Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa

VALTIONEUVOSTON JULKAISUJA 2023:31

vn.fi

VALTIONEUVOSTO
STATSRÅDET

Valtioneuvoston julkaisuja 2023:31

Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa

Valtioneuvosto Helsinki 2023

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

ISBN pdf: 978-952-383-542-9
ISSN pdf: 2490-0966

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2023

Kuvailulehti

11.4.2023

Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa

Valtioneuvoston julkaisuja 2023:31

Julkaisija	Valtioneuvosto		
Yhteisötekijä	Kyberselvityshankkeen työryhmä		
Kieli	suomi	**Sivumäärä**	48

Tiivistelmä

Sisäministeriö ja puolustusministeriö asettivat 15.2.2022 selvityshankkeen viranomaisten toimintaedellytysten arvioimiseksi kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa.

Hankkeessa on arvioitu viranomaisten tämän hetken toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa vakavia kyberuhkia vastaan sekä tunnistettu keskeiset kehittämistarpeet, arvioitu tämän hetken toimintatapamallia vakavissa kyberturvallisuutta vaarantavissa tilanteissa sekä viranomaisten välistä tiedonvaihtoa ja yhteistoimintaa koskevia kehittämistarpeita sekä ehdotettu toimenpiteitä lainsäädännön kehittämiseksi.

Raportti on valmisteltu laajassa yhteistyössä kyberturvallisuuteen liittyvien ministeriöiden ja virastojen kanssa. Nykytilassa viranomaisilla ei ole riittäviä toimintaedellytyksiä tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Raportti sisältää työryhmän ehdotukset sekä nopeasti toimeenpantavista että lainsäädäntömuutoksia vaativista kehittämistoimenpiteistä seitsemältä keskeiseltä osa-alueelta: kyberturvallisuuden strateginen tavoitetila, yhteistoiminta ja viranomaisprosessit, tilannekuva, tiedonvaihto, vaikuttaminen ja vastatoimet, tiedonhankinta ja viranomaisverkkojen suojaus.

Asiasanat	kyberpuolustus, kyberuhat, kybervaikuttaminen, viranomaistoiminta, kyberturvallisuus, kansallinen turvallisuus, kyberrikollisuus, varautuminen		
ISBN PDF	978-952-383-542-9	**ISSN PDF**	2490-0966
Asianumero	VN/2434/2022	**Hankenumero**	PLM003:00/2022
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-383-542-9		

Presentationsblad

11.4.2023

Utredning om myndigheternas verksamhetsförutsättningar i fråga om cybersäkerhet

Statsrådets publikationer 2023:31

Utgivare	Statsrådet		
Utarbetad av	Arbetsgruppen för projektet för cyberutredning		
Språk	finska	**Sidantal**	48

Referat

Den 15 februari 2022 tillsatte inrikesministeriet och försvarsministeriet ett utredningsprojekt för att bedöma myndigheternas verksamhetsförutsättningar i fråga om tryggandet av den nationella cybersäkerheten, bekämpandet av cyberbrottslighet, cyberförsvaret och situationer som utvecklas snabbt och som hotar cybersäkerheten i samhället.

I projektet har det gjorts en bedömning av de nuvarande verksamhetsförutsättningarna i fråga om att trygga cybersäkerheten och de viktigaste utvecklingsbehoven har identifierats. Det har även gjorts en bedömning av den nuvarande verksamhetsmodellen vid situationer där cybersäkerheten är allvarligt hotad och av utvecklingsbehov som gäller informationsutbytet och samarbetet mellan myndigheterna samt getts förslag på åtgärder som utvecklar lagstiftningen.

Rapporten har beretts i brett samarbete mellan de ministerier och ämbetsverk som har att göra med cybersäkerhet. I nuläget har myndigheterna inte tillräckliga verksamhetsförutsättningar för en effektiv beredskap för och bekämpning av allvarliga cyberhot som äventyrar den nationella cybersäkerheten och försvaret. Rapporten innehåller arbetsgruppens förslag på både utvecklingsåtgärder som kan genomföras inom kort och utvecklingsåtgärder som kräver ändringar i lagstiftningen inom sju viktiga delområden: den strategiska målbilden för cybersäkerheten, samarbete och myndighetsprocesser, lägesbild, informationsutbyte, påverkan och motåtgärder, informationsinhämtning och skydd av myndighetsnätverk.

Nyckelord	cyberförsvar, cyberhot, cyberpåverkan, myndighetsverksamhet, cybersäkerhet, nationell säkerhet, cyberbrottslighet, beredskap

ISBN PDF	978-952-383-542-9	**ISSN PDF**	2490-0966
Ärendenummer	VN/2434/2022	**Projektnummer**	PLM003:00/2022

URN-adress https://urn.fi/URN:ISBN:978-952-383-542-9

Description sheet

11 April 2023

Report on the authorities' capacity to act in cyber security matters

Publications of the Finnish Government 2023:31

Publisher	Finnish Government		
Group author	Working group on cyber security project		
Language	Finnish	**Pages**	48

Abstract

The Ministry of the Interior and the Ministry of Defence set up a project on 15 February 2022 to assess the capacity of authorities to ensure national cyber security, prevent cybercrime, implement cyber defence and respond to rapidly evolving situations that threaten society's cyber security.

The project assessed the current capacity of authorities to ensure national cyber security against serious cyber threats, identified key development needs, assessed both the current operating model in situations that seriously endanger cyber security and the exchange of information between authorities with related development needs. The working group also proposed measures to develop legislation.

The report was prepared in broad-based cooperation with the ministries and agencies that deal with cyber security. In the current situation, the authorities do not have sufficient capacity to effectively prepare for and combat the most serious cyber threats that endanger national cyber security and national defence. The report contains the working group's proposals, for both development measures that can be rapidly implemented and those that require legislative amendments, in seven key areas: the desired strategic end state in cyber security, cooperation and official processes, situation awareness, exchange of information, influencing and countermeasures, information gathering and protection of the authorities' networks.

Keywords cyber defence, cyber threats, cyber interference, official activities, cyber security, national security, cybercrime, preparedness

ISBN PDF	978-952-383-542-9	**ISSN PDF**	2490-0966
Reference number	VN/2434/2022	**Project number**	PLM003:00/2022

URN address https://urn.fi/URN:ISBN:978-952-383-542-9

Sisältö

1 Johdanto

Suomen turvallisuusympäristö on merkittävästi muuttunut ja monimutkaistunut erityisesti Venäjän hyökättyä Ukrainaan helmikuussa 2022. Samaan aikaan kiihtyvä digitalisaatio on tehnyt yhteiskunnat yhä riippuvaisemmiksi tietoverkkojen ja järjestelmien häiriöttömästä toiminnasta. Digitalisaatiokehitys on antanut valtioille ja ei-valtiollisille toimijoille mahdollisuuden hyödyntää kybertoimintaympäristöä aiempaa tehokkaammin vaikuttamisen kanavana. Teknologian kehittyminen on puolestaan mahdollistanut kansallista turvallisuutta vaarantavien tekojen toteuttamisen kybertoimintaympäristössä entistä peitellymmin, lyhyemmällä valmisteluajalla ja vakavammin seurauksin. Näin myös kybertoimintaympäristömme on muuttunut pysyvästi.

Vihamielinen kybertoiminta on vakiintunut osaksi kybertoimintaympäristöä. Se ei rajoitu vain poikkeusoloihin, vaan kohdistuu joka päivä myös Suomeen kybervaikuttamisena, kybervakoiluna ja kyberrikollisuutena. Niin valtiollisten toimijoiden kuin kyberrikollistenkin kyky tunkeutua tietojärjestelmiin on kehittynyt vauhdilla ja näin kyberturvallisuusuhat ovat sekä monimuotoistuneet että lukumääräisesti kasvaneet.

Vakaville kyberuhkille luonteenomainen jatkuva, usein yllätyksellinenkin kehittyminen edellyttää kyberuhkiin varautumisen ja vastaamisen jatkuvaa kehittämistä. Suomen valtionhallinnossa tietoturvallisuus on hyvällä tasolla ja varautuminen kyberuhkiin on osa viranomaisten päivittäistä toimintaa. Tästä huolimatta niin kansallisen turvallisuuden suojaamiseksi kuin viranomaisten tehokkaan toiminnan turvaamiseksi on valtionhallinnossa tunnistettu tarve kehittää edelleen viranomaisten toimintaedellytyksiä varautua ja vastata vakaviin kyberuhkiin.

1.1 Selvitystyön tausta

Kyberturvallisuus oli esillä jo vuoden 2010 yhteiskunnan turvallisuusstrategiassa (valtioneuvoston periaatepäätös 16.12.2010). Siinä kyberuhat tunnistettiin yhdeksi mahdolliseksi uhaksi ja tietojärjestelmiin tunkeutumisen todettiin tietyissä olosuhteissa voivan täyttää jopa sotilaallisen voimankäytön tunnusmerkit. Suomen kyberturvallisuusstrategiassa 2013 (valtioneuvoston periaatepäätös 24.1.2013) linjattiin visio, jonka mukaan Suomi

on vuoteen 2016 mennessä globaali edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. Strategiassa linjattiin lisäksi monta keskeistä seikkaa, joiden kehittämistä esitetään tässä asiakirjassa.

Suomen kyberturvallisuusstrategiassa 2019 (valtioneuvoston periaatepäätös 3.10.2019) asetettiin keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Strategian tarkoituksena on myös tukea luotettavien digitaalisten palveluiden saatavuuden ja liiketoiminnan kehittämistä. Kansallisen kyberturvallisuuden toteutus kansallisen turvallisuuden ja maanpuolustuksen osa-alueena kytkeytyy yhteiskunnan turvallisuusstrategiaan 2017 (Valtioneuvoston periaatepäätös 2.11.2017) ja siinä kuvattuihin yleisiin varautumisen ja turvallisuuden yhteensovittamisen sekä toimivaltaisen viranomaisen periaatteisiin. Suomen kantoja kansainvälisestä oikeudesta kybertoimintaympäristössä avataan puolestaan vuonna 2020 julkaistussa kannanotossa (kansainvälinen oikeus kybertoimintaympäristössä, Suomen kansallisia kantoja, UTP 13/2020 vp).

Sisäministeriö ja puolustusministeriö asettivat 15.2.2022 sisäisen turvallisuuden ja puolustusselontekojen linjausten sekä Kyberturvallisuuden kehittämisohjelman (valtioneuvoston periaatepäätös 10.6.2021) mukaisen yhteisen selvityshankkeen viranomaisten toimintaedellytysten arvioimiseksi kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa, ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuvan kehittymisen (PLM003:00/2022).

Työryhmän puheenjohtajana on toiminut sisäministeriön kansallisen turvallisuuden yksikön johtaja Petri Knape, varapuheenjohtajana puolustusministeriön tietohallintojohtaja Mikko Soikkeli ja sihteereinä erityisasiantuntija Hannu Kotipelto sisäministeriöstä sekä vanhempi hallitussihteeri Kosti Honkanen puolustusministeriöstä. Työryhmän jäseninä ovat toimineet erityisasiantuntija Outi Slant liikenne- ja viestintäministeriöstä, johtava asiantuntija Kimmo Janhunen oikeusministeriöstä, neuvotteleva virkamies Harri Ohra-aho puolustusministeriöstä, lainsäädäntöneuvos Tiina Ferm sisäministeriöstä, kansainvälisten asioiden neuvonantaja Aliisa Tornberg tasavallan presidentin kansliasta, tiiminvetäjä Stefan Lee ulkoministeriöstä (7.12.2022 saakka), erityisasiantuntija Marko Sjöroos valtioneuvoston kansliasta sekä tietohallintoneuvos Tuija Kuusisto valtiovarainministeriöstä.

Työryhmässä asiantuntijoina ovat toimineet erikoistutkija Sari Kajantie ja päälakimies Jan Sjöblom suojelupoliisista, rikostarkastaja Anu Jaakkola keskusrikospoliisista, apulaisosastopäällikkö, insinöörieversti Janne Jokinen Puolustusvoimista, yksikönpäällikkö Jani Mattila ja tuotepäällikkö Kasperi Havupolku Valtorilta, pääjohtaja Kirsi Karlamaa

Liikenne- ja viestintävirastosta, ylijohtaja Sauli Pahlman Liikenne- ja viestintäviraston kyberturvallisuuskeskuksesta, poliisitarkastaja Kimmo Ulkuniemi Poliisihallituksesta sekä valtion kyberturvallisuusjohtaja Rauli Paananen liikenne- ja viestintäministeriöstä.

Lisäksi työryhmän työskentelyyn ovat osallistuneet johtava asiantuntija Tarja Fernández ulkoministeriöstä, apulaiskyberturvallisuusjohtaja Stefan Lee liikenne- ja viestintäministeriöstä (8.12.2022 alkaen), osastoesiupseeri, everstiluutnantti Tuomo Rusila Puolustusvoimista sekä tietohallintoneuvos Timo Nuutinen valtiovarainministeriöstä. Työn aikana kuultiin myös muita asiantuntijoita.

1.2 Selvitystyön tavoitteet ja tehtävät

Maaliskuussa 2022 käynnistetyn selvitystyön tavoitteena oli laatia kehittämisehdotuksia, joiden avulla voidaan parantaa viranomaisten toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa ja nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa. Tarkennuksena asettamispäätöksessä todettiin selvitystyön tehtäviksi

- arvioida viranomaisten tämän hetken toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa vakavia kyberuhkia vastaan sekä tunnistaa keskeiset kehittämistarpeet
- arvioida kansallisista ja kansainvälisistä toimintaympäristön muutoksista johtuvat kehittämiskohteet
- arvioida tämän hetken toimintatapamallia vakavissa kansallista kyberturvallisuutta vaarantavissa tilanteissa, ja tarvittaessa laatia ehdotus toimintatapamallista, joka mahdollistaa oikea-aikaisen ja oikeantasoisen päätöksenteon, tehokkaan proaktiivisen toiminnan ja reagoinnin sekä mahdolliset vastatoimet
- arvioida edelliskohtaan liittyen viranomaisten välistä tiedonvaihtoa ja yhteistoimintaa koskevia kehittämistarpeita johtamisen ja yhteistoiminnan eri tasoilla
- selvittää tarvittavassa laajuudessa hankkeen kannalta keskeisten maiden viranomaisten toimintaedellytyksiä kyberuhkien ennaltaehkäisyssä ja torjunnassa
- antaa tarvittaessa ehdotus lainsäädännön muutostarpeista
- koordinoida hankkeen toimenpiteet muiden kyberturvallisuuden kehittämishankkeiden ja yhteiskunnan turvallisuusstrategian valmistelun kanssa.

Selvityksessä tarkastelun kohteena ei ollut tavanomaisena pidettävä verkkorikollisuuden torjunta, vaan yhteiskunnan kannalta vakavimpien – yleensä kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvien – kyberuhkien ja -rikosten havaitseminen,

tunnistaminen, torjunnan mahdollistaminen ja uhkiin reagoiminen. Tavoitteena oli laatia kehittämisehdotuksia, jotka mahdollistaisivat turvallisuusviranomaisille paremmat toimintamahdollisuudet suojata kansallista turvallisuutta.

Yhtenä tehtävänä oli myös koordinoida hankkeen toimenpiteet muiden kyberturvallisuuden kehittämishankkeiden, kuten eduskunnalle 27.10.2022 annetun hallituksen esityksen laeiksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain 29 §:n ja henkilötietojen käsittelystä poliisitoimessa annetun lain 22 §:n muuttamisesta (HE 243/2022 vp), kanssa. Tästä syystä selvitystyössä nähtiin tarkoituksenmukaisena hyödyntää keskeisten maiden viranomaisten toimintaedellytysten selvittämisessä edellä mainitun hallituksen esityksen esitöitä. Hallituksen esityksen valmistelun yhteydessä arvioitiin Ruotsissa, Norjassa, Saksassa, Iso-Britanniassa ja Ranskassa toteutettua kyberturvallisuuteen liittyvää sääntelyä ja viranomaisten tehtäviä. Esitöissä havaittiin viranomaisten tehtävien ja toimivaltuuksien vaihtelevan valtioittain niin suuresti, ettei ulkomaisia kokemuksia ja käytäntöjä voida suoraan hyödyntää kansallisten ratkaisujen kehittämisessä. Sen lisäksi, että sensitiivinen aihepiiri tekee eri maiden lainsäädännön kirjausten ja niiden todellisen käytännön implementaation arvioinnin ulkopuoliselle erittäin vaikeatulkintaiseksi, nähtiin käsillä olevassa selvitystyössä tarkoituksenmukaisemmaksi keskittyä kehittämisehdotusten luomiseen kansallisista lähtökohdista käsin.

Kybertoimintaympäristön monitahoisen luonteen ja koko yhteiskuntaa läpileikkaavien vaikutusten takia selvityksessä tarkasteltiin turvallisuusviranomaisten ja kybertoimintaympäristöön keskeisesti liittyvien muiden viranomaisten ja tahojen tiedontuottamisen ja toimintamahdollisuuksien nykytilaa ja kartoitettiin näihin liittyviä kehittämisehdotuksia. Osa ehdotetuista kehittämistoimenpiteistä arvioitiin voitavan käynnistää ilman lainsäädännöllisiä muutoksia, kun taas osan todettiin vaativan jatkoselvityksiä lainsäädännön muutostarpeiden yksityiskohtaiseksi arvioimiseksi.

