

Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta

Jarno Limnéll

Kansanedustajien arvioita Suomen kyberturvallisuuden nykytilasta ja tulevaisuudesta

Jarno Limnell

Jarno Limnell

Professori, Kyberturvallisuus

Aalto-yliopisto

jarno.limnell@aalto.fi

Tel. +358-40-5276173

Aalto-yliopiston julkaisusarja
TIEDE + TEKNOLOGIA 1/2016

© Jarno Limnell

ISBN 978-952-60-6687-5 (pdf)

ISSN-L 1799-487X

ISSN 1799-487X (painettu)

ISSN 1799-4888 (pdf)

<http://urn.fi/URN:ISBN:978-952-60-6687-5>

Unigrafia Oy

Helsinki

2016

Julkaisutilaukset:

jarno.limnell@aalto.fi

Sisältö

1.	Johdanto	3
2.	Tutkimuksen tavoite ja kyselyn toteutus.....	5
3.	Kyselyn vastaukset.....	9
3.1	Suomen edelläkävijyys kyberturvallisuudessa	9
3.2	Kyberuhkiin varautuminen.....	10
3.3	Vakava kyberhyökkäys Suomen kriittiseen infrastruktuuriin	10
3.4	Poliisin, Puolustusvoimien ja Viestintäviraston kyvykkyys.....	11
3.5	Lainsäädännön ajanmukaisuus	12
3.6	Kansalaisten turvallisuus ja perusoikeuksien toteutuminen...	12
3.7	Tietoisuuden taso.....	13
3.8	Liiketoiminnallinen mahdollisuus suomalaisille yrityksille....	14
3.9	Kiinnostus kansanedustajien käsittelemään tietoon.....	14
3.10	Vapaa sana, avoin palaute.....	15
4.	Johtopäätöksiä.....	16
	Lähdeluettelo	19
	Liite (kyselyn saatekirje).....	21

1. Johdanto

Kyberturvallisuus on tämän päivän suomalaisessa yhteiskunnassa, liiketoiminnassa ja kansalaisten arjessa erottamaton osa turvallisuutta. Kyberturvallisuuden käsite itsessään on kuitenkin edelleen epäselvä¹, mikä osaltaan kuvastaa meneillään olevan digitaalisen turvallisuuskulttuurin muutosvaihetta. Kyberturvallisuudesta kuitenkin puhutaan ja aiheesta uutisoidaan Suomessa tänä päivänä aktiivisesti.

Kyberturvallisuudella voi arvioida olevan kaksi lähtökohtaista haastetta. Ensinnäkin kyberturvallisuudesta, digitaalisen toimintaympäristön turvallisuutena, keskustellaan edelleen varsin teknologiapainotteisesti. Teknologiaa ja teknisiä ratkaisuja luonnollisesti kyberturvallisuuden parantamiseksi tarvitaan, mutta tämän päivän Suomessa kyberturvallisuus tulee ymmärtää ensisijaisesti strategisena ja vahvaa poliittista ohjausta vaativana asiana. Kyberturvallisuuden asiat ovat esimerkiksi yksi erottamaton osa Suomen ulko-, puolustus- ja turvallisuuspolitiikkaa. Poliittisten linjausten ja strategioiden tulee määrittää kyberturvallisuuden kokonaisuuden kehittämistä. Tämän takia voi pitää myönteisenä, että Suomessa julkaistiin vuonna 2013 kansallinen Kyberturvallisuusstrategia, jolla pyritään kokonaisvaltaisesti kehittämään suomalaisen yhteiskunnan kyberturvallisuutta. Hieman yksinkertaisten kyberturvallisuuden kehittämistä voi kuvata taulukon 1 mukaisesti, jossa korostuu ”ylhäältä-alas” ohjaavuuden ja sitoutuneisuuden merkitys.



Taulukko 1. Kyberturvallisuuden poliittinen ja strateginen kehittäminen.

¹ Limnell, Kyber rantautui Suomeen.

Toiseksi, kyberturvallisuudesta keskustellaan usein hyvin uhkapainotteisesti. Uhkien lukumäärän ja kehittyneisyyden sekä vaikutusten vakavuuden voi arvioida kasvavan entisestään lähivuosina digitaalisen riippuvuuden kasvaessa², mutta samalla on tärkeää ymmärtää digitaalinen toimintaympäristö myös mahdollisuutena ja voimavarana. Lähtökohtaisesti digitaalisen toimintaympäristön turvallisuus tulee ymmärtää sekä digitalisaation ja nopeasti kehittyvän teknologian³ sekä välttämättömyytenä että etenkin mahdollistajana täysimää-
räisten hyötyjen saavuttamiseksi. Vuonna 2016 julkaistussa Suomen tietotur-
vallisuusstrategiassa nostetaankin digitaalinen toimintaympäristö positiivi-
sena mahdollisuutena esille, kun strategian visioksi määritellään ”Maailman
luotetuin digitaalinen liiketoiminta tulee Suomesta.”⁴

*Tutkimuksen lähtökohtana ja motiivina oli selvittää Suomen poliittisten
päättäjien näkemyksiä Suomen kyberturvallisuuden nykytilasta ja tulevai-
suudesta. Tutkimus pyrkii lisäämään tarpeellista strategista ja poliittista sekä
myös positiivista keskustelua kyberturvallisuuden kehittämisestä suomalai-
sessa yhteiskunnassa.*

² Ks. mm. Suomen kansallinen riskiarvio 2015.

