluun, tiedolla voidaan kiristää kohdetta tai tieto voidaan tarvittaessa myydä eteenpäin pimeän verkon markkinapaikoilla. Myös tieto itsessään voi olla arvokasta hyökkääjälle.

BIANLIAN

KUVAUS: Alun perin jo vuonna 2019 havaittu uhkatoimija, joka vuonna 2022 nousi uudelleen esiin nyt nimellä BianLian ransomware. Tarkkaa tietoa ryhmän kotimaasta ei ole, mutta se tunnetaan etenkin Yhdysvaltoihin ja sen liittolaismaihin kohdistuvista kiristysiskuista. Nimi BianLian viittaa kiinalaiseen teatteriin liitettävästä kasvojen vaihdon käsitteestä, mutta nimen lisäksi mikään muu seikka ei indikoi millään tavoin ryhmän mahdollista kotimaata.

VIIME AIKOJEN TOIMINTA: Jatkuvat hyökkäykset englanninkielisillä alueilla toimivia yrityksiä ja julkishallinnon elimiä kohtaan. Viime aikoina kohteet etenkin Yhdysvalloissa, mutta myös eurooppalaisia ja australialaisia organisaatioita on joutunut ryhmän uhriksi.

TOIMINTATAVAT JA TAKTIIKAT: Ryhmä valikoi kohteikseen haavoittuvia VPN:n tai pilvipalveluita käyttäviä kohteita ja hyödyntää iskuissaan itse luomiansa Go-ohjelmointikieleen pohjautuvia kiristyshaittaohjelmia. Etenkin yhdysvaltalaisen Sonicwall yrityksen asiakkaat ovat olleet kohteena, palveluntarjoajan VPN sovelluksesta löytyneiden heikkouksien vuoksi.

CACTUS RANSOMWARE

KUVAUS: Aktiivinen maaliskuusta 2023 alkaen. Kohdistaa hyökkäyksiään suurille kaupallisille aloille, taloussektorille sekä rakennusalalle. Ryhmä käyttää tyypillisiä kiristyshaittaohjelmataktiikoita mutta omana erikoisuutenaan sillä on lisänä jäljityksen esto -ominaisuus. Toistaiseksi ryhmän alkuperää ei ole tuotu julkisuuteen.

VIIME AIKOJEN TOIMINTA: Ryhmän tiedetään lisänneen pimeän verkon sivustolleen äskettäin viisi korkean profiilin uhria. Uhrit ovat eri puolilta maailmaa ja edustavat eri toimialoja. Viimeisen listauksen suuryritykset ovat pääosin Yhdysvalloista, Kanadasta tai esimerkiksi Ranskasta.

TOIMINTATAVAT JA TAKTIIKAT: Ryhmä hyödyntää etenkin tunnistettuja VPN haavoittuvuuksia saadakseen pääsyn kohdejärjestelmiin. Käyttää monia eri taktiikoita ja tekniikoita kiristyshaittaohjelmahyökkäyksissään. Kiristyshaittaohjelmaiskujen lisäksi ryhmä myös varastaa uhreiltaan tietoja.

EVASIVE GELSENIUM

KUVAUS: Evasive Gelsenium on vuodesta 2014 asti toiminut kybervakoiluryhmä, APT-ryhmä, jonka operaatiot on suunnattu Itä-Aasian ja Lähi-idän viranomais-, koulutus- ja elektroniikkavalmistajille. Ryhmä omaa valtavan teknisen kapasiteetin ja ohjelmointiosaamisen, jonka vuoksi ryhmä on onnistuneet toteuttamaan pitkiäkin operaatioita ilman paljastumista.

VIIME AIKOJEN TOIMINTA: Kohdisti pitkään jatkuneen vakoiluoperaationsa Kaakkois-Aasian hallintoelimiä kohtaan vuosina 2022–2023. Kohteina etenkin Tiibetin alue, Taiwanin hallinto sekä uiguurit.

TOIMINTATAVAT JA TAKTIIKAT: Hyödyntää operaatioissaan takaovia ja on hyvin edistyksellinen APT-ryhmä.

POIMINNAT CYBERWATCHFINLAND VIIKKOKATSAUKSISTA

// Cyberwatchin analyysitiimi

TÄSSÄ KOOSTEESSA SEURAAVAT ARTIKKELIT

Viikolta 32:
- Venäjä jatkaa hybridioperaatioitaan verkossa
- Lasten älylaitteet vaikuttavat oppimiseen ja lisäävät kyberuhkia

Viikolta 34:
- SIM-kortin kaappaus kyberrikollisten työkaluna

Viikolta 35:
- Kyberhyökkäykset nopeutuvat – päivitystahtivaatimus kasvaa

VENÄJÄ JATKAA HYBRIDIOPERAATIOITAAN VERKOSSA

Venäjä ja Venäjään liitännäiset toimijat ovat jatkaneet paitsi sotatoimiaan Ukrainassa, myös hybridivaikuttamisoperaatioitaan ympäri maailmaa. Hybridivaikuttamisella ei ole universaalisti hyväksyttyä määritelmää, mutta laajassa mielessä sillä yleensä tarkoitetaan vihamielisen vaikuttamisen muotoja, joiden tavoitteena voi olla poliittisen järjestelmän tai koko yhteiskunnan vakauden horjuttaminen. Hybridivaikuttamisen keinot voivat olla esimerkiksi poliittisia, diplomaattisia, taloudellisia ja sotilaallisia sekä informaatio- ja kybervaikuttamista. Erityisesti verkossa tapahtuva Venäjän hybridivaikuttaminen informaatio- ja kyberkeinoin on ollut voimissaan kesän aikana. Pääasiallisesti Venäjän vaikuttaminen on tapahtunut kahdella tavalla: kyberhyökkäyksillä ja valeuutisten levittämisellä. Myös muuta hybridivaikuttamista tapahtuu, ja todennäköisesti näkyvillä on vain jäävuoren huippu.