Selvitystyö keskittyi tehtävänannon mukaisesti viranomaisten toimintaedellytysten ja kehittämistarpeiden arviointiin, mutta selvityksessä tunnistettiin osalla ehdotetuista kehittämistoimenpiteistä olevan liityntäpintoja myös yksityisen sektorin toimijoihin. Näiden kehittämistoimenpide-ehdotusten osalta tunnistettiin tarve yksityisen sektorin osallistamiselle ehdotusten mahdollisessa myöhemmässä jatkovalmistelussa.

2 Kybertoimintaympäristö ja sen uhkat

2.1 Kybertoimintaympäristö

Modernin yhteiskuntamme jokapäiväiset elintärkeät toiminnot, kuten johtaminen, vesi- ja energiahuolto, pankkijärjestelmä, terveydenhuolto sekä logistiikka, ovat kasvavassa määrin riippuvaisia tietoverkoista. Viestintäverkkojen toimivuus sekä viranomaisten tietovarantojen eheys, luottamuksellisuus ja saatavuus ovat digitalisoituneen yhteiskuntamme ja valtion tehokkaan toiminnan edellytyksiä. Niin ikään väestölle tarjotaan entistä laajempia mahdollisuuksia hyödyntää julkisen hallinnon digitaalisia palveluita ja näistä palveluista on tullut osa normaalia arkielämää. Digitaalisten palveluiden lisääntyessä ja käyttäjämäärien kasvaessa lisääntyy myös rikollisia kiinnostavan tiedon määrä ja mahdollisuudet verkkorikollisuudelle.

Yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuva, usein myös maantieteellisesti rajoittumaton kybertoimintaympäristö on tullut entistä vahvemmin osaksi myös ulko- ja turvallisuuspolitiikkaa. Kybertoimintaympäristöä käytetään sekä tiedonhankinnan että informaatiovaikuttamisen väylänä esimerkiksi osana hybridivaikuttamisen keinovalikoimaa. Sotilaallisesti kybertoimintaympäristö on noussut perinteisten toimintaympäristöjen rinnalle ja siellä toimeenpannuilla kyberoperaatioilla tuetaan sotilaallista vaikuttamista ja mahdollistetaan jo normaalioloissa vihamielinen vaikuttaminen kohdeyhteiskuntaa vastaan perinteisen aseellisen hyökkäyksen kynnyksen alapuolella.

Kybertoimintaympäristön ilmiöt kehittyvät ja monimuotoistuvat kiihtyvällä vauhdilla osana teknologista kehitystä ja kybertoimintaympäristön toimijoiden resurssien ja kykyjen kasvaessa. Tulevina vuosina esimerkiksi tekoälyjärjestelmien tarjoama automaatio ja kvanttitietokoneiden huomattava laskentateho voivat tehdä kyberhyökkäyksistä aiempaa kehittyneempiä, kohteelle räätälöidympiä, reaaliajassa muovautuvia sekä vaikeammin havaittavia ja torjuttavia.

Yhteiskuntien digitalisoituminen, teknologinen kehitys ja toimijoiden kykyjen kasvu ovat moninaistaneet ja kasvattaneet kyberuhkia. Tämä on näkynyt niin vakavan kyberrikollisuuden kasvuna kuin kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvina uusina uhkina.

2.2 Valtiolähtöiset kyberuhat

Suomeen kohdistuvissa valtiollisissa kyberuhkissa voi olla kyse kybervakoilusta, jolla hankitaan ei-julkisesti saatavilla olevaa tietoa esimerkiksi Suomen kriittisestä infrastruktuurista, ulko- ja turvallisuuspoliittisesta päätöksenteosta, valtionhallinnosta tai maanpuolustuksesta. Suomeen kohdistettavan kybervakoilun avulla selvitettävät tiedot ja siinä käytettävät menetelmät yhdessä julkisesti saatavien tietojen kanssa voivat myös mahdollistaa myöhemmässä vaiheessa tapahtuvan Suomeen kohdistuvan kybervaikuttamisen, jolla esimerkiksi häiritään elintärkeiden tietoverkkojen tai ohjausjärjestelmien toimintaa, estetään niiden käyttö tai tuhotaan ne. Lisäksi valtiollista kybervakoilua kohdistuu niin ikään huipputeknologiayritysten tuotekehitystietoon sekä yliopistojen ja muiden tutkimuslaitosten tutkimustietoon. Usein kybertoimintaympäristön valtiollisiin toimijoihin tai niiden toiminnan jättämiin jälkiin viitataan kehittyneinä ja kohdistettuina APT-uhkina (Advanced Persistent Threat).

Kybervakoilua on usein erittäin vaikea havaita. Menetelmistä kehitetään tarkoituksella sellaisia, etteivät kaupalliset tietoturvatuotteet ja -järjestelmät havaitsisi niitä. Kybervakoilulla voidaan kerätä tietojärjestelmissä käytännössä kaikkea niissä olevaa tietoa: asiakirjoja, sähköpostikirjeenvaihtoa sekä käyttäjätietoa. Lisäksi tiloja voidaan esimerkiksi salakuunnella ja -katsella tietokoneiden ja muiden laitteiden sisäisten mikrofonien ja kameroiden kautta. Vakoilussa kybermenetelmien etuna suhteessa muihin menetelmiin on muun muassa alhainen hinta, pieni riski ja toiminnan alkuperän kiistämisen helppous. Kybervakoilu voi kohdistua organisaatioiden tietojärjestelmien lisäksi henkilökohtaisiin laitteisiin. Kybervakoilua tuetaan muilla menetelmillä, kuten henkilötiedustelulla sekä avoimien lähteiden tiedustelulla.

Kybervakoilun lisäksi valtiolliset toimijat kehittävät kybersuorituskykyjään osaksi sotilaallisia ja hybridivaikuttamisen suorituskykyjä, mutta voivat myös hankkia tarvittavia kykyjä kaupallisilta, rikollisilta tai muilta sopivilta toimijoilta. Lisäksi valtiolliset toimijat voivat tarvittaessa ulkoistaa kybertoimintaansa rikollisryhmille, millä voidaan pyrkiä salaamaan ja kiistämään toiminnan taustalla oleva valtiollinen taho. Kyberrikollisryhmiä voidaan käyttää tietomurtoihin valtiollista toimijaa kiinnostavien tietojen hankkimiseksi tai häirintä- ja informaatiovaikuttamistarkoituksissa esimerkiksi palvelunestohyökkäyksiin. Toiminnassa voidaan pyrkiä käyttämään myös niin sanottuja sisäpiiriläisiä eli henkilöitä, joilla on laillinen pääsy haluttuun tietojärjestelmään. Sisäpiiriläiset voivat toimia vieraan valtion tai rikollisten lukuun taikka aiheuttaakseen haittaa edustamalleen organisaatiolle esimerkiksi koston tai ideologisten syiden vuoksi.

Kybertoimintaympäristö on kehittynyt omaksi sotilaalliseksi toimintaympäristökseen. Nato totesi jo vuoden 2016 Varsovan huippukokouksessaan kybertoimintaympäristön olevan samankaltainen sotilaallinen toimintaympäristö kuin perinteisemmät maa-, meri-,

ilma- ja avaruustoimintaympäristöt. Perinteisiä toimintaympäristöjä vastaavalla tavalla kyberoperaatioita voidaan käyttää sodankäynnin tai sen valmistelun keinoina ja tässä tarkoituksessa kyberoperaatioilla voidaan hankkia tietoa myös esimerkiksi kohdevaltion kriittisen infrastruktuurin teollisuusautomaatiojärjestelmistä. Kyberoperaatiot voidaan toteuttaa itsenäisinä tai muihin operaatioihin, kuten erikoisjoukko-operaatioihin, tiedusteluun, elektroniseen sodankäyntiin ja erityisesti informaatio-operaatioihin, yhdistettyinä. Kyberoperaatioita voidaan toteuttaa sotilaallisen voimankäytön kynnyksen alapuolella jo normaalioloissa, mikä on osaltaan hämärtänyt rajanvetoa rauhan ja sodan välillä. Ne voivat olla valtiollisille toimijoille informaatiovaikuttamisen ohella yksi hybridivaikuttamisen väline, jolla pyritään edistämään omien tavoitteiden saavuttamista jo rauhan aikana.

Sen lisäksi, että kyberoperaatioita kohdistetaan Suomeen, voidaan Suomessa sijaitsevaa tietoverkkoinfrastruktuuria pyrkiä hyödyntämään kolmanteen osapuoleen kohdistuvassa kybertoiminnassa.

2.3 Vakava kyberrikollisuus

Kyberrikolliset voivat tavoitella taloudellista hyötyä tai onnistuneen tietomurron mahdollisesti tuomaa mainetta ja arvostusta. Uhreiksi voi joutua yksittäisten kansalaisten ja yritysten lisäksi yhteiskunnan kriittisiä toimijoita. Kansallista turvallisuutta vaarantavia kyberrikollisuuden kohteita voivat olla esimerkiksi terveydenhuollon merkittävät palvelun-tuottajat tai huoltovarmuuden kannalta kriittiset energia-alan toimijat. Yrityksiin kohdistetut kiristyshaittaohjelmahyökkäykset voivat pahimmillaan vaikuttaa myös globaalisti raaka-aineiden tai komponenttien saatavuuteen tai tietomurto voi kohdistua laajaan joukkoon kansalaisia ja heidän arkaluonteisiin henkilötietoihinsa. Vakavalla kyberrikollisuudella voidaan myös luoda pohjaa ja valmistella yhteiskuntaan laajasti kohdistuvia tekoja esimerkiksi hankkimalla tietoa tai pääsy tietojärjestelmiin.

Kyberrikollisryhmät hyödyntävät toiminnassaan esimerkiksi tietojenkalastelua, tietomurtoja, palvelunestohyökkäyksiä ja kiristyshaittaohjelmia. Kyberrikollisten kohteet valikoituvat usein opportunismin ja hyöty-kustannusanalyysin perusteella, jolloin tietomurtoon vaadittava resurssien käyttö pyritään minimoimaan ja saadut voitot vastaavasti maksimoimaan. Tietoteknisesti taitavat kyberrikolliset myyvät osaamistaan myös palveluna (cybercrime as a service, CaaS), jota voivat hyödyntää kyberrikollisten lisäksi valtiolliset toimijat. Viimeaikaiset kriisit ovat myös osoittaneet, että itsenäisesti toimivien kyvykkäiden yksilöiden tekemät teot voivat kohdistua myös toisiin valtioihin, jolloin teko voidaan tulkita joko tarkoitushakuisesti tai virheellisesti toisen valtion tekemäksi.

3 Kansainvälinen toimintaympäristö

3.1 Kansainvälinen oikeus

Kansainvälinen oikeus luo yleiset puitteet valtioiden toiminnalle myös kybertoimintaympäristössä. Tämä lähtökohta on tunnustettu laajasti muun muassa YK:n hallitustenvälisten asiantuntijoiden (GGE) työryhmän raporteissa (2013 ja 2015) sekä yleiskokouksen kaikille avoimen työryhmän raportissa 2021. Siitä, miten kansainvälinen oikeus koskee kybertoimintaympäristöä ja miten sääntöjä tulkitaan, vallitsee kuitenkin näkemyseroja eri valtioiden välillä. Valtioiden väliset keskustelut kansainvälisen oikeuden soveltamisesta kybertoimintaympäristössä jatkuvat YK:n puitteissa.

Ulkoministeriö on koonnut Suomen kantoja kansainvälisen oikeuden soveltamisesta kybertoimintaympäristössä vuonna 2020 laadittuun kannanottoon. Suomen kannat lähtevät yleisesti tarpeesta

1. vahvistaa, että Suomella on mahdollisuus reagoida poliittisen itsenäisyytensä tai alueellisen koskemattomuutensa loukkauksiin myös silloin, kun ne tapahtuvat kybertoimintaympäristössä,
2. vahvistaa, että kaikilla valtioilla on oikeudellinen velvoite välttää rajat ylittäviä vakavia haittoja myös kybertoimintaympäristössä ja
3. torjua sellaisia kansainvälisen oikeuden tulkintoja, joihin sisältyy merkittävä aggressiivisen kybertoiminnan eskaloitumisen uhka.

Kannanotot koskevat muun muassa valtion suvereenisuutta, velvoitetta toimia rajat ylittävien vahinkojen estämiseksi, valtion vastuuta ja aseellisen voimankäytön tilanteita.

Kansainvälisen oikeuden yleisen periaatteen mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Suvereenisuus suojaa niin valtion aluetta ja ilmatilaa kuin sen alueella olevaa kyberinfrastruktuuria ja siihen tukeutuvia tietojärjestelmiä. Viime aikoina on esitetty, että suvereenisuus olisi vain yleinen periaate, josta ei voisi johtaa oikeudellisia seurauksia kybertoimintaympäristössä. Suomi ei jaa tätä näkemystä. Alueellisen koskemattomuuden ja poliittisen riippumattomuuden loukkauksia on vakiintuneesti pidetty suvereenisuuden loukkauksina ja oikeudenvastaisina tekoina.

Jos hyväksyttäisiin, että sääntö ei päde kybertoimintaympäristössä, valtioiden kyberhäirintä toisten valtioiden verkoissa jäisi sääntelemättä siinäkin tapauksessa, että sillä on haitallisia seurauksia. Kiellettyä olisi voimankäyttöön tai aseelliseen hyökkäykseen rinnastettavan kyberhyökkäyksen ohella vain valtion sisäisiin asioihin puuttuminen (laiton väliintulo), joka rajoittuu tiettyihin kysymyksiin ja edellyttää lisäksi vaikeasti osoitettavaa pakottamisen tarkoitusta.

Suomi katsoo, että luvaton tunkeutuminen toisen valtion alueella sijaitsevaan kyberinfrastruktuuriin tukeutuviin tietoverkkoihin ja -järjestelmiin voi loukata kyseisen valtion suvereenisuutta. Asiaa on arvioitava tapauskohtaisesti ottaen huomioon kybertunkeutumisen luonne ja seuraukset, kuten aineellisen vahingon aiheuttaminen, häiriöiden aiheuttaminen laitteiden toiminnassa tai tietojen muokkaaminen tai tuhoaminen.

Luvatonta kybertunkeutumista voidaan pitää kohdevaltion suvereenisuuden loukkauksena myös silloin, kun se kohdistuu sellaisiin tietoihin tai palveluihin, jotka ovat välttämättömiä valtion olennaisten tehtävien hoitamiseksi. Suvereenisuuden loukkauksina voidaan lisäksi pitää suvereenin immuniteetin suojaamia kohteita vastaan (sota-alukset, valtion alukset, joita käytetään yksinomaan julkiseen tai ei-kaupalliseen toimintaan, valtion ilma-alukset) toteutettuja kyberoperaatioita. Suomen näkemyksen mukaan suvereenisuuden loukkaus on kansainvälisesti oikeudenvastainen teko, joka synnyttää valtion vastuun.

Suomi on tunnustanut myös huolenpitovelvoitteen soveltamisen kybertoimintaympäristössä. Kyseessä on vakiintunut kansainvälisen oikeuden periaate, jonka mukaan valtiolla on velvoite estää alueensa käyttö toisen valtion oikeuksia loukkaavalla tavalla. Kiellettyä on sellaisten kyberoperaatioiden tietoinen salliminen valtion alueella tai sen valvonnassa, joista aiheutuu vakavia haitallisia seurauksia muille valtioille. Vaikka valtioiden on osoitettava asianmukaista huolenpitoa alueensa valvonnassa, tämä ei vapauta niitä noudattamasta muita kansainvälisiä velvoitteita, kuten esimerkiksi ihmisoikeusvelvoitteita.

Vain valtiot voivat loukata suvereenisuutta, mutta suvereenisuuteen perustuva huolenpitovelvoite koskee myös yksityisiä toimia valtion alueella. Yksityisistä kybertoimista muille valtioille aiheutuva vakava haitta voi johtaa valtion kansainväliseen vastuuseen, mutta vain siinä tapauksessa, että kyseinen valtio on rikkonut huolenpitovelvoitettaan.

Valtion toimista kybertoimintaympäristössä ei ole kansainvälistä erityissääntelyä, minkä vuoksi niihin sovelletaan valtiovastuun yleisiä sääntöjä. Valtiovastuu on merkityksellistä erityisesti mietittäessä sitä, mitkä ovat kansainvälisen oikeuden mukaisia mahdollisia vastatoimia kansainvälisesti oikeudenvastaisiin tekoihin. Kansainvälisen oikeuden vastaiseen tekoon vastaamisen tulee täyttää tietyt oikeudelliset kriteerit. Vastatoimien tulee olla suhteellisia ja niiden tavoitteena tulee olla oikeudenvastaisesti toimineen valtion

taivuttaminen noudattamaan velvoitteitaan. Vastauksen ei kuitenkaan tarvitse vastata alkuperäistä oikeudenvastaista tekoa. Toisin sanoen kyberoperaatioon voidaan vastata monenlaisin keinoin, jotka eivät rajoitu vain kybertoimintaan.