³ Ks. Teknologian kehityksestä ja digitalisaatiosta mm. Megatrendit 2016.

⁴ Suomen tietoturvallisuusstrategia, s. 3.

2. Tutkimuksen tavoite ja kyselyn toteutus

Tutkimuksen tavoitteena oli selvittää Suomen poliittisten päättäjien näkemyksiä kyberturvallisuuden nykytilasta ja tulevaisuudesta Suomessa. Tutkimuksen kohderyhmä rajattiin kansanedustajiin (200) ja heidän näkemystensä selvittämiseen. Tietojen kerääminen tehtiin internetin kautta toteutetulla kyselyllä. Kyselytutkimusta voi pitää perusteltuna tiedon keräämisen metodina, sillä esimerkiksi kansanedustajien haastatteleminen olisi käytännössä ollut hyvin haastava toteuttaa. Kyselyn tulosten analyysissä ja raportoinnissa käytettiin hyväksi Webropol-kyselytyökalua.

Kansanedustajia motivoitiin vastaamaan kyselyyn kahdella tapaa. Ensinnä, kyselytutkimus tehtiin lyhyeksi (15 kysymystä⁵) ja kysymyksiin vastaaminen tapahtui monivalintavaihtoehtoina (asteikolla 1-9). Kysymysten lopussa oli ”vapaa sana, avoin palaute” -kenttä, johon vastaajilla oli mahdollisuus kirjoittaa kommenttejaan ja ajatuksiaan vapaamuotoisesti. Kysely toteutettiin verkkokyselynä, webropol-kyselytyökalua hyödyntäen, mikä mahdollisti kyselyyn vastaamisen vaivattomasti millä tahansa vastaajan käyttämällä äylaitteella tai tietokoneella. Toisena vastaajien motivointikeinona korostettiin kyselyn saatekirjeessä⁶ aiheen yhteiskunnallista merkityksellisyttä ja vastaamisen tärkeyttä sekä vastaamisen nopeutta.

Kyselytutkimus toteutettiin anonymisti eli vastaajien henkilöllisyyttä ei tuoda tutkimustuloksissa esille. Tämä luvattiin vastaajille kyselyn saatekirjeessä. Anonymiteetin arvioitiin lisäävän vastaamisen aktiivisuutta.

Koska ”kyberturvallisuus” on käsitteenä edelleen varsin epäselvä, kyselyn saatteessa kyberturvallisuus kuvattiin seuraavasti: ”Yksinkertaistaen kybertur-

⁵ Kysymysten muotoilemiseen osallistui laaja joukko yhteistyötahoja. Erityisesti kiitän Turvallisuuskomitean sihteeristöä, Liikenne- ja viestintäministeriön asiantuntijoita sekä FISC ry:n johon henkilöitä.

⁶ Liite 1.

vallisuuden voi ajatella tarkoittavan digitaalisen toimintaympäristön turvallisuutta. Suomen kyberturvallisuusstrategian mukaan kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.”

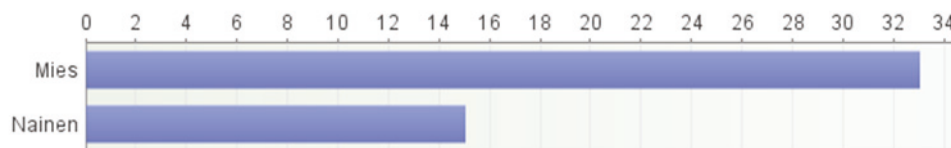
Kysely lähetettiin sähköpostina (saatekirje ja linkki kyselyyn) kansanedustajille 13.1.2016 kansanedustajien etunimi.sukunimi@eduskunta.fi -sähköpostiosoitteisiin. Vastaamatta jättäneille kansanedustajille lähetettiin kaksi muistutusviestiä sähköpostitse 26.1.2016 ja 1.2.2016. Kysely suljettiin 8.2.2016.

Kyselyyn vastasi 48 kansanedustajaa. Kyselyn vastausprosentti oli siten 24 prosenttia, mitä voi pitää riittävänä johtopäätösten tekemiseen. Kyselyn johtopäätöksissä on tosin otettava huomioon, että kyselyyn ei vastannut 152 kansanedustajaa. Webropol-kyselytyökalun analyysin mukaan vastanneiden kansanedustajien lisäksi kyselyn avasi (painoi saatteessa ollutta linkkiä kyselyyn) 47 kansanedustajaa, mutta he eivät vastanneet kyselyyn.

Vastaajien taustatietoina kysyttiin kahta asiaa: sukupuolta sekä puoluekanta.

1. Olen

Vastaajien määrä: 48



Taulukko 2. Vastaajien sukupuolijakauma.