Kesällä venäläiset ovat olleet aktiivisia kyberhyökkääjiä. Esimerkiksi haktivistiryhmä NoName057(16) on iskenyt lähes päivittäin palvelunestohyökkäyksillä. Kohteina ovat olleet ryhmän russofobisiksi määrittelemät valtiot, jotka tukevat Ukrainan sotatoimia. Uhreiksi ovat valikoituneet esimerkiksi Suomi, Liettua ja Italia, joissa hyökkäykset ovat kohdistuneet paitsi julkisen myös yksityisen sektorin toimijoihin. Toinen kesän aikana pinnalla ollut merkittävä toimija on Anonymous Sudan – niin ikään erityisesti palvelunestohyökkäyksiä suosiva toimija – joka on hyökännyt Euroopan investointipankkia vastaan ja uhannut muun muassa Israelia kyberhyökkäyksillä. Ryhmä pyrkii esiintymään sudanilaisena ja islamistisena, mutta on asiantuntijoiden mukaan venäläinen toimija. Se on omien sanojensa mukaan suorittanut myös edistyksellisempiä operaatiota. Heinäkuun alussa Anonymous Sudan ilmoitti saaneensa haltuunsa yli 30 miljoonan Microsoft-käyttäjän käyttäjätietoja ja olevansa valmis myymään ne eteenpäin 50 000 dollarin maksua vastaan. Microsoft on kiistänyt tapahtuneen, ja on todennäköistä, että tietovuotoa ei ole tapahtunut. Kolmas merkittävä toimija on Turla, usein FSB:hen liitetty toimija, joka on kesällä pyrkinyt hyökkäämään erityisesti vakoiluhaittaohjelmilla Ukrainan puolustusvoimia vastaan.

Eri toimijoilla vaikuttaa olevan erilaiset toimintatavat ja tavoitteet. Esimerkiksi NoNamen pyrkimyksenä vaikuttaa olevan lähinnä julkisten propagandavoittojen saaminen Ukrainaa tukevista valtioista ja se toimii avoimesti Venäjän nimissä. Anonymous Sudan taas toimii peitellymmin ja kiistää yhteydet Venäjään, mutta suorittaa Venäjän intresseissä olevia hyökkäyksiä. Turla suorittaa teknisesti vaativampia operaatioita, ja sen viime aikojen operaatiot vaikuttavat liittyvän lähinnä Ukrainan sotaan. Venäläisessä kybertoiminnassa merkittävää on yksityisen ja valtiojohtoisen toiminnan rajojen hämärtyminen. Edellä mainitut ryhmät tekevät ideologisia iskuja, mutta pelkän maksimaalisen tuhovaikutuksen lisäksi esittävät myös lunnasvaatimuksia. Myös yllättäviä kohteita on nähty. Anonymous Sudanin on kohdistanut hyökkäyksiään muun muassa Keniaan, mikä vaikuttaa päällisin puolin sattumanvaraiselta kohteelta. Selittävänä tekijänä voivat kuitenkin toimia Kenian presidentin esittämät kommentit Venäjästä, joissa syytetään Venäjää Afrikan selkään puukottamisesta viljasopimuksesta vetäytymisellä. Tapaus osoittaa, miten pitkä käsi Venäjällä on, ja kuinka yllättäviinkin kohteisiin venäläiset ovat valmiita käyttämään resurssejaan. Venäjällä riittää kyberkapasiteettia myös ei-ensisijaisiin kohteisiin, sillä todennäköisesti kyberoperaatioiden painopiste on edelleen Ukrainassa.

Toinen verkossa tapahtuva Venäjän vaikuttamisen muoto on valeuutisten levittäminen, joka on jatkunut niin Euroopassa kuin muualla maailmassa. Kesäkuussa Ranskassa paljastui informaatiooperaatio, jossa venäjämielistä sisältöä pyrittiin levittämään. Teemoja olivat muun muassa Venäjäpakotteiden väheksyminen, Ukrainan syyttäminen natsismista sekä länsimaiden russofobia. Väitteitä levitettiin oikeita uutissivustoja, kuten Le Mondea ja Le Figaroa sekä Ranskan viranomaisten verkkosivuja ulkonäöllisesti muistuttavien sivustojen kautta. Sisältöä jaettiin myös valetilien kautta. Toinen huomionarvoinen tapaus on Ruotsissa tapahtuneet koraanin poltot, jotka ovat aiheuttaneet suurta vastustusta islamilaisessa maailmassa. Ruotsin viranomaiset ovat löytäneet taustalla vaikuttavan venäläisen informaatiooperaation, jonka myötä valeuutisia on syötetty maailmalle ja pyritty lietsomaan vihaa Ruotsia kohtaan. Valeuutisia on tehty esimerkiksi arabiaksi ja sitä on levitetty länsimaissa jo sanktioiden alla olevien Russia Todayn ja Sputnikin uutissivustojen kautta.

Kokonaisuutena Venäjän verkossa suorittamat hybridioperaatiot kyberhyökkäyksin ja disinformaatiokampanjoin jättävät kaksijakoisen kuvan. Esimerkiksi palvelunestohyökkäysten vaikutus on usein varsin pientä ja väliaikaista. Toisaalta maalla on myös edistyksellisiä ja vaativiin operaatioihin kykeneviä yksiköitä. Venäjän valeuutisten on taas ehkä ajateltu olevan menneen talven lumia, sillä Ukrainan sodan myötä Venäjän potentiaali saada omaa narratiiviaan läpi länsimaissa on käytännössä olematon. Sen sijaan Venäjä on suunnannut katseensa muualle, kolmansiin maihin, jotka Venäjä voi kenties edelleen suostutella puolelleen. Olennaista on huomata verkkoulottuvuus vain yhtenä monista toimintakentistä, joilla Venäjä pyrkii vaikuttamaan. Toiminnan muodostamaa uhkaa ei pidä vähätellä tai unohtaa.