Yhdistyneiden Kansakuntien (YK) peruskirjan 2 artiklan 4 kappaleen mukaan kaikkien jäsenmaiden on pidätyttävä kansainvälisissä suhteissaan väkivallalla uhkaamisesta tai sen käyttämisestä. Tämä sääntö on myös yleisesti hyväksytty kansainvälisen tapaoikeuden normiksi. Luonnollinen oikeus yksilölliseen ja kollektiiviseen itsepuolustukseen vastauksena aseelliseen hyökkäykseen on tunnustettu kansainvälisessä tapaoikeudessa ja peruskirjan 51 artiklassa. Aseellinen hyökkäys tai sen välitön uhka oikeuttavat itsepuolustuksellisen voimankäytön hyökkäyksen torjumiseksi ja välittömän uhan poistamiseksi.

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. Vallitsevan tulkinnan mukaan kyberoperaation on aiheutettava samankaltaisia vaikutuksia kuin aseellinen voimankäyttö, jotta se voitaisiin rinnastaa aseelliseen voimankäyttöön. Myös kyberhyökkäyksellä uhkaaminen voisi loukata voimankäytön kieltoa, jos uhka olisi riittävän täsmällinen ja kohdistuisi toiseen valtioon.

On laajasti hyväksyttyä, että kohdevaltio voi vastata aseelliseen hyökkäykseen rinnastettavaan kyberoperaatioon kyberkeinoja käyttämällä tai erilaisilla vastatoimilla sotilaalliset keinot mukaan luettuina. Itsepuolustuksellisten toimien on kaikissa tapauksissa noudatettava YK:n peruskirjan ja kansainvälisen tapaoikeuden mukaisia oikeussääntöjä, kuten tarpeellisuuden ja suhteellisuuden vaatimuksia.

Edellä mainittujen kansainvälisen oikeuden sääntöjen lisäksi kybertoimintaympäristössä on noudatettava myös esimerkiksi sodan oikeussääntöjä ja ihmisoikeusvelvoitteita. Sodan oikeussäännöt soveltuvat kyberoperaatioihin vain, jos ne ovat osa aseellista konfliktia tai käynnistävät aseellisen konfliktin.

Rikosoikeuden puolella Euroopan neuvoston 23.11.2011 tehty Budapestin yleissopimus on ainoa erityisesti tietoverkkorikollisuutta koskeva kansainvälinen sopimus. Se on avoin myös Euroopan neuvoston ulkopuolisille maille. Lisäksi käynnissä on neuvottelut YK:n kyberrikollisuusyleissopimuksesta, joihin Suomikin osallistuu osana Euroopan unionia. Euroopan unionissa EU:n asetusehdotus sähköistä todistusaineistoa rikosasioissa koskevista eurooppalaisesta esittämis- ja säilyttämismääräyksestä (niin kutsuttu e-Evidence -asetus) tullaan hyväksymään kevään 2023 aikana. Lisäksi kyberturvallisuusdirektiivi (NIS2) on hyväksytty ja kansallisen täytäntöönpanon vaiheessa. Niin ikään sähköisen viestinnän tietosuojaa koskevan ePrivacy-direktiiviä uudistetaan ja ehdotusta datasäädökseksi sekä tietoverkkorikollisuutta koskevan Budapestin yleissopimuksen toista lisäpöytäkirjaa valmistellaan.

3.2 Kyberturvallisuus osana ulko- ja turvallisuuspolitiikkaa

Ulko- ja turvallisuuspoliittisen toimintaympäristön muutosten heijastuminen kybertoimintaympäristöön nostettiin esiin kevään 2022 ulko- ja turvallisuuspoliittisessa ajankohtaiskatsauksessa. Ajankohtaiskatsaus kartoitti Suomeen kohdistuvaa kyberuhkaympäristöä sekä keinovalikoimaa Suomen kyberkykyjen vahvistamiseksi niin kansallisesti kuin kansainvälisen yhteistyönkin kautta.

Kansainvälinen yhteistyö on keskeistä EU:n ja Suomen kyberturvallisuudelle ja -puolustukselle. Suomen etu on tehdä tiivistä yhteistyötä kansainvälisten toimijoiden kanssa monenvälisesti, alueellisesti ja kahdenvälisesti. Tämä koskee niin teknistä yhteistyötä ja kansainvälisten normien ja standardien kehittämistä kuin poliittista vuoropuhelua. Venäjän hyökkäys Ukrainaan on vaikuttanut myös kansainväliseen yhteistyöhön muun muassa YK:ssa kärjistäen entisestään arvopohjaista vastakkainasettelua. On odotettavissa, että yhteistyötä tehdään jatkossa enemmän rajatummissa kokoonpanoissa yhteisesti jaetun arvopohjan, demokratian ja ihmisoikeusperustaisuuden ja sääntöpohjaisuuden perusteella. Ajankohtainen tilanne on tiivistänyt EU:n rivejä myös kyberturvallisuudessa. Poliittisen päätöksenteon tueksi on tuotettu yhteistä kyberturvallisuuden tilannekuvaa, joka on tärkeää liittää osaksi strategista kokonaistilannekuvaa.

Koska kansainvälisessä sääntöpohjaisessa järjestelmässä ei ole vielä saavutettu kattavaa ymmärrystä tai toimivaa globaalia mekanismia vihamielisen valtiotoimijan kybertoimintaympäristössä tapahtuvien hyökkäyksien käsittelyyn, on ajankohtainen kansainvälispoliittinen tilanne tiivistänyt samanmielisten maiden yhteistyötä kyberuhkiin vastaamiseksi ja kyberresilienssin vahvistamiseksi.

Suomi on toiminut EU:ssa aktiivisesti kyberdiplomatian kehittämiseksi. EU:n neuvoston päätelmät yhteisistä diplomaattisista toimista kolmansien maiden kyberuhilta suojautumiseen hyväksyttiin vuonna 2017. Kyberdiplomatian välineistöön (niin kutsuttu työkalupakki) kuuluvat kolmasmaa-kyberdialogit, kyberhyökkäyksiä ehkäisevät toimet sekä rajoittavat toimet (pakotteet). Rajoittaviin toimiin sisältyvät matkustuskielto EU:n alueelle sekä henkilöiden ja yhteisöjen varojen jäädyttäminen. Ensimmäiset pakotteet asetettiin vuonna 2020. Diplomaattisina keinoina on käytetty myös kolmansiin maihin suunnattuja demarsseja ja julkilausumia. Työkalupakkia kehitetään edelleen ja vahvistetaan.

Euroopan komission ja Euroopan ulkosuhdehallinnon joulukuussa 2020 hyväksymä EU:n kyberturvallisuusstrategia vahvistaa EU:n diplomaattista toimintaa kyberhyökkäysten torjumiseksi. EU:n monitoimijapohjaiset kyberdialogit, joissa myös edistetään EU:n standardisointeja, ovat tärkeä osa kyberdiplomatiaa ja kyberresilienssin vahvistamista.

EU:n kyberpuolustuspolitiikan kehittäminen etenee kyberdiplomatian rinnalla. Tavoitteena on parantaa EU:n kyberpuolustuksen suorituskykyjä ja tehostaa sotilas- ja siviilialan kyberyhteisöjen välistä koordinointia ja yhteistyötä.

EU:n ohella kybertoimintaympäristökeskustelua käydään muun muassa YK:ssa, Euroopan turvallisuus- ja yhteistyöjärjestö Etyjissä, Euroopan neuvostossa, Taloudellisen yhteistyön ja kehityksen järjestö (Organization for Economic Co-operation and Development) OECD:ssä ja Natossa. YK:n yleiskokouksen puolella on otettu ensimmäiset askeleet kohti globaalia vastuullista valtiotoimijaa tarkastelevaa prosessia (Program of Action to advance responsible State behaviour in the use of ICT in the context of international security). YK:ssa ja alueellisissa järjestöissä, kuten Etyjissä, keskiössä ovat luottamuksen lisääminen jakamalla tietoja kyberhyökkäyksistä ja -vaikuttamisesta sekä kyberkapasiteettien vahvistaminen.

Suomen Nato-jäsenyysprosessin kautta osallistuminen liittokunnan kyberpuolustukseen tuo uuden tason Suomen kyberpuolustukseen ja kyberresilienssin vahvistamiseen. EU:n ja Naton kyberkyvykkyyksiä vahvistetaan koordinoidusti.

Suomen kyberdiplomatiassa dialogit arvopohjaltaan samanmielisten maiden kanssa ovat tiivistyneet. Yhteistyötä syvennetään eri ryhmissä sekä kahdenvälisissä dialogeissa keskeisten kumppanimaiden kanssa.

3.3 Ulko- ja turvallisuuspoliittinen reagointi

Suomeen kohdistuvaan valtiolliseen vihamieliseen kybertoimintaan reagoinnista päätetään vakiintuneissa ulko- ja turvallisuuspoliittisissa prosesseissa. Ulkoministeriö valmistelee asiaa ja kokoaa eri lähteistä saatavilla olevan tiedon. Suomen reaktiosta linjataan tarvittaessa ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisessä kokouksessa (TP-UTVA). Ulko- ja turvallisuuspoliittisessa reagoinnissa on kyse vihamielisestä kybertoiminnasta vastuussa olevan tahon – yleensä valtion – tunnistamisesta sekä toimintaan vastaamisesta tai reagoimisesta erilaisin keinoin. Tätä menettelyä kutsutaan attribuutioksi.

Attribuutio on tässä mielessä erotettava oikeudellisen vastuun syyksilukemisesta. Jos valtion elimiä tai sen puolesta toimivia yksityisiä ryhmiä tai henkilöitä voidaan tunnistaa valtion kansainvälisiä velvoitteita loukkaavan kyberoperaation tekijöiksi, valtiolla on niistä kansainvälinen vastuu. Valtion kansainvälisen vastuun syyksilukeminen tapahtuu vakiintuneiden oikeudellisten kriteereiden mukaisesti.

Attribuutio eli vastuullistaminen tai syyksilukeminen on moniulotteinen käsite, jolla valtiollisesta vihamielisestä kybertoiminnasta (kybervakoilu ja -vaikuttaminen) puhuttaessa tarkoitetaan yhtäältä vastuussa olevan valtiollisen tahon tunnistamista koskevaa prosessia ja toisaalta sen pohjalta vastatoimena tehtyä julkista attribuutiota.

Julkisessa keskustelussa sana attribuutio yhdistetään ensisijaisesti vihamielisen kybertoiminnan julkiseen tuomitsemiseen. Attribuutio voi kuitenkin tarkoittaa yhtäältä vihamielisen kybertoiminnan kohteeksi joutuneen valtion vastatoimivalikoimaa ja toisaalta myös edellä mainittuja vastatoimia pohjustavaa analyysi- ja päätöksentekoprosessia.

Attribuutiossa on useita toisistaan erillisiä prosesseja, joilla on selkeä oma päämäärä ja toisaalta osittain lomittaisia prosesseja, jotka rikastavat toisiaan niin tiedolla kuin menetelmilläänkin. Yksinkertaistettuna attribuutio on tosiseikkojen keräämistä ja analyysiä, teknistä ja oikeudellista arviointia, päätöksentekoa ja lopulta tehdyn päätöksen kommunikointia eri tahoille. Attribuutiokyky on yksi keskeisimmistä kansallisista kyvykkyyksistä kansallisen turvallisuuden varmistamiseksi ja kybertoimintaympäristöön liittyvän ulko- ja turvallisuuspoliittisen päätöksenteon tukemiseksi.

Kokonaisvaltaisessa attribuutioprosessissa on kyettävä hyödyntämään kaikki attribuutioon liittyvä tieto, jota tuottavat muun muassa tiedustelu-, kyberturvallisuus- sekä esitutkintaviranomaiset osana lakisääteisiä tehtäviään. Myös muut julkisen hallinnon organisaatiot sekä yksityiset yritykset tuottavat tarvittavaa tietoa osana omia tehtäviään ja tapauksiin liittyvää selvitystyötä.

Julkinen attribuutio vastatoimena on osa kokonaisvaltaista ulko- ja turvallisuuspoliittista arviointia ja tarkoituksenmukaisuusharkinnan pohjalta tehtävää päätöksentekoa. Näin ollen se ei voi olla ennalta määriteltyihin kriteereihin pohjautuvaa automatiikkaa. On myös syytä muistaa, että julkinen attribuutio on vain yksi käytössä olevista reagointivaihtoehdoista muiden ulko- ja turvallisuuspoliittisten keinojen joukossa. Ulko- ja turvallisuuspoliittisen attribuution yhteyteen on mahdollista liittää erilaisia taloudellisia ja poliittisia vastatoimia joko yksin tai kansainvälisen yhteisön osana. Näin voidaan nostaa vihamielisen toiminnan kynnystä kybertoimintaympäristössä.

Valtiolliseen vihamieliseen kybertoimintaan liittyvän reagoimisen muoto, keino ja ajoitus ovat kaikki kokonaisvaltaisen ulko- ja turvallisuuspoliittisen punninnan perusteella tehtäviä valintoja, joissa huomioitavina näkökohtina ovat muun muassa:

a. valtiollisen vihamielisen kybertoiminnan kohde, laajuus ja seurausten vakavuusaste, intensiteetti sekä motiivit suhteutettuina Suomen kokonaisturvallisuuteen ja ulko- ja turvallisuuspoliittisiin suhteisiin,

b. pidemmällä aikavälillä tavoiteltava ulko- ja turvallisuuspoliittinen tavoitetila erityisesti vastuullisen valtionkäyttäytymisen ja sääntöpohjaisuuden vahvistaminen kybertoimintaympäristössä ja
c. julkisella attribuutiolla, erityisesti yhteisrintamana samanmielisten kumppanimaiden kanssa tehdyllä yhteisattribuutiolla, luodaan ja ylläpidetään myös pidäkevaikutusta nostamalla vihamielisestä kybertoiminnasta aiheutuvia poliittisia ja diplomaattisia kustannuksia (maine- ja legitimiteettihaitta).

Kyberhyökkäysten ja -vakoilun tuomitseminen julkisesti on tärkeä osa EU:n ja eurooppalaisten valtioiden turvallisuuden vahvistamista sekä kansallisesti Suomen kyberturvallisuuden parantamista. Tavoitteena on tuoda vihamieliset teot ja niiden havainnointikyky näkyväksi ja mahdollisesti indikoida valmiutta vastatoimiin. EU:n yhtenäisyyttä ja kansainvälistä solidaarisuutta korostavilla viesteillä ja vastatoimenpiteillä on oleellinen merkitys pyrkimykselle luoda tehokkaita pidäkkeitä vihamielistä kybertoimintaa vastaan.

Euroopan unionissa attribuutio on jokaisen jäsenmaan oman suvereenin päätösvallan piirissä. Vaikka EU:n periaatteiden mukaisesti jokainen jäsenmaa on vapaa valitsemaan omat metodinsa ja lähestymistapansa attribuutioon, EU:n rooli koordinoijana on silti keskeinen. EU:n diplomaattisen vastauksen laatiminen riippuu Euroopan unionin neuvoston päätöksestä. Neuvoston todettua ulkoisen uhan olemassaolon, prosessi voi edetä. Neuvoston päätöksen on oltava yksimielinen, jonka jälkeen luonnollisia tai juridisia henkilöitä ja muita toimijoita voidaan asettaa sanktiolistalle. EU:n kybertyökalupakki sisältää lukuisia toimia, joita voidaan ottaa käyttöön tapauskohtaisesti. Jäsenmaat voivat myös pyytää toimien aktivointia. Vastatoimien taso määritellään linjassa kansainvälisen oikeuden kanssa EU:n valtiojohtajien ja hallitusten toimesta.

4 Kyberuhkien torjunnan nykytila Suomessa

Kybertoimintaympäristön turvallisuutta vaarantava tapahtuma voi olla samanaikaisesti tietoturvauhka, rikos sekä kansallista turvallisuutta ja maanpuolustusta vaarantava uhka, millä on ulko- ja turvallisuuspoliittisia vaikutuksia. Siksi poikkeaman selvitys on samanaikaisesti usean viranomaisen vastuulla (ks. taulukko 1). Niillä kaikilla on oma tehtävänsä, jota toisen viranomaisen toimenpiteet eivät voi korvata. Tietoturvapoikkeaman hallintaa koordinoi Liikenne- ja viestintäviraston kyberturvallisuuskeskus, esitutkinnasta vastaa poliisi, ulko- ja turvallisuuspoliittisen päätöksenteon valmisteluun tietoa tuottavat tiedusteluviranomaiset ja puolustusjärjestelmän turvallisuudesta vastaa Puolustusvoimat.

Lisäksi kyberturvallisuuden tuottamiseen osallistuu laaja joukko muita viranomaisia sekä julkisia ja yksityisiä toimijoita, kuten teleoperaattorit, joita koskien on säädetty erityisiä velvoitteita ja oikeuksia sähköisen viestinnän palveluista annetussa laissa (917/2014, jäljempänä SVPL). Laki tosin asettaa rajoitteita muun muassa tiedon luovutukselle sekä tilannekuvan tuottamiselle ja sen hyödyntämiselle.

