Nelli Sviili
nekasvii@student.jyu.fi
30.1.2020

OPPIMISPÄIVÄKIRJA

4.11.2019

What is CYBER?

Aiempien opintojen valossa tulkitsen kyberin käsittävän kaiken, mikä liittyy jollain tavalla tietoverkkoihin ja tietoliikenteeseen. Tämän lisäksi väitän, että kyberiä on loppuen lopuksi kaikki, mikä tapahtuu tietokoneessa. Luen esimerkiksi Internettiin yhdistettyjen laitteiden (IoT) kuuluvan kyberkäsitteen alaisuuteen niiden tietoverkkosidonnaisuutensa seurauksena.

Ensimmäisellä luennolla esitettiin näkemys kyber(avaruuden) luonteesta. Sen mukaan kyber on toisistaan riippuvainen tietotekniikan infrastruktuurien verkko, joka sisältää Internetin, televerkot, tietojärjestelmät, tietokoneet ja tietokonejärjestelmät, sulautetut prosessorit ja ohjaimet, protokollat, datan, kuten ohjelmistot, kaikki tietokoneille tallennettu ja välitetty tieto sekä liikenne- että kontrollidatan.

Mielestäni luennolla esitetty määritelmä on kattava. Itse lisäisin määritelmään vielä jotain dataliikenteistä perinteisten tietokoneiden ulkopuolellakin. IoT-laitteet yleistyvät kovaa vauhtia. Niiden kautta kulkema datan määrä kasvanee ainakin lähes eksponentiaalisesti. Kyberrikolliset ja -vakoojat ovat varmasti yhä enenevimmissä määrin kiinnostuneita IoT-laitteiden kautta tapahtuvasta urkinnasta ja mahdollisesti myös tulevaisuudesta IoT-laitteiden kautta aukeavista vaikuttamismahdollisuuksista. Ajatellaanpa vaikkapa ihmisen sisään asennettu insuliinipumppu, joka on yhdistetty Internetin välityksellä kännykkäsovellutukseen. Rikollisia tahoja voisi kiinnostaa mahdollisuus päästä ohjailemaan insuliinipumppua eliminoidakseen kyseisen ihmisen syystä tai toisesta. Tulkitsen sanan kyber käsittävän kaiken sen, mikä tapahtuu Internetin välityksellä, joten tässä esimerkissä kyse olisi siis kyberrikollisuudesta.

Mikäli pohditaan vaikkapa Iranin ydinaseohjelmaan kohdistunutta Stuxnet-kyberhyökkäystä, voimme todeta sanan kyber käsittävän myös Internetistä riippumattomat tietotekniset ohjelmat ja ohjelmistot. Stuxnet-hyökkäyksessä haittaohjelma (mato) ujutettiin ydinasetutkimuslaitoksen sisäiseen verkkoon USB-tikun avulla. Hyökkäystä ei ole toteutettu Internetin yli vaan ennemminkin sosiaalisen manipuloinnin kautta (social engineering).

Miten kybermaailma muuttuu seuraavana vuosikymmenenä?

Maailma on muuttunut suuresti viimeisten 150 vuoden aikana. 1800-luvun loppupuolella ihmisten elämä oli pääsääntöisesti hyvin kapea-alaista verrattuna nykypäiväiseen elämään tekniikan ympäröimänä. Muutos on käynnissä yhä ja kovemmalla vauhdilla kuin koskaan ennen. Teknologian käyttö on nykyään

epätasaista eri väestöryhmien kesken. Suomessa 1990-luvulla alkaneen teknologisaation seurauksena osa väestöstä ei ole ollut näiden 30 vuoden aikana halukas kesyttämään teknologioita omaan käyttöönsä. Teknologian domestikaation jäädessä vajavaiseksi tai pinnalliseksi, on suuri riski pudota kokonaan teknologian kyydistä. Erityisen alttiita teknologisesta kehityksestä syrjäytymiselle on matalasti koulutetut ihmiset, joilla ei ole riittäviä teknologiankäyttötaitoja pärjätä teknologisoituvassa työelämässä.

Tulevaisuuden työelämässä pärjäämisen edellytyksenä on yhä enenevissä määrin kykyä adaptoida uusia teknologioita. Nykyään ja tulevaisuudessa teknologioiden kesyttäminen (domestikaatio) vaatii laajempaa ymmärrystä vanhemmista teknologioista, ja kun aiempaa ymmärrystä ei ole tai se on vajaata, on riskinä, että teknologian kesyttäminen viivästyy kulttuurisen viiveen (cultural lag) seurauksena. Tämän takia tietty osa väestöstä on alttiimpi kybervaikuttamiselle, urkinnalle ja kyberrikollisuudelle.

Tutkijat, tieteiskirjailijat ja poliitikot maalailevat erinäisiä utopioita ja dystopioita riippuen heidän intresseistään. Omien tietojeni valossa uskon tulevaisuuden kybermaailman olevan utopistista niille, joilla on kyky kesyttää teknologioita, mutta dystopiaa niille, jotka jäävät tai jättäytyvät pois teknologian vankkureista. Perustelen väitettä osittain kyberturvallisuuden näkövinkkelistä. Nykyään on nähtävissä kehitystä siihen suuntaan, että ihmiset, jotka tuntevat kybermaailmaa (tietotekniikkaa) perusteellisemmin, osaavat suojautua paremmin myös kybermaailman haittoja vastaan (mielipidevaikuttaminen, kohdennettu mainonta, virukset, madot, haittaohjelmat, sosiaalinen manipulaatio jne.), kun taas ihmiset, joiden ymmärrys tekniikasta ja sen kehittymisestä on vajavaista, ovat alttiimpia kyberrikollisuudelle.

Automatisaatio, robotisaatio, tekoäly ja digitaaliset alustat muokkaavat kaikkia aloja. Tällä hetkellä vaikuttaa, että kehityksen myötä varallisuus kertyy sille ihmisryhmälle, joka on kykeneväinen kehittämään tai omistamaan uusia teknologioita. Tulevaisuudessa, mahdollisesti jo seuraavan 10 vuoden aikana, merkittävä osa ihmisten työvoimasta tulee tarpeettomaksi robotisaatio, automaation ja teknologistumisen myötä. Ongelmaksi muodostuu epätasainen tulonjako ja sitä kautta kulutuksen vähentyminen. Merkittävänä kybermaailman kasvamisen sivutuotteena ihmisille syntyy myös enenevissä määrin vapaa-aikaa. Merkittäväksi kysymykseksi nouseekin, miten ihminen sietää tylsyyttä mentaalitasolla.

Valtiolta tarvittaisiin rohkeita uudistuksia verotukseen (kuten esimerkiksi kansalaispalkka tms.), jotta sillä olisi vaikutusta tulevaisuuden tulojakoon. Suomessa luokkaerot ovat jatkaneet kasvuaan 1990-luvulta; köyhät köyhtyvät, rikkaat rikastuvat. Sosioekonomisen luokan periytyvyys jälkipolville on voimistunut. Perheen sosioekonominen luokka vaikuttaa sekä opiskeluun ja työllistymiseen että sitä kautta kykyyn kesyttää teknologioita. Uskon nykyisten trendien valossa luokkahierarkioiden kasvuun niin Suomessa kuin maailmallakin. Tämä vaikuttaa negatiivisesti uusien teknologioiden domestikaatioon valtiotasollakin. Mikäli

kansa velvoitetaan käyttämään arjessaan uusia teknisiä innovaatioita, on aina tietty kansan osa, joka ei pysty kesyttämään kyseistä teknologiaa.

Teknologia kehittyy nopeasti. Kehitys luo talouskasvua, mikäli riittävän suuri osa väestöstä kykenee pysymään kehityksessä mukana. Tällöin monen utopian on mahdollista toteutua (esim. bio- ja fuusiovallankumoukset), koska talouden vakaus luo mahdollisuuksia sijoittaa kehitykseen. Mikäli valtioiden taloudellinen valta ja rahat luisuvat suuryrityksille, on riskinä dystopioiden toteutuminen. Kehitys voisi johtaa esimerkiksi siihen, että terveysteknologia on saatavilla vain hyväosaiselle väestölle. Ääritapauksessakehityksen seurauksena voisi olla jopa tekoälyn valjastamiseen itseohjautuviin tappokoneisiin. Kansainvälisin sopimuksin ja laein voidaan pyrkiä ennaltaehkäisemään osittain dystopioiden kehittymistä, mutta suurempi valta on valtioilla ja suuryrityksillä. Joka tapauksessa kybermaailma globalisoituu entistä voimakkaammin.