LASTEN ÄLYLAITTEET VAIKUTTAVAT OPPIMISEEN JA LISÄÄVÄT KYBERUHKIA

Älylaitteet ovat lähes jokaiselle kansalaiselle osa päivittäisiä arjen toimintoja. Suurimpina poikkeavina ihmisryhmänä tästä ovat kaikista nuorimmat ja vanhimmat kansalaiset. Kuitenkin ollaan menossa suuntaan, jossa yhä nuorempana erilaisia älylaitteita otetaan käyttöön. Jo pienetkin lapset ovat tänä päivänä hyvin taidokkaita älylaitteiden käyttäjiä. Viimeistään koulutien alkaessa lapsi saa ensimmäisen oman matkapuhelimen tai muun älylaitteen, kuten esimerkiksi älykellon, jolla voi olla yhteydessä vanhempiin koulupäivän aikana. Lapset oppivat myös nopeasti etsimään sisältöä älylaitteista sovellusten kautta eikä vanhempien valvova katse aina näe, mikäli lapsi epähuomiossa harhautuu sellaisen sisällön äärelle, joka ei ole lapsille tarkoitettu.

Espanjalainen neuropsykologian tohtori Alvaro Bilbao on julkaissut tutkimuksen lasten lisääntyneen ruutuajan yhteyksistä lasten neuropsyykkisiin oireisiin. Bilbaon mukaan lasten masennuksen ja riippuvaisuuksien sekä keskittymishäiriöiden riski kasvaa sitä suuremmaksi, mitä enemmän he viettävät varhaislapsuudessaan aikaa mobiiliruutujen äärellä. Tutkimuksen perusteella erityisesti alle kuusivuotiaiden ruutuaikaa mobiililaitteilla tulisikin rajoittaa huomattavasti tai jopa kieltää se kokonaan. Tähän samaan kuuden vuoden suositukseen ovat päätyneet muutkin tahot, kuten Yhdysvaltain lastenlääketieteen seura.

Yhdistyneiden kansakuntien kasvatus-, tiede- ja kulttuurijärjestö Unesco on myös vaatinut koulumaailmaan tiukempia älylaiterajoituksia. Kuten Bilbao, myös YK:n kasvatus-, tiede- ja kulttuurijärjestöUnescon raportti tuo esille, kuinka älypuhelimien käyttö aiheuttaa keskittymishäiriöitä ja vaikuttaa lasten ja nuorten oppimiseen sekä hyvinvointiin kielteisesti. Jo pelkästään puhelimien läsnäolon on havaittu vaikuttavan kielteisesti oppimiseen. Unescon raportissa peräänkuulutetaan opetusteknologian parempaa sääntelyä. Puutteellinen koulutusteknologian valvonta altistaa lapset myös monille turvallisuusuhkille, kuten kyberhyökkäyksille sekä nettikiusaamiselle. Unescon raportin mukaan tietotekniikkaa pitäisi käyttää oppitunneilla vain sellaiseen tarkoitukseen, josta on oikeasti hyötyä oppimiselle. Kun puhelimet ovat mukana luokissa, johtaa se helposti niiden käyttöön opiskeluun liittymättömissä asioissa, mikä taas vaikuttaa kielteisesti muistamiseen ja ymmärtämiseen.

Lähes neljäsosa maista on tällä hetkellä kieltänyt puhelimen käytön kouluissaan kokonaan. Suomessakin hallitus on selkeyttänyt ohjeistuksia ja sääntelyä kännyköiden käytöstä kouluissa. Suomessa opettajat saavat tällä hetkellä kieltää puhelinten käytön ja kerätä ne myös pois, mikäli niiden käyttö koetaan häiritseväksi. Haastavaa on kuitenkin valvoa puhelimien käytön täyskieltoa esimerkiksi välitunneilla. Monien opettajien harmina saattaa tänä päivänä myös olla luvaton kuvaaminen ja muunlainen kiusanteko.

Matkapuhelimen tai jonkun muun älylaitteen olemassaolo antaa kuitenkin mielenrauhaa niin lapselle itselleen kuin hänen huoltajalleenkin. Älylaitetta hankkiessa on kuitenkin hyvä varmistua siitä, että puhelin tai laite on edelleen valmistajansa tuen piirissä, jotta puhelin saa tarvittavat tietoturvakorjaukset sekä päivitykset. On myös vanhempien tehtävä valvoa sitä, miten alaikäinen käyttää puhelintaan ja millaisia sovelluksia hän pystyy omatoimisesti älylaitteeseen lataamaan. Esimerkiksi monet kyberrikolliset hyödyntävät juuri lapsille suunnattuja pelisovelluksia rikostensa mahdollistamiseen. Erilaisia sovellus- ja käyttörajoituksia on verraten helppo kuitenkin laittaa lasten puhelimiin tänä päivänä. Aikuisten tehtävänä on myös toimia lapsen tärkeimpänä mediakasvattajana, opettaa älylaitteiden oikeaoppista käyttöä ja myös nettietikettiä, koska lapset eivät aina tiedä, mikä on riskialtista toimintaa. Kyberturvallisuuskoulutus pitäisi olla osa älylaitteiden käytön aloittamista. Haasteena on, ettei monet vanhemmatkaan ole tunnistaneet digilaitteiden riskejä.