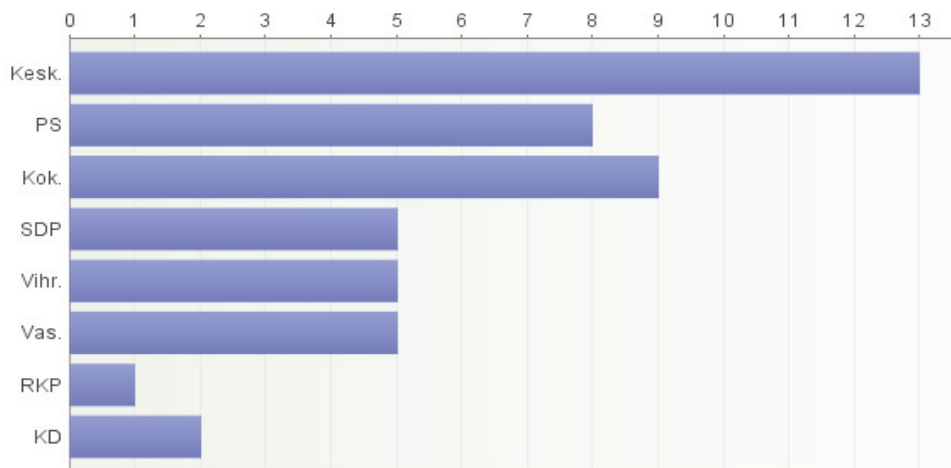
Vastaajien sukupuolijakauma on prosentteina: miehet 68,75 prosenttia ja naiskansanedustajat 31,25 prosenttia. Kun vastaajien määrän sukupuolen perusteella suhteuttaa kaikkiin kansanedustajiin⁷, on mieskansanedustajien vastausprosentti 28,2 prosenttia ja naiskansanedustajien 18,1 prosenttia. Mieskansanedustajat olivat siten aktiivisempia kyselyyn vastaajia.

⁷ Tilanne kyselyn sulkeutumishetkenä (8.2.2016), 117 mies- ja 83 naiskansanedustajaa. Eduskunta 2016.

Vastaajien puoluekanta jakaantui seuraavasti:

2. Puolueeni on

Vastaajien määrä: 48



Taulukko 3. Vastaajien puoluekanta.

Kaikista vastanneista (48) puolueiden prosenttiosuudet jakaantuvat seuraavasti: Suomen keskusta 27,08 %, Perussuomalaiset 16,67 %, Kansallinen Kokoomus 18,75 %, Suomen Sosiaalidemokraattinen puolue 10,42 %, Vihreä Liitto 10,42 %, Vasemmistoliitto 10,42 %, Suomen Ruotsalainen Kansanpuolue 2,08 % ja Suomen Kristillisdemokraatit 4,12 %.

Vastaajien määrää puolueittain suhteutettaessa puolueiden eduskuntaryhmien voimasuhteisiin⁸, voidaan vastaamisaktiivisuutta tulkita seuraavasti.

Suomen Keskusta: vastaajia 13, kansanedustajia 49, vastausprosentti 26,5.

Perussuomalaiset: vastaajia 8, kansanedustajia 38, vastausprosentti 21,1.

Kansallinen Kokoomus: vastaajia 9, kansanedustajia 37, vastausprosentti 24,3.

Suomen Sosiaalidemokraattinen Puolue: vastaajia 5, kansanedustajia 34, vastausprosentti 14,7.

Vihreä Liitto: vastaajia 5, kansanedustajia 15, vastausprosentti 33,3.

Vasemmistoliitto: vastaajia 5, kansanedustajia 12, vastausprosentti 41,7 prosenttia.

⁸ Eduskunta 2016.

Suomen Ruotsalainen Kansanpuolue: vastaajia 1, kansanedustajia 10, vastausprosentti 10.

Suomen Kristillisdemokraatit: vastaajia 2, kansanedustajia 5, vastausprosentti 40.

Puolueiden kansanedustajien yhteismäärään suhteutettuna korkein vastausprosentti oli Vasemmistoliiton ja Suomen Kristillisdemokraattien kansanedustajilla. Myönteisenä voi tutkimustulosten kannalta pitää, että kaikista eduskuntapuolueista kyselyyn vastasi vähintään yksi kansanedustaja, joten tutkimustuloksissa on kaikki eduskuntapuolueet edustettuina. Vastaajien voi arvioida edustavan niitä kansanedustajia, jotka ovat normaalia kiinnostuneempia kyberturvallisuuden asioista ja vaikuttavan näihin asioihin eduskunnassa. Kyselyn anonymiteetin takia tähän johtopäätökseen tulee kuitenkin suhtautua varauksella. Vastaajien itsensä mielestä heidän oma tietämyksensä taso kyberturvallisuuteen liittyvissä asioissa on suhteellisen korkea.⁹

⁹ Kyselytutkimuksen kysymyksen 15 vastaukset, jotka esitetään myöhemmin tässä tutkimusraportissa.

3. Kyselyn vastaukset

Kyselyn varsinaisissa kysymyksissä (13) painottuivat Suomen kyberturvallisuusstrategiassa esitetyt kymmenen strategista linjausta¹⁰ sekä kyberturvallisuuden ajankohtaisaiheet. Kyselyn tiivistäminen yhteensä 15 monivalintakysymykseen oli haasteellista, mutta tarpeellista vastausprosentin saamiseksi mahdollisimman korkeaksi.