Onko olemassa kyberkonflikteja?

Virallisesti yksikään maa ei ole keskenään kybersodassa. Kuitenkin lähteiden valossa voi väittää, että kyberkonflikteja on olemassa. Kyberhyökkäystä tai -urkintaa on vaikea näyttää toteen etenkin kolmannelle osapuolelle. On kuitenkin olemassa aihetodisteita, joiden perusteella voi päätellä tiettyjen valtiollisten tahojen toimineen toisen valtion suvereniteettia rikkoen liittyen kyberturvallisuuteen.

Käyttäkäämme esimerkkinä aiemmin tehtävässä mainittua Stuxnet-kyberhyökkäystä. Hyökkäyksen kohteena oli Iranin ydinohjelma. Stuxnetin taustalla on epäilty olleen Israel tai USA (lähteenä Snowden). Taustalla voi kuitenkin olla moni muukin valtio. Iranin ja sekä Israelin että USA:n kahdenkeskisissä suhteissa ei ole kehuttavaa. Iran on reagoinut Stuxnetiin moninkertaistamalla kyberturvallisuuden budjettinsa. Iranin väitetään hyökänneen 2012 Saudi Arabian Aramcon öljy-yhtiöön, Qatarin RasGas luonnonkaasufirmaan ja Sands casinoon vuonna 2014. Iranin väitetään olleen myös USA:n pankkeihin kohdistuneen kyberhyökkäyksen taustalla vuonna 2012.

Saudi Arabia ja Qatar ovat USA:n liittolaisia. Lähteiden valossa näyttää, että Stuxnetin kyberhyökkäys on osaltaan johtanut Iranin tekemään kyberhyökkäysten sarjan kostotoimenpiteenä. Tämän perusteella voi todeta, että on olemassa kyberkonflikteja. Kyseenalaiseksi jää se, että ovatko konfliktit todellakin niiden valtioiden välillä, jotka ovat rikkoneet toistensa kybersuvereniteetteja, vai ovatko konfliktit laajentuneet koskemaan myös liittolaismaita.

Nelli Sviili
nekasvii@student.jyu.fi
30.1.2020

Miksi tarvitaan kansainvälisiä lakeja?

Kansainvälisten lakien merkittävyydestä voidaan olla montaa mieltä. Faktuaalisesti näyttää, ettei kansainvälisillä lailla ole suurta merkitystä, koska yleensä niiden rikkominen ei saata lainrikkojaa tuomioistuimeen. Kansainvälisillä laeilla on kuitenkin suuri merkitys valtioiden välisissä toimissa. Moni valtioiden välinen sopimus nojaa kansainvälisiin lakeihin. Valtioiden väliset sopimukset rakennetaan siten, etteivät ne riko kansainvälisiä lakeja. Tavoitteena on kunnioittaa valtioiden suvereniteetteja.

Kansainvälisten lakien merkitys näkyy siten sopimusten kautta. Lait antavat normatiivisen taustan valtioille toimia kansainvälisessä yhteisössä. Mikäli valtio rikkoo kansainvälisiä lakeja ja sopimuksia, voivat toiset valtiot pyrkiä vaikuttamaan rikkojavaltioon neuvottelemalla, painostamalla ja esimerkiksi talouspakottein. Usein vaikuttaminen on poliittista ja tapahtuu mahdollisesti suljettujen ovien sisäpuolella. Politiikalla onkin usein suurempi merkitys valtioiden välisissä kiistoissa kuin suoranaisesti kansainvälisillä laeilla.

Näen, että nykyisessä maailmassa olisi tärkeää kirjata kansainvälisiin lakeihin yhteisiä rajoja kybermaailman suhteen. Esimerkiksi perusteltua olisi kieltää itsenäiset tekoälypohjaiset tappajakoneet (kuten robotit, lennokit ja panssarivaunut). Päätöstä tappamisesta ei tulisi ulkoistaa tekoälylle.

OSION LÄHTEET

Atlantic Council. Iran's Growing Cyber Capabilities in a Post-Stuxnet Era. https://www.atlanticcouncil.org/blogs/new-atlanticist/iran-s-growing-cyber-capabilities-in-a-post-stuxnet-era/ (lainattu 11.11.19).

SITRA (2017). Megatrendit. https://www.sitra.fi/aiheet/megatrendit/#ota-yhteytta (lainattu 11.11.19).

Thomson, I. (2013). Snowden: US and Israel did create Stuxnet attack code. The Register 8.7.2013. https://www.theregister.co.uk/2013/07/08/snowden_us_israel_stuxnet/ (lainattu 11.11.19).

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.

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

Vahvanen, P. (2013). Työn loppu (essee). Suomen Kuvalehti 31/2013.

Nelli Sviili
nekasvii@student.jyu.fi

7.11.2019

Miten itsemääräämisoikeuden (sovereignty) ja tuomiovallan (jurisdiction) periaatteiden avulla voidaan ratkaista tietty kybertapausta?

Nykymaailman poliittinen valta perustuu pitkälti valtioiden itsemääräämisoikeuksiin. Itsemääräämisoikeuden periaatteiden mukaan, kukin valtio kunnioittaa toisten valtioiden omistusoikeutta. Yleisellä tasolla itsemääräämisoikeuden tulkitaan tarkoittavan valtion oikeutta olla joutumatta sotilaallisen hyökkäyksen kohteeksi ja käydä puolustussotaa, määrätä alueen luonnonvarojen käytöstä ja siitä, miten paljon maahan otetaan siirtolaisia ja pakolaisia. Valtioilla on myös lainkäytöllinen immuniteetti, joka turvaa sen, ettei kyseinen valtio ole velvollinen alistumaan oikeudenkäyntiin toisen valtion tuomioistuimessa. Valtion sisäisen suvereniteetin periaatteet käsittävät muun muassa oikeuden alueloukkausten torjuntaan voimakeinoja käyttäen.

Passiivisen personallisuuden periaate (the passive personality principle) antaa valtiolle mahdollisuuden hakea lainkäytäntövaltaa ulkomaalaisen oikeudenkäynnille ulkomailla tehdyistä rikoksista, jotka vaikuttavat sen kansalaiseen. Passiivinen persoonallisuuslainkäyttövalta on kiistanalaista. Monet valtiot ovat perinteisesti vastustaneet sen lainkäyttövaltaa. Siihen on kuitenkin tukeuduttu kuitenkin terrorismisyytöksissä. Tätä valtaa on noudatettava varovasti, jottei loukattaisi toisen valtion itsemääräämisoikeutta. Passiivinen persoonallisuusperiaate on viimeinen keino lainkäyttövallan muodossa. Tällä hetkellä periaate keskittyy tukemaan yksittäisten valtioiden etuja kansainvälisen oikeuslaitoksen etujen kustannuksella.

Kun edellisten tietojen valossa pohtii Montenegron NATO-vaalien hakkerointitapausta vuodelta 2017, voi todeta hakkerointien primaarikohteena olleen NATO-negatiivisten äänten kasvattaminen vaaleissa ja sekundaarikohteena olleen Montenegron itsemääräämisoikeuden loukkaus. Useilla kyberiskuilla pyrittiin vaikuttamaan merkittävien medioiden ja valtion sivujen kautta vaalien lopputulemaan. Kolme näkyvää IT-turvallisuusyritystä on tutkinut tapausta todeten Venäjän olleen hyökkäysten takana. Montenegron virallisen tiedotteen mukaan hyökkäykset tulivat lukuisista IP-osoitteista eri maista. Hyökkäyksillä ei saatu aikaan merkittävää tuhoa ja näkyvät vaikutukset jäivät pieniksi. Virallisen kannan mukaan valtio on ottanut käyttöönsä kaikki tuomiovallan keinot estääkseen vastaavanlaiset tulevat hyökkäykset.

