Kansainvälinen oikeus kyberympäristössä
Suomen kansallisia kantoja

Johdanto

Suomi tukee sääntöpohjaista kansainvälistä yhteistyötä ja kansainvälisen oikeuden kunnioittamista. Tämän yleislinjan mukaisesti katsomme, että kansainvälinen oikeus luo olennaiset puitteet vastuulliselle valtiokäyttäytymiselle kyberympäristössä. Myös YK:n hallitustenvälinen asiantuntijaryhmä (GGE) on samansuuntaisesti vahvistanut, että ”kansainvälinen oikeus ja varsinkin Yhdistyneiden Kansakuntien peruskirja ovat sovellettavissa [kyberympäristössä] ja olennaisia tekijöitä rauhan ja turvallisuuden ylläpitämisen samoin kuin avoimen, turvallisen, vakaan, saavutettavan ja rauhanomaisen informaatio- ja kommunikaatioteknologisen ympäristön edistämisen kannalta”.[1] Koska tämä muotoilu GGE:n erityistä toimeksiantoa heijastaen keskittyy kansainvälisen rauhan ja turvallisuuden kysymyksiin, on tarpeen painottaa, että sama koskee valtioiden muitakin oikeuksia ja velvollisuuksia riippumatta siitä, perustuvatko ne valtiosopimuksiin tai kansainväliseen tapaoikeuteen.

Kansainvälisen oikeuden olemassa olevat säännöt ja periaatteet koskevat myös kyberympäristöä. Tästä huolimatta kyberympäristön erityispiirteet voivat herättää kysymyksiä joidenkin säännösten käytännön soveltamiseen liittyen. Suomi pitää sen vuoksi tervetulleena näkemysten vaihtoa siitä, miten kansainvälinen oikeus tietyissä kysymyksissä sääntelee informaatio- ja kommunikaatioteknologioiden käyttöä valtioiden toimesta. Suomi haluaa antaa panoksensa tähän keskusteluun kommentoimalla muutamia viime aikoina esiin nostettuja kysymyksiä.

Suvereenisuus

Valtion täysivaltaisuuden eli suvereenisuuden periaate koskee kiistatta kyberympäristöä. Vaikka kyberympäristö kokonaisuudessaan ei ole minkään valtion vallattavissa, valtiolla on alueellinen toimivalta suhteessa sekä alueellaan sijaitsevaan kyberinfrastruktuurin että siellä kybertoimintoihin osallistuviin henkilöihin. [2] Suvereenisuus antaa valtiolle yksinomaisen oikeuden käyttää valtiollista toimivaltaa omalla alueellaan.[3] Lisäksi suvereenisuus suojaa valtion

[1] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, vuoden 2013 raportti (UN Doc. A/68/98, kpl.20; vuoden 2015 raportti (UN Doc. A/70/174), kpl. 24.

[2] GGE on todennut tässä yhteydessä seuraavasti: “State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related and to their jurisdiction over ICT infrastructure within their territory”. Ks. vuoden 2015 raportti, kpl. 27. Muut kansainvälisen oikeuden mukaiset toimivaltaperusteet voivat soveltua kybertoimintoihin.

[3] Tuomari Max Huber totesi *Island of Palmas* –välitystuomiossa seuraavasti: “Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.” Ks. *Island of Palmas (Netherlands v. the US),* 2 UNRIAA 829, 838 (PCA 1928).

alueellista koskemattomuutta ja poliittista itsenäisyyttä muiden valtioiden puuttumiselta.[4] Suvereenisuus on tässä mielessä yksi kansainvälisen oikeusjärjestyksen perusperiaatteista mutta siihen pohjautuen on syntynyt myös erityisiä sääntöjä kuten voimankäytön kielto ja toisten valtioiden sisäisiin asioihin puuttumisen kielto. Kaikkia valtioita sitoo myös velvoite pidättyä loukkaamasta toisten valtioiden alueellista koskemattomuutta tai poliittista itsenäisyyttä. Tämä velvoite korostuu silloin, kun toiminta ei yllä kielletyn väliintulon tasolle.

Kansainvälinen tuomioistuin on johdonmukaisesti vahvistanut kaikille valtioille kuuluvan velvoitteen kunnioittaa toistensa suvereenisuutta. Tämä velvoite koskee luvatonta tunkeutumista valtion fyysisille alueille kuten esimerkiksi ylilentoa toisen valtion ilmatilassa valtiolle kuuluvalla tai sen valvonnassa olevalla ilma-aluksella,[5] vieraiden sota-alusten luvatonta tunkeutumista toisen valtion aluevesille,[6] tiettyjen toimien harjoittamista tosien valtion alueella ilman sen lupaa[7] mutta myös tiettyjen vaikutusten aiheuttamista toisen valtion alueella ilman fyysistä tunkeutumista.[8] Tuomioistuimen mukaan on ”varsin ilmeistä, että valtiolla on oikeudellinen intressi alueensa suojelemiseen **miltä tahansa** ulkopuoliselta haitalliselta toiminnalta.”[9]

Luvaton tunkeutuminen tietoverkkoihin ja -järjestelmiin, jotka tukeutuvat toisen valtion alueella sijaitsevaan kyberinfrastruktuuriin voi samoin loukata kyseisen valtion suvereenisuutta. Kielto loukata toisen valtion alueellista koskemattomuutta kyberoperaation keinoin suojelee ensinnäkin sen alueella tai muutoin sen lainkäyttövallan piirissä sijaitsevaa kyberinfrastruktuuria samoin kuin siihen tukeutuvia tietoverkkoja ja -järjestelmiä aineellisilta vahingoilta. Tilanne on sama riippumatta siitä, onko kyberinfrastruktuuri valtiollisten instituutioiden, yksityisten tahojen tai yksityishenkilöiden omistuksessa tai käytössä. Mahdollisesti aiheutetun aineellisen vahingon ohella tällaisia operaatioita arvioitaessa voidaan ottaa huomioon, johtaako kyberinfrastruktuuriin tunkeutuminen häiriöihin siihen tukeutuvien laitteiden toiminnassa taikka kohdevaltiolle tai yksityisille toimijoille sen alueella kuuluvien tietojen muokkaamiseen tai tuhoamiseen.

Luvatonta kyber-tunkeutumista voidaan yleensä ottaen pitää kohdevaltion suvereenisuuden loukkauksena myös silloin, kun se kohdistuu sellaisiin tietoihin tai palveluihin, jotka ovat välttämättömiä valtion olennaisten tehtävien hoitamiseksi. Tämä Tallinn Manual 2.0 –teokseen

[4] Kansainvälisen tuomioistuimen mukaan “between independent States, respect for territorial sovereignty is an essential foundation of international relations.” Ks. *Corfu Channel Case (UK v. Albania)*, ICJ reports 1949, p. 4, at 35.

[5] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgment, I.C.J. Reports 1986, p. 14, kpl. 251, 253, 292.

[6] *Corfu Channel case (United Kingdom v. Albania), Judgment, I.C.J. Reports 1949, p. 4, s.* 26, 35, 36.

[7] *Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v,. Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v. Costa Rica)*, Judgment, I.C.J. Reports 2015, p.665, kpl. 66,67,69, 93, 221-223 and 229.

[8] *Nuclear Tests (Australia v. France)*, Judgment, I.C.J. Reports 1974, p. 253, kpl. 454.

[9] *Ibid*. kpl. 456, lihavointi lisätty.

sisältyvä sääntö[10] on yhdenmukainen sen käsityksen kanssa, että valtiollisen toimivallan (julkisen vallan) luvaton käyttö toisen valtion alueella on suvereenisuuden loukkaus. Lisäksi myös kyber-operaatioita suvereenin immuniteetin suojaamia kohteita vastaan (sota-alukset, valtion alukset, joita käytetään yksinomaan julkiseen tai ei-kaupalliseen toimintaan, valtion ilma-alukset) voidaan luonnehtia suvereenisuuden loukkauksiksi.[11]

Hiljattain on esitetty, että suvereenisuuteen yleisenä periaatteena ei ainakaan kyberympäristössä liittyisi oikeudellisia seurauksia. Tätä näkemystä on vaikea sovittaa yhteen sen kanssa, että suvereenisuuden loukkaukset kieltävällä säännöllä on vakiintunut asema kansainvälisessä oikeudessa. Lisäksi sitä on vaikea perustella poliittisesti. Jos kiellettyä väliintuloa vähäisempiä vihamielisiä kyberoperaatioita ei voitaisi pitää kansainvälisesti oikeudenvastaisina tekoina, ne jäisivät sääntelyn ulkopuolelle eikä niiden kohteeksi joutuneella valtiolla olisi mahdollisuutta vaatia oikeuksiaan.

Suomen näkemyksen mukaan suvereenisuus on kansainvälisen oikeuden primäärinormi, jonka loukkaus merkitsee kansainvälisesti oikeudenvastaista tekoa ja synnyttää valtion vastuun. Tämä sääntö koskee täysin myös kyberympäristöä. Luvattoman kybertunkeutumisen luonteesta ja seurauksista riippuu, katsotaanko sen loukkaavan kohdevaltion suvereenisuutta. Kyse on tapauskohtaisesta arvioinnista.

Laiton väliintulo

Vihamielinen kyberhäirintä voi rikkoa myös tapaoikeudellista toisen valtion sisäisiin asioihin sekaantumisen kieltoa edellyttäen, että sen tarkoituksena on painostaa tai pakottaa kyseistä valtiota asioissa, joiden suhteen sillä on vapaa määräysvalta (nk. *domaine réservé*). Pakottamisen vaatimus jättää käsitteen ulkopuolelle vähäisemmät vaikuttamisen ja taivuttelun muodot, jotka ovat tavanomaisia kansainvälisissä suhteissa. Kielletyn väliintulon rajaaminen suvereenisuuden piiriin kuuluviin kysymyksiin – esimerkkeinä valtion poliittinen, taloudellinen tai kulttuurinen järjestelmä tai sen ulkopoliittinen suuntaus[12] – erottaa kielletyn väliintulon myös sellaisista toimista, joiden tarkoituksena on painostaa valtiota noudattamaan kansainvälisiä velvoitteitaan.

Jotta kyberoperaatiota voitaisiin pitää kiellettynä väliintulona, molempien edellä mainittujen elementtien on sisällyttävä siihen. Useimmat avoimet kysymykset liittyvät pakottamisen elementtiin ja siihen, miten se näyttäytyy kybertoiminnassa. Vaikka esimerkiksi vaalien toimittaminen kiistatta kuuluu kunkin valtion sisäisiin asioihin, kaikki vaalihäirinnän menetelmät eivät välttämättä sisällä pakottamista.[13] Äänestäjätiedostojen hakkerointia ja ääntenlaskennan manipuloimista tarkoituksessa muuttaa vaalituloksia on kuitenkin pidetty melko selvinä

[10] Michael N. Schmitt (ed.), *Tallinn Manual 2.0*, Cambridge University Press 2017, sääntö 4, kpl. 15.
[11] Vrt. *Ibid*., Rule 5.
[12] *Military and Paramilitary Activities in and against Nicaragua,* kpl. 205.
[13] Kaikki vaalihäirinnän muodot eivät ole luonteeltaan pakottavia**,** ks.EU vs. disinfo, 10 *Methods of electoral interference* (2019).

tapauksina. Ollakseen verrattavissa reaalimaailman väliintuloihin, kyberhäirinnän on myös oltava vakavaa laatua.

Kansainvälisen tuomioistuimen mukaan pakottamisen elementti on erityisen selvä jos käytetään voimaa joko sotilaallisin toimin, niillä uhkaamalla tai tukemalla kapinallisia tai terroristeja toisessa maassa.[14] Pakottamisen tarkoitus voi kuitenkin ilmetä myös esim. sotilaallisen tai taloudellisen painostuksen kautta. Vihamielinen kyberhäirintä, jonka tarkoituksena on edistää tai tukea aseellisia toimia kohdevaltiossa voisi myös olla esimerkki kielletystä väliintulosta, jos sillä tavoitellaan politiikkamuutosta.[15]

Pakottavan luonteen ja *domaine réservén* vaatimukset nostavat kielletyn väliintulon kynnyksen huomattavasti korkeammalle kuin suvereenisuuden loukkauksen. Tämä korostaa sen merkitystä, että suvereenisuus edelleenkin ymmärretään paitsi periaatteeksi, myös kansainvälisen oikeuden itsenäiseksi primäärinormiksi.

Rajat ylittävä haitta

Toinen perustavanlaatuinen periaate, joka perustuu suvereenisuuteen ja liittyy läheisesti velvoitteeseen kunnioittaa toisten valtioiden suvereenisuutta, on jokaisen valtion velvoite olla sallimatta sitä, että sen aluetta käytetään tavalla, joka aiheuttaa merkittävää haittaa muiden valtioiden oikeuksille. Laajasti on tunnustettu, että tämä, usein asianmukaiseksi huolenpidoksi tai huolenpitovelvoitteeksi (*due diligence*) kutsuttava periaate koskee kaikkia toimintoja joihin sisältyy riski merkittävän rajat ylittävän haitan tuottamisesta.[16] Huolenpitovelvoite on muuttuva mittapuu siinä mielessä, että esimerkiksi teknologinen kehitys tai muuttuneet riskiarviot voivat vaikuttaa sen sisältöön.[17] Tämä myös tukee sen soveltamista kyberoperaatioihin.

Kiellettyä on siis sellaisten kyberoperaatioiden tietoinen salliminen valtion alueella, tai alueella tai kyberinfrastruktuurissa, joka on sen valvonnassa, jotka aiheuttavat vakavia haitallisia seurauksia muille valtioille. Vaikka vain valtiot voivat loukata suvereenisuutta, suvereenisuuteen perustuva huolenpitovelvoite koskee myös yksityisiä toimia valtion alueella. Yksityisistä kybertoimista muille valtioille aiheutuva vakava haitta voi johtaa valtion kansainväliseen

[14] *Military and Paramilitary Activities in and against Nicaragua*, kpl. 247.
[15] *Ibid.*, ks. myös kpl. 241 and 242. Ks. myös Friendly Relations Declaration, UN Doc. A/RES/2625(XXV).
[16] International Law Commission, Draft Articles on the *Prevention of transboundary harm from hazardous activities*, art. 3: "The State of origin shall take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof", *Yearbook…* 2001, vol. II (Part Two), s. 144–170; International Law Association, Second Report on Due Diligence in International Law, July 2016, s. 6: “This broad principle of due diligence can be understood as underlying more specific rules of due diligence. Hence, it can be viewed as a default standard that is triggered in operation if no more specific elaboration of due diligence or stricter standard is in existence.”
[17] International Tribunal for the Law of the Sea, Seabed Disputes Chamber, *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Advisory opinion, 1 February 2011, List of Cases: No. 17, kpl. 117.

vastuuseen mutta vain siinä tapauksessa, että kyseinen valtio on rikkonut huolenpitovelvoitettaan.

Huolenpitovelvoitteesta johtuu tiettyjä oikeudellisia velvoitteita, jotka ovat sille ominaisia ja jotka soveltuvat kybertoimintaan huolimatta siitä, että periaatteesta ei ole tarkempaa kyber-spesifiä kansainvälistä sääntelyä. Jos valtio esimerkiksi tietää alueellaan suunnitellusta kybertoiminnasta, joka todennäköisesti aiheuttaa vakavaa haittaa toiselle valtiolle, sen tulee ilmoittaa asiasta tälle valtiolle. Tosiasiallisen tiedon lisäksi kyseessä voi vastuun syntymisen kannalta olla tilanne, jossa valtion olisi pitänyt tietää alueeltaan lähtöisin olevista haitallisista toimista. Samalla on selvää, että ”pelkästään siitä tosiasiasta, että valtio harjoittaa valvontaa alueellaan, ei voi päätellä, että se välttämättä oli tietoinen, tai että sen olisi tullut olla tietoinen, kaikista siellä tapahtuvista laittomista teoista”. [18]

Jos haitallista kybertoimintaa tapahtuu ja se aiheuttaa merkittävää haittaa toiselle valtiolle, aluevaltion on ryhdyttävä asianmukaisiin toimiin lopettaakseen sen samoin kuin tutkiakseen tapauksen ja saattaakseen siihen liittyvät henkilöt oikeudelliseen vastuuseen. Tämä edellyttää myös asianmukaista lainsäädäntöä ja menettelyjä. On kuitenkin huomattava, että huolenpitovelvoite on toimintaa, ei tulosta koskeva velvoite. Valtioilta edellytetään yleisesti ottaen, että ne ryhtyvät kaikkiin niihin toimiin, jotka ovat vallitsevissa oloissa mahdollisia ja toteuttamiskelpoisia. Tähän liittyy erityinen kysymys sellaisten kauttakulkuvaltioiden asemasta, joiden alueen kautta jotakin tiettyä haitallista dataa reititetään. Paljon riippuu siitä, onko tällaisella valtiolla mitään tietoa meneillään olevasta operaatiosta tai edellytyksiä ryhtyä toteuttamiskelpoisiin toimiin sen pysäyttämiseksi.

Vaikka valtioiden on osoitettava asianmukaista huolenpitoa alueensa valvonnassa, tämä ei vapauta niitä noudattamasta muita kansainvälisiä velvoitteitaan kuten esimerkiksi ihmisoikeusvelvoitteita.

Valtion vastuu

Valtion vastuuta koskevat oikeussäännöt ovat luonteeltaan sekundäärinormeja, jotka soveltuvat yleisesti valtioiden kaikkeen toimintaan silloin, kun ei ole olemassa erityissääntelyä, joka modifioisi niiden vaikutusta. Koska valtion toimista kyberympäristössä ei ole tällaista erityissääntelyä (*lex specialis*), kyberympäristössä toimitaan valtiovastuun yleisten sääntöjen nojalla.

Kun valtion kyberoperaatio loukkaa sen kansainvälisen oikeuden mukaisia velvoitteita, kyseessä on kansainvälisesti oikeudenvastainen teko. Kansainvälisesti oikeudenvastainen teko johtaa valtion kansainväliseen vastuuseen ja luo velvoitteen antaa teolla mahdollisesti aiheutettua vahinkoa vastaava täysi hyvitys. [19] Tämä edellyttää, että teko on luettavissa valtion syyksi.

[18] International Court of Justice, *Corfu Channel case*, Judgment of April 9th, 1949, I.C.J. Reports 1949, p.4, at 18.
[19] International Law Commission, *Responsibility of States for Internationally Wrongful Acts* (2001), www.legal.un.org/ILC (ARSIWA).

Syyksilukemista koskevat säännöt YK:n kansainvälisen oikeuden toimikunnan valtiovastuuartikloissa[20] ovat täysin pätevät myös kyberympäristössä. Jos valtion elimiä tai yksityisiä ryhmiä tai yksityishenkilöitä, jotka toimivat valtion puolesta, voidaan tunnistaa valtion kansainvälisiä velvoitteita loukkaavan kyberoperaation tekijöiksi, valtiolla on niistä vastuu. Tässä suhteessa on hyödyllistä erottaa toisistaan tunnistaminen teknisenä operaationa ja syyksilukeminen oikeudellisena operaationa. Tunnistamiseen liittyy teknisiä haasteita ottaen huomioon, että vihamieliset kyberoperaatiot ovat usein salaisia mutta tällä ei ole vaikutuksia syyksilukemista koskeviin oikeussääntöihin.

Kansainvälisesti oikeudenvastainen teko voi oikeuttaa, että loukattu valtio ryhtyy vastatoimiin, mikäli vastuussa oleva valtio kieltäytyy lopettamasta oikeudenvastaista toimintaa tai maksamasta hyvitystä. Vastatoimien tarkoituksena voi olla vain sen varmistaminen, että vastuullinen valtio noudattaa velvoitteitaan, ei kosto. Vastatoimilla ei myöskään saa loukata voimankäytön ja sillä uhkaamisen kieltoa tai muita pakottavia kansainvälisen oikeuden normeja, ja niiden on noudatettava myös muita vastatoimia koskevia tapaoikeudellisia vaatimuksia ja rajoituksia, jotka on pääosin kirjattu Kansainvälisen oikeuden toimikunnan valtiovastuuartikloihin.[21] Jotkut vastatoimia koskevat menettelyvaatimukset voivat kuitenkin edellyttää tarkistusta. Esimerkkinä voidaan mainita, että vastatoimiin yleensä tulisi ryhtyä oikeudenvastaisen toiminnan vielä jatkuessa. Vihamielisen kyberoperaation syyksilukeminen saattaa kuitenkin olla mahdollista vasta jälkikäteen.

Vastatoimiin ryhtyvällä valtiolla ei ole yleistä velvoitetta paljastaa niitä tietoja, joihin vastatoimet perustuvat. Samalla on kunkin valtion omien etujen mukaista varmistaa, että vastatoimia koskeva päätös perustuu vankkaan näyttöön, ottaen huomioon, että vastatoimiin ryhtyminen muussa tapauksessa olisi kansainvälisesti oikeudenvastainen teko. Valtiolla, joka vastaa vihamieliseen kyberoperaatioon, tulee sen vuoksi olla asianmukaiset todisteet operaation alkuperästä ja vakuuttavaa näyttöä siitä, että kyseinen valtio on siihen vastuullinen.

Julkinen syyksilukeminen on kohdevaltion suvereeni valinta ja sellaisena kysymys, joka vaatii ensisijaisesti poliittista harkintaa. Julkisella syyksilukemisella voi kuitenkin olla myös oikeudellisia vaikutuksia sikäli kuin siinä määritetään käyttäytymistä, joka kyberympäristössä muodostaa kansainvälisesti oikeudenvastaisen teon.

Vastatoimien ohella myös muut valtiovastuun poistavat olosuhteet saattavat oikeuttaa sellaisiin kybertoimiin ryhtymisen, jotka muuten voisivat muodostaa kansainvälisesti oikeudenvastaisen teon.[22] Kyse voi olla esimerkiksi siitä, että kansainvälisestä velvoitteesta poikkeaminen on ainoa tapa, jolla valtio voi vakavan ja välittömän vaaran uhatessa turvata olennaisen etunäkökohtansa.

[20] *Ibid.*, art. 4–11.
[21] *Ibid*., art. 49–54
[22] ARSIWA, Chapter V, Circumstances precluding wrongfulness..

Tällaisessa poikkeuksellisessa tilanteessa valtio voi valtiovastuuta koskevien oikeussääntöjen asettamissa rajoissa toimia vastoin kansainvälisiä velvoitteitaan.[23]

Voimankäyttö/ aseellinen hyökkäys

Vaikka vakiintunutta määritelmää siitä, milloin kyberhyökkäys vastaa YK:n peruskirjan 2 artiklan 4 kappaleen tarkoittamaa voimankäyttöä tai 51 artiklan tarkoittamaa aseellista hyökkäystä, ei ole toistaiseksi olemassa, on laajasti hyväksytty, että vastaavuus riippuu kyberhyökkäyksen seurauksista. Rinnastuakseen aseelliseen voimankäyttöön verkkohyökkäyksen tulee olla riittävän vakava ja aiheuttaa samanlaisia vaikutuksia kuin aseellinen voimankäyttö kohdevaltion alueella tai sen lainkäyttövallan piiriin kuuluvilla alueilla. Myös kyberhyökkäyksellä uhkaaminen voisi loukata voimankäytön kieltoa, jos uhka olisi riittävän täsmällinen ja kohdistuisi toiseen valtioon.[24]

Vastaavasti useimmat asiaa kommentoineet ovat samaa mieltä siitä, että mittakaavaltaan ja vaikutuksiltaan aseelliseen hyökkäykseen verrattava kyberhyökkäys vastaa aseellista hyökkäystä ja siihen voidaan vastata itsepuolustuksellisesti. Selvää on, että hyökkäyksen on tällöin aiheutettava kuolonuhreja, vammoja tai merkittävää aineellista tuhoa, mutta täsmällistä määrällistä rajaa ei ole mahdollista asettaa, ja muutkin olosuhdetekijät on otettava arviossa huomioon. Paljon on pohdittu myös sitä, missä määrin aseelliseen hyökkäykseen rinnastuvan kyberhyökkäyksen määrittelyssä tulisi ottaa huomioon hyökkäyksen välillisiä ja pitkäaikaisia vaikutuksia. Tämä edellyttäisi joka tapauksessa sitä, että vaikutukset kyetään arvioimaan riittävän tarkasti. Samoin on pohdittu, tulisiko kyberhyökkäystä pitää aseellisena hyökkäyksenä, jos se johtaa merkittäviin taloudellisiin seurauksiin kuten esimerkiksi valtion rahoitusjärjestelmän tai joidenkin talouden osa-alueiden romahtamiseen. Tämä kysymys on harkinnan arvoinen.

Kybervoimankäytön määrittelyn tulisi kunnioittaa sekä YK:n peruskirjan kirjauksia että sen tarkoitusta ja päämäärää, joka on aseellisen toiminnan eskaloitumisen estäminen. Tältä pohjalta on tarpeen esimerkiksi säilyttää ero yhtäältä aseellisen hyökkäyksen, joka on erityisen vakava peruskirjan loukkaus, ja toisaalta vähäisemmän voimankäytön kesken. Myös itsepuolustusoikeuden toteuttamisen ehdot ovat kyberympäristössä samat kuin aseellisessa voimankäytössä. Itsepuolustusoikeus syntyy toisin sanoen vain, aseelliseen hyökkäykseen rinnastettavasta kyberhyökkäyksestä, joka voidaan lukea tietyn valtion syyksi. Perustellusti voidaan ajatella, että tällaisen hyökkäyksen uhriksi joutunut valtio voi vastata siihen joko verkkohyökkäyksellä tai aseellisesti. Itsepuolustuksellinen voimankäyttö ei kuitenkaan saa olla suhteetonta tai ylimitoitettua.

Kansainvälinen humanitaarinen oikeus

Kansainvälinen humanitaarinen oikeus soveltuu kyberoperaatioihin vain, jos ne ovat osa aseellista konfliktia tai käynnistävät aseellisen konfliktin. Useimmat toistaiseksi tunnetut

[23] *Ibid*., art. 25. Ks. myös Tallinn Manual 2.0, sääntö 26.

[24] Vaikka ei voida kiistää sitä mahdollisuutta, että kyberhyökkäys nousisi aseellisen hyökkäyksen mittasuhteisiin ilman minkään valtion myötävaikutusta, itsepuolustukseen ei-valtiollisia toimijoita vastaan liittyy kysymyksiä, jotka ovat liian monimutkaisia käsiteltäviksi tässä yhteydessä.

kyberoperaatiot eivät ole toteutuneet aseellisen konfliktin oloissa tai ylittäneet aseellisen konfliktin kynnystä. Ei ole kuitenkaan perusteltua kiistää sitä, että kansainvälisen humanitaarisen oikeuden tarjoamaa suojaa tarvitaan silloin, kun kyberkeinoihin turvaudutaan käynnissä olevissa aseellisissa konflikteissa, kuten monissa nykyisissä konflikteissa on tapahtunutkin.

Kaikkia aseita ja sodankäyntimenetelmiä on käytettävä siten, että kyetään noudattamaan muun muassa erotteluperiaatetta, suhteellisuusperiaatetta ja varotoimien periaatetta samoin kuin näihin periaatteisiin perustuvia erityisiä sääntöjä. Arvioitaessa sitä, voivatko tietyt kyberkeinot tai menetelmät tuottaa kiellettyä vahinkoa, myös niiden nähtävissä olevat suorat ja epäsuorat vaikutukset tulee ottaa huomioon. Aina tulee pitää huolta siitä, että siviiliväestön samoin kuin olennaisen siviili-infrastruktuurin, siviileille tarkoitettujen palvelujen ja siviilitietojen suoja voidaan varmistaa.

Kyberympäristön erityiset piirteet kuten verkottuneisuus (*interconnectedness*) ja anonymiteetti voivat vaikuttaa siihen, miten kansainvälistä humanitaarista oikeutta sovelletaan kyberkeinojen ja menetelmien käyttöön aseellisessa konfliktissa. Useimmat ongelmat voidaan kuitenkin ratkaista olemassa olevien sääntöjen nojalla. Uudet teknologiat eivät tee olemassa olevista aseellisia konflikteja koskevista säännöistä merkityksettömiä eikä välttämättä edellytä uutta sääntelyä. Vaikka kansainvälinen humanitaarinen oikeus on aseellisessa konfliktissa sovellettavaa erityissäännöstä (*lex specialis*), se ei sivuuta muita kansainvälisen oikeuden aloja, jotka voivat olla sovellettavissa koko konfliktin ajan, kuten esimerkiksi ihmisoikeussääntely.

Ihmisoikeuksia koskevat oikeussäännöt

Tietyt ihmisoikeudet kuten mielipiteen vapaus ja sananvapaus, mukaan lukien oikeus saada tietoa, ja oikeus yksityisyyteen ovat erityisen merkityksellisiä kyberympäristössä. Samalla on kuitenkin korostettava, että yksilöt nauttivat samoista ihmisoikeuksista suhteessa kybertoimintoihin kuin muutenkin. Vastaavasti valtioita sitovat kaikki niiden ihmisoikeusvelvoitteet sekä verkossa että sen ulkopuolella. Lisäksi kullakin valtiolla on alueellaan ja lainkäyttövaltansa piirissä velvoite suojella yksilöitä näiden oikeuksien loukkauksilta muiden tahojen toimesta.