SIM-KORTIN KAAPPAUS KYBERRIKOLLISTEN TYÖKALUNA

SIM-kortin kaappaushyökkäykset ovat yleistyneet kansainvälisesti samaa vauhtia, kun älypuhelinten määrä on kasvanut. Kasvun myötä niitä katoaa koko ajan enemmän ja niiden käyttäminen esimerkiksi kaksivaiheisessa tunnistautumisessa on lisääntynyt. Mobiililaitteisiin kohdistuvat hyökkäykset ovat usein huomaamattomia aina siihen asti, kunnes on todennäköisesti liian myöhäistä. Onnistunut SIM-kortin kaappaus mahdollistaa hyökkääjän pääsyn muun muassa uhrin viestihistoriaan, yhteystietoihin, sähköposteihin, sosiaalisen median profiileihin, pankkitunnuksiin sekä kaikkiin niihin palveluihin, jotka ovat linkitetty kaapattuun puhelinnumeroon. Useimmiten SIM-kortin kaappauksen päätavoite on taloudellinen. Hyökkäys perustuu tekstiviesteihin perustuvan kaksivaiheisen tunnistautumisen heikkouksien hyödyntämiseen.

SIM-kortti aktivoi puhelimessa puhelut, tekstiviestit sekä datapalvelut ja kussakin SIM-kortissa on yksilölliset tunnisteet, jotka yhdistävät sen vain yhteen matkapuhelinliittymään. SIM-kortin siirtäminen toiseen puhelimeen siirtää myös automaattisesti kortin mobiilipalvelut uuteen laitteeseen. Fyysistä korttia ei aina tarvitse siirtää, vaan mobiilipalvelut voidaan helposti siirtää SIM-kortilta toiselle. Toiminta on teleoperaattoreille arkipäiväistä ja tätä tehdään esimerkiksi, jos puhelin on hävinnyt tai varastettu. Juuri tästä syystä mobiililaitteet ovat alttiita SIM-swapille eli SIM-kortin kaappauksille. Näissä hyökkäyksissä huijari saa puhelinnumeron hallintaansa käyttämällä uhrin henkilöllisyyttä ja muita henkilökohtaisia tietoja saaden puhelinoperaattorin liittämään uhrin numeron huijarin hallussa olevaan SIM-korttiin. Onnistuttuaan huijari pystyy ohittamaan kaikki tekstiviestipohjaiset kaksivaiheiset todennusprosessit kyseistä numeroa käyttäville käyttäjätileille. SIM-kortin kaappauksessa käyttäjän kaikki tiedot aina puhelinnumerosta alkaen siirretään uudelle kortille, jolloin alkuperäinen lakkaa toimimasta.

Kiristyshaittaohjelmaryhmä Lapsuksen on raportoitu hyödyntäneen SIM-kortin kaappausmenetelmää monipuolisesti tietomurroissaan ja kiristyshaittaohjelmaiskuissaan. Lapsus$ on nuorista englantilaisista ja brasilialaisista koostuva, löyhästi sitoutunut kyberrikollisryhmä, joiden toiminnan motivaationa on pääosin vaikuttanut olevan maineen saaminen. Yhdysvaltain turvallisuusviranomaiset julkaisivat heinäkuun lopulla laajan raportin ryhmän toimintatavoista ja hyökkäysmenetelmistä. Ryhmä on aiemmissa rikoksissaan käyttänyt SIM-kortin kaappausta hyökkäysmenetelmänä erityisesti päästäkseen kohdeyrityksen sisäiseen verkkoon varastamaan luottamuksellista tietoa, kuten lähdekoodia, käyttäjätunnuksia tai asiakkaiden tietoja. Osa ryhmän toteuttamista SIM-korttien vaihdoista on tehty suoraan teleoperaattoreilta kaapattujen asiakashallintatyökalujen kautta. Ryhmä hyödynsi joissakin hyökkäyksissään teleoperaattorien tai kohdeorganisaatioiden sisäpiiriläisiä maksamalla heille palveluksista ja tiedoista. Huolta on herättänyt etenkin se, että tämänkaltainen kyberrikollisten ryhmä on näinkin helposti päässyt murtautumaan yritysten arvokkaaseen tietoon hyödyntämällä tekstiviesteihin pohjautuvaa tunnistautumista.

SIM-korttien kaappaaminen ei siis kosketa pelkästään yksittäistä mobiililaitteen käyttäjää, vaan voi olla myös kyberrikollisryhmän yleisin sisäänpääsytekniikka valittuun kohteeseen. Hyökkäysten toteuttamiseksi tarvitaan tietty määrä tietoa kohteesta. Näihin tietoihin päästään verraten helposti käsiksi pelkästään ostamalla tiedot pimeiltä markkinoilta tai keräämällä tiedot sosiaalisen median profiileista. SIM-kortin kaappaus nojaakin vahvasti mahdollisimman suuren henkilötietomäärän keräämiseen. Monet tätä kyberhyökkäystapaa käyttävät hyötyvätkin potentiaalisen uhrin kaikista yksilöivistä tiedoista, joita sosiaalisen median alustat ja pimeillä markkinoilla kiertävät tietoja yhdistelevät kombolistat ovat täynnä. Huijarit usein myös seulovat someprofiileja löytääkseen vihjeitä, kuten lemmikkien nimiä, joita voidaan käyttää salasanan palauttamiseen liittyvinä turvakysymyksinä ja joiden avulla kaapata puhelimia. SIM-korttien kaappaamisen ehkäisemiseksi toimii esimerkiksi melko yksinkertainen keino: siirtyminen tekstiviesteihin perustuvasta kaksivaiheisesta tunnistautumisesta salasanattomiin vaihtoehtoihin tai erillisiin todennussovelluksiin.