Montenegron tapauksessa tuomiovallan mahdollisuudet saattaa hakkeroinnista vastuussa tahot vastuuseen teoistaan ovat hyvin rajalliset. Kansainväliset rajat eivät rajoita samanlailla verkossa toimivia tahoja, kuin perinteisiä rikollisia. Verkko ei ole fyysinen ympäristö, joten se luo lainsäädännöllisiä haasteita saattaa rikollisia vastaamaan edesottamuksistaan.

Asiaa pohdittaessa maallikkojärjellä, vastaus on hyvin selkeä; Venäjä on loukannut Montenegron itsemääräämisoikeutta pyrkiessään vaikuttamaan NATO-vaalien lopputulemaan, mutta lain näkökulmasta asia ei ole niin yksiselitteinen. Mikäli oletamme hyökkäysten takana olleen esimerkiksi tiimin moskovalaisia kyberneroja, jotka työskentelevät Venäjän valtion palkkalistoilla, tulisiko tuomiovallan rankaista yksittäisiä tekijöitä vai voisiko kansainvälinen oikeus langettaa Venäjälle sanktioita asiasta. Mikäli päädyttäisiin tavoitteeseen rankaista yksittäisiä hakkereita passiivisen personallisuus periaatteen mukaisesti, miten tekijöiden jäljille pääsisi? Voisi olettaa Venäjän pyrkivän suojelemaan hakkerinerojensa identiteettejä. Mikäli taasen syytettäisiin valtiota, miten voisi todistaa valtion olleen asialla yksittäisten hakkereiden sijaan?

Datan eli tiedon käsittäminen uhkatekijänä on myös kyseenalaista itsemääräämisoikeutta tukevien periaatteiden valossa. Data ei ole mitään fyysistä, eikä tässä Montenegron tapauksessa vaikutuksetkaan olleet fyysisiä. Miten joku ei-fyysinen voi loukata valtion itsemääräämisoikeutta lain silmissä. Montenegro voi pyrkiä vaikuttamaan uusiin kyberhyökkäyksiin politiikan keinoin, mutta siinäkin tilanteessa Venäjällä on etulyöntiasema, vaikka Montenegro onkin sittemmin saanut NATO:n jäsenyyden.

Miten kansainväliset lait vaikuttavat elämääni?

Kansainväliset lait ja sopimukset vaikuttavat osaltaan kaikkien jokapäiväiseen elämään. Esimerkiksi isäni asuu Virossa. Hän on muuttanut sinne viettämään leppoisempia eläkepäiviä. Kv-lait ja sopimukset mahdollistavat hänen asumisensa vieraan valtion alueella ja eläkkeen juoksemisen sinne. Hänellä on myös oikeus käyttää Viron valtion palveluita, kuten terveydenhuollon tarjoamia palveluita. Hän voi käydä äänestämässä Suomen konsulaatissa vaalien aikaan.

Minä taasen voin soittaa edullisesti Viroon, voin matkustaa sinne ongelmitta, ja tarpeen vaatiessa voin myös saada kiireellisiä terveyspalveluita Suomen valtion piikkiin Virossa. Nykyään suomalaisilla lääkeresepteillä saa ostaa lääkkeitä Viron apteekeista. Euroopan telelait myös turvaavat kohtuuhintaisen suomalaisen kännykkäliittymän käytön Virossa. Halutessani voin siirtää rahaa isäni virolaiselle pankkitilille tai postittaa etanapostia suoraan hänen virolaiseen osoitteeseensa.

Mikäli sortuisin rikolliseen toimintaan Virossa ja jäisin kiinni, minua turvaisi myös monet Viron ja Suomen kahdenväliset sopimukset. Mikäli jäisin kiinni rikoksistani vasta Suomessa, Suomi pitäisi huolen, että joutuisin kantamaan vastuuni tekemistäni rikoksista siitä huolimatta. Jos pakenisin kolmanteen maahan, minut voitaisiin tavoittaa erimaiden välisten rikollisten luovutussopimusten valossa kantamaan vastuuni rikoksistani Virossa.

Nelli Sviili
nekasvii@student.jyu.fi
30.1.2020

Miten kybermaailma on muuttanut kansainvälisten lakien toimintaympäristöä

Kansainväliset lait perustuvat pitkälti fyysisiin elementteihin, jotka ovat määritteiden avulla ymmärrettävissä suhteellisen yksiselitteisesti. Teknologian kehitys haastaa myös kansainväliset periaatteet ja lait muutokseen. Uudet teknologiat (kuten big data, pilviteknologia, dronet ja tekoäly) mahdollistavat uudenlaisten valtioiden rajat ylittävien uhkien synnyn ja nopean kehittymisen. Uudet uhat ovat usein myös ei-fyysisiä uhkia, joilla voi kuitenkin olla fyysisiä vaikutuksia.

2000-luvulla sodankäynnistä on tullut hybridistä. Sota on usein ei-kineettistä sotaa, joka perustuu ihmisiin vaikuttamiseen niin sanotusti valtion sisältäpäin. Sodankäynninrajat ovat hämärtyneet ja kansainvälisten lakien ja periaatteiden vaikutusmahdollisuudet kaventuneet. Asetelma on johtanut kansainvälisen politiikan ja pakotteiden merkityksen kasvuun. Voimme myös kyseenalaistaa demokratian arvojen validiteetin valeuutisten ja verkkovaikuttamisen aikakautena. Tuleeko jokaisella olla rajaton pääsy Internettiin, jossa algoritmit ohjaavat mielenkiinnonkohteitamme ja sisällön näkyvyyttä antaen vieraan vallan edustajille avoimen väylän vaikuttaa yksittäisiin kansalaisiin omien etujensa nimissä? Rikkooko esimerkiksi algoritminen vaikuttaminen valtion itsemääräämisoikeuden periaatteita?

Esimerkiksi Ukrainan ja Venäjän konfliktissa Venäjä on käyttänyt laajasti vaikuttamista aseenaan. Venäjä on panostanut hybridisodankäynnissään ei-fyysisiin sotatoimiin, kuten poliittiseen ja taloudelliseen painostukseen sekä strategiseen kommunikaatioon. Kybermaailma mahdollistaa vaikuttamisen toisen valtion alueella poliittisten ja sotilaallisten tavoitteiden saavuttamisen. Valtioiden toteuttamat kyberhyökkäykset tulevat vaikuttamaan enenevissä määrin poliittisiin suhteisiin ja valtarakenteisiin. Kansainvälisten lakien ja periaatteiden tulisi kehittyä näkemään myös kybermaailman uhat. Kansainvälisen yhteisön tulisi toimia nopeasti ehkäistäkseen kyberkonfliktien syntyä.

OSION LÄHTEET

Lehto, M., (2008). Kybermaailma ja tiedustelu. Jyväskylän yliopisto, Informaationteknologian tiedekunta. http://docplayer.fi/110898294-Kybermaailma-ja-tiedustelu.html (lainattu 20.11.2019)

Ministry for Information Society and Telecommunications of Montenegro (2016). Web portal of the Government of Montenegro exposed to DDoS attacks. http://www.mid.gov.me/en/news/166902/Web-portal-of-the-Government-of-Montenegro-exposed-to-DDoS-attacks.html (lainattu 20.11.2019)

NATO (2017). Relations with Montenegro. https://www.nato.int/cps/en/natohq/topics_49736.htm (lainattu 20.11.2019)

Suomen suurlähetystö, Viro (2019). Kahdenväliset suhteet. Suomen ulkoministeriö. https://finlandabroad.fi/web/est/kahdenvaliset-suhteet (lainattu 20.11.2019).

Suomen suurlähetystö, Viro (2019). Hädässä ulkomailla. Suomen ulkoministeriö. https://finlandabroad.fi/web/est/hadassa-matkalla (lainattu 20.11.2019).

Suomen suurlähetystö, Viro (2019). Pidätettynä ulkomailla. Suomen ulkoministeriö. https://finlandabroad.fi/web/est/pidatettyna (lainattu 20.11.2019).

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.

Watson, G., R. (1993). The Passive Personality Principle. The Catholic University of America, Columbus School of Law. https://scholarship.law.edu/cgi/viewcontent.cgi?article=1410&context=scholar (lainattu 20.11.2019).