3.1 Suomen edelläkävijyys kyberturvallisuudessa

Suomen Kyberturvallisuusstrategian visiossa ”vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.”¹¹ Kyselytutkimuksessa kysyttiin kansanedustajien näkemystä tavoitteen saavuttamisesta. Vastaukset jakaantuivat seuraavasti.

3. Vuoden 2013 Kyberturvallisuusstrategiassa asetettiin tavoite, että Suomi on kyberturvallisuudessa maailmanlaajuinen edelläkävijä vuonna 2016. Miten tavoite on mielestänne saavutettu?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huonosti - 9 = erittäin hyvin	1	1	11	10	10	6	9	0	0	48	4,69

Taulukko 4. Kyberturvallisuuden edelläkävijyyden saavuttaminen.

Huomioitavaa vastauksissa on, että keskivälille (vastausvaihtoehdot 4-7) annettujen vastausten prosentuaalinen osuus on yhteensä 73 prosenttia. Jos tähän lisää vastausvaihtoehdon kolme, on vastausvaihtoehtojen 3-7 prosentuaalinen osuus yhteensä 95,9 prosenttia. Yksikään vastanneista ei antanut arvoa 8 tai 9. Vastausten perusteella kansanedustajat eivät koe Suomen saavuttaneen kyberturvallisuuden maailmanlaajuista edelläkävijyyttä ”erittäin hyvin”. Vastaajien keskiarvona tavoite on saavutettu ”arvosanalla” 4,69.

¹⁰ Suomen kyberturvallisuusstrategia, 7-11.

¹¹ Ibid. 3.

Mieskansanedustajien vastausten keskiarvo on 4,8 ja naiskansanedustajien 4,3.

3.2 Kyberuhkiin varautuminen

Suomessa on viime vuosina käyty yhteiskunnallista keskustelua niin yhteiskunnan kuin yrityselämän varautumisesta erilaisiin kyberuhkiin. Kansanedustajilta kysyttiin heidän arviotaan kokonaisvarautumisen nykytasosta.

4. Mikä on arvionne, miten kyberturvallisuuden uhkiin on varauduttu suomalaisessa yhteiskunnassa ja yrityselämässä kokonaisuudessaan?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huonosti - 9 = erittäin hyvin	1	2	6	9	10	12	7	1	0	48	4,96

Taulukko 5. Arvio kyberuhkiin varautumisesta.

Vastaajat arvioivat varautumisen tasoa kokonaisuutena keskiarvolla 4,96 (asteikolla 1-9). Mieskansanedustajien vastausten keskiarvo on 5,2 ja naiskansanedustajien 4,3. Mieskansanedustajat arvioivat siten varautumisen tason korkeammaksi kuin naiskansanedustajat.

3.3 Vakava kyberhyökkäys Suomen kriittiseen infrastruktuuriin

Julkisessa keskustelussa niin Suomessa kuin kansainvälisesti on esitetty erilaisia arvioita mahdollisesta digitaalisen toimintaympäristön kautta kriittiseen infrastruktuuriin suuntautuvan hyökkäyksen mahdollisuudesta. Ajankohittaiseksi keskustelun on tehnyt Ukrainassa tapahtunut sähkökatko joulukuussa 2015, jossa ainakin osatekijänä on ollut haittaohjelma.¹²

Kyselyssä kysyttiin kansanedustajien arviota Suomen kriittiseen infrastruktuuriin kohdistuvan vakavan kyberhyökkäyksen todennäköisyydestä seuraavan kolmen vuoden aikana.

5. Miten todennäköisenä pidätte, että Suomen kriittiseen infrastruktuuriin kohdistuu vakava kyberhyökkäys seuraavan kolmen vuoden aikana?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin epätodennäköinen - 9 = erittäin todennäköinen	0	3	6	2	7	8	11	9	2	48	5,88

Taulukko 6. Vakavan kyberhyökkäyksen todennäköisyys.

¹² Ks. esim. "Yhdysvallat tutkii Ukrainan joulukuista sähkökatkosta – Ukraina syyttää venäläisiä hakkereita", Yleisradio 13.1.2016.

Huomioitavaa on, että vastaajista lähes puolet (45,9 prosenttia) piti todennäköisyyttä korkeana (vastausvaihtoehdot 7-9). Vastausten voi tulkita poliittisesti viestivän tarpeellisuudesta kiinnittää erityinen huomio kriittisen infrastruktuurin suojaamiseen kyberuhkia vastaan.