4.1 Kyberturvallisuuteen liittyvät viranomaiset ja niiden lakisääteiset tehtävät

Suomeen kohdistuva kyberuhka käynnistää samanaikaisesti toimenpiteitä sekä poikkeaman kohteina olevissa organisaatioissa että useassa eri operatiivisessa viranomaisessa, joilla kaikilla on kokonaisuudessa oma tehtävänsä tapauksen selvittämiseksi ja vahingon rajaamiseksi. Osalla organisaatioista on tehtävä myös mahdollisen seuraamusmenettelyn (rikosprosessi tai ulko- ja turvallisuuspoliittinen attribuutio) valmistelussa. Keskeisten viranomaisten tehtävät on kiteytetty alla olevaan taulukoon ja näiden kyberturvallisuuteen liittyviä tehtäviä kuvataan tarkemmin jäljempänä.

Taulukko 1. Keskeisten kyberturvallisuusviranomaisten tehtävät ja roolit

	Kohdeorganisaation tietoturva	Valtori	Traficom	Esitutkintaviran-omaiset	Tiedusteluviranomaiset	Puolustusvoimat
Tapahtuma	Tietoturva-poikkeama organisaatiossa	Tietoturva-poikkeama valtion yhteisissä palveluissa tai tur-vallisuusverkossa	Tietoturva-poikkeama	Rikos, sen yritys ja valmistelu	Kansallisen turvallisuuden tai maanpuolustuksen uhka	Aseellinen hyökkäys tai sitä vastaava ulkoinen uhka
Toimivaltuus-säännökset	SVPL 272 §	SVPL 272 § TUVE-laki TORI-laki	SVPL 172, 244 a, 273 ja 316 §	PKL 10 ja PolL 5-luvut (poliisi ja Supo) SKRTL (PV)	PolL 5 a (Supo) SotTiedL (SotTiedVir)	PVL 4 §, SVPL 272 §
Tavoite	Organisaatioon vaikuttavan teknisen poikkeaman selvittä-minen (tekninen tieto-turva) ja/tai vahingon kartoitus ja rajaus (hal-linnollinen tietoturva)	Valtion yhteisissä palveluissa tai turvallisuusverkossa olevan teknisen poikkeaman selvittäminen	Suomeen vai-kuttavan tekni-sen poikkeaman selvittäminen	Tapahtuman osapuolten ja tosiseikkojen selvittäminen rikosprosessissa	Vahingon selvittäminen ja tiedon tuottaminen muille turvallisuusviranomaisille (supo) tai puolustusvoimil-le (SotTiedVir) sekä valtion ylimmälle johdolle (molemmat).	Suomen sotilaallinen puolustaminen ja suvereniteetin turvaaminen
Keskeisiä kysymyksiä	Miten teknisesti estetään jatkossa?	Miten teknisesti estetään jatkossa?	Miten teknisesti estetään jatkossa? Onko muita kohtei-ta? Miten tunniste-taan jatkossa?	Epäilty rikos, sen teko-olosuhteet, sillä aiheutettu vahinko ja siitä saatu hyöty?	Mikä tekijätaho, miten teknisesti estetään jatkossa, mikä vahinko, mikä intressi, mikä merkitys Suomen intresseille? Kuinka tunnis-tetaan? Arvio vihamielisen toiminnan jatkosta.	Mikä intressi? Mitkä vaikutukset? Kuinka torjutaan? Tuleeko vaikuttaa toiminnan keskeyttä-miseksi? Onko kyseessä aseel-linen hyökkäys vai sitä alempi-tasoinen vaikuttaminen?
Toimenpide; toimija	Tietoturva-toimenpiteet; Organisaation johto	Tietoturva-toimenpiteet; Valtorin johto ja asiakkaat, joita poikkeama koskee	Tietoturva-toimenpiteet; Päätöksen sisällöstä riippuen Traficom, LVM tai VN	Rikosprosessi; Poliisi, syyttäjä, tuomioistuin	Torjuntatoimenpiteet tai UTP-prosessi; Päätöksen edellyttämä taho	Vastatoimet. Vaikuttaminen aseellisessa hyökkäyksessä. UTP-päätöksenteko ja päätök-senteko sotilaskäskyasioissa

Valtion tieto- ja viestintätekniikkakeskus Valtorin tehtävänä on valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013, jäljempänä TORI-laki) nojalla tuottaa valtion yhteisiä perustietotekniikka- ja tietojärjestelmäpalveluja, joita valtion virastoilla ja laitoksilla on lähtökohtaisesti velvollisuus käyttää. Valtorilla on velvollisuus huolehtia siitä, että toiminta ja palvelujen tuotanto jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä poikkeusoloissa.

Viranomaisten turvallisuusverkkotoiminnasta säädetään julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015, jäljempänä TUVE-laki). Turvallisuusverkolla mahdollistetaan jokapäiväinen työskentely sekä operatiivisessa toiminnassa että hallinnollisissa tehtävissä. Turvallisuusverkon verkko- ja infrastruktuuripalveluja tuottaa yksinoikeudella valtion omistama **Suomen Erillisverkot Oy**, joka tuottaa myös TUVE-lain mukaisia viranomaisradioverkon sekä viranomaisten aikakriittisen laajakaistaisen matkaviestinnän tieto- ja viestintäpalveluja. Valtori tuottaa yksinoikeudella turvallisuusverkon tieto- ja viestintäteknisiä palveluita sekä integraatiopalveluita. Turvallisuusverkon palveluntuottajalle on TUVE-laissa asetettu vaatimukseksi vastata tehtäväalueellaan turvallisuusverkkoa koskevien turvallisuus-, valmius-, varautumis- ja jatkuvuusvaatimusten toteuttamisesta normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa. Turvallisuusverkon palvelut ovat keskeisiä viranomaisten kesken vaihdettavan tiedon välityksessä myös tietoturvaloukkausten häiriötilanteissa.

Liikenne- ja viestintävirasto Traficom kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta sekä selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvia tietoturvaloukkauksia ja niiden uhkia. Kyberturvallisuuskeskus kerää tietoja tietoverkkotapahtumista ja välittää sitä eri toimijoille sekä muodostaa ja jakaa kyberturvallisuuden yhdistettyä kansallista tilannekuvaa. Kyberturvallisuuskeskuksen asiakkaat voivat hyödyntää tilannekuvatietoa oman varautumisensa järjestämisessä ja priorisoinnissa. Tilannekuvan muodostamisessa hyödynnetään Traficomin koko liikenne- ja viestintäsektorin toimialaa sekä kansallisten lähteiden, kuten huoltovarmuuskriittisten organisaatioiden verkostoja, turvallisuusviranomaisia ja lisäksi Kyberturvallisuuskeskuksen virallisia tai vapaaehtoisuuteen ja molemminpuoliseen luottamukseen perustuvia kansainvälisiä yhteistyöverkostoja.

Kyberturvallisuuskeskus on myös kehittänyt vakavien tietoturvauhkien keskitetyn havainnointijärjestelmän (HAVARO) yhteiskunnan kokonaisturvallisuuden kannalta merkittävimpien tahojen suojaksi. Kyberturvallisuuskeskus tarjoaa myös valtionhallinnolle vastaavaa tietoturvauhkien havainnointipalvelua nimeltään GovHAVARO. Lisäksi Kyberturvallisuuskeskus toimii tietoturvallisuusviranomaisena turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvissä turvallisuusasioissa.

Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisin tehtävänä on suorittaa myös muut sille laissa erikseen säädetyt tehtävät sekä antaa jokaiselle tehtäväpiiriinsä kuuluvaa apua. Poliisi tutkii tietoverkkorikoksia ja pyrkii saamansa tiedon avulla myös estämään ennalta mahdollisia tulevia rikoksia. Poliisi ylläpitää tietoverkkorikosten kansallista tilannekuvaa.

Suojelupoliisin tehtävänä on ennaltaehkäistä ja torjua kaikkein vakavimpia kansallisen turvallisuuden uhkia, kuten terrorismia ja vieraiden valtioiden Suomeen kohdistamaa laitonta tiedustelua kybervakoilu mukaan lukien. Sen tehtävänä on havaita, estää ja paljastaa sellaisia toimia, hankkeita ja rikoksia, jotka voivat uhata valtio- tai yhteiskuntajärjestystä tai Suomen sisäistä tai ulkoista turvallisuutta. Suojelupoliisi suorittaa siviilitiedustelua muun muassa verkossa tapahtuvien kyberhyökkäysten taustojen ja motiivien selvittämiseksi kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi myös attribuutioprosessissa sekä muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

Sotilastiedustelun tarkoituksena on hankkia ja käsitellä tietoa Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta ylimmän valtiojohdon päätöksenteon tukemiseksi ja Puolustusvoimien tehtävien suorittamiseksi sekä ennakkovaroituksen antamiseksi. Sotilastiedusteluviranomaiset voivat hankkia tietoa luonteeltaan sotilaallisesta toiminnasta sekä vieraan valtion toiminnasta tai muusta sellaisesta toiminnasta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja. Sotilastiedustelun kohteena oleva toiminta voi tapahtua myös kybertoimintaympäristössä.

Puolustusvoimien tehtäviin kuuluu muun muassa Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen sekä kansainvälisen avun antaminen, yhteistoiminta ja muu kansainvälinen toiminta. Suomen sotilaalliseen puolustamiseen kuuluu maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen sekä kansan elinmahdollisuuksien, perusoikeuksien ja valtionjohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen. Puolustusvoimien tehtävien voidaan katsoa kattavan myös kybertoimintaympäristön.

Puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan kohdistuessa Suomeen. Sotilaallisten voimakeinojen tulee olla sopusoinnussa Suomea sitovien kansainvälisten velvoitteiden kanssa. Sotilaallisilla voimakeinoilla tarkoitetaan sotilaan henkilökohtaisen aseen ja sitä voimakkaampaa asevoiman käyttöä.

Puolustusvoimat toimii myös aluevalvontaviranomaisena. Lisäksi Puolustusvoimat vastaa sotilastiedustelusta edellä kuvatun mukaisesti.

Valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen. Valtioneuvoston tilannekeskuksen tehtävänä on tasavallan presidentin ja valtioneuvoston päätöksenteon ja toiminnan tueksi koota ja analysoida tietoa turvallisuustilanteesta ja sellaisista häiriöistä ja niiden uhista, jotka vaarantavat yhteiskunnan elintärkeitä toimintoja, hoitaa ja koordinoida tilannekuvan ylläpitämiseen, kokoamiseen, yhteensovittamiseen ja välittämiseen liittyviä poikkihallinnollisia tehtäviä sekä jakaa yhteen sovitettua tietoa tasavallan presidentille, valtioneuvostolle ja muille viranomaisille.

Valtioneuvoston tilannekeskus tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja muista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille.

Ulkoministeriölle kuuluu muun muassa ulko- ja turvallisuuspolitiikan valmistelu ja toimeenpano, ulkopoliittisesti merkittävien kannanottojen ilmoittaminen muille valtioille ja kansainvälisille järjestöille sekä kansainvälisen oikeuden kehittäminen ja muut kansainvälistä oikeutta koskevat asiat. Kansainvälisten tietoturvallisuusvelvoitteiden toteuttaminen Suomen kansallisena turvallisuusviranomaisena kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2004) nojalla kuuluu myös ulkoministeriön vastuualueisiin. Kyberkysymysten osalta kyberdiplomatia, kybertoimintaympäristön kansainvälisoikeudellinen kehittäminen ja valtiosopimuksiin liittyvät kysymykset, kaupallis-taloudelliset suhteet sekä Suomen etujen edistäminen edustustoverkon kautta kuuluvat ulkoministeriön vastuualueisiin. Attribuutiota valmisteltaessa ulkoministeriöllä on keskeinen rooli. Valmistelua tehdään usein yhteistyössä Suomen kansainvälisten kumppanimaiden kanssa.

Eri hallinnonalojen politiikkatoimia ohjataan useasta ministeriöstä käsin. Liikenne- ja viestintäministeriössä valmistellaan yleiset kyberturvallisuuteen liittyvät politiikkatoimet ja sinne on sijoitettu myös valtion kyberturvallisuusjohtajan virka, jonka tehtävänä on koordinoida ja sovittaa yhteen kansallista kyberturvallisuuden kehittämistä, suunnittelua ja varautumista sekä toimia valtionjohdon neuvonantajana. Sisäministeriöstä johdetaan kyberrikollisuuden torjunnan ja siviilitiedustelun politiikkatoimia. Puolustusministeriön tehtävänä on kehittää kyberpuolustukseen ja sotilastiedusteluun liittyviä politiikkatoimia. Lisäksi valtiovarainministeriön tehtävään kuuluu kehittää julkisen sektorin kyberturvallisuutta. Edellä mainittujen viranomaisten lisäksi kybertoimintaan liittyy myös muita viranomaisia, kuten EU:n verkko- ja tietoturvadirektiivin (niin sanottu NIS-direktiivi) mukaiset valvovat viranomaiset. Yhteiskunnan kriittisten toimintojen näkökulmasta Huoltovarmuuskeskus on keskeinen toimija.

5 Nykytilan arviointi ja kehittämistarpeet

Reaalimaailmassa viranomaisilla on yleensä selkeät tehtävät eri uhkatilanteiden hallinnassa ja viranomaisten väliset vastuualueet sekä yhteistyövelvoitteet on määritelty. Kybertoimintaympäristön osalta Suomessa ei ole laissa riittävässä laajuudessa säädetty viranomaisten välisestä koordinaatiosta ja yhteistoiminnasta eri tasoilla, eikä lainsäädäntö ota tarvittavassa määrin huomioon kybertoimintaympäristön erityispiirteitä kyberuhkiin vastaamisessa ja tiedonvaihdossa. Kybertoimintaympäristön suojaaminen on jakaantunut usealle eri hallinnonalalle eikä koko kybertoimintaympäristöä ole osoitettu eikä voida osoittaa yhdenkään hallinnonalan tehtäväksi. Uhkiin reagoiminen edellyttää tiivistä hallinnonalojen välistä yhteistyötä niin strategisella kuin operatiivisellakin tasolla. Yhteistyötä entisestään tiivistämällä voitaisiin varmistaa se, että oikea viranomainen suorittaa toimenpiteitä oikeaan aikaan kuitenkaan vaarantamatta toisen viranomaisen tehtäviä ja toisaalta se, että toiminnassa saadaan käyttöön paras osaaminen.

Nykytilassa viranomaisilla ei ole riittäviä toimintaedellytyksiä tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Toimintaedellytysten parantamiseksi on tunnistettu kehittämistoimenpidetarpeita seitsemän keskeisen osa-alueen osalta: kyberturvallisuuden strateginen tavoitetila, yhteistoiminta ja viranomaisprosessit, tilannekuva, tiedonvaihto, vaikuttaminen ja vastatoimet, tiedonhankinta ja viranomaisverkkojen suojaus.

5.1 Strateginen tavoitetila

Kyberturvallisuutta ja sen kansallisia tavoitteita ja rakenteita on kehitetty kansallisten strategioiden ja niiden perusteella laadittujen kehittämisohjelmien pohjalta. Kyberturvallisuusstrategia on osa EU:n kyberturvallisuusstrategian toimeenpanoa ja yhteiskunnan turvallisuusstrategiaa. Strategioiden asettamaa tavoitetilaa ei kuitenkaan ole kaikilta osin saavutettu. Suomen ja Euroopan turvallisuus- ja toimintaympäristössä tapahtuneen perustavanlaatuisen muutoksen valossa on tarve arvioida uudelleen kyberturvallisuuden kansallisia strategisia linjauksia sekä tavoitetilaa myös Nato-jäsenyyteen liittyen. Kokonaisuudessa painottuu aikaisempaa enemmän kansallisen turvallisuuden ja maanpuolustuksen sekä kyberturvallisuuden kytkös ulko- ja turvallisuuspolitiikkaan.

Myös EU:n kyberturvallisuusdirektiivin (NIS2) ja kriittisen infrastruktuurin häiriönsietokykyä koskevan CER-direktiivien täytäntöönpanon myötä syntyy tarve uudistaa kansallista kyberturvallisuusstrategiaa. NIS2-direktiivin mukaan kunkin jäsenvaltion on hyväksyttävä kansallinen kyberturvallisuusstrategia, jossa määritellään strategiset tavoitteet, tavoitteiden saavuttamiseksi tarvittavat resurssit sekä asianmukaiset politiikka- ja sääntelytoimenpiteet kyberturvallisuuden korkean tason saavuttamiseksi ja ylläpitämiseksi ottaen huomioon julkisen sektorin ja yksityisen sektorin välinen yhteistyö sekä kansallinen riskiarvio.

Kyberpuolustus on kansallisen kyberturvallisuuden maanpuolustuksellinen osa-alue, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä sekä erilaisista tukitoiminnoista. Tuleva Nato-jäsenyys luo tarpeen määritellä kyberpuolustus osana kansallista kyberturvallisuutta ja luo samalla rinnakkaisen rakenteen EU:n puitteissa tehtävälle yhteistyölle. Tämä edellyttää kansallista toimintamallia, jossa sovitetaan yhteen kantojen ilmaiseminen EU:lle ja Natolle.

Tarkennettua kansallista tavoitetilaa kaivataan erityisesti sen määrittämiseksi, miten vihamieliseen toimintaan kansallisesti reagoidaan, millaisella prosessilla määritetään toimenpiteiden luonne, mitkä ovat nykyisten lisäksi tarvittavat toimivaltuudet ja kenelle ne osoitetaan. Näiden kysymysten selkeyttäminen ohjaisi osaltaan viranomaisten välisen yhteistyön kehittämistä, parhaiden kyvykkyyksien hyödyntämistä kansallisen turvallisuuden parantamiseksi sekä lainsäädännön muutostarpeiden arviointia.

Kehittämisehdotukset

Kansallinen tavoitetila tulee määritellä uudessa kyberturvallisuusstrategiassa, jossa otetaan huomioon muutokset turvallisuusympäristössä, vastataan EU-lainsäädännön vaatimuksiin sekä määritellään tavoitteet EU:n ja Naton puitteissa tehtävälle yhteistyölle. Tavoitetilassa olisi vaikutettava vielä nykyistä kokonaisvaltaisemmin kybertoimintaympäristön olosuhteisiin ja vihamieliseen toimintaan, mikä olisi linjassa EU:n kyberpuolustuksen ja Naton kyberpuolustuksen kehittämisen linjauksien kanssa ja edellyttäisi kyberpuolustusdoktriinin laatimista.

Myös teknologian kasvava merkitys geopolitiikassa vaikuttaa kansallisen kyberturvallisuuden tavoitteisiin ja toteuttamiseen. Tavoitetilassa olisikin otettava huomioon teknologian kehittyminen, määritellä siihen liittyvät valinnat ja arvioida vaikutukset huoltovarmuuteen.

5.2 Yhteistoiminta ja viranomaisprosessit

Kyberpoikkeamatilanteessa viranomaisten välinen yhteistyö on välttämätöntä, koska useammalla viranomaisella on velvoite selvittää tapausta oman tehtävänsä puitteissa. Yhteistyössä on otettava huomioon erilaisten kyberuhkien luonne ja niiden torjunnan edellyttämät erilaiset toimivaltuus- ja yhteistoimintavaatimukset. Vieraiden valtioiden tiedustelupalveluiden ja asevoimien räätälöidyt ja korkeasti resursoidut operaatiot edellyttävät erilaisia ratkaisuja kuin päivittäisten, tavanomaisempien uhkien torjunta. Proaktiivinen yhteistyö on keskeisessä asemassa jatkuvan tilannekuvan ja tilanneymmärryksen ylläpitämisessä sekä samalla merkittävien tapausten tunnistamisessa eri viranomaisten tietoja yhdistelemällä. Yleensä mukana on myös kohdeorganisaation edustaja, sillä kyberpoikkeamaa ei käytännössä ole mahdollista selvittää eikä vaikutuksia rajata ilman kohteena olevan järjestelmän ylläpidon toimenpiteitä. Keskeiseksi haasteeksi muodostuu kuitenkin se, että saman ilmiön eri ulottuvuuksissa toimivalta kuuluu eri viranomaiselle. Omasta perustehtävästä ja toimivallasta johtuen viranomaisten välinen yhteistyö ja sen tarve koetaan eri tavoin ja sille on viranomaisesta riippuen erilaisia odotuksia.

Kansainvälisen tilanteen kiristymisen seurauksena asetettiin valtioneuvostoon 16.5.2022 ministeriötason koordinaatioryhmä tukemaan kyberturvallisuuden yhteistyötä ja tilannekuvan muodostamista. Yhteistyöryhmä onkin selvästi lisännyt eri hallinnonalojen välistä vuorovaikutusta ja edistänyt strategisen tason yhteistä tilanneymmärrystä valtioneuvostotasolla. Niin ikään asiantuntijatasolla eri kyberturvallisuusviranomaisten välillä on vakiintuneita yhteistyömuotoja. Sen sijaan strategisen ja asiantuntijatason väliin jäävällä päätöksentekotasolla ei ole säännöllisesti kokoontuvia, tehtävään asetettuja virallisia rakenteita.

Yhtenä yhteistyön muotona viranomaisten välillä toimii myös virka-apu. Tyypillisesti virka-apua ovat voineet antaa Puolustusvoimat ja poliisi. Tietoturvaloukkaustilanteissa myös Liikenne- ja viestintävirasto on voinut antaa virka-apuna asiantuntija-apua muille viranomaisille. Voimassa olevat virka-apusäännökset eivät kuitenkaan mahdollista esimerkiksi Liikenne- ja viestintävirastolle virka-avun vastaanottamista muilta viranomaisilta. Virka-apua koskeva sääntelykehikko kaipaakin kybertoimintaympäristön osalta tarkastelua ja täydentämistä.

Viranomaisyhteistyön tiivistämistarpeen ohella on syytä ottaa huomioon se, että monet yhteiskunnan kriittisistä toiminnoista ovat vahvasti yksityisen sektorin omistuksessa ja vaihtelu näiden toimijoiden kyberturvallisuusvalmiuksissa on merkittävää. Kyberturvallisuuskeskuksen CERT-toiminto (Computer Emergency Response Team) avustaa tarvittaessa ensivaiheessa toimijoita tietoturvaloukkausten selvittämisessä, mutta laajemmat selvittämistoimet ja jatkotoimet toteutetaan esimerkiksi yksityisen sektorin palveluja hyödyntäen. Kaikki viranomaiset eivät voi nykytilassa resursseista tai toimivaltuuksista

johtuen riittävästi tukea yhteiskunnan toiminnan ja huoltovarmuuden kannalta kriittisten toimijoiden varautumista ja palautumista kyberpoikkeamien aiheuttamista vakavista häiriötilanteista. Nykyisenkaltainen tilanne, jossa kaikkien viranomaisten osaaminen ja kyvykkyydet eivät ole käytössä, voi johtaa etenkin sofistikoituneissa kyberhyökkäyksissä siihen, että vakavan hyökkäyksen vaikutuksia yhteiskunnan toimintaan ei pystytä riittävässä määrin rajaamaan tai niistä ei kyetä riittävän nopeasti toipumaan.

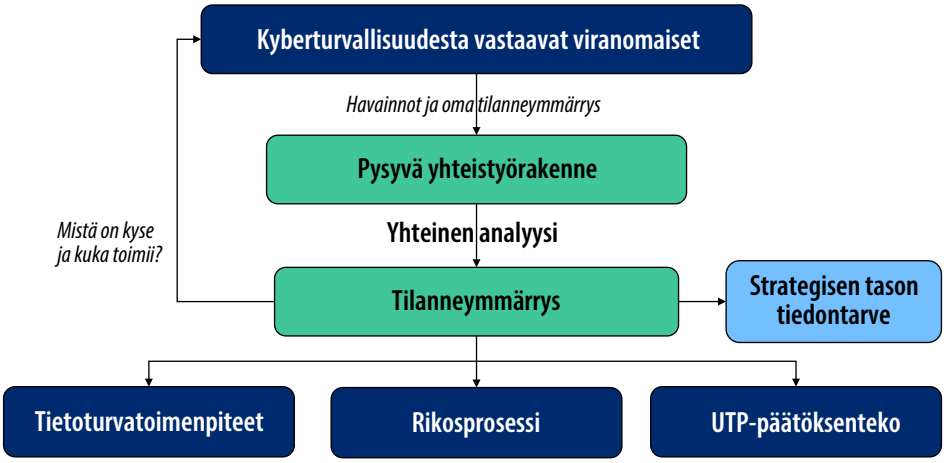
Nykytilassa myös toimitusketjujen monimutkaisuus hankaloittaa osaltaan kriittisten asiakkaiden ja näiden palvelutarjoajien tunnistamista. Jollei näitä ole tunnistettu etukäteen, Liikenne- ja viestintävirasto tai muut viranomaiset eivät välttämättä ryhdy tilanteen vaatimiin toimenpiteisiin ja tiedonvaihtoon esimerkiksi muiden viranomaisten kanssa. Kriittisten asiakkaiden ja palveluntarjoajien tarkempi kuvaus edistäisi merkittävästi Liikenne- ja viestintäviraston ja muiden viranomaisten toimintakykyä ja yhteistyötä.

Kehittämisehdotukset

Viranomaisyhteistyölle olisi luotava edellä kuvatuille valtioneuvostotason ja teknisen asiantuntijatason väliselle virastotasolle pysyvä, säännöllisesti kokoontuva, tehtävään asetettu yhteistyörakenne, jossa viranomaiset yhteistyössä analysoivat omista lähteistään kerättyjä tilannetietoja ja muodostavat yhteisen tilanneymmärryksen päätöksenteon ja kulloinkin toimivaltaisten viranomaisen jatkotoimien perustaksi kuvan 1 periaatteiden mukaisesti. Hallinnonalojen rakenteiden välillä on eroavaisuuksia, mikä edellyttää eri hallinnonalojen horisontaalisten tasojen tunnistamista jatkotyössä.

Yhteinen tilanneymmärrys parantaa edellytyksiä tunnistaa vakavia kyberuhkia ja mahdollistaa nykyistä kokonaisvaltaisemman tiedon välittämisen strategiselle tasolle tai muille yhteiskunnan toimijoille. Pysyvän rakenteen lisäksi eri viranomaisten tulee varmistaa oma osallistumisensa jo olemassa oleviin ja toimiviin yhteistyö- ja tiedonvaihtoryhmiin, mikä luo edellytykset niissä vaihdettavan tiedon paremmalle hyödyntämiselle. Yhteistyörakenne ei korvaisi viranomaisten lakisääteisiä tehtäviä eri prosesseissa, mutta varmistaisi, että kussakin prosessissa olisi käytössä kaikki tarvittava tieto ja että tilanneymmärrys olisi kokonaisvaltaisempi.

Kuvio 1. Viranomaisyhteistyön periaate



Yhteistyörakenteessa syntyvän yhteisen tilanneymmärryksen perusteella voidaan koordinoida ja arvioida tarvittavia viranomaistoimenpiteitä tai suosituksia muille toimijoille riippumatta siitä, onko kyse tietoturvatoimenpiteistä, rikosprosessiin kuuluvista asioista tai ulko- ja turvallisuuspoliittisen päätöksenteon tukemisesta. Viranomaisten tehokkaan yhteistoiminnan mahdollistamiseksi vakiinnutettu yhteistyörakenne vaatii prosessien kuvaamista ja tarkentamista sekä saattaa lisäksi edellyttää lainsäädäntömuutoksia. Yhteistyörakenteessa olisi huomioitava myös riittävä tiedonkulku hallinnonalojen sisällä.

Viranomaisten tulisi voida tukea nykyistä laajemmin yhteiskunnan kannalta kriittisiä toimijoita niihin kohdistuvien hyökkäysten vaikutusten vähentämiseksi. Tämä edellyttää kriittisten toimijoiden määrittelyä ja yksilöintiä toimialoittain. Koska kriittisetkin toimijat ovat riippuvaisia omista palveluntuottajistaan, tulee nämä ottaa tarkasteluun mukaan.

Virka-avun näkökulmasta olisi tarpeen täydentää sääntelyä virka-avun laajemmaksi mahdollistamiseksi eri viranomaisten välillä, kuten jo esitettiin eduskunnassa rauenneessa hallituksen esityksessä HE 243/2022 vp.

5.3 Tilannekuva

Kyberturvallisuuden tilannekuvan muodostaminen edellyttää riittävää kyvykkyyttä havainnoida kybertoimintaympäristöön kohdistuvia uhkia. Havainnointia tehdään nykyisellään eri viranomaisissa eri tavoin ja viranomaisen laissa säädetyn tehtävän edellyttämään tarkoitukseen sen lisäksi, että kunkin tietojärjestelmän tietoturvaylläpito pyrkii havainnoimaan tietojärjestelmässä tapahtuvia poikkeamia. Liikenne- ja viestintävirasto muodostaa kansallista kyberturvallisuuden tilannekuvaa eri lähteistä.

Viranomaiset tuottavat tälläkin hetkellä tehtäviensä hoitamiseksi tilannekuvia eri tasoilla, eri käyttötarkoituksiin ja erilaisella sisällöllä. Suomessa on pitkään tuotettu ja jaettu viranomaisten asiantuntijoiden välillä teknistä tilannekuvaa sekä vuoden 2022 kesästä lähtien myös kyberturvallisuuden strategista tilannekuvaa. Strategisen tilannekuvan tietopohjan laajentamiseksi ja tiedon jakamisen tehostamiseksi on perustettu aiemmin mainittu ministeriötason koordinaatioryhmä, joka tilannekuvan lisäksi tukee kyberturvallisuuden yhteistyötä. Ryhmän toiminta perustuu koordinointiin viranomaisten lainsäädännössä vahvistettujen toimivaltuuksien puitteissa. Toimivaltaisten viranomaisten väliltä puuttuu kuitenkin yhdistetty ja analysoitu, niiden keskenään koordinoima tilannekuva.

Valtioneuvoston puolustusselonteon linjausten mukaan kaikkia toimintaympäristöjä on kyettävä valvomaan. Valvonnalla ei tarkoiteta tiedonhankintaa kansalaisten luottamuksellisesta viestinnästä, vaan ennen kaikkea paremman kybertilannekuvan luomista, systemaattisempaa kokoamista sekä siihen vaikuttavien tietovirtojen mahdollistamista yhteisen tilanneymmärryksen luomiseksi erityisesti valtiollisten tai muiden kansallista turvallisuutta vaarantavien toimijoiden toiminnasta Suomen kybertoimintaympäristössä. Kyberpuolustuksen tilannekuva muodostaa osan viranomaisten yhteisestä tilanneymmärryksestä. Puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien estäminen ja torjuminen edellyttävät tiedonvaihtoa, toimivaltuuksia ja kansallisia yhteistyörakenteita viranomaisten välillä.

Kybertilannekuvan muodostamiseen liittyen on syytä huomata, että rikosilmoituksen tekeminen on nykyisellään tietoturvaloukkauksen kohteena olleen yrityksen oman harkinnan varassa. Myöskään NIS-direktiivin piiriin kuuluvilla toimijoilla, kuten keskeisillä huoltovarmuuskriittisillä toimijoilla ja palveluntarjoajilla, ei ole velvollisuutta tehdä tapauksista rikosilmoitusta. NIS-toimijoiden osalta ilmoitus tehdään sektorikohtaiselle valvovalle viranomaiselle, joka raportoi tapaukset Liikenne- ja viestintävirastolle. Lisäksi tapauksia voi tulla Liikenne- ja viestintäviraston tietoon vapaaehtoisen ilmoittamisen myötä.

Nykytilassa Liikenne- ja viestintäviraston kyberturvallisuuskeskus ei kuitenkaan voi automaattisesti informoida muita viranomaisia vakavissakaan kansallista turvallisuutta tai maanpuolustusta uhkaavissa tietoturvaloukkauksissa ilman ilmoittajan nimenomaista suostumusta.

Kehittämisehdotukset

Kybertoimintaympäristön havainnoinnin osalta on tarve systematisoida tietojen kokoamista siten, että saavutetaan laajempi tilanneymmärrys Suomeen kohdistuvista vakavista kyberuhista. Havainnoinnin osalta on tosin säilytettävä tasapaino sen suhteen, ettei viestinnän luottamuksellisuutta ja yksityisyyden suojaa jatkossakaan tarpeettomasti rajoiteta viranomaisten toimesta. Tämä on merkityksellistä erityisesti arvioitaessa kyberuhkien havainnointia. Toisaalta vakavien kyberuhkien havainnoinnissa ja kriittisen infrastruktuurin teknisessä ohjaustoiminnassa havainnoinnin kohteena ei ole viestin semanttinen sisältö, vaan esimerkiksi haittaohjelmakoodi, joka saa kohteena olevan järjestelmän toimimaan haittaohjelman tarkoittamalla tavalla. Lisäksi vieraan valtion vihamielisen toiminnan ei katsota nauttivan viestinnän luottamuksellisuuden tai yksityisyyden suojaa. Myöskään strategisessa tilannekuvassa käsiteltävissä ja vaihdettavissa tiedoissa ei useinkaan ole kyse henkilötiedoista tai muista perusoikeussuojan piiriin kuuluvista tiedoista toisin kuin voi olla teknisen tilannekuvatiedon vaihtamisessa.

Kybertoimintaympäristön tehokkaampi havainnointi sekä poikkihallinnollinen tilannekuvan muodostaminen ja analyysi edellyttävät riittäviä tiedonluovutus- ja tiedonsaantioikeuksia sekä tiedonvaihtomahdollisuuksia asianomaisille viranomaisille sekä nykyistä laajempia ja velvoittavampia ilmoitusvelvollisuuksia toiminnan kohteeksi joutuvilta tahoilta. Tämä edellyttäisi muutoksia lainsäädäntöön, mutta mahdollisen uuden sääntelyn ohella tiedonvaihdon mahdollisuuksia tulisi tarkastella myös jo nykyisen sääntelyn pohjalta peilaten niitä eri viranomaisten tehtäviin ja tietotarpeisiin muuttuneessa turvallisuusympäristössä. Huomioon on otettava myös käynnissä oleva säädösvalmistelu NIS2-direktiivin velvoitteiden saattamiseksi osaksi kansallista lainsäädäntöä, jossa ilmoitusvelvollisuuden laajentaminen on yksi käsiteltävistä kysymyksistä. Lisäksi tulee tarkastella ilmoitusvelvollisuuden alan laajentamista kansallisesti koskemaan myös sektoreita, jotka eivät kuulu direktiivin soveltamisalaan, kuten puolustus- ja turvallisuusalaa. Tämä saattaa edellyttää niin ilmoitusvelvollisuuden kuin muunkin sääntelyn ulottamista kansallisen turvallisuuden ja maanpuolustuksen kannalta keskeisille sektoreille.

Tiedon luovuttamista koskevaa sääntelyä arvioitaessa on tärkeää, että se perustuu viranomaisten tehtävien hoitamiseen perustuvaan tarpeeseen tai välttämättömyyteen ja on oikeasuhtaista sekä riittävän tarkasti määriteltyä. Tietojen luovuttamisessa olisi huomioitava myös viranomaisen itsenäinen mahdollisuus luovuttaa tietoja toimivaltaiselle viranomaiselle ilman nimenomaista pyyntöä.

Tilannekuvan muodostaminen viranomaisten välillä tulisi nähdä jatkumona ja prosessi tulisi kuvata ja vakiinnuttaa. Yhteisten tilannekuvaprosessien kehittäminen voisi lähteä liikkeelle siitä, että tunnistetaan nykyiset prosessit ja yhteistyöryhmät sekä kuvataan niiden tehtävät ja toiminnan tavoitteet aiempaa tarkemmin. Eri viranomaisilla tulisi olla jaettu ymmärrys tilannekuvan tuottamisen ja vastuutahojen lisäksi eri tilannekuvista, mikä edellyttäisi tilannekuvien yhtenäistä määrittelemistä ja käytettävästä terminologiasta sopimista. Esimerkiksi Liikenne- ja viestintävirasto voisi toimia yhteisten tilannekuvaprosessien ja tiedon keräämisen ja analysoinnin koordinoivana tahona.

Jaetun tilannekuvan tuottaminen edellyttää niin ikään tiiviimpää viranomaisyhteistyötä käytännön toimenpiteistä vastaavalla johtotasolla. Osassa viranomaistoimintoja on tunnistettu, että kyberturvallisuutta koskeva tilannekuva jää helposti tekniselle tasolle, jolloin asiat eivät päädy ylemmän johdon keskusteluihin ja päätöksenteossa oikealle tasolle.

Viranomaisten ja valtion johdon lisäksi tilannetietoja vakavista kyberuhista olisi voitava jakaa entistä tehokkaammin huoltovarmuuskriittisille yrityksille, kunnille sekä hyvinvointialueille tarkoituksenmukaisella tavalla tiedon turvaluokat huomioiden. Tämä tukisi organisaatioiden varautumista ja vahvistaisi kyvykkyyttä toimia nopeasti ja tehokkaasti häiriötilanteissa. Samalla, kun viranomaisten tiedonsaantia koskevia oikeuksia ja organisaatioiden niihin liittyviä velvollisuuksia tarkennettaisiin lainsäädännössä, tulisi varmistaa, ettei lainsäädäntöön jäisi sellaisia esteitä, jotka estävät kyberturvallisuuden keskeisiä viranomaisia toimittamasta kybertilannekuvatietoa edellä mainituille tahoille tai jotka estäisivät näitä vastaanottamasta kybertilannetietoja.

5.4 Tiedonvaihto

Viranomaisten välinen tiedonvaihto asiantuntijatasolla on pääosin vakiintunutta ja toiminut aktiivisesti 2000-luvun alusta alkaen lainsäädännön asettamissa puitteissa. Yhteistyöstä esimerkkinä mainittakoon Liikenne- ja viestintäviraston verkostoyhteistyö, joka mahdollistaa suhteellisen laajan tiedonvaihdon. Tiedonvaihto on luonteeltaan osin reaktiivista, mikä ei aina mahdollista riittävän aktiivista kyberuhkiin varautumista, niiden ennalta estämistä ja toimivaltuuksien käytön valmistelua.

Suomen kansallisen turvallisuuden ja maanpuolustuksen kannalta vihamielisen toiminnan aiheuttamien vahinkojen tehokkaan estämisen kannalta yhteistyön ja tiedonvaihdon olisi kuitenkin oltava tiiviimpää erityisesti uhkaympäristön havainnointiin liittyen. Tiedonvaihtoon vaikuttaa eri viranomaisten puutteellinen ymmärrys toistensa tehtäväkentästä, tietotarpeista tai tiedon liitynnöistä toisen viranomaisen tehtävään. Lisäksi

kybertoimintaympäristön keskinäisriippuvuudet voivat johtaa ennakoimattomiin vaikutuksiin toisen viranomaisen tehtäviin, joita ei ensimmäisen asteen vaikutusarvioinnissa ole kyetty tunnistamaan.

Viranomaisverkoston yhteistyön toimivuudesta huolimatta ei ole täysin selvää, osallistuvatko kaikki tarvittavat tahot tiedonvaihtoon liittyvään yhteistyöhön. Esimerkkinä tästä voidaan todeta, että tiedusteluviranomaisten ja Kyberturvallisuuskeskuksen edellytykset vaihtaa tietoa kyberpoikkeamatilanteen arvioimiseksi ovat hyvät, mutta Puolustusvoimien kyberpuolustuksen operatiivinen toimija tai poliisi jää tiedonvaihdon ulkopuolelle tämänhetkisestä lainsäädännöstä johtuen. Toisaalta Liikenne- ja viestintävirasto ei pysty lainsäädännöstä johtuen luovuttamaan kaikkea tarpeellista tietoa esimerkiksi tiedusteluviranomaisille ilman tietoturvaloukkauksen kohteen lupaa.

Viranomaisten toimivalta sekä erilaiset tehtävät ja tiedon käyttötarkoitukset rajoittavat tällä hetkellä kyberuhkiin liittyvän yksityiskohtaisemman tiedon vaihtamista. Tämän voidaan katsoa pohjautuvan yksityiselämän suojaan, viestinnän luottamuksellisuuteen sekä oikeusturvaan palautuviin kysymyksiin.

Lainsäädännöltä edellytetään tarkkuutta, jotta on selvää, millä edellytyksin, missä laajuudessa, missä tilanteissa ja mitä tietoa viranomaisten välillä voidaan vaihtaa. Henkilötietoja koskevan tiedonvaihdon osalta on huomioitava tiedon käyttötarkoitus erityisesti liikuttaessa yleisen tietosuoja-asetuksen ja rikosasioiden tietosuojalainsäädännön välimaastossa. Usean eri säädöspohjan soveltaminen henkilötiedoiksi katsottavan tiedon käsittelyyn vaikeuttaa myös viranomaisten toimintaa käytännön lainsoveltamistilanteissa. Sääntelyn tarkkuudella ja selkeydellä on merkitystä myös yksittäisen virkahenkilön oikeusturvan kannalta.

Kuten aiemmin on jo todettu, viranomaiset käyttävät laajalti yksityisten yritysten tuottamia palveluita ja tukeutuvat siten niiden omistuksessa olevaan infrastruktuuriin. Yksityisen sektorin toimijoiden kanssa solmittavissa sopimuksissa voitaisiin kannustaa näitä toimijoita tietojen jakamiseen asianomaisille viranomaisille voimassa olevan lainsäädännön puitteissa.

Kehittämisehdotukset

Olemassa olevien tiedonvaihdon mallien kehittämisellä voidaan välttää ainakin pääosin päällekkäisten ratkaisujen luominen. Toiminnan muuttaminen ennakoivaan suuntaan edellyttää kuitenkin uusien mallien ja rakenteiden luomista sekä lainsäädännön tarkastelua.

Tiedonvaihtoon liittyvä lainsäädäntö vaatii selkeyttämistä, koska voimassa olevan lainsäädännön ei voida katsoa mahdollistavan riittävää tiedonvaihtoa useiden kyberuhkien torjunnan kannalta keskeisten viranomaisten välillä riittävän laajasti. Viranomaisten toimintaedellytyksiä ja tiedonvaihtoa olisikin tarkasteltava uudella tavalla kokonaisuutena, jotta viranomaisilla olisi vakavissa kyberuhkatilanteissa tehokkaat, nopeasti käyttöön otettavissa ja toteutettavissa olevat keinot. Tiedonvaihdon laajentaminen edellyttää lainsäädäntöön kirjattuja, selkeiden tiedonvaihdon edellytyksien ja tiedonvaihtoon osallistuvien tahojen määrittelyä ja toisaalta tiedonvaihdon nykyisten rajoitteiden perusteiden arviointia sekä mahdollisten tiedonhankinnan toimivaltuuksien muutosten huomioimista. Tämä takaisi sen, että tiedonvaihto tapahtuisi selkeämmin organisaatioiden välillä ja sidottuna tiettyihin, niihin toimijoiden ennalta määrittelemiin virkatehtäviin, joihin kuuluisi tiedonvaihtoon liittyviä vastuita. Tällä taattaisiin tiedonvaihdon jatkuvuus myös tilanteissa, joissa tietty henkilö poistuisi organisaatiosta, ja toisaalta se, että tieto tulee organisaation käyttöön. Selkeä lainsäädäntö parantaisi myös viranomaisten toiminnan oikeusvarmuutta, tapahtumien jäljitettävyyttä ja selkeyttäisi yksittäisen virkamiehen vastuuta.

Viranomaisten tiedonvaihtomahdollisuuksiin yhteiskunnan toiminnan kannalta vakavissa tietoturvaloukkaustilanteissa esitettiin parannuksia hallituksen esityksellä HE 243/2022 vp. Koska esityksen käsittelyä ei kuitenkaan ehditty saada päätökseen eduskunnassa ennen vaaleja, on edelleen olemassa tarve ehdotetun kaltaiselle lainsäädännölle.

Tiedonvaihdon tulisi olla kaksisuuntaisuuden lisäksi tasapainoista ja käyttötarkoitussidonnaista perustuen tiedon saamisen oikeuteen ja tiedon jakamisen intressiin sitä tarvitsevien kesken. Tiedonvaihdon kannalta paras lopputulos voidaan arvioida saavutettavan tilanteessa, jossa lainsäädäntö mahdollistaisi siirtymisen tietotarvelähtöisestä ajattelusta (need to know) tiedon jakamisen tarve -ajatteluun (need to share), eli tiedon tuottaja tai haltija pystyisi tunnistamaan ja jakamaan tiedon oma-aloitteisesti toimivaltaiselle viranomaiselle. Tämä edellyttää arviointia perusoikeuksien kannalta, missä määrin tarvepohjainen tiedonvaihto voi olla mahdollista erityisesti, kun puhutaan esimerkiksi välitystiedoista.

Lainsäädännön asettamissa rajoissa tehokas ja relevantin tiedon vaihtaminen edellyttää sitä, että tietoa jakava taho tunnistaisi, mitä tietoa tarvitsija mahdollisesti tarvitsee. Selkeä lainsäädäntö edellyttää tiedonvaihdon prosessien tarkastelua ja viranomaisen ydintoiminnan määrittelyä kybertoimintaympäristössä sekä ymmärryksen saavuttamista tietotarpeista viranomaisten kesken. Määrittelyn olisi tapahduttava organisaatiokohtaisesti ja jokaisen organisaation olisi määriteltävä omat tiedonkäsittelyprosessinsa.

Tiedonvaihdossa olisi voitava huomioida tiedon suojaamistarpeiden suhde tiedon jakamisen tärkeyteen. Lainsäädännössä voitaisiin huomioida tiedonkäsittelyrajoitteita, joita tiedon alkuperäinen luovuttaja voisi tiedolle asettaa. Tämä mahdollistaisi tiedon

luottamuksellisen käsittelyn ja luottamuksen säilyttämisen eri toimijoiden välillä sekä tarpeelliset oikeusturvakeinot. Esimerkkinä tällaisesta rajoitteesta voisi olla se, että luovutettua tietoa ei saisi käyttää rikosprosessissa todisteena.

Kyberrikostorjunnan ja kyberrikollisuuden tilannekuvan näkökulmista erityisenä tiedustelumenetelmiä koskevana kysymyksenä voidaan nostaa esille tiedustelulainsäädännön niin kutsuttu palomuurisääntely. Sääntely antaa mahdollisuuden luovuttaa tiedustelumenetelmillä hankittua tietoa rikostorjuntaan tietyissä säädetyissä tilanteissa. Palomuurisääntely olisi otettava arvioitavaksi niin, että se mahdollistaisi myös riittävän tiedon luovuttamisen rikostorjuntaviranomaiselle kyberuhkien ennalta estämiseksi.

Olemassa olevaa palomuurisääntelyä ja muita vastaavia rajoitteita tulisi kehittää siten, että tiedoille voitaisiin asettaa tiedonkäyttörajoituksia rikosoikeudellisessa prosessissa, mutta esitutkintaviranomainen voisi kuitenkin hyödyntää tietoja muussa yleisen järjestyksen ja turvallisuuden tai esimerkiksi vihamielisen valtiollisen toiminnan ennalta estämisessä ja torjunnassa. Tiedustelutiedon hyödyntämiskieltoon voisi näissä tapauksissa olla kuitenkin poikkeuksena esimerkiksi tapaukset, joissa tiedon voitaisiin katsoa olevan syytetyn eduksi. Palomuurisääntelyn tulisi kuitenkin aina sallia valtiollisia toimijoita koskevan tiedon jakaminen uhkien torjumiseksi, koska rikosprosessi ei näiden osalta käytännössä toteudu.

Jotta tiedon hyödyntäminen eri viranomaistoiminnoissa laajojen kokonaisuuksien selvittämiseksi ja estämiseksi on mahdollista, on tärkeää, että saatujen tietojen käyttöä ei ole esimerkiksi rajattu vain yksittäisen tapauksen tai loukkauksen selvittämiseen.

Viranomaisten välisen tehokkaan tiedonvaihdon mahdollistamiseksi kyberuhkiin vastaamisessa tarvittaisiin myös viranomaisten yhteinen, korkean turvaluokan tiedonvaihtoon soveltuva järjestelmä.

Niin ikään yhteiskunnan kriittisten toimintojen kyberturvallisuuden kokonaisuuden kannalta olisi tärkeää, että tietoturvahäiriöistä ja poikkeamista olisi mahdollista jakaa tietoa nykyistä tehokkaammin tiedon turvaluokat huomioiden myös huoltovarmuuskriittisille yrityksille, hyvinvointialueille, kunnille sekä kuntaomisteisille palveluntarjoajille.

Tiedonvaihdon parempi huomioiminen sopimusehdoissa edellyttää viranomaisten yhteistyötä sopimusehtojen ja -prosessien määrittelyssä. Tähän liittyen tiedonhallintalautakunta on parhaillaan päivittämässä julkisten hankintojen tietoturvallisuuden vaatimuksia, missä yhteydessä viranomaiset voivat tuoda esille tarpeitaan muun muassa kyberturvallisuuteen liittyen. Yksityisiltä toimijoilta voitaisiin edellyttää myös ensi-ilmoittamista Liikenne- ja viestintävirastolle sekä sopimuskumppanina olevalle viranomaiselle voimassa oleva lainsäädäntö huomioon ottaen.

Hankintojen yhteydessä tulisi aina myös selvittää, olisiko hankinta mahdollista toteuttaa puolustus- tai turvallisuushankintana, jolloin edellytykset asettaa laatukriteereitä olisivat olennaisesti tavanomaista hankintaa paremmat.

5.5 Vaikuttaminen ja vastatoimet

Kybervaikuttamisella voidaan ymmärtää tarkoitettavan tietojärjestelmissä tai -verkoissa tai niiden kautta toteutettavia toimenpiteitä, joilla vaikutetaan tietojärjestelmään tai sovelluksiin, tietoverkkoihin tai -järjestelmiin liitettäviin laitteisiin tai tietoverkoissa tai -järjestelmissä olevaan tietoon, laitteisiin, niiden toimintaan tai henkilöihin. Kybervaikuttamisen tavoitteena on estää, keskeyttää, rajoittaa, poistaa, heikentää tai häiritä kohteen toimintaa taikka tuhota, manipuloida tai harhauttaa vaikuttamisen kohteena olevan toimijan kykyä toteuttaa omaa toimintaansa.

Kyberhyökkäyksien ja -vaikuttamisen torjunta edellyttää kyvykkyyttä vastatoimiin, joiden avulla hyökkääjän vihamielisten toimien vaikutuksia voidaan vähentää tai estää kokonaan. Vastatoimien avulla nostetaan hyökkäyskynnystä ja heikennetään hyökkääjän toiminta-edellytyksiä tarvittaessa jo ennen varsinaista hyökkäystä. Vastatoimet tulee kyetä mitoittamaan suhteessa vihamielisen toiminnan oletettuihin tai toteutuneisiin vaikutuksiin.

Tekniseen ympäristöön kohdistuneeseen toimintaan vastataan tietoturvatoimenpitein omassa tietoteknisessä ympäristössä. Jos samanaikaisesti kyseessä on rikos, käytetään lisäksi tarvittavia rikostorjunnan keinoja. Mikäli vihamielisessä toiminnassa on kyse valtiollisesta toiminnasta, tulevat kyseeseen kansallista turvallisuutta suojaavat ulko- ja turvallisuuspoliittiset toimet, jotka voivat vaihdella tapauskohtaisen harkinnan perusteella diplomaattisista keinoista aina sotilaallisiin keinoihin.

Liikenne- ja viestintävirastolla on mahdollisuus ryhtyä välttämättömiin tietoturvallisuustoimenpiteisiin fi-verkkotunnuksia hyödyntämällä toteutettavien, yleisiin viestintäverkkoihin tai -palveluihin tai niiden käyttäjiin kohdistuvien merkittävien tietoturvaloukkausten havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Toimet voivat sisältää muun muassa verkkotunnukseen suuntautuvan liikenteen estämisen tai rajoittamisen ja verkkotunnukseen suuntautuvan liikenteen ohjaamisen toiseen verkko-osoitteeseen. Lisäksi Liikenne- ja viestintävirastolla on oikeus yksittäistapauksessa päättää merkittävää haittaa aiheuttavan viestintäverkkolaitteen korjaustoimenpiteistä ja sen irrottamisesta yleisestä viestintäverkosta. Liikenne- ja viestintäviraston kyberturvallisuuskeskuksella on myös oikeus velvoittaa viestintäverkon omistaja tai muu haltija poistamaan viestintäverkkolaite verkkonsa kriittisistä osista kansallisen turvallisuuden ja maanpuolustuksen vaarantuessa.

Poliisi voi rikosvahinkojen ja -vaikutusten estämiseksi takavarikoida fyysisiä laitteita, katkaista tietoliikenteen tilapäisesti televalvontatoimivaltuudella ja määrätä keskeytettäväksi sisällöltään laittomien verkkoviestien jakelun. Toimenpiteillä pystytään vaikuttamaan ja puuttumaan mahdollisesti yksittäiseen laitteeseen tai ohjelmistoon ja sen sisältämään tietoon, mutta ei verkottuneessa ympäristössä tapahtuvaan suunnitelmalliseen rikolliseen toimintaan kokonaisuutena. Siltäkin osin kuin toimivaltuudet olisivat soveltuvia, niiden käsitteistö ja perusteluissa esitetyt soveltamistilanteet eivät vastaa tämän hetkisen kybertoimintaympäristön asettamia vaatimuksia. Voimassa olevaa poliisin toimivaltuuslainsäädäntöä säädettäessä kehittyvän kybertoimintaympäristön erityispiirteitä ja monimuotoisuutta ei ole pystytty huomioimaan ja tunnistamaan siinä laajuudessa, että lainsäädäntö vastaisi nykytilaa edes tulkintakäytännössä.

Jos valtiolliseen kybervakoiluun tai -vaikuttamiseen käytetty laite tai ohjelmisto sijaitsee ulkomailla, on tilanne toinen. Lähtökohtaisesti tällaisiin tilanteisiin pyritään puuttumaan kansainvälisen oikeusavun kautta, hyödyntämällä kansainvälisiä yhteistyöverkostoja tai esimerkiksi aiemmin kuvattuja diplomatian keinoja. Jos lähtömaalla ei ole halukkuutta tai tulkintansa mukaan toimivaltaa ja käytännön mahdollisuutta puuttua vahingolliseen toimintaan, ovat Suomen viranomaisten toimintamahdollisuudet rajalliset. Viranomaiset eivät voi käyttää toimivaltuuksiaan toisen valtion alueella. Poikkeuksen muodostavat tiedusteluviranomaiset, jotka voivat käyttää tiedustelumenetelmiä tiedon hankkimiseksi myös Suomen rajan ulkopuolella.

Jos rikosvahingot ilmenevät muissa maissa kuin Suomessa ja Suomi on toiminut kybertoimintaympäristössä haitallisen toiminnan kauttakulkumaana, Suomella voidaan katsoa olevan valtiona myös kansainvälisen oikeuden sääntöjen mukainen huolehtimisvelvoite. Sen mukaan Suomi ei voi sallia alueellaan sellaista toimintaa, mikä aiheuttaa merkittävää haittaa muiden valtioiden oikeuksille.

Puolustusvoimien kyberpuolustuksen osalta vihamielisen kybervaikuttamisen keskeyttämisen toimivaltuuspohja perustuu ennen kaikkea sotilaallisen voimankäytön määrittelyyn. Kansainvälisoikeudellisesti arvioituna sotilaallista voimankäyttöä tai aseellista voimankäyttöä kybertoimintaympäristössä ei ole pystytty kattavasti ja yhteneväisesti määrittelemään. Lisäksi kansallisesti aseellisen hyökkäyksen kynnyksen määritelmän alle jäävän kybervaikuttamisen keskeyttämisen toimivaltuuspohja on Puolustusvoimien osalta epäselvä. Puolustusvoimia koskevassa lainsäädännössä voidaan katsoa olevan puutteita myös kybervakoilun ja -vaikuttamisen estämiseen tai keskeyttämiseen tähtäävien toimenpiteiden valmistelun sekä oman toiminnan suojaamisen ja vihamielisen kybervaikuttamisen keskeyttämiseen välittömästi liittyvän kohdetiedustelun osalta.

Kehittämisehdotukset

Eri viranomaisilla olisi oltava oikeus lakisääteisten tehtäviensä hoitamiseksi kansainvälisen oikeuden asettamissa rajoissa estää ja keskeyttää vihamielinen kybertoiminta, joka vakavasti uhkaa Suomen kansallista turvallisuutta tai maanpuolustusta. Viranomaisilla olisi myös oltava joustavampi mahdollisuus osallistua yhteisoperaatioihin muiden valtioiden viranomaisten kanssa oikeudettoman toiminnan keskeyttämiseksi, ja osallistuvilla viranomaisilla olisi oltava oikeus käyttää tässä tarkoituksessa tarvittavia menetelmiä ja keinoja.

Poliisilaissa olisi säädettävä tarvittavista oikeuksista ja toimivaltuuksista estää ja keskeyttää laitteen tai ohjelmiston toiminta, jota käytetään systemaattiseen ja tahalliseen Suomen kansallista turvallisuutta horjuttavaan kybervakoiluun tai vihamieliseen kybervaikuttamiseen. Toimenpiteen tarkoituksena olisi välittömästi uhkaavan tai meneillään olevan rikoksen tai muun vaarallisen teon tai tapahtuman estäminen tai keskeyttäminen. Poliisilla olisi oltava myös oikeus ottaa hallintaan vahinkoa aiheuttavassa toiminnassa käytetty ohjausosoite eli komentopalvelimen verkko-osoite. Toimivaltuudella pystyttäisiin selvittämään entistä paremmin esimerkiksi bottiverkkojen rakentamiseen liittyviä rikoksia. Lisäksi pystyttäisiin estämään uudet rikokset ja vahingot, joita rikollinen toimija tulisi erittäin todennäköisesti aiheuttamaan komentopalvelimensa ja rakentamansa etäohjattavan verkon avulla. Viranomaiset saisivat näin myös paremmin tietoa vahinkoa kärsineistä asianomistajista.

Puolustusvoimien kyberpuolustuksen säädöspohjaa olisi selkiytettävä Puolustusvoimien kyberpuolustuslainsäädännöllä. Tämä loisi entistä paremmat edellytykset kyberpuolustuksen sisällyttämiselle eri toimialojen, viranomaisten ja muun yhteiskunnan väliseen tiiviiseen yhteistyöhön. Vihamielisen kybervaikuttamisen keskeyttämisen ja siihen liittyvän tiedonhankinnan sekä oman toiminnan suojaamisen toimivaltuuspohja tulisi säätää niin, että Puolustusvoimien suorituskyvyn käyttö olisi mahdollista myös tilanteissa, joissa sotilaallisen voimankäytön kynnyksen ei katsota ylittyvän tämän hetkisen kansainvälisoikeudellisen tulkintakäytännön mukaan.

Kyberpuolustuksen riittävät toimintaedellytykset ja mahdollisuudet eri valmiustiloissa tulisi varmistaa erityyppisten uhkien torjunnassa yhdessä muiden viranomaisten ja toimijoiden kanssa niin, että Puolustusvoimat voi tarvittaessa tukea muita viranomaisia omilla suorituskyvyillään.

5.6 Tiedonhankinta vakavista kyberuhkista

Tiedonhankinnalla kybertoimintaympäristössä saaduilla tiedoilla on erittäin tärkeä merkitys yhteiskunnan turvallisuuden kokonaisuudessa. Sen avulla hankittu tieto muodostaa viranomaisten ja valtiojohdon kybertilannekuvien ja -tilannekäsityksen yhden

keskeisen lähteen. Se muodostaa myös yhden tärkeän syötteen sellaiseen tietoturva- ja muuhun toimintaan, mukaan lukien HAVAROon ja tietoliikennetiedusteluun, jonka avulla havaitaan kriittisiin tietoverkkoihin ja kriittisen tärkeisiin yhteiskunnallisiin toimijoihin kohdistuvia kyberloukkauksia ja suojataan niitä loukkauksilta. Tiedonhankinnalla kybertoimintaympäristössä saadut tiedot uhkista ja niiden valtiollisista taustatahoista ovat myös edellytys attribuutiolle ja vihamielisen toiminnan pysäyttämiselle vastatoimilla.

Vakavista kyberuhista saadaan tietoa Kyberturvallisuuskeskuksen vapaaehtoisuuteen pohjautuvalla HAVARO-järjestelmällä. Lisäksi tiedonhankinta kybertoimintaympäristössä voi tapahtua siviili- ja sotilastiedustelun keinoin tai kyberrikoksen selvittämiseen tähtäävän esitutkinnan tai rikosten ennalta estämisen ja paljastamisen puitteissa. Tästä johtuen on olennaisen tärkeää, että lainsäädäntö vastaa tosiasiallisia tarpeita ja että se mahdollistaa riittävän tehokkaan tiedonhankinnan kybertoimintaympäristössä huomioiden kuitenkin perusoikeuksien rajoittamiseen liittyvät vaatimukset. Kybertoimintaympäristön tiedonhankintatoimivaltuuksien on tosiasiallisesti mahdollistettava kyberuhkien valtiollisten taustatahojen ja niiden toimintamotiivien sekä toiminnasta aiheutuvien vahinkojen ja riskien selvittäminen sekä suojautumisen parantaminen.

Kybertoimintaympäristössä tapahtuva viranomaisten tiedonhankinta kohdistuu yleensä erilaisiin teknisiin laitteisiin, telepäätelaitteisiin ja tietojärjestelmiin sekä niiden väliseen tietoliikenteeseen. Menetelmien käyttö kohdennetaan sillä perusteella, että jotain tiettyä laitetta tai järjestelmää on havaittu hyödynnettävän Suomeen kohdistuvassa kybervakoilussa tai muussa vihamielisessä kybertoiminnassa. Keskeisen haasteen ja esteen tehokkaalle tiedonhankinnalle kybertoimintaympäristössä muodostaa se, että viranomaisen on esitettävä tiedonhankinnan kohteena olevaa laitetta koskevat yksilöintitiedot tuomioistuimelle esittämässään lupavaatimuksessa. Valtiollisen kybervakoilun ja -vaikuttamisen osalta tai rikosten selvittämisessä ratkaisu ei ole toimiva, koska tuomioistuimen toimenpiteen kohteeksi hyväksymän ensimmäisen teknisen laitteen takaa paljastuu säännönmukaisesti kymmeniä tai jopa satoja muita laitteita, joita vieras valtio hyödyntää Suomeen kohdistuvan vakoilun tai vihamielisen vaikuttamisen ketjutuksessa. Vihamielisessä valtiollisessa kybertoiminnassa hyväksikäytettävien laitteiden väliset yhteydet ja ketjut rakentuvat ja häviävät erittäin nopeasti, mistä johtuen niihin kohdistuvaan tiedusteluun ei ole tällä hetkellä mahdollista hakea tuomioistuimelta lupaa käytettävissä olevan aikaikkunan puitteissa. Tästä seuraa, ettei laitteiden muodostamia ketjuja voida tunnistaa ja tiedonhankinta voi jäädä tuloksettomaksi.

Tiedustelumenetelmien osalta erityisenä huomiona voidaan nostaa tietoliikennetiedustelun kohdentamisen kannalta olennainen teknisten tietojen käsittely, jonka käyttö on sidottu hetkellisyyteen. Käsittelyn perusteella hankittuja tietoja ei voi myöskään käyttää varsinaisessa tietoliikennetiedustelussa käytettävien hakuehtojen muodostamiseen. Kyberuhkien tunnistamista ja seurantaa puolestaan vaikeuttaa nykylainsäädännön

rajoitus, joka sallii ainoastaan lyhytkestoisten näytteiden ottamisen viestintäverkon osasta. Rajoitus heikentää mahdollisuuksia havaita reititysmuutoksia ja tunnistaa tietoliikenteestä uusia tiedustelun kohteita, kuten kyberuhkia.

Tietoverkkoinfrastruktuuri on Suomessa yksityisten yritysten hallinnassa, mistä johtuen eräiden viranomaisille säädettyjen tiedustelumenetelmien ja tiedonhankintatoimivaltuuksien käyttö edellyttää välttämättä kyseisten yritysten myötävaikutusta. Tästä johtuen poliisilaissa säädetään teleyrityksen, joilla tarkoitetaan verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille tarjoavia yrityksiä, velvollisuudesta avustaa viranomaista tekemällä televerkkoon telekuuntelun ja televalvonnan edellyttämät kytkennät sekä antamalla poliisiviranomaisen käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Tiedot Suomessa toimivista teleyrityksistä on kerätty Liikenne- ja viestintäviraston teletoimintarekisteriin. Poliisilain mukaan teleyrityksillä on oikeus saada korvaus viranomaisten avustamisesta. Sotilastiedustelun osalta vastaavista velvollisuuksista on säädetty sotilastiedustelussa annetussa laissa.

SVPL:ssä säädetään teleyritysten velvollisuuksista liittyen telekuuntelun ja -valvonnan toteuttamiseen ja mahdollistamiseen. SVPL:n mukaan yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että telekuuntelu ja televalvonta sekä muut viranomaisten tiedonsaantioikeuksia koskevat pyynnöt voidaan toteuttaa siten kuin niistä erikseen säädetään. SVPL:ssä säädetään viranomaisten avustamista koskevista vaatimuksista liittyen telekuuntelun ja televalvonnan toiminnallisiin laatuvaatimuksiin ja teknisiin vaatimuksiin. Lisäksi SVPL:ssä säädetään teleyritysten velvollisuudesta luovuttaa viranomaisille telekuuntelun ja televalvonnan toteuttamiseksi tarpeelliset tiedot, joiden saamiseen viranomaisella on erikseen säädetty oikeus.

Menetelminä telekuuntelulla ja televalvonnalla on erittäin tärkeä merkitys valtiollisiin kyberuhkiin kohdistettavassa tiedonhankinnassa, mutta niiden käytännön hyödynnettävyyden näkökulmasta huomattavan ja lähes päivittäisen ongelman muodostaa se, että avustamisvelvollisuus ja avustamisesta seuraava oikeus korvauksen saamiseen on edellä ilmenevästi säädetty ainoastaan perinteisille teleyrityksille. Nyky-yhteiskunnassa viestinnän välittäjien joukko on huomattavasti niitä laajempi ja heterogeenisempi. Valtiollisten kyberuhkien torjunnassa esimerkiksi konesaliyritysten rooli telekuuntelussa ja -valvonnassa avustamisessa olisi keskeinen ja yhä kasvava viestintäteknologioiden edelleen kehittyessä. Velvollisuutta avustaa viranomaisia telekuuntelun ja -valvonnan toteuttamisessa ei kuitenkaan ole ulotettu niihin, kuten ei myöskään oikeutta korvauksen saamiseen avustamistoimenpiteistä.

Kehittämisehdotukset

Viranomaisten kykyä havaita ja tunnistaa ja tarvittaessa yksilöidä vihamielinen valtiollinen tai rikollinen toiminta kybertoimintaympäristössä tulisi kehittää, jotta haitallinen toiminta saadaan estettyä, vaikutukset minimoitua ja vieraan valtion vahingolliseen toimintaan vastaamiseksi tarvittavat jatkotoimet arvioitua. Tämä edellyttäisi erityisesti tiedonhankinnan toimivaltuuksien ja tiedustelumenetelmien kehittämistä vastaamaan toimintaympäristön nykyhetken ja arvioidun kehityksen asettamia vaatimuksia.

Eri viranomaisten tiedonhankintavaltuuksien tulisi olla nykyistä teknologiariippumattomampia, jotta oikeudettomasta toiminnasta voitaisiin hankkia tarvittavat lisätiedot toimintaan puuttumiseksi.

Kybertoimintaympäristössä tapahtuvaan tiedusteluun ja tiedonhankintaan liittyvää määrittelyä ja tehtäviä tulisi tarkentaa tiedonhankintavaltuuksien päivittämisen lisäksi. Lainsäädännössä tulisi nykyistä selkeämmin määritellä eri viranomaisten tehtäviin kybertoimintaympäristössä liittyvä sotilas- tai siviilitiedustelun toimivaltuuksilla tapahtuva strateginen tiedustelutoiminta sekä poliisin, suojelupoliisin ja Puolustusvoimien kybervaikuttamiseen liittyvä tiedustelutoiminta, jotta kaikilla keskeisillä kyberturvallisuuden viranomaistoimijoilla olisi tiedonhankintaan nykyistä selvempi toimivaltapohja.

Viranomaisten tiedonsaantioikeuksia ja tiedonhankintamenetelmiä arvioitaessa on yleisesti huomioitava myös siihen liittyvät perus- ja ihmisoikeuksista johtuvat vaatimukset. Pyrittäessä havaitsemaan esimerkiksi valtiollisen toimijan haitallista tietoliikennettä, käsitellään tyypillisesti myös muuta tietoliikennettä. Haittaohjelmaliikenne tai valtiolliset toimijat eivät vallitsevan tulkinnan mukaan nauti vastaavaa yksityisyyden suojaa verrattuna esimerkiksi yksityisten henkilöiden väliseen viestintään. Valtiollisen toimijan tietoliikenteen erottaminen ja toisaalta attribuution tekeminen ei aina ole siinä määrin suoraviivaista, että tämä olisi toteutettavissa alusta lähtien. Tästä syystä lainsäädäntömuutosten yhteydessä olisi arvioitava niiden suhdetta esimerkiksi viestinnän luottamuksellisuuteen ja oikeusturvakeinojen toteutumiseen. Myös viranomaisten toiminnan valvonnan merkitys ja oikeusturvan takeet korostuvat toimivaltuuksien ja kybertoimintaympäristön tiedonhankintaan liittyvien muutosten valmistelussa.

Suomeen kohdistuvassa kybervakoilussa ja vihamielisessä vaikuttamisessa käytettävien hyökkäyslaitteiden ketjutukset muuttuvat nopeasti, mikä aiheuttaa tiedonhankinnassa kohdistamisongelman. Tiedonhankinnan lupaedellytyksenä olevassa kohdentamisessa olisi voitava ottaa huomioon laitteiden looginen kokonaisuus yksittäisten telepäätelaitteiden, teleosoitteiden ja henkilöiden lisäksi.

Tiedustelumenetelmän lupavaatimukseen olisi voitava yksilöidä esimerkiksi jokin sellainen laite tai muu ohjelmisto tai järjestelmä, jonka on havaittu kuuluvan kyseiseen kokonaisuuteen, jolloin tämän ketjun lähtöpisteen yksilöinti voisi jo antaa oikeuden tiedusteluviranomaiselle kohdentaa tiedonhankintansa laitteisiin sekä virtuaalisiin ohjelmistoihin ja järjestelmiin, jotka vakoilu- tai vihamielisessä vaikuttamistarkoituksessa kommunikoivat tai ovat ketjuuntuneet lähtöpisteen kanssa.

Tietoliikenteen teknisten tietojen käsittelyssä saadulla tiedolla on välitön vaikutus tietoliikennetiedustelulla toteutettavaan tiedonhankintaan ja erityisesti sen kohdentamiseen. Nykysääntelyä olisi arvioitava saatujen kokemusten valossa, ja sääntelyssä toimivaltuudelle olisi harkittava muita rajoitteita kuin pelkkä ajallisuus. Samoin kerättyjä teknisiä tietoja olisi voitava hyödyntää nykysääntelyä paremmin tiedustelun kohdentamiseksi viestintäverkon osaa ja niissä tapahtuvia muutoksia tarkemmalle tasolle.

5.7 Viranomaisverkkojen suojaus

Viranomaisverkoilla tarkoitetaan erityisesti keskeisten turvallisuudesta vastaavien viranomaisten käyttöön rakennettua yhteistä viestintäverkkoa. Laajemmin tarkasteluna viranomaisverkoilla voidaan myös tarkoittaa keskitettyjä julkisen hallinnon viranomaisten käyttöön rakennettuja tai erotettuja tieto- ja viestintäteknisiä palveluja. Viranomaisverkoista säädetään muun muassa TUVE-, TORI- sekä SVPL -laeilla.

Viranomaisten käyttöön erotetuissa viranomaisverkoissa käsitellään laajasti viranomaistoiminnoissa tarvittavaa ja myös kansalaisia koskevaa tietoa. Viranomaisverkkojen ja niissä käsiteltävän tiedon suojaaminen edellyttää merkittävästi resursseja sekä yhteistoimintaa viranomaisverkkojen yhteisten palvelujen tuottajien ja käyttäjien, muiden viranomaisten sekä kaupallisia tietoturvapalveluja tuottavien yritysten kesken. Viranomaisverkkoihin kohdistuvan uhkan voidaan arvioida olevan korkeampi kuin yleisesti saatavilla oleviin palveluihin kohdistuvien uhkien, ja on syytä olettaa, että valtiolliset toimijat kohdentavat viranomaisverkkoja vastaan räätälöityjä ja korkeasti resursoituja operaatioitaan. Tällaisten operaatioiden havaitseminen ei ole tyypillisesti mahdollista kaupallisiin, vakiomuotoisiin ratkaisuihin tukeutumalla.

Voimassa olevan lainsäädännön mukaiset viranomaisten toimivaltuudet mahdollistavat viranomaisten tehokkaan yhteistoiminnan ja tiedonvaihdon viranomaisverkkojen suojaamiseksi vain rajallisesti. Esimerkiksi TUVE-lain mukaisesti Puolustusvoimat, poliisi, Rajavartiolaitos ja Liikenne- ja viestintävirasto ovat valtiovarainministeriön pyynnöstä velvollisia mahdollisuuksiensa mukaan antamaan virka-apua turvallisuusverkon häiriöttömän toiminnan takaamiseksi. Virka-apu on kuitenkin aina luonteeltaan tilapäistä ja

ehdollista eikä sen varaan voida rakentaa jatkuvaa yhteistoimintaa, eikä se ilman nimenomaista sääntelyä mahdollista salassa pidettävän tiedon luovuttamista virka-avun antajalta virka-avun pyytäjälle.

Valtiovarainministeriön tekemissä turvallisuusverkon tietoturvasuojauksen parantamista koskevissa selvityksissä on nostettu esiin Puolustusvoimille säädettävä mahdollisuus osallistua turvallisuusverkon kyberturvallisuuden varmistamiseen. On myös huomattava, että viranomaisverkkojen palveluntuottajat voivat halutessaan vapaasti hankkia tietoturvallisuuspalveluita yksityisiltä palveluntuottajilta, mutta eivät vastaavasti muilta viranomaisilta.

Nykytilassa viranomaisverkkojen ja niissä käsiteltävän tiedon suojaamisen vastuut jakautuvat palvelujen tuottajille ja palveluja käyttäville viranomaisille. Vastuita on määritelty myös tietosuojan ja tietoturvan osalta palvelujen käyttöä koskevissa sopimuksissa ja tietoturvaa koskevan yleislainsäädännön perusteella. TUVE- ja TORI-laeissa säädettyjen yhteisten palvelujen tuottajien ja toisaalta palvelujen käyttäjäviranomaisten tietoturvallisuuden hallintaan ja tietosuojaan liittyvien vastuiden jakautumiseen liittyy kuitenkin kysymyksiä, joita tulisi analysoida tarkemmin palvelukohtaisesti. Valtorin tehtäviin puolestaan liittyy myös kysymys henkilötietojen käsittelystä, mikä on nykytilassa epäselvä.

Kehittämisehdotukset

Valtiovarainministeriön ja Puolustusvoimien vuonna 2019 tekemässä selvityksessä todettiin, että olisi tarkoituksenmukaista säätää Puolustusvoimille rooli myös turvallisuusverkon tietoturvapalvelujen tuottajana, joka antaisi Puolustusvoimille mahdollisuuden tarjota turvallisuusverkon suojaamiseksi tarvittavia tietoturvallisuuspalveluja. Tehtäviin kuuluisi muun muassa SVPL:ssä kuvattujen toimenpiteiden suorittamista tietoturvan toteuttamiseksi viranomaisverkon palvelutuottajan hallinnoimissa yhteisissä palveluissa ja niihin liittyvissä laitteissa ja erikseen asianomaisen viranomaisen kanssa sovittaessa viranomaisen tietojärjestelmissä ja laitteissa. Lisäksi tehtäviin kuuluisi tietoturvaloukkauksia ja -uhkia koskevien tietojen analysointia turvallisuusverkon ja sen käyttäjien palvelujen suojaamiseksi tietoturvauhkilta sekä turvallisuusverkon palvelujen toimivuutta ja tietoturvallisuutta koskevan tilannetietoisuuden ylläpitämiseksi. Tehtävien määrittämiseksi tarvitaan vielä lisäarviointia muun muassa siitä, miten suunnitellut toimenpiteet suhtautuvat SVPL:n mukaisiin toimivaltuuksiin ja tarvitaanko mahdollisesti täydentävää lainsäädäntöä.

Turvallisuusverkon osalta tulisi arvioida tarve säätää TUVE-laissa erikseen turvallisuusverkon palvelujen tuottajien, käyttäjäorganisaatioiden ja Puolustusvoimien välisestä tiedonvaihdosta ottaen huomioon myös mahdollisuus luovuttaa välitystietoja ja haittaohjelmia sisältävä viestejä, sillä niitä ei voida luovuttaa yleisluontoisten

tiedonluovutusoikeuksien perusteella. Viranomaisverkkojen suojaamiseksi tarvittavan viranomaisten välisen tiedonvaihdon kehittämisen lisäksi on viranomaisten ja kaupallisten tietoturvapalveluja ja tieto- ja viestintätekniikkapalveluja tarjoavien yritysten yhteistoiminnan parantamiseksi käynnistettävä tarvittavat tiedonvaihdon, kybertilannekuvan muodostamisen ja uhkatiedon käsittelyn mahdollistavat lainsäädännölliset toimet.

Valtorin tietoturvallisuuden hallintaan liittyvät tiedonvaihtovelvoitteet ja -oikeudet TUVE- ja TORI-palveluiden osalta tulisi täsmentää ja säätää niistä lainsäädännöllä. Tarkastelun tulisi kattaa myös luottamuksellisen viestinnän suojan, henkilötietojen suojan ja yksityisyyden suojan toteutuminen sekä erityisesti niihin liittyvien käsittelyoikeuksien tarkentaminen eri rooleissa turvallisuusverkkotoiminnassa. Samalla on tarpeen täsmentää Valtorin tietoturvallisuuden hallintaan liittyvät palvelut ja kuvata ne palvelukuvauksin.

6 Johtopäätökset

Työryhmän selvitystyön perusteella seuraavilla kehittämistoimenpiteillä voitaisiin parantaa viranomaisten toimintaedellytyksiä suojata kansallista kyberturvallisuutta, torjua vakavaa kyberrikollisuutta ja kehittää kyberpuolustusta vastaamaan kehittyvän kyberuhkaympäristön tuomiin vaatimuksiin.

6.1 Nopeasti toimeenpantavat kehittämistoimenpiteet

1. Määritellään strateginen tavoitetila
   - Uudistetaan Suomen kyberturvallisuusstrategia, jossa määritellään kansallinen tavoitetila ja otetaan huomioon muutokset turvallisuusympäristössä, vastataan EU-lainsäädännön vaatimuksiin sekä määritellään tavoitteet EU:n ja Naton puitteissa tehtävälle kyberyhteistyölle.
   - Strategiatyön osana valmistellaan kyberpuolustusdoktriini.

2. Parannetaan viranomaisten yhteistoimintaa ja prosesseja
   - Luodaan pysyvä viranomaisyhteistyörakenne jo olemassa olevien valtioneuvostotason ja teknisen asiantuntijatason väliselle virastotasolle.
   - Selkeytetään viranomaisten yhteistyön koordinaatiota, kehitetään tiedonvaihtoa sekä kuvataan ja vakiinnutetaan eri kybertoimintaympäristöön liittyvät viranomaisprosessit.

3. Tehostetaan tilannekuvan tuottamista ja jakamista
   - Kehitetään ja vakiinnutetaan jatkuvan tilannekuvan tuottamisen ja jakamisen viranomaisprosessi.
   - Otetaan tietoturvapoikkeamista ilmoittaminen paremmin osaksi yksityisten palveluntuottajien kanssa tehtäviä sopimuksia.
   - Tehostetaan tiedon jakamista vakavista kyberuhista sekä tietoturvahäiriöistä ja poikkeamista tarkoituksenmukaisella tavalla myös huoltovarmuuskriittisille yrityksille, hyvinvointialueille ja kunnille sekä kuntaomisteisille palveluntarjoajille, huomioiden tiedon turvaluokat.
   - Tunnistetaan yhteiskunnan elintärkeitä toimintoja tuottavat tahot toimitusketjuineen.

4. Kehitetään yhdessä viranomaisten välistä tiedonvaihtoa kaksisuuntaiseksi, käyttötarkoitussidonnaiseksi ja organisaatioiden väliseksi voimassa olevan lainsäädännön puitteissa.
   - Jatketaan olemassa olevien toimintamallien ja prosessien kehittämistä.
   - Arvioidaan viranomaisten tiedonvaihtoon liittyvien rajoitteiden merkitys muuttuneessa turvallisuusympäristössä, keskeisten käsitteiden sisältö laeissa sekä niiden tulkintaan liittyvät reunaehdot ja mahdolliset muutostarpeet.
   - Luodaan korkeasti turvaluokitellun tiedon jakamiseen soveltuva yhteinen viestintäjärjestelmä.

5. Käynnistetään kyberturvallisuuden sanaston päivittäminen.

6.2 Lainsäädäntömuutoksia vaativat kehittämistoimenpiteet

Työryhmä ehdottaa seuraavia lainsäädäntömuutoksia edellyttäviä kehittämistoimenpiteitä:

6. Kybertoimintaympäristön suojaamiseen liittyvän tiedonvaihdon tehostaminen
   - Suositellaan annettavaksi uudelleen rauennut hallituksen esitys (HE 243/2022 p) viranomaisten yhteistoiminnan edistämiseksi yhteiskunnan toiminnan kannalta vakavissa tietoturvaloukkaustilanteissa.
   - Mahdollistetaan Puolustusvoimien, poliisin, suojelupoliisin ja Liikenne- ja viestintäviraston tiedon koordinoitu tuottaminen, analysointi ja jakaminen yhteisen tilanneymmärryksen muodostamiseksi.
   - Arvioidaan HAVARO-järjestelmän tuottamien tietojen laajempaa hyödyntämistä.
   - Arvioidaan kohdassa 2. mainitun pysyvän viranomaisyhteistyörakenteen tehokkaan toiminnan mahdollisesti vaatimia lainsäädäntömuutostarpeita.
   - Parannetaan tietoturvaloukkauksiin liittyvien ilmoitusten nojalla luovutettujen tietojen jakamista viranomaisten välillä nykyistä laajemmin.
   - Selvitetään, tulisiko perinteisille teleyrityksille säädettyä velvollisuutta avustaa viranomaisia korvausta vastaan laajentaa koskemaan muita merkittäviä palveluntarjoajia.

7. Otetaan kybertoimintaympäristön haasteet huomioon jo käynnissä olevassa valmiuslainsäädännön uudistuksessa.

8. Viranomaisverkkojen ja yhteisten palveluiden kyberturvallisuuden parantaminen
   - Luodaan edellytykset turvallisuusverkon suojaamiselle siten, että suojaamiseen voivat osallistua siihen soveltuvat viranomaiset kuten Puolustusvoimat.
   - Huomioidaan myös Valtorin TORI-palvelujen suojauksen parantaminen ja täsmennetään Valtorin tietoturvallisuuden hallintaan liittyviä tiedonvaihtovelvoitteita ja -oikeuksia.

9. Poliisin toimintaedellytykset kybertoimintaympäristössä
   - Arvioidaan poliisin toimivaltuuksia sekä tiedonvaihdon ja tietojen luovutuksen edellytyksiä.
   - Arvioidaan esitutkinnan toimittamisvelvollisuuden rajaamista sekä oikeutta olla toimittamatta tai lopettaa esitutkinta tietyissä tapauksissa.
   - Luodaan edellytykset tiedonluovuttajalle asettaa rajoitteita tietojen edelleen käytölle.
   - Huomioidaan rikostiedustelua koskevan selvityksen ehdotukset kybertoimintaympäristöön liittyen.

10. Puolustusvoimien toimintaedellytykset kybertoimintaympäristössä
    - Luodaan Puolustusvoimien kyberpuolustustehtävät mahdollistava lainsäädäntö mukaan lukien riittävät toimivaltuudet sekä tiedonvaihdon ja tietojen luovutuksen edellytykset.
    - Kehitetään Puolustusvoimien virka-apua ja avun antamista yhteiskunnan elintärkeitä toimintoja tuottaville tahoille tietyissä tilanteissa.
    - Otetaan huomioon Nato-jäsenyyden ja kollektiivisen puolustuksen edellyttämät säädösmuutostarpeet.

11. Tiedusteluviranomaisten toimintaedellytykset kybertoimintaympäristössä
    - Arvioidaan tiedusteluviranomaisten kybertoimivaltuuksia ja sen osana luodaan edellytykset tiedustelumenetelmien kohdistamiselle laitteiden ja virtuaalisten järjestelmien muodostamaan kokonaisuuteen.
    - Kehitetään palomuurisääntelyä riittävän tiedon luovuttamiseksi rikostorjuntaviranomaisille kansallisen turvallisuuden suojaamiseksi.
    - Kehitetään tietoliikennetiedustelun teknisten tietojen käsittelyä.

12. Arvioidaan tarvittavia lainsäädäntömuutoksia viranomaisten laajemmalle mahdollisuudelle avustaa yhteiskunnan toiminnan ja huoltovarmuuden kannalta kriittisten yritysten varautumista ja palautumista kyberpoikkeamien aiheuttamista vakavista häiriötilanteista.

SNELLMANINKATU 1, HELSINKI
PL 23, 00023 VALTIONEUVOSTO
valtioneuvosto.fi
julkaisut.valtioneuvosto.fi

ISBN: 978-952-383-542-9 PDF
ISSN: 2490-0966 PDF