Nelli Sviili

# ONKO PAREMPI JOUTUA TYKINRUOAKSI KUIN KYBERASEEN TÄHTÄIMEEN?

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

## SISÄLLYS

# 1 JOHDANTO

Kybermaailma ja sen ongelmat puhuttavat paljon läntisen maailman tiedotusvälineissä. Media kuvailee kybermaailman olevan konfliktissa, ellei jopa sotatilassa. Yksityisillä ihmisillä, organisaatioilla ja valtioilla on huoli joutua kyberiskun kohteeksi.

Valtiolliset tahot toteuttavat kybervakoilua ja kybersabotaasia. Missä menee nykyään kybersodan ja kyberrauhan raja? Onko parempi joutua tykin ruoaksi kuin kyberaseen tähtäimeen?

Tämä kirjallisuuskatsaus pyrkii vastaamaan edellä mainittuihin kysymyksiin. Kirjallisuuslähteiden perusteella pohditaan, ovatko pelätyt kybersotadystopiat totta vai tarua, onko kybersodan pelolle syytä.

Kirjallisuuskatsauksessa pohditaan keskeisiä kybertermejä ja niiden merkityksiä, mitä ovat kyberrikollisuus, -sabotaasi, -vakoilu ja -ase, mitä eroa on kybersodalla ja hybridisodalla sekä miten kybersotatoimet voivat vaikuttaa tietoyhteiskuntaan.

# 2 TURVALLISUUS KYBERMAAILMASSA

Läntinen maailma on digitalisoitunut viimeisen neljänkymmenen vuoden aikana voimakkaasti. Tietoverkkojen kehittymisen myötä ja tekniikan hinnan laskiessa myös kehittyvämaailma on pääsemässä osaksi digitalisaatiota. Maailman digitalisoituminen, kybermaailman syntyminen, edesauttaa merkittävästi niin ihmisiä arkisissa askareissa kuin yrityksiä, organisaatioita ja valtioitakin toimissaan. Teknologian kaikkiallistuminen ja tietoverkkojen laajentuminen mahdollistaa myös vaikuttamisen, vakoilun, rikollisuuden, sabotaasin ja sodan siirtymisen osittain tai kokonaan kyberavaruuteen. (mm. Lehto; 2019, Vahvanen, 2008; Harkness, 2016.)

Etuliitteen kyber- merkitys liittyy digitaalisessa muodossa olevan informaation käsittelyyn, kuten tietotekniikkaan, tietojärjestelmiin, tietokonejärjestelmiin tai digitaaliseen viestintään. Sanan taustat ovat kreikankielen sanassa *kybereo*; ohjata, opastaa, hallita. (Sanastokeskus TSK, 2018, s. 21.)

Kybermaailma ei kuitenkaan ole muinaisten kreikkalaisten keksintö. Kyber-etuliitettä on käytetty jo 1950-luvun puolivälissä liitettynä neuvostoliittolaiseen kyberetiikkaan, joka liittyi tietotekniikkaan ja robotiikkaan, ja Chilessä 1970-luvulla Cybersky'n yhteydessä, joka oli utopistinen visio valtiojohtoisen tuotannonohjausjärjestelmän rakentamisesta. Vasta 1980-luvulla kyberetuliite yhdistettiin laajamittaisemmin scifi-kirjallisuudessa kyberavaruuteen, termillä kuvattiin klassikkokirjassa Neuromancer tietoverkkojen luomaa matriisia. Internetin leviämisen seurauksena myös termi ”kyber” aloitti maailmanvalloituksena. Suomessa lanseerattiin termi kyberturvallisuus vuonna 2011 Valtioneuvoston ulko- ja turvallisuuspoliittisen ministerivaliokunnan toimesta. (Järvinen, 2018, s. 11-13; Lehto, 2019, s. 6-8; Vahvanen, 2008.)