3.4 Poliisin, Puolustusvoimien ja Viestintäviraston kyvykkyys

Kyselyssä selvitettiin kansanedustajien arvioita kolmen viranomaisen kyvykkyudesta digitaalisessa toimintaympäristössä. Suomen kyberturvallisuusstrategian strategisissa linjauksissa todetaan, että:

- Huolehditaan, että poliisilla on tehokkaat edellytykset ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.
- Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.
- Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilan-tietoisuutta ja tilanneymmärrystä.¹³

6. Mikä on arvionne Poliisin kyvystä ja mahdollisuuksista torjua kyberrikollisuutta?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huono - 9 = erittäin hyvä	1	2	5	13	12	6	7	2	0	48	4,85

7. Mikä on arvionne Puolustusvoimien kokonaisvaltaisen kyberpuolustuskyvyn tasosta?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huono - 9 = erittäin hyvä	1	0	1	6	8	14	9	8	1	48	6

8. Mikä on arvionne Viestintäviraston kyvystä kerätä ja jakaa tietoa tietoturvaloukkauksista?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huono - 9 = erittäin hyvä	0	1	5	11	8	9	10	4	0	48	5,35

Taulukko 7. Arvio Poliisin, Puolustusvoimien ja Viestintäviraston kyvykkyudesta.

Poliisin kykyä ja mahdollisuutta torjua kyberrikollisuutta vastaajat arvioivat keskiarvolla 4,85. Mieskansanedustajien arvio (keskiarvo 5,0) on naiskansanedustajien arviota (keskiarvo 4,5) korkeampi.

Puolustusvoimien kokonaisvaltaisen kyberpuolustuskyvyn (tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyt) tasoksi kansanedustajat arvioivat

¹³ Suomen kyberturvallisuusstrategia, 7-8.

6,0 (asteikolla 1-9). Huomioitavaa on, että mieskansanedustajien vastausten keskiarvo 6,3 on naiskansanedustajien keskiarvoa (5,4) korkeampi. Huomioitavaa myös on, että vastauksissa molemmat vastausvaihtoehtojen ääri vaihtoehdot (1 ja 9) saivat arvion osakseen.

Viestintäviraston kykyä kerätä ja jakaa tietoa tietoturvaloukkauksista arvioitiin keskiarvolla 5,35. Naiskansanedustajien vastausten keskiarvo (4,93) on mieskansanedustajien arviota (5,55) alhaisempi.

3.5 Lainsäädännön ajanmukaisuus

Suomen kyberturvallisuusstrategia korostaa yhtenä strategisena linjauksena kansallisen lainsäädännön merkitystä tehokkaan kyberturvallisuuden toteuttamisen edellytyksenä.¹⁴ Kyselyssä kysyttiin kansanedustajien arviota kyberturvallisuuteen liittyvän lainsäädännön ajan tasaisuudesta.

9. Onko kyberturvallisuuteen liittyvä lainsäädäntö mielestänne Suomessa ajan tasalla?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huonosti - 9 = erittäin hyvin	2	6	13	8	7	5	1	6	0	48	4,27

Taulukko 8. Lainsäädännön ajantasaisuus.

Vastausten perusteella voi todeta, että kansanedustajat eivät pidä kyberturvallisuuteen liittyvää lainsäädäntöä kovinkaan ajan tasalla olevana. Vastausvaihtoehdot 1-4 muodostavat vastauksista 60,4 prosentin osuuden. Toisaalta on huomioitava, että vastaajista 16,7 prosenttia arvioi lainsäädännön ajantasaisuuden korkeaksi (vastausvaihtoehto 8). Mieskansanedustajien vastausten keskiarvo (4,06) on alhaisempi verrattuna naiskansanedustajien vastausten keskiarvoon (4,73).

3.6 Kansalaisten turvallisuus ja perusoikeuksien toteutuminen

Kyselyssä selvitettiin kansanedustajien näkemyksiä sekä digitaalisen toimintaympäristön vaikutuksista kansalaisten turvallisuuteen että kansalaisten yksityiselämän ja viestinnän luottamuksellisuuden suoja koskevien perusoikeuksien toteutumisesta digitaalisessa toimintaympäristössä.

¹⁴ Suomen kyberturvallisuusstrategia, 10.

10. Oletteko huolestunut digitaalisen toimintaympäristön vaikutuksista kansalaisten turvallisuuteen?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin vähän - 9 = erittäin paljon	0	0	2	3	3	5	13	11	11	48	7,1

11. Oletteko huolestunut kansalaisten yksityiselämän ja viestinnän luottamuksellisuuden suoja koskevien perusoikeuksien toteutumisesta digitaalisessa toimintaympäristössä?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin vähän - 9 = erittäin paljon	0	1	1	4	3	7	8	13	11	48	7,02

Taulukko 9. Kansalaisten turvallisuus ja perusoikeuksien toteutuminen.

Vastauksista ilmenee, että kansanedustajat ovat huolestuneita varsin korkealla keskiarvolla (7,1, mieskansanedustajat 7,06, naiskansanedustajat 7,2) digitaalisen toimintaympäristön vaikutuksista kansalaisten turvallisuuteen. Lähes samalla vastausten keskiarvolla (7,02, mieskansanedustajat 6,8, naiskansanedustajat 7,6) kansanedustajat ovat huolestuneita kansalaisten yksityiselämän ja viestinnän ja viestinnän luottamuksellisuuden suoja koskevista perusoikeuksien toteutumisesta digitaalisessa toimintaympäristössä. Turvallisuutta ja perusoikeuksien toteutumista ei tule nähdä vastakkainasetteluna vaan sekä turvallisuuden että perusoikeuksien toteutumisen huomioonottamisen tärkeenä digitaalisen toimintaympäristön ratkaisuja pohdittaessa.

3.7 Tietoisuuden taso

Kyberturvallisuuden yleisen tietoisuuden tasoa selvitettiin kyselyssä kahdella kysymyksellä. Ensinnäkin kysyttiin kansanedustajien arviota yleisestä kyberturvallisuuden tietoisuuden tasosta suomalaisessa yhteiskunnassa, ja toiseksi kysyttiin kansanedustajien arviota omasta tietämyksen tasosta.

12. Miten arvioitte yleistä kyberturvallisuuden tietoisuuden tasoa suomalaisessa yhteiskunnassa?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huono - 9 = erittäin hyvä	1	5	13	6	11	8	4	0	0	48	4,27

Taulukko 10. Arvio yleisestä kyberturvallisuuden tietoisuuden tasosta.

Kansanedustajien arvio kyberturvallisuuden yleisestä tietoisuudesta suomalaisessa yhteiskunnassa on suhteellisen heikko. Vastausten keskiarvoksi määritetty 4,27. Vastausvaihtoehtojen 1-4 osuus vastauksista on hieman yli puolet (52,1). Naiskansanedustajat (keskiarvo 3,7) pitävät tietoisuuden tasoa miehiä (keskiarvo 4,5) heikompana.

Kyselyn vastausten mukaan kansanedustajat arvioivat oman tietämyksensä yleistä yhteiskunnallista tietoisuuden tasoa korkeammalle.

15. Mikä on mielestänne oma tietämyksenne taso kyberturvallisuuteen liittyvissä asioissa?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = riittämätön - 9 = riittävä	0	1	4	6	7	12	13	5	0	48	5,75

Taulukko 11. Kansanedustajien arvio omasta tietoisuudesta.

Mies- (5,9) ja naiskansanedustajien (5,5) vastausten välillä ei ole suurta eroavaisuutta.

3.8 Liiketoiminnallinen mahdollisuus suomalaisille yrityksille

Kybertoimintaympäristön korostuminen merkitsee samalla ratkaisujen osalta lisääntyvää liiketoiminnallista aluetta. Kansanedustajat näkevät kyberturvallisuus-alan merkittävänä liiketoiminnallisena mahdollisuutena suomalaisille yrityksille.

13. Millaisena liiketoiminnallisena mahdollisuutena näette kyberturvallisuus-alan suomalaisille yrityksille?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin huonona - 9 = erittäin hyvänä	0	0	0	0	0	2	14	18	14	48	7,92

Taulukko 12. Kyberturvallisuus-ala liiketoiminnallisena mahdollisuutena.

Kansanedustajien vastausten keskiarvoa (7,92) on pidettävä hyvin korkeana. Mies- (7,91) ja naiskansanedustajien (7,93) vastaukset olivat lähes identtiset.

3.9 Kiinnostus kansanedustajien käsittelemään tietoon

Kansanedustajat arvioivat ulkopuolisen tahon¹⁵ kiinnostuksen kansanedustajien käsittelemää tietoa kohtaan suhteellisen korkeana uhkana.

14. Millaisena uhkana näette ulkoisen tahon kiinnostuksen kansanedustajien käsittelemää tietoa kohtaan?

Vastaajien määrä: 48

	1	2	3	4	5	6	7	8	9	Yhteensä	Keskiarvo
1 = erittäin vähäisenä - 9 = erittäin korkeana	0	0	4	9	6	6	9	10	4	48	6,1

Taulukko 13. Kiinnostus kansanedustajien käsittelemää tietoa kohtaan.

¹⁵ "Ulkopuolista tahoa" ei kyselytutkimuksessa määritelty tarkemmin.

Mieskansanedustajien arvio (keskiarvo 6,12) on hieman naiskansanedustajien arviota (keskiarvo 6,07) korkeampi.

3.10 Vapaa sana, avoin palaute

Kyselyn lopussa annettiin vastaajille mahdollisuus kirjoittaa vapaamuotoisesti ajatuksiaan ja kommenttejaan. Kahdeksan kansanedustajaa kommentoi kyselytutkimusta ja kyselyn aihepiiriä seuraavasti¹⁶:

- UM:n tapaus epäonnistui täydellisesti tiedottamisessa EKn ulkoasiainvaliokunnalle.
- Ongelman vakavuus käsitetään osittain, mutta ei sitä, että asian kuntoon saaminen vaatisi valtiolta olennaisesti suurempia taloudellisia panostuksia, jotka mielestäni tulisi tehdä asap. Kyberstrategiaa leimaa toiveajattelu ja lämmittely menneen erinomaisuuden jälkitulilla.
 - Hyvä & tärkeä kysely!
 - Tarvitsemme ajanmukaisen tiedustelulainsäädännön mahdollisimman pikaisesti.
 - Heräsimme myöhään, mutta nyt ollaan hyvän kehityksen vauhdissa.
 - Suomessa on riittävä tieto ja lainsäädäntö kyberturvallisuuden osalta. Ongelma on, ettei varautumiseen ja turvaamiseen ole riittävästi resursseja.
 - Tämän hetkinen keskustelu painottuu melkein kokonaan julkishallinnon kyberturvallisuuteen. Se on tietenkin tärkeää, mutta huomiota pitää kiinnittää enemmän yritysten ja sitä kautta kansalaisten kyberturvaan. Varsinkin erilaiset häiriötilanteet esim. laajat sähkökatkot, avaavat verkkoja hyökkäyksille ja aiheuttavat suuria vahinkoja ja turvattomuutta. Operaattoreiden vastuuta verkkojen toiminnasta tulee myös lisätä.
 - Puolustusvoimien ja poliisin osittain erilaisista intresseistä kyberturvallisuuden ja tiedonkeruun osalta pitäisi käydä nykyistä analyyttisempää keskustelua. Vaarana on, että kansalaisten tietosuojaan tulee aukkoja, jotka osaltaan vähentävät kokonaisturvallisuutta. Terrorismin uhkaa perusteena käyttäen voidaan tehdä kansalaisten perusoikeuksia loukkaavaa lainsäädäntöä.

¹⁶ Kirjoitetut kommentit esitetään tässä siinä muodossa kuin vastaajat ovat ne kirjoittaneet. Yhdessä kommentissa kansanedustajan henkilöllisyys tulee esille ja tämä kohta on poistettu esitetyistä kommentteista.

4. Johtopäätöksiä

Suomessa ei ole aiemmin selvitetty tässä laajuudessa kansanedustajien näkemyksiä kyberturvallisuudesta. Tutkimusta voi tässä mielessä pitää sekä tarpeellisenä että uutta tietoa esittävänä. Kyselytutkimus osoittautui varsin hyväksi ja tehokkaaksi tavaksi kerätä kansanedustajien näkemyksiä, joskin vastausprosentti olisi voinut olla korkeampi. Vastaajien kokonaismäärä (48) mahdollistaa kuitenkin johtopäätösten tekemisen ja niistä keskustelemisen.

Merkittävimpänä tutkimustuloksina on pidettävä seuraavia kolmea asiaa, jotka edellyttävät jatkopohdintoja ja tarpeellisia toimenpiteitä suomalaisessa yhteiskunnassa.

Ensinnä, kansanedustajien näkemysten mukaan Suomi ei ole saavuttanut kansallisessa kyberturvallisuusstrategiassa asetettua tavoitetta maailmanlaajuisesta edelläkävijyydestä kyberturvallisuudessa. Kansanedustajien vastauksen keskiarvon (4,69, asteikolla 1-9) edelläkävijyyden saavuttamisen kysymyksen voi arvioida ilmentävän, että Suomessa on kyberturvallisuusstrategian ilmentymisen jälkeen tehty hyviä ja tarpeellisia toimenpiteitä kyberturvallisuuden kehittämiseksi¹⁷, mutta maailmanlaajuisen edelläkävijyyden tavoitetta ei ole saavutettu. Nyt on tarpeellista laajemminkin pohtia askeleita eteenpäin sekä myös arvioida tarpeellisia toimenpiteitä edelläkävijyyden saavuttamiseksi, mikäli tavoite halutaan poliittisesti edelleen pitää voimassa. Helmi-kuussa 2016 julkaistussa ”Kyberosaaminen Suomessa” -selvitysraportin johtopäätöksissä todetaan osuvasti, että ”On päätettävä, halutaanko, että Suomi todella on globaali edelläkävijä kyberturvallisuudessa. Resurssit ja toimenpiteet tulee suhteuttaa asetettuun visioon ja tavoitteisiin.”¹⁸ Tämä edellyttää vahvaa poliittista sitoutuneisuutta ja tietoisuutta kyberturvallisuudesta sekä tarpeellista yhteiskunnallista keskustelua.

Toiseksi, tutkimuksen tuloksissa on erityisen huomionarvoisena pidettävä kansanedustajien hyvin myönteistä arviota kyberturvallisuus-alan liiketoiminnallisista mahdollisuuksista suomalaisille yrityksille (vastauksen keskiarvo 7,92 asteikolla 1-9). Suomessa onkin suhteellisesti katsottuna melko laaja kyberturvallisuuteen liittyvä yrityskehitys, ja alalla on vahvoja ja innovatiivisia

¹⁷ Suomalaisen yhteiskunnan kokonaisvarautumisen tason kyberuhkiin kansanedustajat arvioivat keskiarvolla 4,95 (asteikolla 1-9).

¹⁸ Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen, s. 66.

yrityksiä. Alan globaalin markkinoiden arvioidaan olevan lähivuosina voimakkaassa kasvussa¹⁹, mikä tarjoaa kasvavia mahdollisuuksia suomalaisille yrityksille. Suomalaisilla yrityksillä on myös vahva kansainvälinen luottamus pääoma puolellaan. Nyt on tarpeellista pohtia niin yhteiskunnan kuin suomalaisen yrityskentän näkökulmista niitä toimenpiteitä, joilla suomalaisyrityksien menestymisen mahdollisuuksia voidaan parantaa. Poliittinen tahtotila ilmenee tämän tutkimuksen perusteella voimakkaana.

Kolmanneksi, digitalisaatio on läpäissyt tänä päivänä jo lähes kaikki suomalaisen yhteiskunnan, yrityselämän ja ihmisten arkipäivän rakenteet ja toimintaulottuvuudet. Sanotaan, että kaikki mikä voidaan digitalisoida, digitalisoidaan.²⁰ Tämä edellyttää lisääntyvissä määrin digitaalisen turvallisuuden huomioimista sekä erityisesti digitaalisen turvallisuus tietoisuuden vahvistamista. Kyse on hiljalleen muuttuvan ja muotoutuvan digitaalisen turvallisuuskulttuurin luomisesta, mikä koskettaa jokaista suomalaista. Kansanedustajien näkemysten mukaan suomalaisten yleisessä tietoisuudessa on vielä paljon parannettavaa ja yleisen tietoisuuden lisäämisen tuleekin olla yksi suomalaisen yhteiskunnan kyberturvallisuuden painopistealueita lähivuosina.

¹⁹ Ks. mm. Cyber Security Market 2015-2025.

²⁰ Ks. mm. Jungner, Otetaan digiloikka! Suomi digikehityksen kärkeen, s. 5.

Lähdeluettelo

- Eduskunta. Kansanedustajat. 2016. <https://www.eduskunta.fi/FI/kansanedustajat/Sivut/default.aspx> (8.2.2016).
- Jungner, Mikael. Otetaan digiloikka! Suomi digikehityksen kärkeen. Elinkeinoelämän keskusliitto. 2015. http://ek.fi/wp-content/uploads/Otetaan_digiloikka_net.pdf (8.2.2016).
- Kiiski, Elina. Megatrendit 2016. Taustamuistio. Sitra. 14.1.2016. https://www.sitra.fi/julkaisut/Muut/Megatrendit_2016.pdf (8.2.2016).
- Liikenne- ja viestintäministeriö. Suomen tietoturvallisuusstrategia. Luonnosversio 9.12.2015. <http://www.lvm.fi/lvm-site62-mahti-portlet/download?did=188979> (8.2.2016).
- Limnell, Jarno. Kyber rantautui Suomeen. Aalto-yliopiston julkaisusarja, Tiede + Teknologia 12 / 2014. Unigrafia Oy, Helsinki 2014.
- Sisäministeriö. Suomen kansallinen riskiarvio 2015. Sisäministeriön julkaisu 3/2016. Helsinki 2016.
- Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. Turvalisuus- ja puolustusasiain komitean sihteeristö. Forssa print. Helsinki 2013.
- Valtioneuvoston selvitys- ja tutkimustoiminta. Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016. Valtioneuvoston kanslia 2016.
- Visiongain. Cyber Security Market 2015–2025. <https://www.visiongain.com/Report/1405/Cyber-Security-Market-2015-2025> (8.2.2016).
- Yleisradio. “Yhdysvallat tutkii Ukrainan joulukuista sähkökatkosta – Ukraina syyttää venäläisiä hakkereita”, 13.1.2016. http://yle.fi/uutiset/yhdysvallat_tutkii_ukrainan_joulukuista_sahkokatkosta__ukraina_syyttaa_venalaisia_hakkereita/8592656 (15.2.2016).

Liite 1

Kyberturvallisuuskysely kansanedustajille

Arvoisa kansanedustaja.

Kyberturvallisuus on erottamaton osa tämän päivän turvallisuutta niin ihmisten arjessa kuin Suomen ulko- ja turvallisuuspolitiikassa. Yksinkertaistaen kyberturvallisuuden voi ajatella tarkoittavan digitaalisen toimintaympäristön turvallisuutta. Suomen kyberturvallisuusstrategian mukaan ”kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.”

Pyydämme ystävällisesti vastaamaan lyhyeen Teille kansanedustajille suunnattuun kyselyyn kyberturvallisuudesta – arvioonne kyberturvallisuuden nykytilasta ja tulevaisuudesta. Vastaukset käsitellään luottamuksella ja nimettöminä.

Pyydämme vastaamaan tammikuun loppuun mennessä. Kyselyn tuloksista tehtävän raportin tulette saamaan käyttöönnne.

Vastaan mielelläni mahdollisiin kysymyksiin: Professori Jarno Limnell, Aalto-yliopisto, puh. 040 527 6173, jarno.limnell@aalto.fi

Kiitän Teitä lämpimästi jo etukäteen. Kyberturvallisuus on maamme turvallisuuden kehittämisessä hyvin merkityksellistä ja vastaustenne tieto antaa kehittämiselle tärkeitä perusteita.

Vastaamaan pääsette alla olevan linkin kautta ja vastaaminen vie vain hetken ajastanne.

ISBN 978-952-60-6687-5 (pdf)
ISSN-L 1799-487X
ISSN 1799-487X (painettu)
ISSN 1799-4888 (pdf)

Aalto-yliopisto

Sähkötekniikan korkeakoulu
www.aalto.fi

**KAUPPA +
TALOUS**

**TAIDE +
MUOTOILU +
ARKKITEHTUURI**

**TIEDE +
TEKNOLOGIA**

CROSSOVER

**DOCTORAL
DISSERTATIONS**