KYBERHYÖKKÄYKSET NOPEUTUVAT – PÄIVITYSTAHTIVAATIMUS KASVAA

Tietoturvayhtiö Sophos julkaisi viime viikolla kyberhyökkäysten trendejä tarkastelevan raportin, jonka mukaan sekä hyökkäysten havainnointi että uhkatoimijoiden toiminta on merkittävästi tehostunut viimeisen vuoden aikana. Käytännössä tämä näkyy lyhentyneenä ”oleskeluaikana” (dwell-time), jonka hyökkääjä viettää kohdeorganisaation järjestelmissä ennen varsinaisen iskun toteuttamista tai kiinnijäämistä. Tällä hetkellä noin kahdeksan vuorokauden mediaaniin lyhentynyt aika voi kertoa raportin mukaan siitä, että kehittynyt torjunta- ja havainnointikyky on heikentänyt hyökkääjien mahdollisuuksia iskujen valmisteluun. Toisaalta yhtä todennäköinen selitys on, että nimenomaan hyökkääjien toiminta on kehittynyt ja tehostunut mahdollistaen entistä nopeamman syklin operaatioissa. Jälkimmäistä ajatusta tukee myös muut tilastot jatkuvasti lisääntyvistä onnistuneista hyökkäyksistä; toisaalta epäonnistuneista hyökkäyksistä on vaikea saada tilastotietoja. Joka tapauksessa lyhentynyt oleskeluaika tarjoaa puolustavalle organisaatiolle vähemmän mahdollisuuksia verkkoon tunkeutuneen toimijan havaitsemiseen ja iskun vaikutusten vähentämiseen. Vaikka kyseessä olisikin puolustuksellisen kyvyn kehittyminen, johtaa tämä väistämättä siihen, että myös rikolliset enemmin tai myöhemmin reagoivat nopeuttamalla operaatioitaan, jolloin lopputulos on joka tapauksessa entistä vauhdikkaammin toteutettavat kyberiskut.

Nopeutuneiden operaatioiden lisäksi viime aikoina jonkin verran huomiota on saanut se, miten nopeasti kyberhyökkääjät hyödyntävät sekä itse löytämiään että julkisesti tiedotettuja haavoittuvuuksia kohdejärjestelmissä. Haavoittuvuuden löytymisestä ei tyypillisesti mene montaakaan päivää ennen kuin nopeasti reagoivat uhkatoimijat ovat valmiita sitä hyödyntävän hyökkäystavan tai työkalun käyttöön. Sekä lyhentynyt oleskeluaika että kiihtyvä tahti, jolla haavoittuvuuksia hyödynnetään, haastaa organisaatioita ottamaan kyberturvallisuuden suhteen entistä aktiivisemman ja enemmän toimia vaativan otteen. Kerran viikossa suoritettavat järjestelmäskannaukset tai uusien päivitysten asentaminen eivät enää riitä, sillä isku voidaan suunnitella, valmistella ja toteuttaa parhaimmillaan tämän ajanjakson sisällä. Lisäksi monen organisaation kohdalla löytyy huomattavasti vanhempia ja huomiotta jääneitä haavoittuvuuksia, jotka kuitenkin ovat jo yleisesti tiedossa.

Päivitysten tahdin kiihdyttäminen on myös monen sovellustarjoajan huomaama tarve. Esimerkiksi Google ilmoitti elokuussa tihentävänsä Chrome-selaimeen julkaistavien päivitysten tahtia kerran viikossa ilmestyviksi aiemman joka toisen viikon sijaan. Samoin Apple on ottanut tänä vuonna käyttöön entistä tiheämmin julkaistavat ja nimenomaan tietoturvahaavoittuvuuksia korjaavat pikapäivitykset. Moni sovellustarjoaja julkaisee myös aktiivisesti päivityksiä uusia haavoittuvuuksia havaittuaan. On silti eri asia, kuinka nopeasti nämä päivitykset päätyvät organisaatioissa käyttöön. Päivityksen julkaisusta saattaa kulua useitakin päiviä, ennen kuin siihen reagoidaan, ja näin mahdollistetaan hyökkääjille arvokas aikaikkuna, jolloin haavoittuvuus on hyödynnettävissä.

Aktiivinen haavoittuvuuksien seuranta ja päivitysten asentaminen ovat siis jatkuvasti keskeisemmässä asemassa kyberturvallisuuden toteuttamiseksi. Tiedossa olevien haavoittuvuuksien hyödyntäminen on käyttäjätunnusten väärinkäytön ohella yksi yleisimmistä kyberhyökkäysten toteutustavoista, ja pahimmillaan paikkaamattomat tietoturva-aukot tarjoavat uhkatoimijalle helpon ja vapaan pääsyn organisaation järjestelmiin. Kun myös tahti, jolla uhkatoimijat voivat operaationsa suorittaa kiihtyy, korostuu jatkuvasti tarve pysyä tietoisena omia järjestelmiä koskevista haavoittuvuuksista ja niihin saatavilla olevista päivityksistä. Parhaimmillaan ajallaan asennettu päivitys voi estää meneillään olevan tunkeutumisen ja vähimmilläänkin se rajoittaa sitä, miten helposti hyökkääjä voi järjestelmiin päästä. ■

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Cyberwatch Finland

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

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

PALVELUMME

Johdon neuvontapalvelut

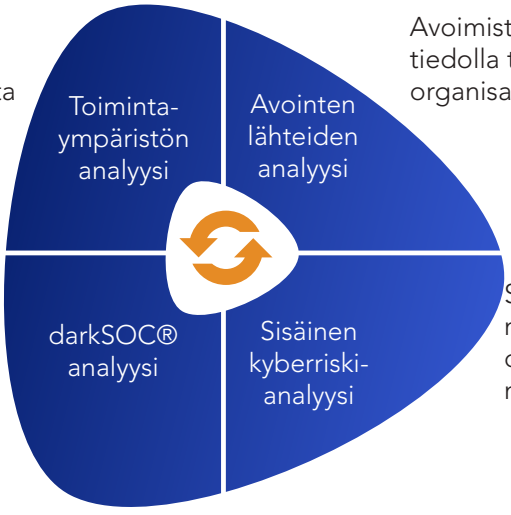
Olemme kokenut ja luotettu johdon neuvonantaja ja asiantuntija. Tuemme sinua kokonaisturvallisuuden, kyberturvallisuuden, sisäisen turvallisuuden asiakokonaisuuksissa ja kumppaniriskien hallinnassa. Työskentelymetodeinamme ovat muun muassa teema-alustukset, muistiot, työpajat ja skenaariotyöskentely.