## 2.1 Kyberuhat

Suojan rakentaminen kybermaailman uhilta vaatii tietoa ja taitoa. Tietoturvan yhteydessä puhutaan yleisesti, että tietoturva on niin vahva kuin sen heikoin lenkki on. Loppuen lopuksi vastuu kyberturvallisuudesta on pitkälti yksittäisten toimijoiden ja ihmisten harteilla. Suomen kyberturvallisuusstrategiassa (2019) nostetaan yhdeksi merkittävimmistä Suomen kokonaisturvallisuutta vahvistavaksi tekijäksi kansakunnan kyberosaamisen kehittäminen (Turvallisuuskomitea, 2019, s. 8). Kybermaailmassa myös fiksu ihminen voi toimia varomattomasti ja haitallisesti, mikäli hän ei tunne vaaroja ja tiedä sääntöjä. Suomessa sekä yksilöihin että yrityksiin kohdistuva kyberrikosten ja -häirinnän määrä on kasvanut merkittävästi 2010-luvulla (Helsingin yliopisto, 2016, s. 147-158).

Lehto (2019) yhteiskuntaan kohdistuvat uhat motiivin perusteella kolmeen ryhmään; fyysiset uhat, taloudelliset uhat ja kyberuhat. Tämän lisäksi hän luokittelee kyberuhat kuuteen ryhmään toimijoiden motiivien perusteella. Taso 1 käsittää kybervandalismin, johon kuuluvat haktivismi, kyberparveilu ja hakkerointi. Yksittäisen yrityksen tai yksilön

kohtaamat haitat voivat olla merkittäviäkin, mutta yhteiskunnan kontekstissa kapea-alaisia. Toisen tason muodostaa kyberrikollisuus. Kyberrikollisuus on monitahoista ja se kattaa kaiken tietoverkoissa tai tietoverkkojen avulla tehdyn rikollisuuden. Kybervakoilu on mallin kolmannella portaalla. Kybervakoilu on salaisen ja mahdollisesti sensitiivisen tiedon hankkimista laittomin menetelmin tietoverkkojen välityksellä. Neljännellä tasolla on kyberterrorismi. Sen avulla tuotetaan pelkoa ja vahinkoa. Kyberterrorismilla hyökätään kriittisiä informaatiojärjestelmiä kohtaan. Viidennellä tasolla on kybersabotaasi, jonka tavoitteena on saada aikaan epätasapainoa ja pelkoa. Viimeisellä, kuudennella tasolla on kybersodankäynti. (Lehto, 2019, s. 16.)

Usein kyberhyökkäykset pyritään toteuttamaan salassa niin, ettei kohde ole tietoinen hyökkäyksestä. Näin ollen hyökkäys voi jatkua pidempään. Kyberhyökkääjien selvittäminen on usein haastavaa, heitä on vaikea nimetä ja saada rikosoikeudelliseen vastuuseen teoistaan (Helsingin yliopisto, 2016, s. 147). Tietoverkkojen yli toteutetussa kyberrikollisuudessa kansallisvaltioiden rajat eivät ole esteenä. Usein kyberrikoksen tekijä ja uhri ovat fyysisesti eri maassa. Suomessa on otettu käyttöön vuonna 2018 tietosuojalaki, joka määrittelee kyberrikollisuutta ja mahdollistaa aiempaa paremmin tuomioiden määräämisen kyberrikoksista (Finlex, 2018). Globaalilla tasolla kybermaailmaan liittyvien lakien ja sopimusten puuttuminen vaikeuttaa sopusointuista yhteiseloa tietoverkkojen reitittämässä maailmassa (Jabbari, 2018).