11.11.2019

Kuinka rauhanomaisen sopimisen keinoja (ref. UN Charter 33(1)) voitaisiin hyödyntää kyberkontekstissa (tietyssä kyberkonfliktissa)? Vai voitaisiinko?

Artikla 33 (1): ”Jokaisessa riidassa, jonka jatkuminen on omiaan vaarantamaan kansainvälisen rauhan ja turvallisuuden ylläpitämistä, on asianosaisten ensi sijassa pyrittävä ratkaisuun käyttämällä neuvotteluja, tutkimusmenettelyä, välitystä, sovintomenettelyä, välitysoikeudellista tai tuomioistuinmenettelyä, alueellisten elinten tai sopimusten apua taikka muita rauhanomaisia keinoja oman valintansa mukaan.”

Väitän karkeasti, että YK:n artikla on hyvä ohjenuora kyberkonfliktienkin ratkaisemiselle. Haastavimpana tekijänä näen, että kyberkonfliktissa voi olla vaikea todistaa pitävästi konfliktihakuinen taho. Kyberkonfliktin aiheuttaja voi olla valtiollinen taho tai vaikkapa itsenäinen hakkerijoukko.

Ottakaamme esimerkki kyberkonfliktiksi TV5Monden hakkeroinnin vuonna 2015. Tapauksessa hakkerit murtautuivat TV5Monden lukuisille sosiaalisen median sivustoille ja aiheuttivat 12 kanavan keskeytymisen 18 tunnin ajaksi. Kyberiskun tekijöinä olivat itseään ISIS verkkokalifaatiksi kutsuva hakkerijoukko. He onnistuivat levittämään ISIS-propagandaa TV5Monden sosiaalisen median alustoilla. FireEye väittää iskujen tulleen Venäjältä.

Kyseisessä tapauksessa YK perustuskirjan artiklaa 33 (1) on haastava soveltaa. Kohteena on ollut TV-asema ja sen palvelut, ei valtiollinen taho. Toki Ranska voisi lähteä hakemaan oikeutusta kansalaisilleen artiklan 33 puitteissa, mutta ketä se vaatisi neuvotteluosapuoleksi? ISIS ei onnistunut luomaan omaa valtiota, jolle toiset valtiot myöntäisivät suvereniteetin omaan maahansa ja kansaansa. ISIS on kansainvälisissä silmissä vain terroristijärjestö. Mikäli Ranska lähtisi syyttämään Venäjää hyökkäyksen mahdollistajana, Venäjä pesisi varmasti kätensä puhtaaksi ISIS-terroristijärjestön hakkereiden touhuista. YK:n perustuskirjasta ei ole hyötyä tässä kyseisessä tapauksessa.

Kuinka due diligence -periaatteita ja velvollisuuksia voidaan soveltaa kyberkontekstissa? Hyvät ja huonot puolet.

Due diligence -periaatteen mukaan jokaisen valtion itsemääräämisoikeuksista huolimatta valtiolla ei ole oikeutta aiheuttaa harmia toiselle valtiolle omassa maassa tapahtuneiden asioiden seurauksena, kuten esimerkiksi saasteiden kulkeutuminen toisen maan alueelle. Ongelman lähtömaalla on velvollisuus periaatteen mukaan tehdä kohtuudella toimenpiteitä auttaakseen toista valtiota ongelmansa kanssa. Mielestäni due diligence -periaatetta ja velvollisuuksia voidaan soveltaa myös kyberkontekstissa. Periaatteet tarvitsevat uusia näkökulmia kybermaailmaan soveltuakseen.

Due diligence -periaatten pohjalta on jo lähdetty kehittämään ohjeita ja sääntöjä kybermaailman tarpeisiin. Saksa toimii hyvänä esimerkkinä siitä, miten se on hyödyntänyt due diligence -periaatetta kyberpolitiikassaan. Due diligance -periaatetta hyödynnetään tietoverkkorikollisuuden torjunnassa ei-sotilaallisissa toimenpiteissä, joiden tavoitteena on turvata siviilikohteita (kuten kriittistä infrastruktuuria ja henkilökohtaisia kansalaisoikeuksia) digitaalisilta hyökkääjiltä. Eurooppa-neuvosto on myös julkaissut Budapestin yleissopimuksen kyberrikollisuudesta (jo vuonna 2001), joka koskee tietoverkkorikollisuutta. Sopimus pohjautuu due diligence -periaatteelle.

EU on määritellyt kyberturvallisuusstrategiassaan (vuonna 2003) tavoitteekseen luoda turvallisen, avoimen ja suojatun kybertilan rakentamisen suhteen. Toimet keskittyvät viiden periaatteen varaan: 1) joustavien IT-rakenteiden luomiseen, 2) tietoverkkorikollisuuden torjuntaan, 3) puolustavan kyberkapasiteetin kehittämiseen, 4) teollisuuden ja teknologian kehittymisen edistämiseen kyberturvallisuuden parissa ja 5) kansainvälisen verkkodiplomatian kehittämiseen.

Rikokset globalisoituvat, automatisoituvat ja teollistuvat. Tämä vaatii sekä kansainvälistä että eurooppalaista koordinointia ja rakenteellista tietojenvaihtoa syyttäjäviranomaisten välillä. Due diligence -periaatteen pohjalta on hyvä kehittää periaatteita myös kybermaailmaan ja kyberrikollisuuden torjumiseen. Kyberrikosten torjuminen yli valtioiden rajojen voi parhaimmillaan luoda rauhaa ja turvallisuutta globaalilla

tasolla, mutta pahimmillaan mahdollistaa liiallisen valvonnan ja urkinnan valtiollisilta tahoilta. Kyberrikollisuuden suitsemiseen keskittyvien toimien tulisi olla mahdollisimman globaaleita, jotta voitaisiin mahdollistaa jokaiselle valtiolle tasapuolisesti kyberrauha.

Suurimpina haasteina kyberrikollisuuden torjunnassa lienee se, että maat (kuten USA ja Venäjä), joilla on poliittisesti paljon sananvaltaa, toimivat myös kyberrikollisten etujoukoissa. Siten näillä valtioilla ei ole todellisia intressejä edistää globaalia kyberrauhaa. Valtioiden välillä käydään tällä hetkellä tietynlaista kyberajan kylmää sotaa, jossa pyritään vahvistamaan omaa etulyöntiasemaa suhteessa vastapeluriin. Pienemmät pelurit on helppo syödä pois pelilaudalta (kuten kävi esimerkiksi Itä-Ukrainalle) ilman, että siitä on itselle mitään suurempaa haittaa. Due diligence -periaatteen soveltaminen laajemmin kyberrikollisuuden torjunnassa voisi vähentää kybermaailman polarisoitumista, mutta pahimmillaan dystopioissa se antaisi vain uusia keinoja vahvoille kontrolloida heikompia osapuolia kybershakkilaudalla.

OSION LÄHTEET

Bendiek, A. (2016). Due diligence in cyberspace: guidelines for international and European cyber policy and cybersecurity policy. Stiftung Wissenschaft und Politik (SWP), Research Paper 7/2016, Berlin. https://www.ssoar.info/ssoar/handle/document/47152 (lainattu 20.11.2019)

Eurooppa-neuvosto (2009). Euroopan unionin turvallisuusstrategia – Turvallisempi Eurooppa oikeudenmukaisemmassa maailmassa. Euroopan yhteisöt, Belgia. https://www.consilium.europa.eu/fi/documents-publications/publications/european-security-strategy-secure-europe-better-world/ (lainattu 20.11.2019)

Eurooppa-neuvosto (2001). EST 185 - Convection on cybercrime. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (lainattu 20.11.2019)

Finlex. Yhdistyneiden kansakuntien perustuskirja 1/1956. https://www.finlex.fi/fi/sopimukset/sopsteksti/1956/19560001/19560001_2#idp446449328 (lainattu 21.11.2019)

Kulesza, J. (2016). Due diligence in international law. Series: Queen Mary studies in international law; Volume 26, Hollanti. https://books.google.fi/books?id=pi_ODAAAQBAJ&pg=PA57&lpg=PA57&dq=due+diligence+sovereign&source=bl&ots=qBDJ95nLt3&sig=ACfU3U1_FWtbQ4IiwvtPhSi97PZK_8Do1w&hl=en&sa=X&ved=2ahUKEwiEn9T

T2PjlAhUqwqYKHUKkA9MQ6AEwAnoECAoQAQ#v=onepage&q=due%20diligence%20sovereign&f=false (lainattu 20.11.2019)

Paganini, P. (2015). FireEye speculates that behind the hack of France's TV5Monde television channel there is the popular APT28 that used the pseudonymous ISIS Cyber Caliphate. Security affairs. http://securityaffairs.co/wordpress/37710/hacking/apt28-hacked-tv5monde.html (lainattu 21.11.2019)

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.

20.11.2019

What technological development or which technologies can have profound change in societal life and international affairs?

Viimevuosina teknologioiden kehitys on kasvanut merkittävästi. Kuitenkin päätöksenteon hitaus ja päättäjien tietämättömyys hidastavat osaltaan niin teknologioiden kehitystä kuin niiden käyttöönottoakin. Kuitenkin yhteiskunnalla on kiire ymmärtää teknologioiden mahdollisuudet ja riskit, koska pahimmillaan yksittäiset uhat voivat aiheuttaa katastrofin. Merkittävimmät mahdollisuudet nivoutuvat uusien materiaalien käytön ympärille ja uusien energiamuotojen hyödyntämiseen. Mahdollisuuksien laaja-alainen ymmärtäminen takaa yhteiskunnalle paremmat kasvuedellytykset globaaleilla markkinoilla.

Suurimpia uhkatekijöitä yksilön oikeuksien, yhteiskunnan vakauden ja globaalin tasapainon ylläpitämisen näkökulmasta on datan siirtyminen valtaisiin tietokantoihin. Yksilötasolla riskinä on urkinnan kohteeksi joutuminen, yhteiskunnan tasolla uhkana on kansallisesti arkojen tietojen vuotaminen ulkovalloille tai kyberrikollisjengille, jonka kautta tietojen avulla voidaan toteuttaa esimerkiksi kohdennettua kybervaikuttamista luoden epävakautta kyseisen valtion alueelle. Hyvänä esimerkkinä kybervaikuttamisesta on Itä-Ukrainan tapahtumat, joissa Venäjä tai ainakin venäjämieliset tahot toimivat taustalla. Tietojen virtualisointi ja digitalisointi mahdollistaa myös tietojen valtiollisen hyväksikäytön kansalaisiaan vastaan poliittisten päätösten seurauksena tai epävakaassa poliittisessa tilanteessa. Voimme vain spekuloida, mitä natsi-Saksa olisi tehnyt ei toivotuille kansalaisilleen Toisen maailmansodan aikana, mikäli heillä olisi ollut saatavilla kaikki se tieto ihmisistään, mitä nyky-Suomessa valtionelimillä on saatavilla. Mitä todennäköisemmin he olisivat toteuttaa ihmisten massateurastuksia kohdennetummin ja tehokkaammin. Tästä syystähän saksalaisilla ei ole sosiaaliturvatunnuksiakaan.

Työ on muutoksessa. Niin kuin se on ollut läpi historiankirjoituksen. Tällä hetkellä työ muuttuu suorittavasta työstä aivotyöksi kovaa vauhtia. Muutos luo paineita ihmisten koulutustason nostolle ja uudelleen koulutukselle. Tulevaisuuden työelämä arvostaa luovia ja muuntumiskykyisiä työntekijöitä. Koneet, tekoäly, robotit, automatisaatio, bioteknologia ja nanomateriaalit mahdollistavat ihmisten

korvaamisen työelämässä jopa keskivaativissakin ajattelutyön tasoilla, kuten terveydenhuollossa, asiantuntijatehtävissä ja erikoislääketieteessäkin.

Työn siirtyminen ihmiseltä koneelle tuo mukanaan mahdollisuuksia kyberrikollisille aiheuttaa perustavanlaatuista haittaa tuotannolle, tuotteille tai jopa suoraan ihmiselle. Ajatellaanpa esimerkiksi leikkausta, jota robotti tekee. Miten kaikin tavoin hakkeri voisi aiheuttaa pysyvää harmia tai jopa tuottaa kuoleman potilaalle hyökätessään leikkausrobotin ohjelmistoon. Toinen uhkakuva, joka on nähtävissä työn ja ajattelun siirtyessä koneille on ihmisten fyysinen ja älyllinen passivoituminen. Jo tällä hetkellä mediassa puhutaan kansakuntamme liikkumattomuudesta, mitä se onkaan sitten, kun robotit tekevät kaikki fyysiset toimenpiteen sijastamme. Ihmisten liikkumattomuus on välillinen seuraus teknologioiden kehitykselle. Sen vaikutukset tulevat olemana kalliita yhteiskunnalle ja merkittäviä ihmisten elämänlaadun kannalta. Lisäksi ajattelun siirtyminen tekoälylle ja koneille mahdollistaa entistä suoremman kybervaikuttamisen suoraan koneiden algoritmeihin.

Teknologiat kaikkiallistuvat kovaa vauhtia. Syntyy uusia älykkäitä materiaaleja, joiden ansiosta teknologia on puettavissa päälle ja asennettavissa jopa ihmisen sisään, energiateollisuus uudistuu uusien energialähteiden ansiosta, kuljetus, logistiikka, tuotanto ja palvelut robotisoituvat, bioteknologiaan ja farmakologiaan tulee uusia sovelluksia ja sovellusalueita ja tekoäly kehittyy. Tämä kaikki altistaa niin työelämän kuin arjenjenkin kyberhyökkäyksille, kybervaikuttamiselle ja kyberrikoksille. Uhka voi tulla naapurista tai naapurivaltiosta. Mitä todennäköisemmin teknologisaation seurauksena tulemme näkemään entistä röyhkeämpiä ja suorempia kyberrikos- ja kybervaikuttamisyrityksiä. Tämä tulee vaikuttamaan merkittävästi politiikkaan, yhteiskunnan peruspilareihin ja kansainvälisiin suhteisiin.

What technological development or which technologies could constitute a strategic surprise and to whom?

Algoritmien kehittyminen, niiden kaikkiallistuminen ja jokapäiväistyminen tarjoaa valtaisat mahdollisuudet kybervaikuttamiselle. Algoritmien laskemiseen osallistuu suhteellisen suppea joukko kehittäjiä, siitä huolimatta, että algoritmien avulla vaikuttamista tapahtuu jo nykyään kohdennetusti algoritmien kehittäjien toimesta. Otetaan esimerkiksi Facebookissa esiintyvät mainokset. Niiden taustalla on algoritmi, joka kerää sivuston käyttäjästä mahdollisimman paljon tietoa, jotta voi tarjota käyttäjälle mahdollisimman mielenkiintoisia mainoksia ja sitä kautta lisätä mainostajien hyötyjä mainostaa juuri heidän kanavallaan.

Oletetaan, että joku vaikkapa poliittisella agendalla inspiroitunut taho pääsisi muuttamaan Facebookin mainosalgoritmia siten, että kohdennetuilla mainoksilla pyritään vaikuttamaan ihmisten nettikäyttäytymisen tai vaikkapa äänestämiseen kansallisissa vaaleissa. Vaikuttaminen voisi tapahtua joko

Facebookin toimesta tai ulkopuolisen kyberhyökkääjän toimesta. Näin voitaisiin pyrkiä saamaan aikaiseksi tietynlainen poliittinen tai kansallinen tahtotila muuttaa asioita kyberhyökkääjän toivomaan suuntaan.

Edellä mainittua metodia on käytetty vaikuttamaan USA:n vuoden 2016 presidentin vaalien lopputulokseen. Venäjä osti 100.000 dollarilla nettimainontaa Facebookista liittyen presidentin vaaleihin. Venäjä on mitä ilmeisemmin toiminut täydessä yhteisymmärryksessä Facebookin kanssa, mutta vaikuttamista ei katsota USA:ssa tai globaalillakaan tasolla hyvällä.

OSION LÄHTEET:

Koiranen, I., Räsänen, P., Södergåed, C. (2016). Mitä digitalisaatio on tarkoittanut kansalaisen näkökulmasta (essee). Talous ja yhteiskunta.

Linturi, R. (2015). Technology as an enabler of sustainable well-being in the modern society. Sitra studies 103, Helsinki. https://media.sitra.fi/2017/02/28142509/Selvityksia103.pdf

Nissinen, H. (2015). Teknologia tuo mahdollisuuksia, jos yhteiskunta uudistuu. Sitra.

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.

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

Tuomisto, J. (2017). USA:n vaalien Venäjä-tutkinta: Google, Facebook ja Twitter todistamaan senaatin tiedustelukomitealle. YLE. https://yle.fi/uutiset/3-9855384 (lainattu 10.12.2019)

21.11.2019

How to create efficient national cybersecurity governance model/system? How it would look like? What threats stem from state use of ICTs, and how to best address those threats internationally, regionally, nationally, by corporates, by individuals?

Jokainen kansallisvaltio on erilainen ja jokaisella on omat intressinsä kyberturvallisuuden puitteissa. Intresseihin vaikuttaa niin valtion tekninen kypsyysaste, vauraus, maan poliittinen tilanne ja poliittinen asenneilmapiiri, sisäiset intressit kyberteknologioiden kehittämisen suhteen kuin ulkoiset tekijätkin, kuten kansainväliset sopimukset ja välittömät uhatkin. Palonen korostaa pro gradu -tutkimuksessaan, että kyberturvallisuuden johtamisessa keskiössä on toimijoiden välinen yhteistyö, ajantasainen ja saatavilla oleva informaatio, kyberuhkien tunnistaminen ja niihin vastaaminen, yhteiskunnan toimintojen jatkuvuuden varmistaminen ja toimintoihin kohdistuvista häiriöistä palautuminen mahdollisimman nopeasti.

Nykyisessä kybermaailmassa kaikki toimijat ovat sellaisia toimijoita, joiden tulisi olla tietoisia myös kyberturvallisuudesta tai kyberturvattomuudesta. Kansainvälisellä tasolla tulee olla sopimuksia, joilla turvataan valtioiden suvereniteetti kyberympäristössäkin. Suvereniteetin rikkomisella tulisi olla niin imagollisia, poliittisia kuin taloudellisiakin vaikutuksia. Kansallisella tasolla tulee taata kansalaisten, yritysten ja muiden toimijoiden turvallisuus myös kyberympäristössä. Valtioiden tulee nykyaikana kyetä turvaamaan kansalaisillensa absoluuttinen tietoturva, jota ei murenna niin tietojen kalastaminen (social engineering) tai tietovuodot. Kyberkehittyneessä maassa valtioin on kiinnitettävä erityisen suurta huomiota erinäisten rajapintojen luotettavuuteen eri tietoverkkojen välillä, kuten esimerkiksi Suomessa potilastietojen ja sairaalatietokantojen välillä. Yritysten ja yhdistysten on panostettava erityisesti tietoturvaan. Niin yritysten kuin yhteisöidenkin tietoturva on paikoitellen lähes olematonta ja alttiina niin kyberhyökkäykselle, tuhoutumiselle kuin kalastelullekin.

Valitettavan usein kansalaistasolla pohdittaessa kyberturvallisuutta unohdetaan se yksittäisen ihmisen näkökulmasta keskeisin tietoturvaongelma eli kyseinen ihminen itse kybertoimijana. Taloudellisesti ja poliittisesti vakaassa maassa ihmisen suurin kyberturvallisuuden uhka tulee hänen omasta toiminnastaan. Omien tietoverkkoihin kytkettyjen laitteiden tietoturvasta on huolehdittava, on osattava käyttäytyä järkevästi sosiaalisen median alustoilla, salasanat tulee rakentaa vahvoiksi, on kyettävä näkemään trollitehtaiden tuottamien median taakse, ymmärrettävä algoritmien toimintaa ja niihin perustuvaa kohdentamista ja vaikuttamista sekä pitää olla tietoinen erinäisten huijausviestien ja nigerialaiskirjeiden luovasta moninaisuudesta. Valtiollisellakin tasolla yksi merkittävimmistä uhkatekijöistä on kansalaistensa kykenemättömyys toimia järkevästi kyberympäristössä.

Nykyaikana kehittyneiden valtioiden suvereniteettia ei taata panssarivaunuin ja tykkimiehin vaan kyberosaamisella. Valtion kannalta optimaalisin kyberturvallisuus taataan kattamalla toimet kokonaisvaltaisesti kansainväliseltä tasolta aina yksittäisiin kansalaisiin. Vaikkakin laajamittainen kybersota tai -kriisi on epätodennäköinen skenaario, turvallisuustoimet on tehtävä ennen tilanteen mahdollista eskaloitumista. Kybervahvan valtion on niin osattava puolustaa kuin hyökätäkin kybersodassa. Vahva kyberosaaminen on nykymaailmassa tehokkaampi ase kuin fyysiset aseet yhteensä. Ilman yhtäkään luotia tai pommia voidaan saada mikä tahansa valtio polvilleen oikein suunnitelluilla ja kohdennetuilla kyberhyökkäyksillä. Kaiken lisäksi, mitä kehittyneempi ja vauraampi valtio on, sitä suurempaa tuhoa laajamittainen kyberkonflikti voi aiheuttaa.

Otetaan esimerkiksi Venäjän tai venäjämielisten tahojen CrashOverride-kyberhyökkäys Ukrainaan vuoden 2015 joulukuussa, jolloin tietoverkkojen yli toteutetuilla hyökkäyksillä iskettiin sähkönjakeluun. Hyökkäys toteutettiin kostotoimenpiteenä Ukrainan katkaistua noin puolet Krimin alueen sähköverkoista räjäyttämällä suuria kantaverkkolinjoja. Venäjän kohteena oli sähköjakeluyhtiöiden SCADA-ohjausjärjestelmä, joihin ajetun koodin seurauksena kolmekymmentä sähkömuuntoasemaa sai käskyn

irtautua sähköverkosta. Sähköt katkesivat 1-6 tunniksi 225.000 asiakkaalta. Sähköt saatiin palautettua vielä olemassa olleen manuaalisen järjestelmän avulla. Suomessa vastaavaa manuaalista ohjausjärjestelmää ei enää ole, joten vastaava hyökkäys olisi aiheuttanut Suomessa merkittävästi pidempiä sähkökatkoja. Ukrainassa CrashOverride-kyberhyökkäyksen merkittävimmät vaikutukset liittyivät pelon lietsontaan.

Suomessa Valtioneuvoston tavoitteena on se, että yritykset ja organisaatiot, jotka ovat yhteiskunnan elintärkeiden toimintojen kannalta keskeisiä, ottavat toimintansa turvaamiseksi huomioon niihin kohdistuvat kyberuhat ja ylläpitävät suojautumiskykyään. Suomessa Huoltovarmuuskeskus tukee näiden toimijoiden suojautumista koulutusten, selvitysten ja ohjeistuksien avulla. Sekä Huoltovarmuuskeskus että yhteiskunnan elintärkeistä toiminnoista vastaavat ministeriöt pyrkivät tunnistamaan kriittisimmät tietotekniset rakenteet ja palvelut sekä niiden ylläpito ja tietovarannot. Riskit ja haavoittuvuudet pyritään tunnistamaan ja arvioimaan. Viranomaistahot ovat laatineet kriittisten tieto- ja viestintäjärjestelmien ja niihin liittyvien palveluiden turvaamisen varalle kansalliset vaatimushallinnan perusteet. Huoltovarmuuden kannalta keskeistä on se, että vakavan poikkeusolon sattuessa asiat voidaan hoitaa kansallisin toimenpitein ilman ulkomaista apua. Näillä toimilla pyritään takaamaan Suomessa toimintavarmuuden kannalta kriittisten tahojen toiminta ja kyberresilienssi.

Osion lähteet:

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

Lehto, M., Lemnell, J., Kokkomäki, T., Pöyhönen, J., Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.

Palonen, O-P. (2019). Kyberturvallisuuden johtaminen Virossa, Israelissa ja Alankomaissa – mitä voimme oppia? Jyväskylän Yliopisto, Tietojenkäsittelytieteen laitos, pro gradu -tutkielma. https://jyx.jyu.fi/bitstream/handle/123456789/65430/1/URN%3ANBN%3Afi%3Ajyu-201909064032.pdf

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.

24.11.2019

What is peace?

Perinteisesti ajateltuna rauha on tila, jossa ei ole sotaa ja sortoa. Minulle rauha merkitsee kokonaisvaltaista ideologiaa. Se on tekoja rauhan puolesta ja pyrkimystä pysyvyyteen ja vakauteen. Rauha edellyttää tiedostavaa toimintaa, historian tuntemusta, sekä ihmismielen että tekojen ymmärrystä. Empatia ja ymmärrys ovat keskeisimpiä tekijöitä rauhan turvaamisessa kaikilla tasoilla niin yksilötasosta kansainväliseen ylätasoon. Vastakkainasettelu johtaa helposti rauhan järkkymiseen ja vihollisten määrittelyyn ja sitä kautta konfliktiin.

Rauhaa pyritään tukemaan kansainvälisin sopimuksin ja vuoropuheluin. Tavoitteena on ratkaista mahdolliset rauhaa, tasapainoa ja elämän harmoniaa uhkaavat konfliktit jo ennen niiden eskaloitumista kriiseiksi, konflikteiksi tai sodiksi. Rauhan tilaa turvaa myös valtioiden rajat ylittävät identiteetit. Yksi eittämättä maailman historian merkittävistä rauhanprojekteista – Euroopan hiili- ja teräsyhteisö ja sitä kautta Euroopan Unioni – on edesauttanut yhteisen eurooppalaisen identiteetin syntymistä luoden kaupallisten etujen avulla valtioille vahvat edellytykset kehittää keskinäisiäkin suhteitaan vahvistamaan rauhan tilaa.

Euroopan Unionin aikakausi on historian pisin rauhan kausi Euroopan alueella. Entiset polarisoituneet valtasuhteet ja vanhat heimokiistat on saatu ratkaistuksi sen ansiosta, että kukin valtio tavoittelee niin ikään omia etujaan ajaessaan tiettyjä sopimuksia. Sopimukset, ovat ne sitten kaupallisia tai poliittisia, takaavat sen, että yksittäiselle valtiolle on kaikin puolin edullisempaa kehittää kahdenvälisiä suhteitaan naapurivaltioihin ennemmin kuin lähteä soitellen sotaan, josta seuraisi suurta taloudellista harmia puhumattakaan inhimillisestä kärsimyksestä.

Pysyvä ja pitkäaikainen rauhantila vaatii oman edun tavoittelemisen lisäksi myös intressiä suuremman yhteisen hyvän puolesta. Rauhantilaa voi kehittää passiivisesta rauhasta, sodan vastakohdasta, kattamaan kaikkea toimintaa mikä liittyy arkiseen toisia tahoja kuuntelevaan ja huomioivaan vuorovaikuttamiseen. Nykyään puhutaan paljon kybersodista ja -konflikteista. Väitän, että tällä hetkellä koko kybermaailma elää eräänlaisessa, ellei nyt ihan sotatilassa niin ainakin jatkuvan konfliktin tilassa. Kyberrauhan syntymisen edellytyksenä on se, että kybermaailman eri osapuolet alkaisivat kunnioittamaan toisiaan, ettei toimijoiden edut olisi toistensa vastaisia. Minulla ei ole vastausta siihen, miten kyberrauhaan pääsee. Toivottavasti minua fiksummat keksivät miten etunenässä Venäjä, USA, Israel, Iran ja Pohjois-Korea hautaavat kybersotakirveensä ennen kybersodan eskaloitumista fyysiseksi sodaksi.

What is and what isn't stability of cyberspace?

Käytän tässä tekstissä termiä kyberrauha kuvaamaan kybermaailman vakauden ja harmonian tilaa, tilaa, jossa kybermaailman toimijoiden intressit eivät ole polarisoituneet toistensa vastaiseksi. Kyberrauha on ideaalinen tila, jossa niin USA:lla kuin Venäjälläkin olisi yhteiset intressit toimia yhteistyössä toistensa kanssa vakaamman ja kestävämmän kybermaailman puolesta.

Nykymaailmassa tietyt valtiot kokevat USA:aan niin sanotusti omistavan Internetin. Venäjällä on kehitteillä oma versionsa Internetistä, RusNet, ja Kiinalla omansa ChinaNet. Itse näen tämän kehityksen uhkaavan etenkin kyberrauhaa, ja pahimmassa tapauksessa jopa johtavan fyysisiin konflikteihin jopa sotiin. Kehityksessä on piirteitä kylmästä sodasta, jolloin suurvallat kehittivät omat teknologiansa ja pyrki visusti pitämään kyseisen teknologiaosaamisen omissa hyppysissään. Valtioiden omien tietoverkkojen kehittelyn

taustalla on toki jatkuva tiedonjano, big datan louhinta ja kansalaistensa verkkotoiminnan jatkuva kontrollointi.

Uskon, että yhtenä vähintäänkin yhtä merkittävänä tekijänä on valtioiden intressit pitää viholliseksi katsomansa toimijat poissa omalta kybermaaperältään. Ajatellaanpa esimerkiksi Venäjää, joka on kunnostautunut Internetissä verkkovakoilussa, -vaikuttamisessa ja -hyökkäyksissä, sillä on osaamista toimia Internetissä muun muassa USA:aan etuja vastaan. Venäjä siirtää oman verkkotoimintansa RusNetiin, jossa USA:llä ei ole mahdollista toimia siten, miten Venäjä toimii Internetissä. Mahdollistaako RusNet Venäjän toimimisen Internetissä kansainvälisten käytänteiden ja jopa lakien vastaisesti, koska ei ole olemassa vastatoimia RusNetin puolella? Toki on olemassa perinteiset vastapakotekeinot, kuten kauppasaarrot etc., toisaaltaan Venäjällä on hyvät suhteet itään päin.

28.11.2019

What is cyberweapon?

Wikipedian mukaan “ase on väline, jolla voi tappaa tai vahingoittaa eläviä olentoja, ja jota yleensä käytetään taistelussa tai metsästyksessä” ja ”asetta voi käyttää hyökkäämiseen, puolustamiseen tai uhkailuun”. Perinteisesti ase mielletään fyysiseksi kapistukseksi, jota voi käyttää väkivaltaan tai väkivallalla uhkailuun. Lisättäessä tähän kyberulottuvuuden, lyhyesti avattuna kaiken tietoverkkoihin liittyvän, aseen fyysinen olemus muuttuu abstraktiksi. Mikäli määrittelemme kyberaseen siis olevan jotain tietoverkkoihin liittyvää, jolla voi vahingoittaa toista tai uhata toista, tajuamme kyberaseiden olevan jo tätä päivää, eikä vain osa jotain harmaata tulevaisuuden dystopiaa.

Määritteen mukaisesti kyberaseiksi voi lukea kuuluvaksi niin tietojen kalastelusta trolliarmeijoihin kuin kyberhyökkäyksistä fyysisemmänkin olomuodon omaaviin tietoverkkoja hyödyntäviin aseisiin, kuten esimerkiksi joko puolustus- tai hyökkäysmielessä hyödynnettäviin droneihin. Mielestäni on perusteltua ajatella jopa yksittäisten hakkereiden voivan toimia kyberaseina, mikäli heidät valjastetaan hyökkäämään jotakin tai jotakuta vastaan tarkoituksena tuottaa vahinkoa hyökkäyksen kohteelle. Nykyaikana älyn valjastaminen kybersodan välineiksi – kyberaseiksi – on strategisesti kannattavampaa kuin käyttää fyysisiä aseita ja miesvoimaa. Näin ollen kyberaseita voi hyödyntää esimerkiksi hyökätessä niin sanotun vihollisen satelliitteja vastaan, valtiollista sotilaallista puolustusta kohti, vaikkapa inaktivoidakseen valtion rakettitorjuntajärjestelmän, taikka lamaannuttaessa palvelunestohyökkäyksellä paikallisen maksukorttijärjestelmän.

Nelli Sviili
nekasvii@student.jyu.fi

How governments should regulate the Internet? What about the freedom of the Internet?

Tietoverkot ovat levittäytyneet laajasti eri elämän osa-alueilla kehittyneessä maailmassa. Myös kehittyvässä maailmassa tietoverkkojen merkitys kasvaa hetki hetkeltä. Esimerkiksi Suomessa pelkästään tietoverkkojen kaatuminen pitkäaikaisesti johtaisi suuriin haasteisiin lähes kaikilla elämän osa-alueilla, aina kauppojen toiminnasta liikenteeseen ja sairaaloista sähkön ja veden jakeluun. Mikäli jokin Suomelle vihamielinen taho pystyisi ja haluaisi tehdä suurta haittaa niin sanotusti laukaisemalla kyberaseensa Suomea kohti, hyökkäämällä tietoverkkoja pitkin Suomeen, se taho saisi aikaan suurta tuhoa ja inhimillistä kärsimystä ilman, että yhtäkään konkreettista luotia olisi ammuttu tai pommia räjäytetty.

Kyberturvallisuuden perustana ei tule olla vain vahva kyberpuolustus. Mitä tietotekniikkaan ja tietoverkkoihin tulee, aina on jokin taho, joka on kehityksessä edellä. On lähes mahdoton rakentaa täysin veden – tai siis hakkerin loitolla – pitävä kyberpuolustusjärjestelmä. Hyvä kyberpuolustus on toki merkittävä osatekijä kokonaisturvallisuuden näkökulmasta, mutta sen lisäksi tarvitaan poliittista vuoropuhelua, sopimuksia, ohjeistuksia ja lainsäädäntöä niin valtiollisella kuin kansainväliselläkin tasolla. Myös yksityisen sektorin toimijat on hyvä valjastaa kyberturvallisuuden puolesta taistelevien joukkoon. Monesti juuri yksityiseltä sektorilta löytyy kyberturvallisuuden kärkeä tai ainakin varteenotettavia näkemyksiä ja kokemuksia asioiden ratkaisemiseksi. Monet kybermaailman yksityisen puolen toimijat ovat myös globaaleja toimijoita, kuten vaikkapa Microsoft, Apple ja Samsung. Heiltä voi löytyä sellaista maiden rajat ylittävää tietoa, joita ei valtiollisilla toimijoilla ole.

Nyt olemme vastanneet kysymykseen, että jotain pitäisi tehdä. Vaikeampi on vastata kysymykseen, että mitä. Tulisiko verkkosisältöä jotenkin rajoittaa ja kenen ehdoin vai tulisiko jokaiselta verkkoon asiaa tai tavaroita liittävien tahojen suorittaa jonkun näköinen verkkoajokortti, jotta saataisiin verkossa toimimisen turvallisuus taattua, on vaikea kysymys. Mielestäni yksi keskeisistä lainsäädännöllä mahdollistettavista kyberturvallisuutta parantavista tekijöistä on turvata lainsäädännönkin keinoin avoimuus haavoittuvuuksista ja uhkista, jotta niin valtiolliset, yksityiset kuin yksittäisetkin ihmiset osaisivat hahmottaa paremmin tietoverkkojen uhat. Keskeisessä roolissa mielestäni on myös kansalaisten sivistäminen kyberturva-asioihin liittyen. Valitettavan harva osaa toimia turvallisesti kyberympäristössä.

Osion lähteet:

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

Wikipedia (2020). Ase. Lainattu (27.1.2020): https://fi.wikipedia.org/wiki/Ase

Nelli Sviili
nekasvii@student.jyu.fi

10.1.2020

Are we normalizing cyberwar?

Ensin pitää aloittaa määrittelemällä mitä kyber on ja mitä kybersota on. Mikäli aikaisempiin muistiinpanoihini viitaten määritellään sanan kyber käsittävän käytännössä kaikki tietoverkkosidonnainen teknologia, koodit ja algoritmi ja mikäli johdamme sodan määritelmän rauhantilan vastakohdaksi, jolloin jokin taho turvautuu aseisiin, voimme vähintään todeta kylmän kybersodan olevan käynnissä. Sodan osapuolia ovat etunenässä kybermahdit eli USA, Venäjä, Pohjois-Korea, Kiina ja Israel. Vielä en nimeäisi nykyistä tilaa ensimmäiseksi maailman kybersodaksi, mutta vastakkainasettelu ja kyberhyökkäykset ovat arkipäivää.

On perusteltua väittää, että maailma on jollain tasolla hyväksynyt ja jopa normalisoinut nykyisen vastakkainasettelun kulttuurin myös kybermaailmassa. Kybermaailma hakee vielä sääntöjään ja lakejaan. Ehkäpä kybermaailmaa ei vielä tunneta reaalimaailmassa riittävän hyvin tai kybermaailman uhkakuvat eivät ole riittävän selvät päättäjille, jotta säädettäisiin lakeja ja sopimuksia suitsimaan epätoivottua ja konfliktinhaluista käyttäytymistä kybermaailmassakin. Tämä näyttäytyy helposti siten, että maailma ja sen päättäjät ovat hyväksyneet kyberkonfliktisen tilan ja sitä kautta vaikuttaneet myös kybersodan normalisointiin meillä ja maailmaalla.

Is it better to be hitted by a cybergun like a missile?

Mikäli tehtäisiin laaja kyselytutkimus niin sanotun tavallisen kansan parissa siitä, että kumpi on pahempi paha kyberaseen käyttö ja ohjusisku, näkökannat saattaisivat mennä aika tasan. Mutta jos sanaa kyberase avattaisiin ja käytettäisiin vaikka termejä urkinta, tietoverkkohyökkäys tai mielipidevaikuttaminen, uskon selvän kansan enemmistön vastaavan, että ohjus on pahempi uhka. Perustelen väittämääni tiedolla siitä, kuinka suppeaa kyberturvallisuuden ymmärrys on kansan syvissä riveissä. Valitettavan harvan mielipide perustuisi faktoihin.

Todellisuudessa kyberaseella ja kyberhyökkäyksellä voi saada paljon vakavampaa tuhoa aikaan, mikäli hyökkäyksen tavoitteena olisi aiheuttaa maksimaalista harmia ja kärsimystä kohdemaahan. Mikäli ohjus pääsisi ohjussuojasta läpi, sen tuho on vain ja ainoastaan sen, mitä fyysistä tuhoa se kohteessaan aiheuttaa. Vaikka kohde olisikin huolella valittu niin, että ohjuksen tuhovoima olisi maksimaalinen, puhutaan lähinnä kymmenistä, korkeintaan sadoista ihmisistä joihin isku fyysisesti kohdistuu. Tietenkin ydinkärjellisen ohjuksen vaikutukset olisivat huomattavasti merkittävämmät. Ohjusiskun vaikutusta kansalaisten pelkoihin ei tule väheksyä. Onnistunut kyberisku voisi lamaannuttaa kokonaisen yhteiskunnan. Ajatellaanpa kyberaseen käyttöä valtion sähkönjakelua vastaan. Esitetään hypoteesi, että sähköverkko kaatuisi kovilla talvipakkasilla viikoksi. Jo pelkästään hisseihin loukkuun jääneiden ihmisten lukumäärä ohittaisi nopeasti

ohjusiskun uhrien lukumäärän. Sähköttömyys aiheuttaisi myös suurta pelkoa ja lisäisi ilkivallan ja rikollisuuden määrää.

Ajatellaanpa vaikkapa USA:an Stuxnet-iskua Irania vastaan. Jos se olisi toteutettu ohjusiskuna, se olisi voinut johtaa suurempaan globaaliin kriisiin ja vähintäänkin selkeään USA:an tuomitsemiseen. Mutta kun isku toteutettiin hakkereiden voimalla kyberiskuna, kukaan ei edes ensin huomannut iskun käynnistymistä, saatikka kukaan ei pystynyt heti osoittamaan vedenpitäviä todisteitä USA:ta vastaan. Verrataanpa vaikka Stuxnetiä siihen, kun Venäjä tai venäjämieleiset ampuivat Ukrainassa siviililentokoneen alas. Kansainvälinen yhteisö kääntyi Venäjää vastaan ja tapaus vaikutti ainakin välillisesti Venäjän talouspakotteisiin.

Näin voimme todeta, että kyberhyökkäyksen todellinen vaikuttavuus voi olla fyysistä iskua merkittävämmät, mutta fyysinen isku voi tulla sekä poliittisessa että taloudellisessa mielessä kalliimmaksi iskuntekijälle.