Toimintaympäristön tilannekuva

Kokonaisvaltainen kybertilannekuva muodostuu Cyberwatch Finlandin kehittämän modulaarisen palvelun avulla, johon tarvittavaa dataa kerätään lukuisin eri menetelmin.

Toimintaympäristön analyysilla muodostetaan eri näkökulmista kuva organisaatioon vaikuttavista tapahtumista, ilmiöistä ja trendeistä.

Pimeän ja syvän verkon dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa.



Avoimista lähteistä kerätyllä tiedolla täydennetään organisaatiosta saatua kuvaa.

Sisäisen kyberriskianalyysin avulla muodostetaan kokonaiskuva organisaation sisäpiiriuhkista ja muista riskitekijöistä.

PALVELUMME

Tilannekatsaukset

Cyberwatchin analyysitiimi seuraa jatkuvasti kyberturvallisuuden toimintaympäristöä keräämällä ja analysoimalla tietoa kybermaailman tapahtumista, ilmiöistä ja muutoksista. Tilannekuvaa tuotetaan säännöllisillä tilannekatsauksilla.

Viikkokatsaus

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

Kuukausikatsaus

Kuukausikatsauksessa analysoidaan viikkokatsauksissa seurattuja tapahtumia, trendejä ja niiden keskinäisvaikutuksia.
Kuukausikatsaus kuvaa ilmiöiden kehittymistä erityisesti hybridivaikuttamisen eri näkökulmista.
Kuukausikatsauksen avulla saat syvempää näkemystä siitä, kuinka kybermaailman tapahtumat vaikuttavat yhteiskuntaan ja toimintaympäristöösi.
Kuukausikatsaus ilmestyy 12 kertaa vuodessa suomeksi ja englanniksi.

Cyberwatch Magazine

Cyberwatch magazine on digitaalinen ja painettu aikakauslehtijulkaisumme, jossa omat ja verkostomme huippuasiantuntijat kirjoittavat kybermaailman ajankohtaisista tapahtumista, teknologian ja lainsäädännön kehityksestä ja näiden vaikutuksesta yhteiskuntaan, organisaatioihin ja yksittäisiin ihmisiin.

Special reports

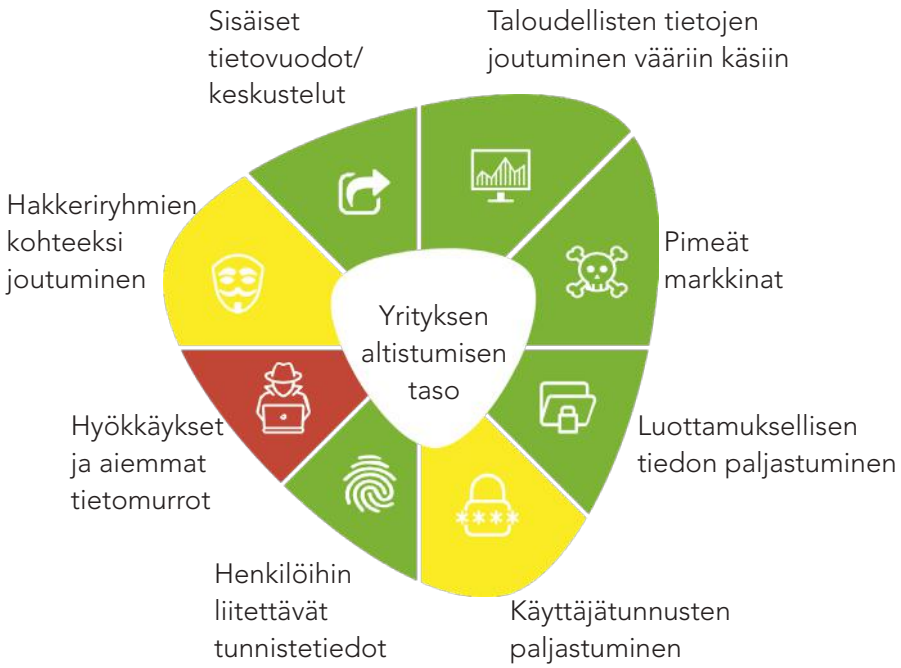
Tuotamme määrittelemästäsi teemasta, esimerkiksi tietystä toimialasta tai kohdemarkkinasta raportteja ja katsauksia: nykytilan arviointeja, uhka-arvioita, toimintaympäristöanalyyseja ja ennusteita

PALVELUMME

darkSOC® –pimeän ja syvän verkon analyysi

DarkSOC® -analyysin avulla selvitämme organisaatiosi profiilin ja altistumisen tason pimeässä ja syvässä verkossa. Dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa. Analyysi paljastaa organisaatiosi kyberturvallisuuden puutteita, vuotaneita tietoja ja muita mahdollisia ongelmakohtia. Analyysin avulla saat näkemyksen siitä, miltä organisaatio näyttää kyberrikollisen silmin katsottuna.

Luokittelemme kyberaltistumisen vaikutukset kahdeksaan kategoriaan. Laadimme analyysista kirjallisen raportin, jossa tuomme esille keskeiset havainnot johdon päätöksenteon tueksi. Raportti sisältää myös havaintojen yksityiskohtaisemman esittelyn. Annamme lisäksi suosituksia välittömistä korjaavista toimista ja strategisen tason kehityskohteista.