Tietoverkkojen yli kybermaailmassa voi toteuttaa lukuisia toimia, joita ei luokitella rikoksiksi. Kvanttitietokoneiden kehittyminen mahdollistaa aiempaa merkittävämmän datanlouhinnan. Data kerätään valtavia määriä ihmisten toimista Internetissä ja sen ulkopuolella. Tätä kutsutaan big dataksi. Big dataa louhimalla voidaan luoda väestöryhmistä käyttäytymis- ja ajattelumalleja. Ihmisen käyttäytyminen on jossain määrin ennustettavissa olevaa. Datanlouhinnan ja koneoppimisen keinoin, voidaan rakentaa malleja, joilla vaikuttaa ihmisten ajatteluun ja käyttäytymiseen. Datanlouhintaa hyödynnetään nykyään esimerkiksi kohdennetussa mainonnassa. Lähitulevaisuudessa on odotettavissa kybervaikuttamisen merkittävä lisääntyminen eri tahojen toimesta. Kybervaikuttamisella pyritään muuttamaan esimerkiksi ihmisten äänestyskäyttäytymiseen. Big data ja sen louhinta on kuin kybermaailman kullankaivuuta. (Harkness, 2016, s. 11-38.)

## 2.2 Kybersota

Sotia ja konflikteja on ollut läpi kirjoitetun ja kuvitetun historian. Historian varhaisina vaiheina sodat ovat tarjonneet mahdollisuuden laajentaa tietyn joukon elinympäristöä ja parantaa sitä kautta heidän elintasoaan tai egoaan. Historiankirjoituksen myöhäisemmällä kaudella sodat ovat yleensä kehkeytyneet valtioiden tai kansojen välisistä konflikteista. Sodat ovat pääsääntöisesti olleet turhia, taloudellisesti tuhoisia, paikalliselle ekosysteemille haitallisia ja tappavia katastrofeja aikalaisilleen. Clausewitz'n historiallisin sanoin, sota on politiikan jatkoa muilla keinoin. (O'Connell, 1990, s. 3.)

Sanastokeskus TSK:n kyberturvallisuussanaston (2018) määrittää kybersodankäynnin synonyymiksi tietoverkkosodankäynnille. Määritelmä rajaa kybersodan koskemaan tietoverkkoja ja niiden haavoittuvuuksia hyödyntäväksi valtioiden vihamieliseksi toiminnaksi. (Sanastokeskus TSK, 2018, s. 21). Terminä kybersota siis rajaa kaikki fyysiset sotatoimet, kuten perinteiset aseet, panssarivaunut, hävittäjät ja dronet kybersotaan kuulumattomiksi.

Sodan luonteeseen vaikuttaa keskeisesti teknologian kehitys. Ihmisellä on ollut tapana laajentaa sota myös kaikkialle, missä ihminen on. Rantapelkosen (2018) mukaan sodan laajentuessa kyberfyysisessä ympäristössä, sodasta tulee kaukaisempaa, jotta sillä voidaan vaikuttaa lähelle. Nykyaikana sota on epäsymmetristä ja verkostomaista, sitä kuvaa hyvin informaatioulottuvuuden merkittävä hyödyntäminen. 2020-luvulla sodassa on pyrkimys yllätykseen, joka vaatii vastaavasti jatkuvaa valveilla olemista. Sotaa pyritään täydentämään perinteisen sodankäynnin lisäksi muilla vaikuttamisen tavoilla. Keskeistä on myös taistelukentän läpinäkyvyys ja sodan globaalit ulottuvuudet. (Rantapelkonen, 2018, s. 7, 203.)

Lehto (2018) määrittelee kyberaseen tarkoittavan tietokoneohjelmaa, joka toimii viruksen kaltaisesti muissa, kuin kyberaseen käyttäjän tietokoneessa. Kyberase on usein luonteeltaan flegmaattinen, varovasti lähiverkossaan liikkuva ohjelma. Mikäli kyberase ei itse kykene liikkumaan, se on asennettava erikseen jokaiseen kohdetietokoneeseen. Stuxnet-ohjelmistoa on kehitetty kyberaseeksi. Siinä on havaittavissa toiminnallisuuden toteuttava niin sanottu taistelukärki ja sitä kuljettava lavettiosa. Ohjausjärjestelmä kuljettaa lavettia. Ohjausjärjestelmä hallitsee niin hyökkäyskärjen aktivoinnin, ohjelman viestinnän kuin liikkuvuudenkin. Murtautumismoduulit hyödyntävät tietojärjestelmien haavoittuvuuksia päästäkseen kohteisiin. Mobiliteetti- ja asennusmoduuli toteuttaa kopioinnin ja liikkuvuuden. (Lehto, 2018, s. 24.)

Kyberaseen vaikutukset voivat olla kapea-alaisia tai koko yhteiskuntarauhaa horjuttavia pitkäaikaisvaikutuksia. On tutkittu, että laajemmalle alueelle kohdistuneet ja yli 12 tuntia kestäneet sähkökatkokset kaupungeissa ovat aiheuttaneet rötöstelyä ja kansalaistottelemattomuutta. Kotien ja yhteiskunnan digitalisaation seurauksena yhteiskunnan infrastruktuuria voi horjuttaa merkittävästi katkaisemalla sähköt. Vedenjakelu, kotien lämmitys, maksujärjestelmät, bensapumput, sairaalat ja tietojärjestelmät tarvitsevat sähköä toimiakseen. Kriittisimmillä toimijoilla on saatavilla varavirtaa, mutta varavirralla ei pidetä koko yhteiskuntaa pystyssä. Laajat sähkökatkokset esimerkiksi kylmään talviaikaan vaikeuttaisi ihmisten elämää, kun veden, lämmön, ruoan ja avun saatavuus olisi uhattuna, liikenne käytännössä pysähtyisi, puhelimet ja tietokoneet eivät toimisi. Suomalainen digitalisoitunut yhteiskunta on erittäin riippuvainen sähkönsaatavuudesta. (Laurila, 2017, s. 26; Vahvanen, 2008; Järvinen, 2018, s. 102-133.)

## 2.3 Kyberiskujen aikakausi

Digitaalisessa maailmassa tapahtuu kyberiskuja jatkuvalla vauhdilla. Check Point tarjoaa Internetissä Live Cyber Threat Map -sivuston, jolle se kerää tiedot maailman tietoverkoissa tapahtuvista hyökkäyksistä luokitellen ne haittaohjelmiksi, tietojen kalasteluksi tai hyödyntämiseksi. Liitteessä 1 on kuvakaappaus kyberuhkatilanteesta 5.3.2020 klo 9:35. Kuvakaappauksessa on nähtävissä Norjan hyökänneen Ranskaan, Ranskan hyökänneen Georgiaan, USA hyökänneen Intiaan, Costa Ricaan, Etelä-Afrikkaan, Italiaan ja Malesiaan, ja Singaporen hyökänneen Kreikkaan. Hyökkäykset on pääsääntöisesti toteutettu haittaohjelmilla. Sivuston mukaan viimeisen 24 tunnin aikana maailmassa on tapahtunut 42.042.853 kyberhyökkäystä keskiarvon ollessa noin 35 miljoonaa kyberhyökkäystä vuorokaudessa. Suomeen viimeisen kolmenkymmenen päivän aikana kohdistuneista kyberhyökkäyksistä on ollut 1,7% finanssialaan kohdistettuja troijalaisia, 2,6% botnet-hyökkäyksiä, 4,0% kryptovaluuttavarkauksia ja 6,2% matkapuhelinhyökkäyksiä (ks. Liite 2). (Check Point, 2020.)

Check Pointin keräämät tiedot tapahtuvista kyberhyökkäyksistä kuvaavat hyvin hyökkäysten arkistumista ja kaikkiallistumista. Tämä ei kuitenkaan kerro laajamittaisen kybersodan olemassa olosta tai edes sen alkamisesta. Valtiot ovat tehneet monia kyberhyökkäyksiä, mutta maailmanlaajuisen kybersodan käynnistyminen 2020-luvun maailmassa ei ole todennäköistä (Järvinen, 2018, s. 37). Tilastot kertovat ennemminkin rikollisuuden, haitanteon ja urkinnan siirtymisestä osaksi kybermaailman arkista todellisuutta.

Check Pointin kyberhyökkäystilastot kuvaavat myös sitä, kuinka tärkeää kyberturvan ja -tietoisuuden kehittäminen on 2020-luvun Suomessa ja maailmalla. Verkkoon kytkettyjen laitteiden lukumäärä kasvaa kovaa vauhtia, niin koodin kuin datankin määrä lisääntyy huimaa vauhtia (mm. Järvinen, 2018; Vahvanen, 2008). Mitä enemmän koodia, sitä enemmän haavoittuvuuksia ja sitä suurempi riski joutua kyberhyökkäyksen kohteeksi.

Yksi tunnetuimmista valtioiden toteuttamista kyberhyökkäyksistä on Iranin ydin reaktoria vastaan toteutettu Stuxnet-hyökkäys. Suljetun tietoverkon hyökkäys toteutettiin todennäköisesti saastuneiden USB-tikkujen avulla vuonna 2010. Kyberhyökkäyksessä hyödynnettiin Windowsin neljää aiemmin tuntematonta haavoittuvuutta eli nollapäivähaavoittuvuutta. Puolentoista megatavun kokoinen Stuxnet-ohjelma pystyi muun muassa vakoilemaan tietoliikennettä, hankkimaan käyttöönsä pääkäyttäjän oikeudet ja ohjailemaan uraanin rikastamisessa tarvittavien sentrifugien kierrosnopeuksia haitaten siten rikastusprosessia. Kyberhyökkäyksen taustalla on Yhdysvallat. Hyökkäyksen seurauksena Yhdysvaltoihin ei ole kohdistettu mitään suoria sanktiotoimia. (Tikk, Hovhannisyan, Kerttunen, Salminen, 2019, s. 18-20; Järvinen, 2018, s. 38-43.)

Mikäli tulkitsemme kybersodan Sanastokeskus TSK:n kyberturvallisuussanaston mukaan käsittämään tietoverkkoja ja niiden haavoittuvuuksia hyödyntäväksi valtioiden vihamieliseksi toiminnaksi, Stuxnet-kyberisku olisi esimerkki nykyajan kybersodasta. On kuiten-

kin perusteltua pohtia, tuleeko kybersodan määritteen sisältää kaikki valtioiden tietoverkkojen yli toteuttama vihamielinen toiminta. Perinteistä fyysistäkään sotaa ei ole vielä yhdellä tykillä ampuminen, vaan sodan toteutumiseen tarvitaan kokonainen armeija. Lehto (2019) luokittelee Stuxnet-hyökkäyksen olevan kybersabotaasiksia (Lehto 2019, s. 17).

Stuxnet-hyökkäys toimii myös hyvänä esimerkkinä siitä, kuinka vahva kyberturvallisuus koostuu niin laadukkaasta ohjelmakoodista, vahvoista suojauksista ja kyberturvatietoisista ihmisistä ja toimijoista. Kyberase ei pääse osumaan kohteeseensa, kun kyberturvallisuus on riittävällä tasolla. Mikäli hyvästä varautumisesta huolimatta kyberase osuu maaliinsa, turvallisuustoimien keskiöön nousee hyökkäyksen havaitseminen ja tuhon minimoiminen.

# 3 JOHTOPÄÄTÖKSET

Yhteiskuntien digitalisoitumisen ja teknologian kaikkiallistumisen seurauksena on syntynyt uusi yhteinen ulottuvuus, kybermaailma, joka on hiipinyt ihmisten läheisyyteen, niin koteihin kuin työpaikoillekin. Kyberfyysisessä maailmassa suurin osa ihmisistä on alttiina kyberuhille. Uhkia on monenlaisia vähäisestä kyberurkinnasta ja -vaikuttamisesta kybersabotaasiin ja jopa kybersotaan asti. Ihmisten kybertaidoissa on merkittävästi parannettavaa, jotta jokainen osaisi suojautua kyberuhilta riittävällä tasolla.

Kirjallisuuskatsaus kävi läpi keskeisimpiä kyberuhkia. Kybersodankäyntiin ja kyberaseisiin luotiin syväluotaavampi katse. Kirjallisuuslähteiden valossa myös spekuloitiin mahdollisen kyberaseen vaikutuksia digitalisoituneen yhteiskunnan perspektiivistä. Kyberiskuja pohdittiin Stuxnet-hyökkäyksen valossa.

Lähdekirjallisuuden perusteella voimme todeta kybermaailman ja sen sääntöjen olevan vielä kehittymässä. Mikäli vertaamme kybermaailmaa atomipommiin, voisimme havaita maailman elävän kilpavarustelun aikakautta. Kyberaseita on jo testattu, mutta Hiroshiman veroinen kyberpommi on vielä näkemättä ja kokematta.

Pahimmillaan tehokas kyberase saattaisi lamaannuttaa kokonaisen valtion, joten voimme todeta kyberaseen tähtäimeen joutumisen johtavan mahdollisesti laajempiin ja kauaskantoisempiin seurauksiin kuin tykinruoaksi joutumisen. Niin kyberdystopian kuin kyberutopiakin toteutuminen on vielä mahdollista.

## LÄHTEET


Check Point (2020). Live Cyber Treat Map. Threatcloud, Check Point. Viitattu:5.3.2020. https://threatmap.checkpoint.com/

Finlex (2018). Tietosuojalaki. Finlex. Viitattu: 6.3.2020. https://www.finlex.fi/fi/laki/alkup/2018/20181050

Harkness, T. (2016). Big Data does size matter? Bloomsbury Sigma, New York.

Helsingin yliopisto (2016). Rikollisuustilanne 2015 – rikollisuuskehitys tilastojen ja tutkimusten valossa. Katsauksia 14/2016. Helsingin yliopisto, Valtiotieteellinen tiedekunta, Kriminologian ja oikeuspolitiikan instituutti.

Jabbari, C. (2018). The Application of International Law in Cyberspace: State of Play. United Nations. Viitattu: 6.3.2020. https://www.un.org/disarmament/update/the-application-of-international-law-in-cyberspace-state-of-play/

Järvinen, P. (2018). Kyberuhkia ja somesotaa, digiaikana sinäkin olet etulinjassa. Docendo, Jyväskylä.

Laurila, A. (2017). Kyberterrorismi ja sen uhat yhteiskunnan tulevaisuudelle. Poliisiammattikorkeakoulu, opinnäytetyö.

Lehto, M. (2019). Kybermaailman ilmiöitä ja määrittelyjä. Jyväskylän yliopisto, Informaatioteknologian laitos.

Rantapelkonen, J. toim. (2018). Tuleva sota – Tulevaisuuden sodan tulevaisuus. Maanpuolustuskorkeakoulu, Otavan kirjapaino Oy, Keuruu.

O'Connell, R. T. (1990). Of arms and men: a history of war, weapons, and aggression. Oxford University Press.

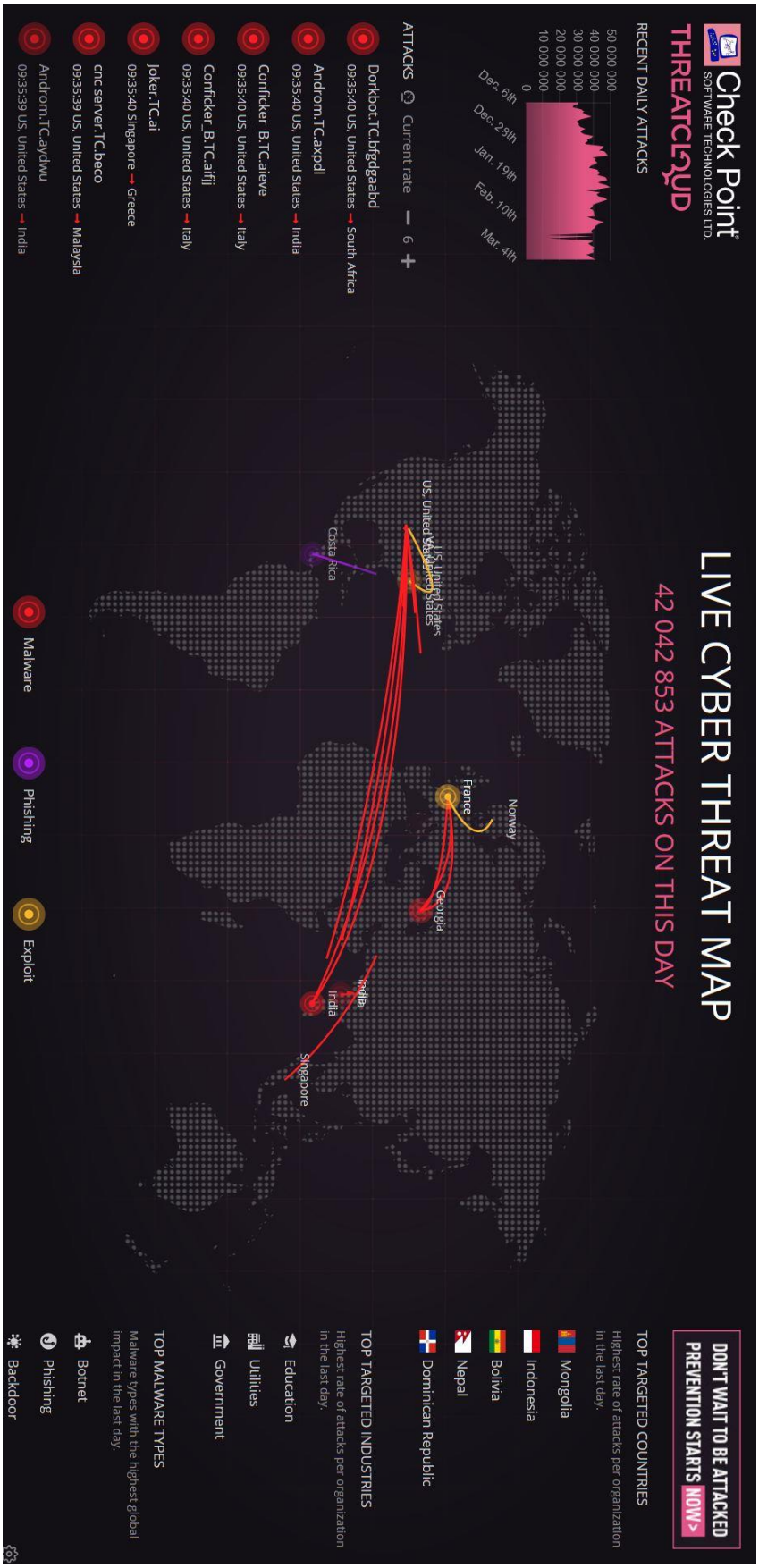
Sanastokeskus TSK (2018). Kyberturvallisuuden sanasto, TSK52. Sanastokeskus TSK, Huoltovarmuuskeskus, Turvallisuuskomitea, Helsinki.

Tikk, E., Hovhannisyan, K., Kerttunen, M., Salminen, M. (2019). Cyber Conflict Factbook: Effect-creating state-on-state cyber operations. CPI cyber policy institute & Microsoft, Tartu-Tallinn-Jyväskylä-Rovaniemi.

Turvallisuuskomitea (2019). Suomen kyberturvallisuusstrategia 2019. Turvallisuuskomitea, Helsinki.

Vahvanen, P. (2018). Teknologian peto on irti (essee). Helsingin Sanomat 21.10.2018.

## LIITE 1 LIVEAIKAINEN KYBERUHKAKARTTA



## LIITE 2 SUOMEEN KOHDISTUNEET HAITTAOHJELMAISKUT