MITÄ HYÖTYJÄ darkSOC® -PALVELU TARJOAA

- Lisää kybertiedustelu-kykyä
- Ennakoi kyber-maailman kehityskulkuja
- Täydentää yrityksen kyber-maturiteettia
- Toimii forensic-tutkinnan apuvälineenä
- Tukee organisaation strategista päätöksentekoa
- Täydentää strategista kybertilanne-kuvaa
- Löytää haavoittu-vuuksia ja heikkouksia
- Fasilitoi kyberstrategia-prosessia

PALVELUMME

Analyysit

Pintaverkon analyysi

Muodostamme ulkopuolisen näkemyksen kyberturvallisuuden tasostasi pintaverkossa ja vertaamme asemaasi muihin saman toimialan organisaatioihin. Analyysimme pohjana on globaalin yhteistyökumppanimme SecurityScorecardin alusta, jonka data perustuu luotettuun, läpinäkyvään luokitusmenetelmään ja miljoonista organisaatioista kerättyihin tietoihin. Analyysimme perusteella annamme suosituksia korjaavista toimenpiteistä ja rakennamme reittikartan niiden käytännön toteuttamiselle organisaatiossasi.

Powered by Security Scorecard

Avoimien lähteiden analyysi

Tuotamme avoimiin lähteisiin perustuvia analyyseja valitsemistanne aiheista. Käytössämme on edistyneitä digitaalisia työkaluja, joiden avulla haemme tietoa julkisista maksuttomista ja maksullisista lähteistä sekä eri medioista ja sosiaalisen median alustoilta. Jalostamme tiedon analyysin tavoitteiden kannalta merkitykselliseen muotoon.

Sisäinen kyberriskianalyysi

Sisäisen kyberriskianalyysin avulla muodostat kokonaiskuvan organisaatiosi kyberturvallisuuteen liittyvistä sisäpiiriuhkista ja muista riskitekijöistä.

Analysoimme organisaatiosi kyberturvallisuuteen liittyvän ohjeistuksen ja muun dokumentaation ajantasaisuuden ja kattavuuden. Lisäksi haastattelemme johtoa ja muuta avainhenkilöstöä.

Analyysin tuloksena saat kuvan organisaatiosi toiminnan ja sitä ohjaavien sisäisten ohjeiden ja ulkoisen sääntelyn välisestä tasapainosta sekä tiekartan toiminnan kehittämiseksi.

PALVELUMME

Analyysit

NIS2 Puuteanalyysi

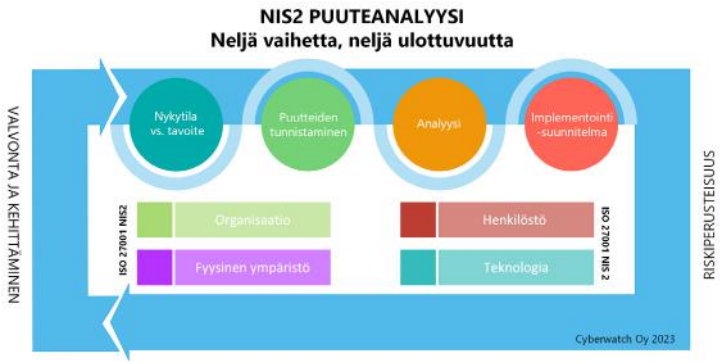
NIS2 kyberturvallisuus direktiivin tavoitteena on parantaa kyberturvallisuuden perustasoa EU:n alueella ja varmistaa kriittisten toimijoiden toiminnan jatkuvuus.
Direktiivi tuli voimaan 17.1.2023, jäsenmaissa aikaa laittaa asiat kuntoon 17.10.2024 mennessä.

NIS2 kyberturvallisuus direktiivi koskee seuraavia toimialoja:

NIS2 kyberturvallisuus direktiivin vähimmäisvaatimukset ovat:

1. Riskianalyysia ja tietojärjestelmien turvallisuutta koskevat politiikat
2. Poikkeamien käsittely
3. Toiminnan jatkuvuuden hallinta, kuten varmuuskopiointi ja palautus sekä kriisinhallinta
4. Toimitusketjun turvallisuus
   - Riskiperusteisuus
   - Datan kanssa tekemisissä olevat
5. Verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja paljastaminen
6. Periaatteet ja menettelyt kyberturvallisuusriskien hallintatoimenpiteiden tehokkuuden arvioimiseksi
7. Kyberhygienian peruskäytännöt ja kyberturvallisuuskoulutus
8. Salauksen ja kryptografian käyttöä koskevat käytännöt ja menettelyt
9. Henkilöresurssien turvallisuus, kulunvalvontakäytännöt ja omaisuudenhallinta
10. Vahvennetun todennuksen tai jatkuvan todennusratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä turvattujen hätäviestintäjärjestelmien käyttö yksikön sisällä.

Oman organisaation nykytilan vastaavuus vähimmäisvaatimuksiin kannattaa aloittaa hyvissä ajoin. Cyberwatchin NIS2 puuteanalyysi on vähimmäisvaatimuksia riskiperusteisesti lähestyvä malli, jossa viitekehyksenä käytetään paitsi direktiiviä, myös ISO 27001 standardia ja siihen liittyviä hallintakeinoja. Analyysin avulla organisaatio voi suunnata kehittämistoimet juuri oikeisiin kohteisiin.



PALVELUMME

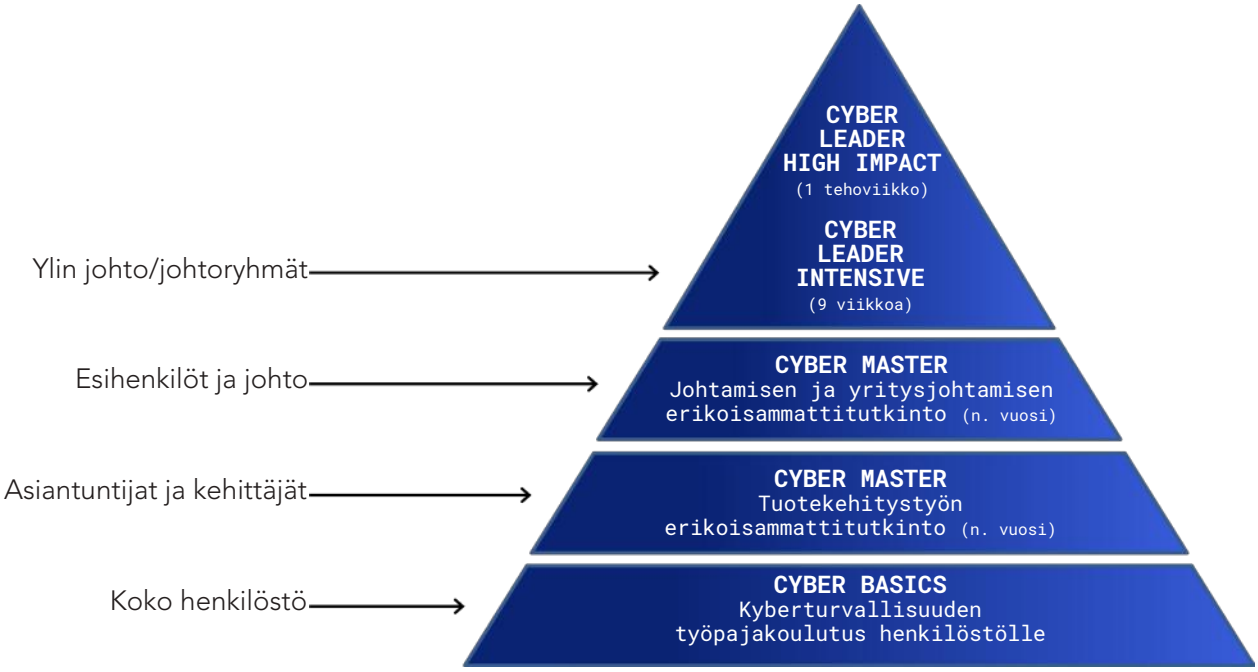
Koulutus ja osaamisen kehittäminen

Tuotamme yhdessä Management Institute of Finlandin (MIF) kanssa Cyber Master erikoisammattitutkintokoulutusta.

Tällä hetkellä ohjelmissa voi suorittaa Johtamisen ja yritysjohtamisen Cyber Master erikoisammattitutkinnon sekä tuotekehityksen Cyber Master erikoisammattitutkinnon.

Toteutamme organisaatiollesi myös räätälöityjä koulutuksia, joiden avulla vahvistat kyberturvallisuuden osaamista ja valmistaudut kohtaamaan digitaalisen toimintaympäristön haasteita.

Kaikki koulutustarjontamme koostuu moduuleista, joista opiskelija tai organisaatio voi valita tilanteeseen tai toimintaan soveltuvat osat.



PALVELUMME

Forensiikkapalvelut

Väärinkäytösselvitykset ja erityistarkastukset

Avustamme organisaatiotasi taloudellisten väärinkäytösten, compliance-rikkomusten ja muun epäeettisen toiminnan estämisessä, tutkimisessa ja niihin liittyvissä korjaavissa toimenpiteissä. Tarjoamme käyttöönne riippumattoman asiantuntijuuden. Suoritamme toimeksiannon itsenäisesti jatkuvasti kommunikoiden tai tuemme toimeksiantajaa sen suorittamassa työssä. Meillä on laaja kokemusta tutkinta- ja tarkastustyöstä ja hallitsemme uusimpien säännösten määräykset menettelyvaatimuksista.

Taustaselvitykset

Selvitämme yritysten ja yrityshenkilöiden mainetta, integriteettiä ja toimintahistoriaa keräämällä ja analysoimalla tietoa päätöksenteon tueksi eri tilanteisissa, kuten yritysjärjestelyissä ja kolmansien osapuolten kanssa toimittaessa.

Riskienhallintapalvelut

Avustamme organisaatiotasi kokonaisvaltaisesti riskien tunnistamisessa, arvioinnissa ja hallinnassa.

Kokeneet asiantuntijamme hyödyntävät työssään uusimpia riskienhallinnan teknologioita.

Rahanpesuntorjunta

Tuemme organisaatiotasi rahanpesulain velvotteiden täyttämisessä.

Asiakkaan tunteminen
Know Your Customer (KYC)
Customer Due Diligence (CDD)

Rahapesun ja terrorismin rahoittamisen torjunnan tuki:
politiikat, ohjelmat, riskiarviot

Cyberwatch eWHISTLE-ilmoituskanava

Cyberwatch eWHISTLE- ilmoituskanavapalvelu tarjoaa vastuullisen, tietoturvallisen ja yksityisyydensuojan varmistavan ilmoituskanavan, jossa ilmoitusten käsittelylle, tutkinnalle ja päätöksenteolle on luotu selkeä ympäristö.

eWHISTLE on täyden palvelun paketti. Laadimme ilmoituskanavan käyttöönoton vaatimat ja sitä tukevat prosessit ja dokumentit, tuemme lakisääteisten velvoitteiden täyttämisessä ja käynnistämme ilmoituskanavan. Kanavan käyttöönoton jälkeen otamme halutessasi ilmoitukset puolestasi vastaan, teemme ensiarvion ja laadimme ehdotuksen jatkotoimenpiteistä.

Ilmoituskanavapalvelun teknisen alustan tuottaa suomalainen Easywhistle Oy. Järjestelmä on helposti saavutettava, turvallinen ja käyttäjäystävällinen. Järjestelmä on saatavana lukuisilla kielellä. Palvelun tuottava yritys on ISO 27001 sertifioitu ja kanava täyttää GDPR-vaatimukset. Sen palvelimet sijaitsevat EU:n alueella.

eWHISTLE

INTOHIMONA KYBERTURVALLISEMPI MAAILMA

Ota yhteyttä

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi