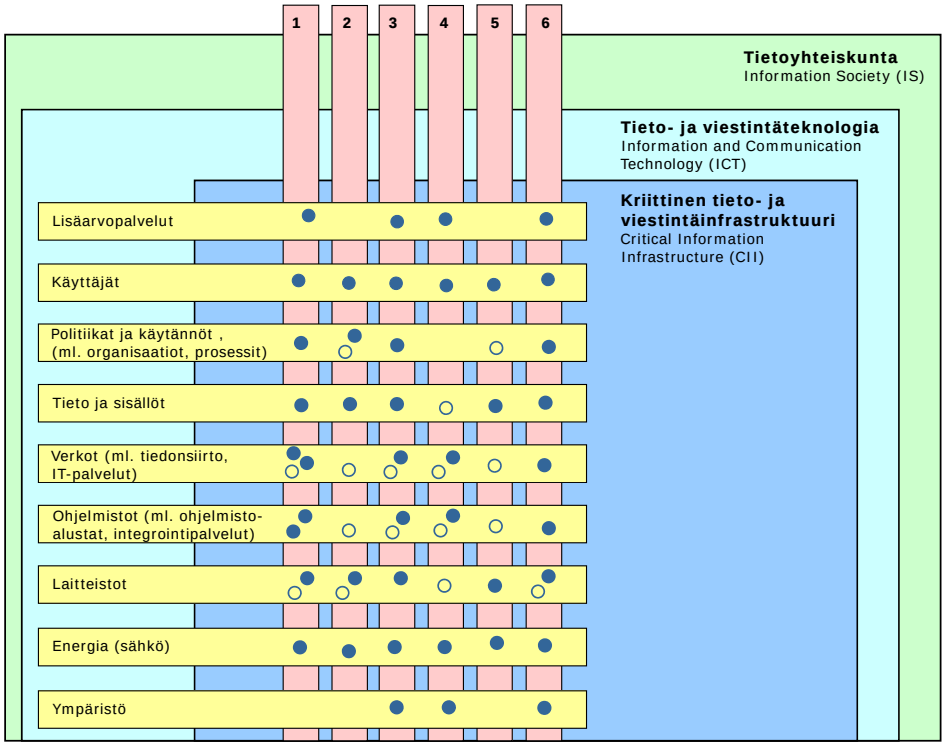


Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien käytettävyyden kehittäminen

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Helsinki, 2009

LIIKENNE- JA VIESTINTÄMINISTERIÖ

KUVAILULEHTI

Julkaisun päivämäärä

4.11.2009

Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri)	Julkaisun laji
Työryhmä, puheenjohtaja. Kari T. Ojala LVM, sihteeri Mats Kommonen Turun yliopisto	Raportti
	Toimeksiantaja: Liikenne- ja viestintäministeriö
	Toimielimen asettamispäivämäärä: 31.8.2008

Julkaisun nimi

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien käytettävyyden kehittäminen

Tiivistelmä

Yhteiskunnan elintärkeiden toimintojen välttämättömien ICT-järjestelmien käytettävyyden kehittäminen on tietoyhteiskunnan syventämistä kaikilla tasoilla yrityksistä ja organisaatioista kansalaiseen saakka sekä kaikissa turvallisuustilanteissa normaalioloista, häiriötilanteisiin ja poikkeusoloihin.

Tietoyhteiskuntakehityksen syventäminen lisää kansantalouden tuottavuutta, kilpailukykyä ja yhteiskunnan kasvua kaikilla lohkoilla sekä lisää kansalaisten viihtyvyyttä vertaistalouksiin nähden. Riippuen kansantalouden piirteistä tietoyhteiskunnan osuus on ollut jopa lähes 40 % tuottavuuden kasvusta.

Tietoyhteiskuntaan vaikuttaa erilaisia kehityspiirteitä ja trendejä uhkakuvineen. Näitä ovat esimerkiksi kansainvälisen yhteistyön ja verkostojen kasvava merkitys, verkkorikollisuuden nopea lisääntyminen ja luonteen muuttuminen sekä tieto- ja viestintäjärjestelmien kasvava rooli ja merkitys uusien globaali ilmiöiden myötä (esimerkiksi päästöjen vähentäminen (vihreä ICT)).

Internetistä on tullut kriittinen infrastruktuuri. Internetin Suomessa sijaitsevat osat ja Suomessa saatavilla olevat palvelut ovat osa yhteiskuntarakennetta. Työryhmä toteaa muun muassa, että Internetin toimivuus neutraalina ja kehittyvänä kriittisenä tiedonsiirtoalustana on turvattava siten, että se palvelee koko yhteiskuntaa riittävästi ja luotettavasti. On turvattava, että eri verkot yhdistyvät yhdeksi, tarpeeksi silmukoiduksi viestintäinfrastruktuuriksi. Tällä parannetaan erityisesti harvaan asuttujen seutujen palveluiden luotettavuutta.

Yhteiskunnalle elintärkeiden tietovarantojen ja datan varmistaminen ja saatavuus tulee olla taattu kaikissa tilanteissa. Esimerkiksi tietovuotojen ja palvelunestohyökkäysten torjumiseksi tietovarannot tulisi olla hajautettu laajalle. Yhteiskunnan toiminnan kannalta kriittisten tieto- ja viestintäjärjestelmien hallinta tulee järjestää siten, että siihen voidaan vaikuttaa kansallisin säädöksin ja päätöksin.

Yhteiskunnan tulee edesauttaa kriittisten ICT-järjestelmien suojausintressin luomisessa niitä tilanteita varten, missä markkinat eivät kannusta riittävästi yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien suojaamiseen yhteiskunnan varautumisen edellyttämälle tasolle.

Avainsanat (asiasanat)

Kriittinen infrastruktuuri, tietoturva, YETT

Muut tiedot

Yhteyshenkilö / LVM: Kari T. Ojala

Sarjan nimi ja numero	ISSN	ISBN
Liikenne- ja viestintäministeriön julkaisuja 50/2009	1457-7488 (painotuote) 1795-4045 (verkkojulkaisu)	978-952-243-119-6 (painotuote) 978-952-243-120-2 (verkkojulkaisu)

Sivumäärä (painotuote)	Kieli	Hinta	Luottamuksellisuus
76	suomi		julkinen

Jakaja	Kustantaja
Liikenne- ja viestintäministeriö	Liikenne- ja viestintäministeriö

KOMMUNIKATIONSMINISTERIET

PRESENTATIONSBLAD

Utgivningsdatum

4.11.2009

Författare (uppgifter om organet: organets namn, ordförande, sekreterare)	Typ av publikation
Arbetsgruppen, ordförande Kari T. Ojala, kommunikationsministeriet, sekreterare Mats Kommonen, Åbo universitet	Rapport
	Uppdragsgivare: Kommunikationsministeriet
	Datum för tillsättandet av organet: 31.8.2009

Publikation

Utveckling av tillgängligheten av informations- och kommunikationssystem som är nödvändiga för tryggandet av samhällets vitala funktioner

Referat

Utvecklingen av tillgängligheten av ICT-system som är nödvändiga för tryggandet av samhällets vitala funktioner innebär en fördjupning av informationssamhället på alla nivåer, från företag och organisationer till den enskilda medborgaren samt i alla säkerhetssituationer från normala förhållanden till störningar och undantagsförhållanden.

En fördjupning av informationssamhällets utveckling ökar den samhällsekonomiska produktiviteten och konkurrenskraften och tillväxten inom alla sektorer i samhället. Dessutom ökar den medborgarnas trivsel i jämförelse med övriga ekonomier. Beroende på samhällsekonomins struktur har informationssamhället stått för upp till 40 procent av tillväxten i produktiviteten.

Informationssamhället påverkas av olika utvecklingsdrag och trender jämte hotbilder. Sådana är bland annat den ökade betydelsen av internationellt samarbete och nätverk, den snabba ökningen av IT-relaterad brottslighet och dess förändrade karaktär samt ICT-systemens växande roll och betydelse till följd av nya globala fenomen (t.ex. utsläppsminskning (grön ICT)).

Internet har blivit en kritisk infrastruktur. De delar av internet som är belägna i Finland och de tjänster som är tillgängliga i Finland är en del av samhällsstrukturen. Arbetsgruppen konstaterar bland annat att funktionaliteten hos internet som en neutral, kritisk och växande plattform för dataöverföring bör tryggas så att det tjänar hela samhället på ett tillräckligt och pålitligt sätt. Man bör säkerställa att olika nätverk sammankopplas till en kommunikationsinfrastruktur med ett tillräckligt antal slingor. Detta förbättrar tjänsternas säkerhet i synnerhet i glesbygden

Säkrandet och tillgängligheten av samhällets vitala dataarkiv och data bör garanteras under alla omständigheter. Dataarkiven bör decentraliseras i så stor mån som möjligt, bl.a. för att förhindra informationsläckor och överbelastningsattacker. Skötseln av samhällets kritiska ICT-system bör ordnas så att den kan regleras genom nationella författningar och beslut.

Samhället bör främja skapandet av incitament för att skydda kritiska ICT-system under förhållanden där marknaden inte tillräckligt uppmuntrar privata aktörer att investera i skyddet av ICT-systemen i den grad som samhällets beredskap förutsätter.

Nyckelord

Kritisk infrastruktur, dataskydd, TSVF

Övriga uppgifter

Kontaktperson/kommunikationsministeriet: Kari T. Ojala

Seriens namn och nummer	ISSN	ISBN
Kommunikationsministeriets publikationer 50/2009	1457-7488 (trycksak) 1795-4045 (nätpublikation)	978-952-243-119-6 (trycksak) 978-952-243-120-2 (nätpublikation)

Sidoantal (trycksak)	Språk	Pris	Sekretessgrad
76	finska		offentlig

Distribution	Förlag
Kommunikationsministeriet	Kommunikationsministeriet

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

DESCRIPTION

Date of publication

4 November 2009

Authors (from body; name, chairman and secretary of the body)	Type of publication
Working group, chair. Kari T. Ojala Ministry of Transport and Communications, secretary Mats Kommonen University of Turku	Report
	Assigned by: Ministry of Transport and Communications
	Date when body appointed: 31 August 2008

Name of the publication

Development of the availability of essential information and communication systems and services to secure the vital functions of society

Abstract

The development of availability of essential ICT systems and services of vital functions in society signifies an advancement of the information society on all sectors and levels, from businesses and organisations to citizens, and within all security situations from normal conditions to disturbances and emergencies.

The advancement of the information society increases productivity, competitiveness and social growth in all sectors, and increases the satisfaction of the individuals therein. Depending on the characteristics of the political economy, the information society represents an increase of nearly 40% in productivity.

The information society is affected by different developmental factors, trends and related threat scenarios, e.g. the growing import of international co-operation and business networking, the rapid growth and innovation in cybersecurity, as well as the growing role and importance of ICT in the face of new global phenomena, such as emission reduction (green ICT).

The Internet has developed into a critical infrastructure. Internet components and services in Finland are an integral part of the society. The working group states that the Internet, as a neutral and critical networking platform, should be secured so that it provides sufficient and reliable services to the entire society. Different networks must be connected to form a single and adequately meshed communication infrastructure, thereby improving the reliability of services, especially in dispersed areas.

The security and availability of vital data pools and information must be quaranteed. For example, in order to prevent data leaks and denials of service, data pools should be widely decentralized. Critical ICT systems should be arranged so that it is possible to affect their management through the use of national regulations and decisions.

Society should assist in overseeing protection interests in situations in which the market does not sufficiently encourage the private sector to invest in ICT protection to the level required by society.

Keywords

Critical infrastructure, information security, YETT

Miscellaneous

Contact person at the Ministry: Mr. Kari T. Ojala

Serial name and number	ISSN	ISBN
Publications of the Ministry of Transport and Communications 50/2009	1457-7488 (printed version) 1795-4045 (electronic version)	978-952-243-119-6 (printed version) 978-952-243-120-2 (electronic version)

Pages, total (printed version)	Language	Price	Confidence status
76	Finnish		Public

Distributed and published by

Ministry of Transport and Communications

Liikenne- ja viestintäministeriölle

Liikenne- ja viestintäministeriö asetti 31.1.2008 työryhmän selvittämään tarvittavat toimenpiteet yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien käytettävyyden parantamiseksi. Yhteiskunnan riippuvuus tieto- ja viestintäjärjestelmistä on hyvin kokonaisvaltaista ja syvenee entisestään. Samalla kuitenkin alalla tapahtuva kilpailu ja pyrkimys kustannustehokkuuteen saattavat vaikuttaa käytettävyyden turvainvestointeihin niitä vähentävästi. Investointihalukkuus sekä -mahdollisuus koskee sekä siviili- että kriisiajan valmiuksia. Työryhmän toimikaudeksi asetettiin 1.2.2008–1.6.2009. Työryhmän toimikautta jatkettiin 15.9.2009 asti kesäkuussa 2009.

Työryhmän puheenjohtajaksi määrättiin viestintäneuvos Kari T. Ojala liikenne-ja viestintäministeriöstä ja sihteeriksi tietoturvapäällikkö Mats Kommonen Turun yliopistosta. Jäseniksi kutsuttiin tietohallintopäällikkö Catharina Candolin valtionhallinnon tietoturvallisuuden johtoryhmästä, erityisasiantuntija Kalevi Halonen valtiovarainministeriöstä, professori Heikki Hämmäinen teknillisestä korkeakoulusta, turvallisuusjohtaja Timo Härkönen valtioneuvoston kansliasta, yksikön päällikkö Sami Kilkkilä viestintävirastosta, neuvotteleva virkamies Tapani Koivumäki työ- ja elinkeinoministeriöstä, valmiuspäällikkö Veli-Pekka Kuparinen huoltovarmuuskeskuksesta, tietoturvapäällikkö Rauli Paananen sisäministeriöstä, vanhempi osastoesiupseeri Olli Peltonen puolustusministeriöstä, varautumispäällikkö Kari Wirman FiCom ry:stä ja yhteysupseeri Jukka-Pekka Virtanen liikenne- ja viestintäministeriöstä. Työryhmä on käyttänyt professori Esa Kerttulaa Proftel Oy:stä pysyvänä asiantuntijana.

Toukokuussa 2009 kutsuttiin huoltovarmuuskeskuksen uudeksi edustajaksi Veli-Pekka Kuparisen tilalle varautumispäällikkö Sauli Savisalo sekä liikenne- ja viestintäministeriön yhteysupseeri Jukka-Pekka Virtasen tilalle yhteysupseeri, komentajakapteeni Sami Vesterinen.

Työryhmä kokoontui toimikautenaan 12 kertaa ja järjesti kaksi seminaaria. Kokouksissa ja seminaareissa kuultiin työryhmän edustamien organisaatioiden lisäksi seuraavien tahojen edustajien näkemyksiä alan kehityssuunnista: TeliaSonera Oyj (Tapani Pökkä), Elisa Oyj (Jaakko Wallenius), DNA Palvelut Oy (Jukka Usmi), OP-Keskus (Markku Mäkinen), Fortum Oyj (Jouni Keronen), Maanpuolustuskorkeakoulu (Hannu Kari), Google Finland Oy (Petri Kokko), Tieto Oyj Erkki Heliö) ja VTT (Raija Koivisto).

Työryhmä on pohtinut käytettävyyden kehittämistä kaikkia turvatilanteita varten sen eri puolilta. Globalisaatio, taloudelliset käänteet ja verkkojen kautta tulevat uhkakuvat ja kompleksiset arvoverkot aiheuttavat pyrkimyksen kriittisten ICT-toimintojen varmistamiseen kansallisin resurssein. Hallinnossakin kaivattaisiin konsernitason vastuuorganisaatiota kriittisille tietojärjestelmille.

Työryhmä toteaa, että yhteiskunnan tulee edesauttaa kriittisten ICT-järjestelmien suojausintressin luomisessa niitä tilanteita varten, missä markkinat eivät kannusta riittävästi yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien suojaamiseen yh-

teiskunnan varautumisen edellyttämälle tasolle. Normien ja tekniikan lisäksi tarvitaan muuta. Käytettävyyden kehittäminen edellyttää asiantuntijaosaamisen vahvistamista ja koulutukseen panostamista. Osaamisen kehittäminen edellyttää myös tämän alueen t&k-hankkeisiin lisäpanostuksia sekä hallinnossa että vastuu- ja omistajaorganisaatioissa sisältäen sopimuskäytännöt. Työryhmä kokee tärkeänä, että YKÄ-toimintaa kehitetään edelleen ja sen jatkamisen muotoja valmistellaan.

Työryhmän raportti on julkinen ja liitteet ovat luottamuksellisia, JulkL (621/1999) 24.1§ 8,9 k.

Helsingissä 4 päivänä marraskuuta 2009

Kari T. Ojala
työryhmän puheenjohtaja

Sami Kilkkilä

Heikki Haukirauma

Catharina Candolin

Sauli Savisalo

Kalevi Halonen

Rauli Paananen

Heikki Hämmäinen

Olli Peltonen

Timo Härkönen

Kari Wirman

Sami Vesterinen

Mats Kommonen

SISÄLLYSLUETTELO

EXECUTIVE SUMMARY 5

1 JOHDANTO 10

1.1 Tietoyhteiskuntamissio—YKÄ-toiminta 10
1.1.1 Käytettävyys 10
1.2 Tietoyhteiskunnan merkitys tuottavuuteen 11
1.2.1 Perusteltu luottamus 11
1.2.2 Toiminnan varmistaminen 12
1.3 Yhteiskunta sähkön varassa 13
1.4 Ekotehokas tietoyhteiskunta 13
1.4.1 ICT-sektorin suuri potentiaali 13
1.5 Kansainvälinen tietoyhteiskuntakehitys 14
1.5.1 Globaalit riskit 14
1.5.2 Muuttuva rikollisuus 15
1.5.3 Critical Information Infrastructure Protection (CIIP) 16
1.5.4 Ennustamaton ICT-ekosysteemi 16
1.6 Suhde varautumiseen - normaaliolojen varautuminen uhkien toteutumisen estämistä 16
1.6.1 Tietoyhteiskuntaan integroitunut varautumisjärjestelmä 16
1.6.2 Uhkiin varaudutaan normaalioloissa 17
1.6.3 Tilannekuvaa kootaan julkisten verkkojen kautta 17
1.7 Raportin tavoitteet 18
1.7.1 Tarkastelukehikko 18
1.7.2 Elintärkeiden infrastruktuurien käytettävyys 18
1.7.3 YKÄ-hankkeen suhde muihin kokonaisuuksiin 18

2 TOIMINTAYMPÄRISTÖ 20

2.1 Yleistilanne 20
2.1.1 Yhteiskunnan elintärkeät toiminnot 20
2.1.2 Kriittiset toimialat 20
2.1.3 Yhteiskuntaan integroitunut varautuminen 20
2.1.4 YKÄ-toiminta 21
2.2 YKÄ-toimintaan liittyvät hallinnon ohjausmekanismit, ohjelmat ja hankkeet 21
2.2.1 Hallinnon ohjausmekanismit 22
2.2.2 Strategiat, ohjelmat ja hankkeet 22
2.2.3 Vastuuorganisaatiot 22
2.2.4 Ministeriöt 23
2.3 Euroopan elintärkeiden infrastruktuurien suojaaminen 23
2.3.1 ECI 23
2.3.2 ECI/IT 24
2.3.3 CIIP-aloite ja EPCIP 24
2.3.4 Direktiivi 24
2.4 Kansainväliset kyberaloitteet 24

3 YHTEISKUNNAN ELINTÄRKEÄT TOIMINNOT JA UHKAMALLIT 25

3.1 Toimintojen kokonaisuus 25
3.2 Turvallisuustilanteet ja uhkamallit 25
3.2.1 Turvallisuustilanteet 26
3.2.2 Uhkamallit 26
3.2.3 Uhka-analyysi 28

4 TIETO- JA VIESTINTÄJÄRJESTELMIEN KRIITTISTEN OSIEN MÄÄRITTELY 30

4.1 Tietoyhteiskunnan kriittinen ICT-infrastruktuuri 30
4.1.1 ICT-evoluutio, uhkat ja haavoittuvuudet 30
4.1.2 Kriittinen ICT-infrastruktuuri 30

5 KRIITTISTEN ICT-JÄRJESTELMIEN NYKYTILA JA KRIITTISYYDEN MÄÄRITTELY 33

5.1 Nykytila 33

5.1.1 Internetin ja mobiiliverkkojen strateginen merkitys ... 33
5.1.2 Internet – kriittinen infrastruktuuri ... 33
5.1.3 Mobiiliverkot ... 34
5.1.4 Kiinteät verkot ... 34
5.1.5 Public/private -partnership ... 35
5.2 Mikä on kriittistä - tahtotila ... 35
5.2.1 Kaikki riippuu kaikesta ... 35
5.2.2 Elintärkeiden ICT-järjestelmien käytettävyysvaatimukset tapauskohtaisia ... 35
5.3 Käytettävyyskriteerien määrittely ... 36
5.3.1 Kansainvälinen näkökulma ... 36
5.3.2 Harmaan alueen kriteerit ... 37

6 ELINTÄRKEIDEN TOIMINTOJEN TURVAAMINEN JA KÄYTETTÄVYYS ... 38

6.1 Motiivi - tietoyhteiskuntakehityksen syventäminen ... 38
6.1.1 Luottamuksen takaaminen ... 38
6.1.2 ICT-toiminnan varmistaminen ... 39
6.1.3 Kriittisten ICT-järjestelmien tunnistaminen ... 39
6.2 Kriittisten ICT-järjestelmien toiminnot ja toimijat prosessin osina ... 39
6.2.1 Käytettävyys muodostuu palvelun komponenttien käytettävyydestä ... 39
6.2.2 Prosessit liiketoiminnassa ... 40
6.2.3 Kriittisen ICT-ratkaisun käytettävyys suunnitteluvaiheessa ... 41
6.2.4 YKÄ-prosessit ... 41
6.3 Identiteetin hallinta – uusi CII ... 43
6.3.1 Kukin kriittinen infrastruktuuri rakentanut omat identiteetin hallintajärjestelmät ... 43
6.3.2 Kymmeniä erilaisia identiteetin todistusmenetelmiä ... 43
6.3.3 Informaation vapautus ... 43

7 TIETO- JA VIESTINTÄJÄRJESTELMIEN KÄYTETTÄVYYDEN SUHDE VARAUTUMISEEN ... 44

7.1 Lähtökohta, nykytila ja normisto ... 44
7.1.1 Varautumisen lähtökohta ... 44
7.1.2 Normisto ... 45
7.1.3 Varautuminen ja YKÄ ... 45
7.1.4 Haasteet - tietoverkot pysyvässä alivarautumisen tilassa? ... 45
7.2 Lainsäädännön riittävyys varautumiseen ... 45
7.2.1 Tieto- ja viestintäjärjestelmien varautumisen lainsäädännön kehittäminen ... 45
7.2.2 Varautumisohjeet ... 46

8 TELEVERKKOJEN ENERGIAHUOLTO JA SUOJAUSTEN RIITTÄVYYS ... 47

8.1 Suomen sähköverkko ... 47
8.2 Sähkön merkitys ... 47
8.2.1 Sähkökatkokset ... 47
8.3 Varavoima ... 48
8.3.1 Normit ... 48
8.4 Nykyisten suojausjärjestelmien riittävyys ... 49
8.4.1 Tilanne ... 49
8.4.2 Valtionhallinnon tietojärjestelmät – tilanne 2008 ... 49
8.4.3 Yksityinen sektori ... 50
8.4.4 Viestintäjärjestelmät ... 51

9 JOHTOPÄÄTÖKSET JA TOIMENPIDE-EHDOTUKSET ... 52

9.1 Johtopäätökset nykytilasta yleisesti ja toimenpide-ehdotukset ... 52
9.1.1 Televiestinnän lainsäädäntö, normit, rakenne, hinnoittelu ... 52
9.1.2 ICT-järjestelmien suojaus ... 54
9.2 Kriittiset viestintäjärjestelmät ... 54
9.2.1 Kriittisten ICT-järjestelmien käytettävyys – yleiset johtopäätökset ... 54
9.2.2 Kiinteät verkot ... 54
9.2.3 Mobiiliverkot ... 55
9.2.4 Internet ... 55
9.2.5 Laajakaistan laatu ... 57
9.2.6 Poikkeustilanteisiin varautuminen yleisesti ... 58
9.2.7 Muita yleisiä haasteita ja toimenpiteitä ... 58

9.3 Omistaja- ja teollisuuspoliittiset kysymykset 59
9.3.1 Muuttuva tilanne – haasteet kasvavat 59
9.3.2 Uhka - markkinahäiriöt 60
9.3.3 Työryhmän toteamukset 60
9.3.4 Huoltovarmuusorganisaatio 60
9.3.5 Huoltovarmuusbudjetin laajentaminen 61
9.4 YKÄ-toiminnan kehittäminen 62
9.4.1 YKÄ-prosessin jatkuvuuden takaaminen 62
9.5 Palveluihin ja tekniikkaan liittyvät toimenpiteet 63
9.5.1 Häiriötapahtumarekisterin perustaminen 63
9.6 Muut toimenpide-ehdotukset 63
9.6.1 Identiteetin hallinta 63

EXECUTIVE SUMMARY

Toimeksiannon tausta ja tavoitteet

Yhteiskunnan elintärkeiden toimintojen välttämättömien tieto- ja viestintäjärjestelmien **KÄ***ytettävyyden* kehittäminen (YKÄ-toiminta) on tietoyhteiskunnan syventämistä kaikilla tasoilla yrityksistä ja organisaatioista yksilöön ja kansalaiseen saakka sekä kaikissa turvallisuustilanteissa normaalioloista, häiriötilanteisiin ja poikkeusoloihin.

Valtioneuvoston päätös huoltovarmuuden tavoitteista (Vnp 539/2008) kuvaa kriittisen infrastruktuurin ja kriittisen tuotannon. Kriittinen infrastruktuuri on järjestelmä prosesseineen, mikä on välttämätön palvelun tai tuotteen tuottamiseksi tai toimittamiseksi.

YKÄ-työn tavoitteena on ollut saada yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien (ICT) *käytettävyydestä* selkeä tilannekuva kaikilla yhteiskunnan tasoilla ja kaikissa turvallisuustilanteissa sekä esittää havaittuihin ongelmatilanteisiin ratkaisumalleja ja konkreettisia parannusehdotuksia sekä toimenpiteitä vastuukysymyksineen ja kustannusvaikutuksineen.

Raportissa on tavoitetta varten määritelty yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien ICT-järjestelmien yleinen toiminnallinen kehikko, minkä pohjalta voidaan tarkastella kriittistä ICT-infrastruktuuria. Kehikolla voidaan määritellä elintärkeiden toimintojen perusrakenteiden kriittiset ICT-toiminnot ja -komponentit sekä näiden päällä ala- ja sektorikohtaiset kriittiset ICT-toiminnot ja -komponentit.

Raportissa on analysoitu yleisellä tasolla tieto- ja viestintäjärjestelmien kriittisyyttä ja nykytilaa sekä suhdetta varautumiseen sekä sitä, tukeeko lainsäädäntö riittävästi käytettävyyttä. Raportissa on selvitetty ovatko nykyiset kriittisen infrastruktuurin suojaustoimet riittäviä. Raportissa on esitetty kriittisen ICT- infrastruktuurin eräitä potentiaalisia ongelma-alueita ja haavoittuvuuskohtia sekä esitetty näihin parannus- ja ratkaisuehdotuksia.

YKÄ-työryhmä on ollut tiiviissä yhteistyössä muiden hallinnon turvallisuushankkeita kehittävien työryhmien kanssa sekä pyrkinyt sovittamaan työnsä siten että päällekkäisyyksiä ei syntyisi.

Kehitystrendejä ja uhkakuvia

Tietoyhteiskuntakehitykseen vaikuttaa erilaisia kehityspiirteitä ja trendejä uhkakuvineen. Näitä ovat esimerkiksi kansainvälisen yhteistyön ja verkostojen kasvava merkitys, verkkorikollisuuden nopea lisääntyminen ja luonteen muuttuminen sekä tieto- ja viestintäjärjestelmien rooli ja merkitys uusien globaali ilmiöiden myötä (esimerkiksi päästöjen vähentäminen (vihreä ICT)).

Tietoyhteiskuntakehityksen syventäminen lisää kansantalouden tuottavuutta, kilpailukykyä ja yhteiskunnan kasvua kaikilla lohkoilla sekä lisää kansalaisten viihtyvyyttä ver-

taistalouksiin nähden. Riippuen kansantalouden piirteistä tietoyhteiskunnan osuus on ollut jopa lähes 40 % tuottavuuden kasvusta.

Verkostoitumisen tuoma markkinatalouden kilpailupaine yrityksissä näyttää minimoivan varautumista. Kilpailu on myös johtanut yritysten lisääntyvään erikoistumiseen, ja sitä kautta arvoverkkojen laajentumiseen ja arvoketjujen pidentymiseen, mikä lisää systeemin haavoittuvuutta kriisitilanteissa. Yksikään osapuoli ei voi yksipuolisesti saavuttaa merkittävää varautumishyötyä. Tarvitaan yhteisiä linjauksia.

Tärkeä osa elinkeinoelämän ja kansalaisten käyttämistä ja tarvitsemista palveluista pohjautuu internetiin. Internetistä on muodostunut kriittinen infrastruktuuri. Maailman talousfoorumi arvioi vuonna 2008, että tietoyhteiskunnan elintärkeiden infrastruktuurien laajan toimintahäiriön todennäköisyys seuraavan 10 vuoden kuluessa on 10–20 %. Toimintahäiriö voisi aiheuttaa maailmanlaajuisesti jopa 170 miljardin euron kustannukset.

Kriittinen ICT ja YKÄ-toiminnan suhde varautumiseen

YKÄ-toiminnalla on suora suhde varautumiseen, koska tietoyhteiskunnan toimintojen tulee olla käytettävissä kaikissa turvallisuustilanteissa. Varautuminen on uhkakuvien analysointia ja toiminnan varmistamista jo normaalioloissa.

Yritysten varautumisen lähtökohtana ovat liiketoiminnalliset perusteet, asiakkaiden kanssa tehdyt sopimukset sekä näihin liittyvä riskienhallinta. Siltä osin, kun tämä ei yhteiskunnan näkökulmasta ole riittävää, täydennetään varautumisvastuita lainsäädännöllisillä velvoitteilla ja muilla erityisillä toimenpiteillä. Joillain alueilla viranomaisen rooli rajoittuu toimintaa ohjaavaksi ja varsinainen toimija on yksityinen yritys. Lakisääteiset varautumisvelvoitteet eivät saa häiritä markkinoiden toimintaa ja tasapuolisia kilpailuedellytyksiä. Tässä on erityisesti huomioitava sekä kansallinen että Euroopan yhteisön kilpailulainsäädäntö. Yritykset ja elinkeinoelämän järjestöt osallistuvat sopimusperusteiseen valmiussuunnitteluun Huoltovarmuusorganisaation eri sektoreissa ja pooleissa.

Kriittiset ICT-infrastruktuurit ovat useissa tapauksissa globaaleja ja liittyneet tiiviisti yhteen. Ne ovat myös keskinäisriippuvia muista infrastruktuureista, joten niiden tietoturvaa ja vioista toipumista ei voida taata pelkästään kansallisesti eikä ilman koordinointia.

Euroopan komission 30.3.2009 julkistamassa tiedonannossa määritellään suunnitelmat välittömille toimenpiteille vahvistaa tietoyhteiskunnan kriittisten infrastruktuurien turvallisuutta ja vahingoista toipumista. Viimeaikaisia esimerkkejä tiedonannon tarkoittamista tilanteista ovat laajat tietoverkkohyökkäykset Viroon vuonna 2007 ja merenalaisten kaapelien katkeamiset.

Johtopäätökset

Seuraavassa esitetyt johtopäätökset ja toimenpiteet eivät ole tärkeysjärjestyksessä.

- Tietoyhteiskunnan telelainsäädäntö, säädösten valvonta ja norminanto sekä verkkojen ja palvelujen rakenne, suojaukset ja operointi ovat Suomessa **käytettävyyttä** sil-

mällä pitäen kansainvälisesti hyvällä tasolla. Rakennemääräykset, turvaluokitukset ja muut normit ovat korkealla tasolla. Jatkuva kehittäminen on kuitenkin välttämätöntä.

- Viestintä- ja tietoliikennejärjestelmien **käytettävyyden varmistaminen** on hallinnoltaan, organisaatioltaan, lainsäädännöltään ja tuotteiltaan/palveluiltaan pääsääntöisesti hyvässä kunnossa.

- Tietojärjestelmien ja -palvelujen **käytettävyydessä** on kehittämisen varaa. Tietojärjestelmä- ja palvelusektorilla ei ole kuitenkaan kattavia normeihin perustuvia säätelymekanismeja kuten sähköisen viestinnän alueella.

- ICT-järjestelmien ja -palvelujen **käytettävyys** suunnitellaan, toteutetaan ja johdetaan liiketoimintaprosessien sisällä. Pelkät tekniset ratkaisut ja normit eivät riitä.

- Suomessa on varauduttu ICT:n osalta poikkeusolojen lisäksi myös normaaliolojen häiriötilanteisiin sektorilainsäädännöllä sekä kaupallisten palvelutasovaatimusten avulla.

- Julkisen ja yksityisen sektorin välinen varautumisen yhteistoiminta toimii hyvin ja on kustannusten jaoltaan vakiintunutta.

- Internetistä on tullut kriittinen infrastruktuuri. Internetin kautta saatavat elinkeinoelämän ja kansalaisten palvelut ovat elintärkeitä. Internetin Suomessa sijaitsevat osat ja Suomessa saatavilla olevat palvelut ovat osa yhteiskuntarakennetta.

- ICT-palvelujen viime vuosien kehitykselle on ollut ominaista tarjonnan globalisoituminen ja toimintojen ulkoistaminen, mihin liittyvistä mahdollisista lieveilmiöistä voi aiheutua vakavia markkinahäiriöitä ja ongelmia ICT-palvelujen saatavuudelle. Globalisaatio, taloudelliset käänteet ja verkkojen kautta tulevat uhkakuvat ovat aiheuttaneet pyrkimyksiä kriittisten ICT-toimintojen varmistamiseen kansallisin resurssein.

- Markkinat eivät välttämättä kannusta yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien suojaamiseen yhteiskunnan varautumisen edellyttämälle tasolle. Tämän on todennut myös EU-komissio.

- ICT-palvelujen **käytettävyyttä** ei kaikissa tapauksissa pystytä takaamaan, mikä vaikuttaa yhteiskunnan varautumiseen. ICT-yritys tai sitä palveleva kriittinen alihankintayritys voi esimerkiksi irtisanoa suuren osan henkilöresursseistaan, lopettaa joidenkin palveluiden tarjoamisen tai mennä jopa konkurssiin.

- Nykymuotoinen tiukka kilpailu ei jätä yritykseen vararesursseja, mikä voi heikentää yrityksen riskinkantokykyä ja sitä kautta tehdä yrityksen toiminnan haavoittuvammaksi erilaisille uhkille kriisitilanteissa.

- Kansainvälisen yhteistyön seurauksena on syntynyt uusia, kompleksisista arvoverkoista muodostuneita toimintamalleja. Organisaation toimintaprosessit voivat sijaita osittain tai kokonaan maan rajojen ulkopuolella, jolloin toiminnan turvallisuus ja luotettavuus ovat vaikeammin hallittavissa.

- Tietoyhteiskunnan verkkoon syntyy perinteisen televiestinnän lisäksi liikennettä myös erilaisista uusista lähteistä, kuten viihdeteollisuudesta ja maksupalveluista. Näiden ohjaus perustuu erilaisiin tarpeisiin kuin mitä ICT-toiminnalla on (esim. suodatus, tallennusvelvoite). Tästä on seurauksena, että verkkojen ja palveluiden käytettävyysvaatimukset voivat olla ristiriitaisia (laatuluokittelu, hinnoittelu).

- Kriittisten ICT-järjestelmien ja niiden komponenttien omistajuuteen raportissa ei oteta kantaa.

Toimenpiteet

- ICT-toiminnan, erityisesti televerkkojen ja -palvelujen, liiketoimintaa ja markkinoita tulisi ohjata vain siinä määrin kuin se on välttämätöntä markkinoiden ja palvelujen pitämiseksi saatavilla monipuolisina ja riittävinä. Ohjausvälineinä ovat normit, toimilupaehdot ja rahoitus. Kilpailu lisää vaihtoehtoja, myös käytettävyyden kannalta.

- Yhteiskunnan tulee edesauttaa kriittisten ICT-järjestelmien suojausintressin luomisessa niitä tilanteita varten, missä markkinat eivät kannusta riittävästi yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien suojaamiseen yhteiskunnan varautumisen edellyttämälle tasolle.

- Internetin toimivuus neutraalina ja kehittyvänä kriittisenä tiedonsiirtoalustana on turvattava kansainvälisen yhteistyön, säännösten ja teknisten ratkaisujen avulla siten, että se palvelee koko yhteiskuntaa riittävästi ja luotettavasti.

- Tulee huolehtia siitä, että EU-tasolla tapahtuva palvelurakenteiden kehitys ja kotimaisten elintärkeiden toimintojen turvaamistoimenpiteet saadaan sovitettua yhteen ja keskenään. Esimerkkinä voidaan mainita finanssitoimialan maksuliikkeen kehitys, tai toimijoiden yhteiset rakenteet (energia, tietoliikenne). Kehitystä tulee edesauttaa siten, että Suomesta viedään hyviä ratkaisumalleja myös EU-tasolle sen rinnalla, kun sieltä tuodaan ratkaisuja Suomeen.

- Yhteiskunnalle elintärkeiden tietovarantojen ja datan varmistaminen ja saatavuus tulee olla taattu kaikissa turvallisuustilanteissa. Esimerkiksi tietovuotojen ja palvelunestohyökkäysten torjumiseksi olisi hyvä, mikäli tietovarannot olisi hajautettu laajalle. Yhteiskunnan toiminnan kannalta kriittisten tietojärjestelmien hallinta tulee järjestää siten, että siihen voidaan vaikuttaa kansallisin säädöksin ja päätöksin.

- Käytettävyyden kehittäminen edellyttää asiantuntijaosaamisen vahvistamista ja koulutukseen panostamista. Kansallisten elintärkeiden ICT-järjestelmien ja palveluiden ylläpitäminen sekä korkealaatuisten hankinta- ja käyttösopimuksien laatiminen edellyttää oman osaamisen vahvistamista normaalioloissa. Osaamisen kehittäminen edellyttää myös tämän alueen t&k-hankkeisiin lisäpanostuksia sekä hallinnossa että vastuu- ja omistajaorganisaatioissa.

- ICT-toiminnan ja logistiikan osuus huoltovarmuuden ylläpitämisessä on strateginen ja sen merkitys koko ajan kasvaa. Tämän lisäksi tietoyhteiskunnan syventynyt merkitys yhteiskunnan elintärkeiden toimintojen varmistamisessa jo normaalioloissa on

entisestään tärkeämpää. Huoltovarmuusorganisaation roolia tulisi edelleen vahvistaa ja laajentaa ICT-alueella.

- Työryhmä kokee tärkeänä, että YKÄ-toimintaa kehitetään edelleen ja sen jatkamisen muotoja valmistellaan. Valmistelutyön omistajaksi ehdotetaan Huoltovarmuusorganisaation tietoyhteiskuntasektoria. Valmistelutyöhön kuuluu myös YKÄ-alueen t&k-toiminta. YKÄ-toiminnan kehittämiseen on osoitettava riittävät resurssit.

- Työryhmä on tehnyt lisäksi joukon tekniikkaan ja palveluihin liittyviä elintärkeiden ICT-järjestelmien käytettävyyttä parantavia toimenpide-ehdotuksia. Nämä on esitetty ja perusteltu raportissa (luku 9).

- Tietoyhteiskunnassa tulee olla käytettävissä toimiva, luotettava ja tarpeeksi laajasti hyväksytty ja yksinkertainen identiteetin tunnistusmenetelmä. Työryhmä ehdottaa, että identiteetin hallinnasta muodostettaisiin kriittisen infrastruktuurin tasoinen konsepti. Konseptin kehittämiseksi tulee selvittää voidaanko se kytkeä osaksi jo jotain meneillään olevaa tarpeeksi laajaa identiteetin hallinnan kehityshanketta.

1 JOHDANTO

1.1 Tietoyhteiskuntamissio—YKÄ-toiminta

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien **käytettävyyden** kehittäminen–YKÄ-toiminta–katsoo haasteita koko yhteiskunnan kannalta (yritykset, organisaatiot, kansalaiset) ja kaikissa turvallisuustilanteissa (normaaliolot, häiriötilanteet, poikkeusolot). YKÄ-toiminnan merkitys ja yleiset tavoitteet on määritelty liikenne- ja viestintäministeriöstä johdetussa Arjen tietoyhteiskunta -ohjelmassa.

YKÄ-toiminnan taustalla nähtävä laajempi missio perustuu siihen, että tietoyhteiskuntakehityksen (ICT) **syventämisellä** on selkeä positiivinen vaikutus koko yhteiskuntaan kaikilla sen sektoreilla

- kansantalouden tuottavuuteen
- kilpailukykyyn
- yhteiskunnan kasvulle, ja
- kansalaisten viihtyvyyteen ja tasa-arvoon.

Missiossa vaikuttaa erilaisia kehityspiirteitä ja trendejä uhkakuvineen, kuten

- kansainvälisen yhteistyön ja verkostojen kasvava merkitys
- verkkorikollisuuden nopea kasvu ja luonteen muuttuminen
- tieto- ja viestintäjärjestelmien (ICT) rooli ja merkitys uusien globaali ilmiöiden myötä (esimerkiksi päästöjen vähentäminen (vihreä ICT), nousu taloustaantumasta).

Mission taustalla yhteiskunnan elintärkeät toiminnot (YETT) ja kriittiset infrastruktuurit sekä sisäisen turvallisuuden ohjelman (STO) tavoitteiden toteuttaminen ovat avainasemassa tietoyhteiskunnan ja kansalaisten luottamuksen kannalta. Ohjelmia kohtaaviin uhkakuviin varautumista on entisestään korostettava.

Häiriö- ja poikkeusoloihin varautuminen normaalioloissa tulee entistä tärkeämmäksi. Yhteiskunta on täysin sähkön ja ICT:n varassa, joten ICT ja sähkö kulkevat tietoyhteiskunnassa kaikkialla käsi kädessä.

1.1.1 Käytettävyys

Tietoyhteiskunnan elintärkeiden ICT-järjestelmien *käytettävyys* on määritelty oheisessa laatikossa[1]. Tässä selvityksessä käytettävyydellä tarkoitetaan sekä helppokäyttöisyyttä että saavutettavuutta. Tietoyhteiskunta on kehittynyt täysin riippuvaiseksi tietoverkkojen 24/7-toiminnasta.

Käytettävyyteen ja saavutettavuuteen liittyy keskeisesti myös tietoturvallisuus. Hyvä tietoturvallisuus tarkoittaa tilannetta, jossa sekä tietojen, järjestelmien, palveluiden että tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää riskiä.

[1] http://fi.wikipedia.org/wiki/Käytettävyys

Käytettävyys on käytännössä määritelty kahdella tavalla (engl. *usability* ja *availability*).

Käytettävyys (usability)
ISO 9241-11 -standardi määrittelee käytettävyyden seuraavalla tavalla: "Se vaikuttavuus, tehokkuus ja tyytyväisyys, jolla tietyt määritellyt käyttäjät saavuttavat määritellyt tavoitteet tietyssä ympäristössä". Vaikuttavuudella tarkoitetaan miten tarkoin ja täydellisesti käyttäjä saavuttaa tavoitteensa. Tehokkuus tarkoittaa tavoitteiden saavuttamista suhteutettuna käytettyihin resursseihin. Tyytyväisyydellä tarkoitetaan käyttäjän tyytyväisyyttä laitteen tai järjestelmän käyttöön, tyytyväisyyttä vuorovaikutuksen sujuvuuteen ja sen tulokseen.

Käytettävyys (availability)
Tuotantoympäristöissä käytettävyydellä tarkoitetaan yleensä järjestelmien teknistä toimivuutta ja toimivuusastetta. Toinen tästä yleisesti käytetty termi on ***saavutettavuus***. Saavutettavuudella (saatavuudella) viitataan siihen, kuinka suuren osan vuorokaudesta järjestelmä on toiminnassa ja käyttäjien saatavilla. Esimerkiksi jonkun järjestelmän saatavuus voi olla 99%, jolla tarkoitetaan sitä, että järjestelmä on ollut toimintakykyinen 99% ajasta.

Saavutettavuus suunnittelun tavoitteena
Verkkopalveluiden suunnitteluvaiheessa pyritään tunnistamaan käyttäjien, käyttötilanteiden ja eri päätelaitteiden asettamat reunaehdot ja vaatimukset. Käyttäjien tarpeiden tunnistamisessa voidaan soveltaa esim. käyttäjäkeskeisen suunnittelun periaatteita. Saavutettavuuden huomioiminen jo suunnitteluvaiheessa takaa paremman lopputuloksen kuin vanhan palvelun "korjaaminen" saavutettavaksi.

Saavutettavuus toteutuksen ominaisuutena
Saavutettavuus voidaan nähdä myös verkkopalvelun ominaisuutena. Verkkopalveluiden suositeltavista ominaisuuksista on laadittu useita erilaisia listoja, esim. W3C:n Web-sisällön saavutettavuusohje 1.0: tarkistuslista. Näitä listoja voidaan hyödyntää myös arvioitaessa verkkopalvelun saavutettavuutta.

Saavutettavuus* ja *käytettävyys
Rajanveto käytettävyys- ja saavutettavuusongelmien välille on vaikeaa. Molemmat liittyvät tuotteen tai palvelun (esim. verkkopalvelun) helppokäyttöisyyteen. Käytettävyys liittyy siihen, miten tehokkaasti, miellyttävästi ja virheettömästi käyttäjät pystyvät verkkopalvelua käyttämään. Saavutettavuus taas liittyy mahdollisuuteen käyttää verkkopalvelua.

1.2 Tietoyhteiskunnan merkitys tuottavuuteen

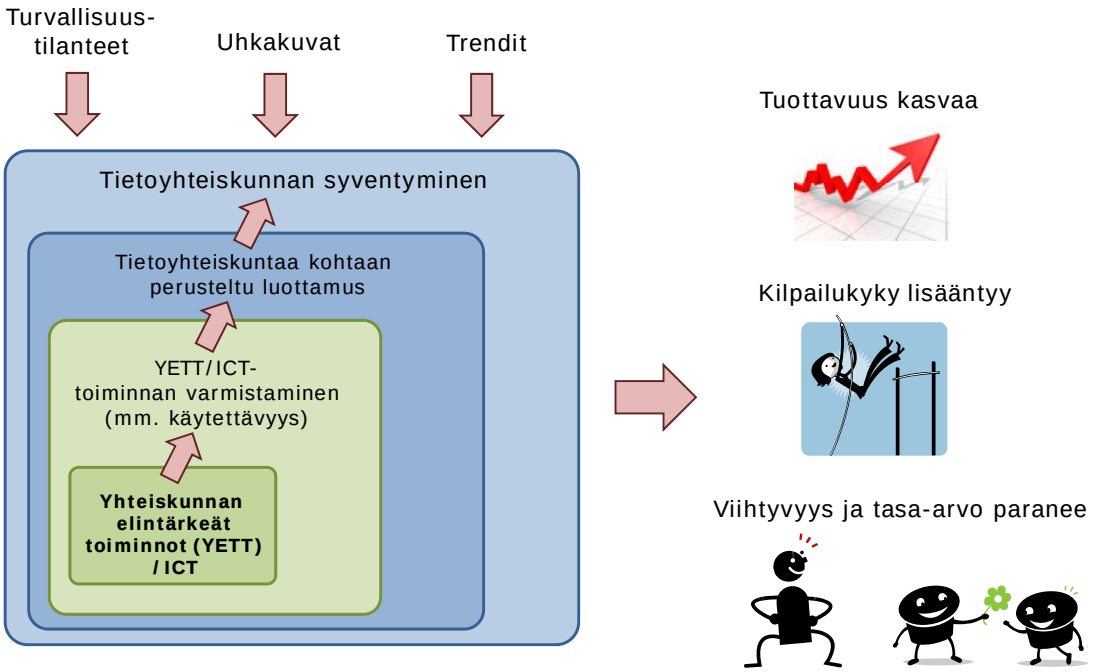
Tietoyhteiskuntakehityksen syventäminen (kuva 1.1) lisää kansantalouden tuottavuutta, kilpailukykyä, yhteiskunnan kasvua kaikilla lohkoilla sekä lisää kansalaisten viihtyvyyttä vertaistalouksiin nähden. Riippuen kansantalouden piirteistä, kuten kansakunnan koosta ja miten se sijaitsee markkinoihin ja kumppaneihin verrattuna, tietoyhteiskunnan merkitys ja osuus on ollut jopa lähes 40 % tuottavuuden kasvusta[2].

1.2.1 Perusteltu luottamus

Tietoyhteiskuntakehitys voi syventyä vain jos tietoyhteiskuntaa ja sen palveluita kohtaan kaikki osapuolet tuntevat riittävää perusteltua luottamusta. Kaikilla osapuolilla on oma näkökulmansa; julkishallinnon kullakin organisaatiolla, yrityksillä ja kansalaisilla.

Eri näkökulmia ovat muun muassa pääsy turvallisesti internetiin, sähköisten palvelujen helppokäyttöisyys ja saatavuus, kuluttajansuoja, sisältöjen laillisuus, tietoturva ja peruspalvelujen käytettävyys (saatavuus) kaikkialla. Kuluttajan aseman parantaminen edellyttää kaikilta toimijoilta vastuullisuutta, myös kuluttajilta itseltään.

[2] Eurostat, Theme: Science and Technology/Information Society, http://epp.eurostat.ec.europa.eu.



Kuva 1.1 Tietoyhteiskunnan syventäminen lisää kansantalouden tuottavuutta ja kilpailukykyä sekä parantaa kansalaisten viihtyvyyttä ja tasa-arvoa

1.2.2 Toiminnan varmistaminen

Luottamuksen edellytyksiä rakennetaan yhteiskunnan elintärkeiden tieto- ja viestintäjärjestelmien toiminnan varmistamisella (käytettävyyden takaamisella, korkealla palvelutasolla), tietoturvatoimin, haitallisiin ja laittomiin sisältöihin puuttumalla, panostamalla CERT-toimintaan, varmistamalla verkkopankkitoimintaa, yksittäisillä suojaushankkeilla, varautumalla verkkohyökkäyksiin ja haittaohjelmiin, jne.

Yhteiskunnan elintärkeiden tieto- ja viestintäjärjestelmien toiminnan varmistaminen edellyttää prosessien, järjestelmien ja niiden komponenttien tunnistamista, uhkien ja riskien realistista kartoitusta sekä ratkaisujen hahmottamista. Tämä on erityisen tärkeää infrastruktuuritasolla missä vaikutukset ovat sekä syvät että laajat.

Komponenttien tunnistamisessa keskeistä on huomioida yksittäiset toiminnot ja toimijat prosessin osina. Tällöin esimerkiksi tietoturvallisuutta voidaan käsitellä osana liiketoimintaprosesseja.

Uhkien ja riskien kartoituksessa tulisi pystyä ottamaan realistisesti huomioon niiden todennäköisyydet ja riskien ja uhkien vuorovaikutuksia.

Lopulta hahmoteltujen ratkaisujen tulisi kohdentua toimintoprosessien varmistamiseen, todennäköisimpiin ja vaikuttavimpiin uhkiin ja riskeihin sekä sisältää kanta omistajuuteen, ratkaisutapoihin, resursseihin ja aikatauluihin. Nämä ovat enemmän kuin haasteellisia tavoitteita.

1.3 Yhteiskunta sähkön varassa

Yhteiskunta on lähes täysin riippuvainen sähköstä. Häiriöt sähkönjakelussa voivat lamauttaa arjen toiminnot. Veden jakelu, viemäreiden toiminta, polttonesteiden jakelu, kauppojen ja pankkiautomaattien toiminta, tietoliikenne ja lämmitys ovat sähkön varassa. Myrskyn tai teknisen häiriön aiheuttaman sähkökatkon tullen nämä toiminnot pysähtyvät. Sähkökatkosten vaikutuksia yhteiskunnan elintärkeisiin toimintoihin on selvitetty tuoreessa Puolustusministeriön julkaisussa[3].

Sähkönjakelu ja tietoliikenne elävät keskinäistä kriittistä symbioosia, jotka riippuvat toisistaan (ks. liite 1, ei julkinen, JulkL 24.1§ 8,9 k).

1.4 Ekotehokas tietoyhteiskunta

Tutkimusyhtiö Gartner arvioi, että tieto- ja viestintätekniikan teollisuudenala tuottaa kaksi prosenttia maailman hiilidioksidipäästöistä[4,5]. Lukema on samaa tasoa ilmailualan kanssa. Huolimatta tietotekniikan ympäristöhyödyistä kokonaisuutta katsoen, Gartner pitää tilannetta kestämättömänä. ICT-päästöjen osuuden ennustetaan jopa kaksinkertaistuvan lähivuosina.

1.4.1 ICT-sektorin suuri potentiaali

ICT-sektorilla on suuri potentiaali vaikuttaa päästöjä vähentävästi niillä yhteiskunnan sektoreilla, jotka tuottavat loput 98 % päästöistä. ICT-teknologia voi vähentää Euroopan kokonaisenergiankulutusta jopa 15 %:lla vuoteen 2020 mennessä[6]. On arvioitu, ettei Euroopan yhteisöjen neuvoston asettamiin vuoden 2020 päästö- ja energiatehokkuustavoitteisiin voida edes päästä ilman tieto- ja viestintäteknologioiden valjastamista edistämään energiatehokkuutta.

ICT-toimiala ei luonnollisestikaan yksin pysty vastaamaan energiatehokkuustavoitteiden saavuttamisesta, mutta sillä on korvaamattoman tärkeä rooli sellaisen rakennemuutoksen vauhdittamisessa, joka johtaa energiatehokkuuden lisääntymiseen eri talouden sektoreilla. Kyse on yhtäältä ICT-toimialan ja muiden toimialojen rakennemuutoksesta kohti parempaa tekniikan antaman lisäarvon hyödyntämistä, kuten teollisuuden ja palveluiden prosessien tehokkaampi hoito, älykkäämpi ICT-ohjattu liikenne ja logistiikka ja sähköinen asiointi ja tietoyhteiskunnan muu syventäminen.

Arjen tietoyhteiskunnan suotuisa kehitys on välttämätöntä sellaisten puitteiden luomiselle, joissa tieto- ja viestintätekniikka voidaan valjastaa energiatehokkuuden parantamiseen ja siten ilmastonmuutoksen hillitsemiseen. Verkkoinfrastruktuurin pitää olla laadukasta ja vastata tietoliikenteen moninkertaisiksi kasvaviin tarpeisiin sekä tukea luottamusta tietoyhteiskunnan palveluihin. Tätä edesautetaan YKÄ-toiminnalla.

---

[3] Pitkä sähkökatko ja yhteiskunnan elintärkeiden toimintojen turvaaminen, Puolustusministeriö, 2009.
[4] Gartner: ict-päästöt ilmailun luokkaa, Digitoday, 27.4.2007.
[5] http://www.vihreaict.fi/fi/fi_6.html
[6] Kohti elogisesti tehokasta tietoyhteiskuntaa, viestintäministeri Suvi Lindén, ICT- ja ympäristöseminaari, 1.4.2009.

1.5 Kansainvälinen tietoyhteiskuntakehitys

1.5.1 Globaalit riskit

Maailmantalouteen ja tietoyhteiskuntakehitykseen vaikuttaa useita globaaleja trendejä, joissa on omat riskifunktionsa. Olosuhteet lisäksi voivat muuttua nopeasti ja riskit sen mukana. Globaalit riskit vaikuttavat globaalitalouden ja muun muassa yritysten operatiivisten toimintojen ulkoistusten kautta myös kansalliselle tasolle ja yhteiskunnan elintärkeisiin toimintoihin (YETT) ja kriittisten infrastruktuurien (CI) ja kriittisten ICT-järjestelmien (CII) kautta kansalliseen tietoyhteiskuntaan.

Tällä hetkellä globaaleista trendeistä voidaan esimerkiksi Maailman talousfoorumin mukaan mainita tärkeimpinä systeemiset finanssiriskit, ruokaturvallisuus, ”hyperoptimointi” ja jakelukanavien haavoittuvuus ja energian rooli[7]:

- Systeemiset finanssiriskit aiheuttavat koko taloudellisen järjestelmän laajuisia finanssikriisejä, mikä näkyy nopeina omaisuuksien arvonalennuksina ja taloudellisten aktiviteettien vähentymisenä. Finanssijärjestelmät ovat näissä olosuhteissa epästabiileja ja epäluottamus finanssialaan kokonaisuutena lisääntyy.

- Ruokaturvallisuus määritellään siten, että kaikilla ihmisillä on kaikkina aikoina fyysiset ja taloudelliset mahdollisuudet riittävään, turvalliseen ja ravitsevaan ruokaan[8]. Ruokaturvallisuus siten, samalla tavalla kuin energiaturvallisuuskin, sisältää fyysisen tarpeen tyydyttämisen lisäksi myös taloudelliset mahdollisuudet.

- Hyperoptimointi ja jakelukanavien haavoittuvuus on näkymätön globaali riski. Taloudellinen globalisaatio on muuttanut sekä yritysten että hallintojen operatiivisia rakenteita. Ulkoistaminen – erityisesti tuotannossa mutta enenevässä määrin myös liiketoiminnan peruspalveluissa–on globaalin vaurastumisen perusvoima, missä allokoidaan rajallisia globaalivoimavaroja sellaisiin yrityksiin ja maantieteellisille alueille, mitkä tuottavat eniten suhteellista kilpailuetua. Globaalisti integroituneempi talous on kuitenkin haavoittuvampi jakelukanavien häiriölle. Talouden turvaaminen ei riipu enää sen sisäisestä toiminnasta.

- Energia ja globaali riski: yhteenkytkeytyneet riskit – erillään olevat kannustimet. Energia on globaalitalouden avaintekijä, mutta samalla energiansaannin turvaaminen ja kestävä toimitus on koko ajan ongelmallisempaa. Monien eri globaali riskien sarjassa - kuten ilmastonmuutos, taloudelliset ja eräät geopoliittiset riskit - nykyiset ja tulevat poliittiset energiapäätökset tulevat väistämättä muovaamaan koko globaalia riskimaisemaa. Mutta näkyvissä ei ole kannustimia uudistaa globaalia energiataloutta tavalla, mikä vähentäisi globaaliriskejä.

Globaalit riskit ovat usein ketjuuntuneita, erityisesti energiansiirron ja ICT-infrastruktuurien osalta. Toteutuneista riskeistä aiheutuneita vahinkoja mitataan yleensä vahinkojen taloudellisilla mittareilla tai ihmishenkien menetyksinä.

[7] World Economic Forum, Global Risks 2008.
[8] Food and Agriculture Organization (FAO).

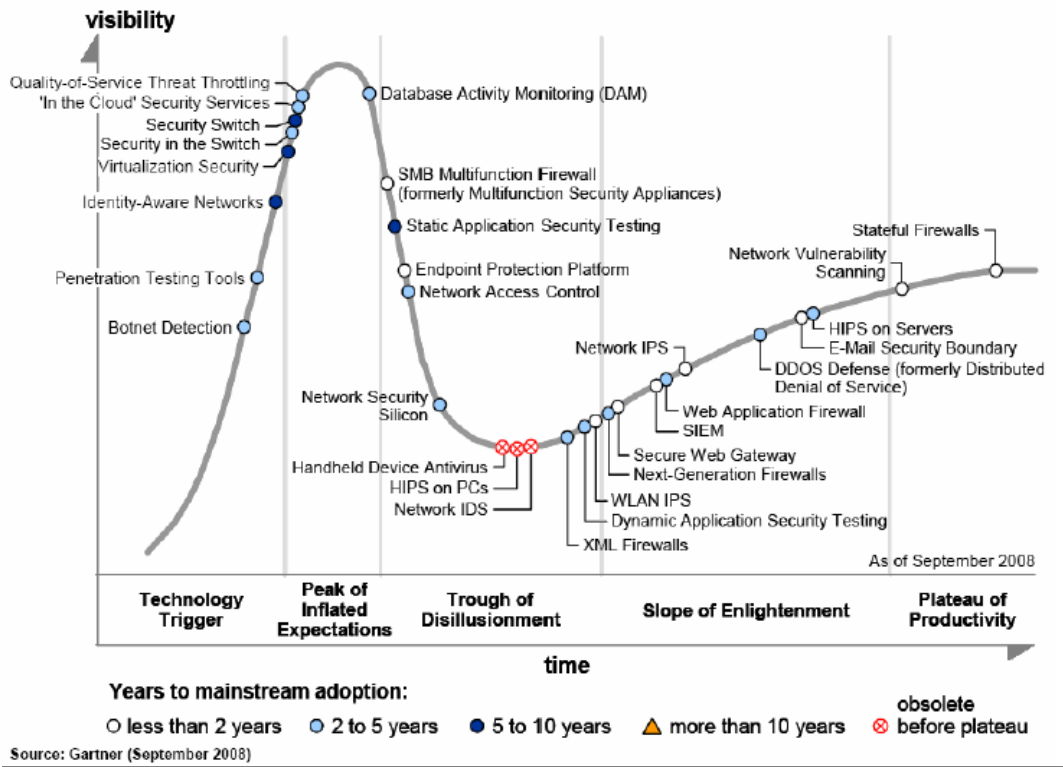
1.5.2 Muuttuva rikollisuus

Järjestäytynyttä ja vakavaa rikollisuutta, tietoverkkorikollisuutta sekä terrorismia on jäsennetty Suomessa yhteiskunnan elintärkeiden toimintojen turvaamisen strategian (YETTS) kautta ja niitä torjutaan mm. sisäisen turvallisuuden ohjelman (STO) avulla. Laajamuotoiseksi ja poikkileikkaavaksi teeman tekevät uudet rikollisuuden muodot mahdollistavat tekijät, kuten tietoverkot ja kriittiset infrastruktuurit.

1.5.2.1 Verkkorikollisuus (cybercrime)

Muuttuvan rikollisuuden yksi nopeimmin leviävä ilmiö on verkkorikollisuus, jonka vakavampi versio on verkkoterrorismi (cyberterrorism). Verkkoterrorismissa terroristit käyttävät tietoverkkoa (pääasiassa internetiä) hyökkäyksiin ja muuhun terrorismia tukevaan toimintaan.

Verkkorikollisuuden torjunta on synnyttänyt lukuisia eri suojautumismenetelmiä ja teknologioita. Kuvassa 1.2 on Gartnerin hype-käyrä[9] koskien infrastruktuurien suojaamista (Syyskuu 2008). Ongelmana on, että suojautumismenetelmät ovat fragmentoituneita, yhteensopimattomia keskenään ja irrallisia muun muassa liiketoimintaprosesseista. Useissa tapauksissa suojautumismenetelmät jopa aiheuttavat uusia tietoturvaongelmia.



DAM	Database Activity Monitoring	IPS	Intrusion Prevention System
DDoS	Distributed Denial of Service	SIEM	Security Information and Event Management
HIPS	Host-based Intrusion Prevention System	SMB	Server Message Block
IDS	Intrusion Detection System	XML	eXtensible Markup Language

Kuva 1.2 Hype cycle, infrastructure protection 2008 (Gartner)[10]

[9] Gartnerin hype-käyrä, http://en.wikipedia.org/wiki/Hype_cycle
[10] Gartner, 2008.

1.5.3 Critical Information Infrastructure Protection (CIIP)

Euroopan komissio julkisti 30.3.2009 tiedonannon tietoyhteiskunnan kriittisten infrastruktuurien suojaamiseksi (CIIP)[11,12]. Politiikka määrittelee suunnitelmat välittömille toimenpiteille vahvistaa tietoyhteiskunnan kriittisten infrastruktuurien turvallisuutta ja vahingoista toipumista. Viimeaikaisia esimerkkejä ovat Viroon keväällä 2007 kohdistunut tietoverkkohyökkäysten sarja, joka pysäytti pankit, poliisiasemat ja hallituksen toimistot viikoksi, ja merenalaisten kaapelien katkeaminen vuonna 2008.

Maailman talousfoorumi arvioi vuonna 2008, että tietoyhteiskunnan elintärkeiden infrastruktuurien laajan toimintahäiriön todennäköisyys seuraavan 10 vuoden kuluessa on 10–20 %. Toimintahäiriö voisi maailmanlaajuisesti aiheuttaa jopa 170 miljardin euron kustannukset[13].

1.5.4 Ennustamaton ICT-ekosysteemi[14]

Internetin teknistaloudellisessa ekosysteemissä osien ja niiden välisten riippuvuuksien määrä on kasvanut niin suureksi, että kokonaisuutta on hyödyllisempää ajatella kompleksisena systeeminä kuin vain koneena. Tällaista systeemiä ei suunnitella vaan se syntyy osiensa ja niiden vuorovaikutusten tuloksena. Häiriö systeemin yhdessä osassa voi aiheuttaa vaikeasti ennustettavia muutoksia toisaalla.

Perinteinen riskinhallinta–tunnista vaarat ja poista ne–ei enää sovellu. On varauduttava selviämään vahingoista (toipuminen ja jatkuvuussuunnittelu). Vahingoista toipumisen rinnalla kokonaisongelma olisi pystyttävä paloittelemaan ohjattaviksi, mutta toimiviksi osiksi, ja operoitava niissä (”new sustainable economy”)[15].

1.6 Suhde varautumiseen - normaaliolojen varautuminen uhkien toteutumisen estämistä

YKÄ-toiminnalla on suora suhde varautumiseen, koska tietoyhteiskunnan toimintojen tulee olla käytettävissä kaikissa turvallisuustilanteissa. Varautuminen on uhkakuvien analysointia ja toiminnan varmistamista normaalioloissa.

1.6.1 Tietoyhteiskuntaan integroitunut varautumisjärjestelmä

Suomessa on varautumisjärjestelmä, joka perustuu yhteiskuntaan integroituun varautumissuunnitteluun ja kriittisten tuotantopanosten varastointiin. Integraatiossa tieto- ja viestintäjärjestelmien (ICT) rooli on keskeinen ja sen merkitys syventyy entisestään. Kriittiset infrastruktuurit ja niiden kautta yhteiskunnan elintärkeät toiminnot ovat riippuvaisia ICT-järjestelmistä ja sähkön saannista.

---

[11] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

[12] Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle sekä alueiden komitealle tietoyhteiskunnan elintärkeiden infrastruktuurien suojaamisesta ”Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja -häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen”, Bryssel 30.3.2009, KOM(2009)149 lopullinen.

[13] Global Risks 2008.

[14] Prof. Heikki Hämmäinen, Tietoverkkojen toiminta halutaan varmistaa, Tiedosta-lehti, Tieke, 9.3.2009.

[15] Leppävuori, 2008.

Valtioneuvosto ja valtioneuvoston päätös huoltovarmuuden tavoitteista (Vnp 539/2008) ohjaavat varautumista, jonka tavoitteena on suomalaisten selviytyminen erilaisissa yhteiskunnan häiriö- ja poikkeustilanteissa. Valtioneuvosto hyväksyi vuonna 2006 Yhteiskunnan elintärkeiden toimintojen turvaamisen strategian (YETTS), jolla eri hallinnonalojen varautuminen sovitetaan yhteen. Ministeriöt ohjaavat ja seuraavat oman alansa varautumista.

Yritysten varautumisen lähtökohtana ovat liiketoiminnalliset perusteet, asiakkaiden kanssa tehdyt sopimukset sekä toiminnan riskienhallinta. Esimerkiksi finanssitoimialaa velvoitetaan lisäksi lainsäädännöllä varautumaan häiriöihin.

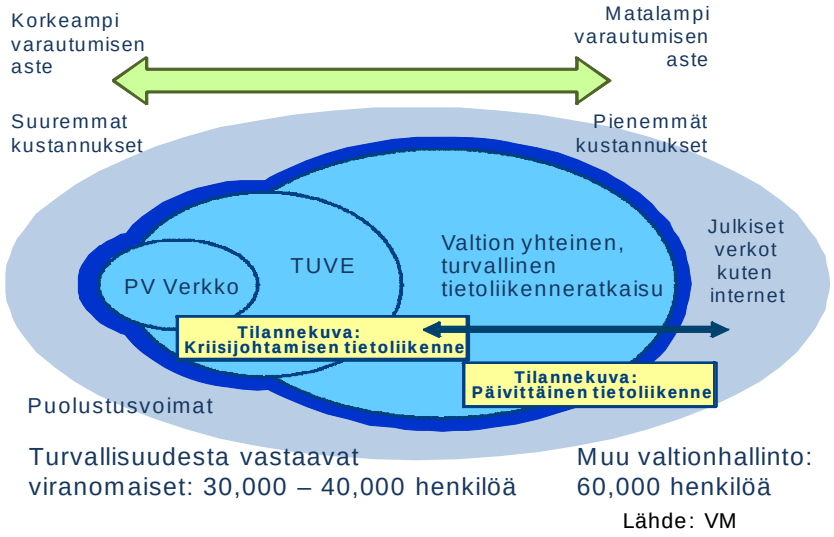
Kansalaisjärjestöillä on merkittävä rooli käytännön turvallisuuden lisäämisessä. Ne lisäävät toiminnallaan myös yhteiskunnan kriisinkestokykyä.

1.6.2 Uhkiin varaudutaan normaalioloissa

Kaikkia uhkia ei laajallakaan varautumisella kyetä ennakoimaan ja ehkäisemään. Yllättäviä ja äkillisiä tapahtumia, jotka myös vaativat normaalista poikkeavaa johtamista ja tiedottamista, kutsutaan erityistilanteiksi. Erityistilanne voi syntyä niin normaalioloissa, häiriötilanteessa kuin poikkeusolojen aikana.

1.6.3 Tilannekuvaa kootaan julkisten verkkojen kautta

Kuvassa 1.3 on valtion tietoliikennekokonaisuus, mistä näkyy valtion eri verkot ja niiden varautumisasteet yleisellä tasolla. Valtion tilannekuvan kokoaa eri ministeriöistä ja muista määrätyistä organisaatioista Valtioneuvoston turvallisuuspalvelut -yksikkö. Julkisten verkkojen (internet, mobiili, yritysverkot, muut) merkitys on suuri päivittäisen tilannekuvan muodostamisessa. YKÄ-toiminnalla on tässä tärkeä rooli elintärkeiden ICT-palveluiden käytettävyyden kehittämisessä.



Kuva 1.3 Valtion tietoliikennekokonaisuus

1.7 Raportin tavoitteet

YKÄ-työn tavoitteena on ollut saada yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien (ICT) *käytettävyydestä* kuva kaikilla yhteiskunnan tasoilla (valtio, julkishallinto, arjen tietoyhteiskunta) ja kaikissa turvallisuustilanteissa (normaaliolot, häiriötilanteet, poikkeustilanteet) sekä esittää havaittuihin ongelmatilanteisiin ratkaisumalleja ja konkreettisia parannusehdotuksia sekä toimenpiteitä vastuukysymyksineen ja kustannusvaikutuksineen.

1.7.1 Tarkastelukehikko

Raportissa on tavoitetta varten määritelty yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien (ICT) yleinen toiminnallinen kehikko, minkä pohjalta voidaan tarkastella kriittistä ICT-infrastruktuuria. Kehikolla voidaan määritellä elintärkeiden toimintojen perusrakenteiden kriittiset ICT-toiminnot ja komponentit sekä näiden päällä ala- ja sektorikohtaiset kriittiset ICT-toiminnot ja komponentit.

Raportissa on analysoitu yleisellä tasolla tieto- ja viestintäjärjestelmien kriittisyyttä ja nykytilaa sekä suhdetta varautumiseen sekä sitä, tukeeko lainsäädäntö riittävästi käytettävyyttä. YKÄ-työryhmä on ollut tiiviissä yhteistyössä muiden hallinnon turvallisuushankkeita kehittävien työryhmien kanssa sekä pyrkinyt sovittamaan työnsä siten että päällekkäisyyksiä ei suuremmin syntyisi.

Raportissa on selvitetty ovatko nykyiset kriittisen infrastruktuurin suojaustoimet riittäviä. Raportissa on esitetty konkreettisia kriittisen ICT- infrastruktuurin potentiaalisia ongelma-alueita ja haavoittuvuuskohtia sekä esitetty näihin parannus- ja ratkaisuehdotuksia. Tämä koskee myös energiahuollon osuutta televerkoille ja siinä potentiaalisia ongelma-alueita.

1.7.2 Elintärkeiden infrastruktuurien käytettävyys

Elintärkeiden toimintojen uhkatekijöiden ja järjestelmien käytettävyyden tarkastelussa on kaksi näkökulmaa ja päätasoa, CIP (*Critical Infrastructure Protection*)- ja CIIP (*Critical Information Infrastructure Protection*) -näkökulma ja sekä prosessi- että rakennetasot. CIP tähtää liiketoimintaprosessien ja rakenteiden jatkuvuuden turvaamiseen kaikissa kriittisissä infrastruktuureissa. CIIP tähtää liiketoimintaprosessien ja rakenteiden käytettävyyden turvaamiseen ja optimointiin kriittisissä ICT-järjestelmissä.

Raportissa luotu tarkastelukehikko mahdollistaa CIP- ja CIIP-tarpeiden tarkastelemisen yleisellä tasolla sekä vaikutuksien analysoimisen yhteiskunnan elintärkeiden ICT-toimintojen ja järjestelmien käytettävyyteen ja liiketoimintaan.

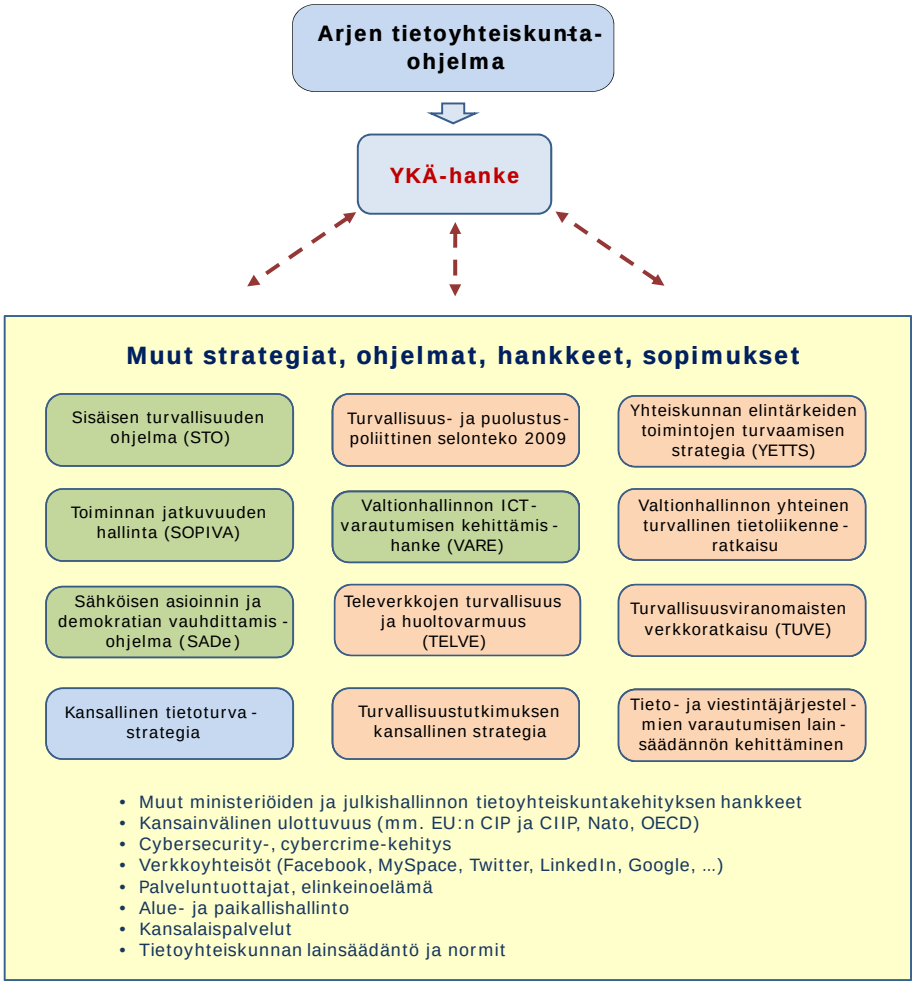
1.7.3 YKÄ-hankkeen suhde muihin kokonaisuuksiin

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien **käytettävyyden** kehittämisen (YKÄ-hankkeen) merkitys ja yleiset tavoitteet on määritelty liikenne- ja viestintäministeriöstä johdetussa **Arjen tietoyhteiskunta** -ohjelmassa.

YKÄ-hankkeella on monia ulottuvuuksia. YKÄ:n työ sivuaa useita julkishallinnon strategia-, ohjelma- ja hankekokonaisuuksia (kuva 1.4). YKÄ-toimintaan liittyy keskeisesti myös EU:n CIP- ja CIIP-kehitykseen osallistuminen ja vaikuttaminen. Tietoyhteiskunnan uudet ilmiöt, kuten verkkoyhteisöt, on myös huomioitava.

Keskeinen YKÄ-akseli on yksityinen sektori ja sen palveluntarjonta–käyttäjät (julkishallinto, yritykset, kansalaiset) sopimuksineen ja kehityshankkeineen.

YKÄ-työllä on läheinen suhde erityisesti valtion ICT-varautumisen VARE-hankkeeseen sekä sisäisen turvallisuuden ohjelmaan (STO). Sekä YKÄ että VARE katsovat samoja haasteita ja uhkakuvia palveluiden tuottajien ja käyttäjien näkökulmasta. Palveluiden tuottajina ovat pääsääntöiset samat yksityisen sektorin toimijat. STO-ohjelman toteutumisessa luottamus tietoyhteiskunnan palveluihin ja niiden saatavuuteen ja käytettävyyteen on ensiarvoisen tärkeää.



Kuva 1.4 YKÄ-hankkeen laaja suhde muihin kokonaisuuksiin

2 TOIMINTAYMPÄRISTÖ

2.1 Yleistilanne

2.1.1 Yhteiskunnan elintärkeät toiminnot

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETTS)[16] määrittelee yhteiskunnan elintärkeiksi toiminnoiksi seuraavat seitsemän (7) toimintoa: *valtion johtaminen, kansainvälinen toiminta, valtakunnan sotilaallinen puolustaminen, sisäisen turvallisuuden ylläpitäminen, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky* ja *henkinen kriisinkestävyys.*

2.1.2 Kriittiset toimialat

Huoltovarmuuden turvaaminen on jaettu seitsemään kriittiseen toimialaan (infrastruktuuriin) [17]:

- tietoyhteiskunta,
- energiahuolto,
- rahoitushuolto,
- kuljetuslogistiikka,
- terveydenhuolto,
- kriittinen perusteollisuus, ja
- elintarvikehuolto.

Kriittiset infrastruktuurit muodostuvat yhteiskunnan jatkuvan toiminnan kannalta välttämättömistä rakenteista ja toiminnoista. Kriittisiin infrastruktuureihin kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja. Näiden turvaaminen tarkoittaa yksittäisten kriittisten kohtien löytämistä ja turvaamista, kuitenkin koko ajan infrastruktuurikokonaisuuden toimintaa silmällä pitäen.

2.1.3 Yhteiskuntaan integroitunut varautuminen

Suomessa on tietoyhteiskuntaan integroitunut varautumisjärjestelmä, joka perustuu kriittisten tuotantopanosten varastointiin ja yhteiskuntaan integroituun varautumissuunnitteluun. Kaikki kriittiset infrastruktuurit ja niiden kautta yhteiskunnan elintärkeät toiminnot ovat riippuvaisia tieto- ja viestintäjärjestelmistä (ICT) ja sähkön saannista.

ICT:n merkitystä kriittisillä toimialoilla on tarkasteltu lyhyesti liitteessä 1 muutamien markkina- ja volyymitunnuslukujen valossa.

Yhteiskunnan elintärkeiden toimintojen turvaaminen, huoltovarmuuden ylläpito ja kehittäminen, on saumatonta yhteistyötä valtion ja elinkeinoelämän välillä. Valtion tasolla kriittisiä yrityksiä on noin 2000 ja näillä suuri määrä verkostokumppaneita. Yhteistyötä koordinoi Huoltovarmuuskeskus.

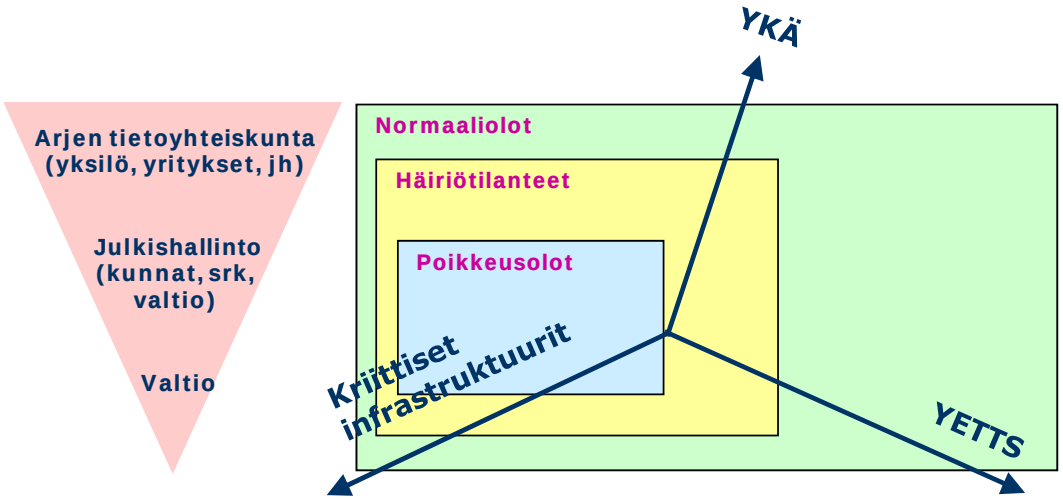
---

[16] Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös, 23.11.2006.
[17] http://www.huoltovarmuus.fi/.

2.1.4 YKÄ-toiminta

Kuvassa 2.1 on yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien ICT-järjestelmien käytettävyyden (YKÄ) suhde YETT-strategiaan ja kriittisiin toimialoihin Arjen tietoyhteiskunnassa.

YKÄ-toiminta ulottuu läpi kaikkien hallinnon alojen (ICT-sektorissa), ja sisältää koko skaalan valtion tarpeista arjen tietoyhteiskuntaan yrityksiin ja yksilöön saakka. YKÄ-toiminta ulottuu lisäksi kaikkiin turvallisuustilanteisiin (normaaliolot, häiriötilanteet, poikkeusolot).



YETTS	Kriittiset toimialat	YKÄ

• Valtion johtaminen
• Kansainvälinen toiminta
• Valtakunnan sotilaallinen puolustaminen
• Sisäisen turvallisuuden ylläpitäminen
• Talouden ja infrastruktuurin toimivuus
• Väestön toimeentuloturva ja toimintakyky
• Henkinen kriisinkestävyys
	• Energiahuolto
	• Tieto- ja viestintäjärjestelmät
	• Elintarvikehuolto
	• Terveydenhuolto
	• Pankki- ja rahoitustoiminta
	• Kuljetuslogistiikka
	• Kriittinen perusteollisuus
		• Tietoyhteiskunnan syventäminen
		  • Perusteltu luottamus (Käytettävyys /saatavuus, palvelutaso, tietoturva, …)
		  • ICT-toiminnan varmistaminen
		  • Kriittiset tieto- ja viestintäjärjestelmät (ICT / CI)
		• Aikajänne
		• Suhde varautumiseen

Kuva 2.1 YKÄ-toiminnan suhde YETT-strategiaan ja elintärkeisiin toimialoihin Arjen tietoyhteiskunnassa

2.2 YKÄ-toimintaan liittyvät hallinnon ohjausmekanismit, ohjelmat ja hankkeet

YKÄ-toiminnan moniulotteisuudesta johtuen siihen viitataan ja sille luodaan puitteita monella tasolla hallinnossa eri organisaatioissa sekä ohjelmissa ja hankkeissa turvallisuus- ja puolustuspoliittisesta selonteosta valtion ja kansalaisen tietoturvastrategioihin ja tieto- ja viestintäjärjestelmien normistoihin saakka.

2.2.1 Hallinnon ohjausmekanismit

Hallinnon strategioita, ohjelmia ja hankkeita ohjataan hallitusohjelmalla, lainsäädännöllä ja oikeuskäytännöillä, normeilla ja ohjeilla, toimilupaehdoilla, teknisillä ohjeilla sekä sopimuksilla tai muilla velvoitteilla. Viranomaisten velvollisuus varautumiseen poikkeusoloihin perustuu valmiuslakiin.

Valtioneuvostolla, valtion hallintoviranomaisilla, valtion itsenäisillä julkisoikeudellisilla laitoksilla, muilla valtion viranomaisilla ja valtion liikelaitoksilla sekä kunnilla, kuntayhtymillä ja muilla kuntien yhteenliittymillä on velvollisuus varmistaa tehtäviensä mahdollisimman hyvä hoitaminen eri tilanteissa.

Osalla strategioista, kuten YETT-strategialla, ohjataan lähinnä hallintoa. YETT-strategiaa ei ole tehty elinkeinoelämää varten. YETT-strategiasta puuttuu rahoitus- ja investointipäätökset sekä tulo-odotukset. Strategiasta puuttuu myös ohjaustyökalut.

2.2.2 Strategiat, ohjelmat ja hankkeet

YKÄ-toiminta ottaa huomioon seuraavat strategiat, ohjelmat ja hankkeet. Arjen tietoyhteiskuntaohjelma on ensimmäisenä koska siinä on luotu tarpeet ja puitteet YKÄ-toiminnalle

- Arjen tietoyhteiskunta -ohjelma
- Sähköisen asioinnin ja demokratian vauhdittamisohjelma (SADe)
- Kansallinen tietoturvastrategia
- Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETTS)
- Sisäisen turvallisuuden ohjelma (STO)
- Valtionhallinnon ICT-varautumisen kehittämishanke (VARE)
- Toiminnan jatkuvuuden hallinta (SOPIVA)
- Televerkkojen turvallisuus ja huoltovarmuus (TELVE)
- Valtionhallinnon yhteinen turvallinen tietoliikenneratkaisu
- Turvallisuusviranomaisten verkkoratkaisu (TUVE)
- Turvallisuus- ja puolustuspoliittinen selonteko 2009
- Tieto- ja viestintäjärjestelmien varautumisen lainsäädännön kehittäminen
- Turvallisuustutkimuksen kansallinen strategia

2.2.3 Vastuuorganisaatiot

YKÄ-toimintaa toteuttavat mm.

- Viestintävirasto (Ficora)
- Valtion IT-palvelukeskus (VIP)
- Huoltovarmuusorganisaatio (ml. HVK)
- Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI)
- Julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA)
- Sektorihallinnon vastuuorganisaatiot (kuten Finanssivalvonta)
- Omistajaohjauksen toimijat (VM:n omistajaohjausyksikkö Solidium)
- Yrityssektori

2.2.4 Ministeriöt

YKÄ-toimintaan liittyviä, eri ministeriöille lailla säädeltyjä vastuita ei poista toteutusvastuun delegointi muille organisaatioille. Vastuut on esitetty liitteessä 2.

Liitteessä 2 on laajempi yhteenveto strategioista, ohjelmista ja hankkeista sekä vastuuorganisaatioista. Ohjausmekanismeja on esitetty lähemmin kunkin strategian tai hankkeen kohdalla. Liitteessä 3 on yhteenveto YKÄ-alueen kansallisesta t&k-toiminnasta, kansainvälisistä CII- ja CIIP-hankkeista sekä alan standardeista ja vaatimuksista.

2.3 Euroopan elintärkeiden infrastruktuurien suojaaminen

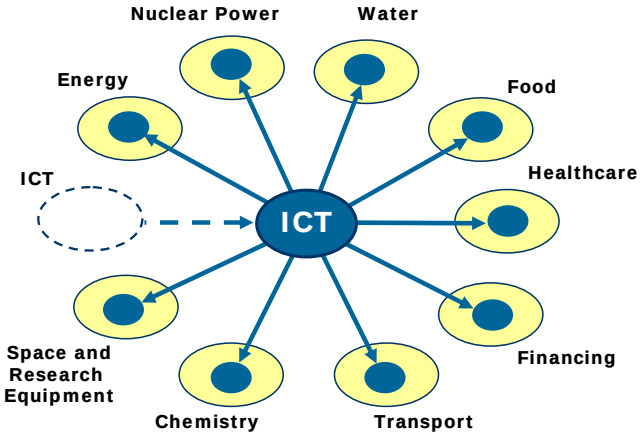
Suomessa elintärkeiden infrastruktuurien suojaamisella on pitkä historia ja toimivat yhteistyömallit. Suomi on vaikuttanut Euroopan unionin käynnistämän kriittisen infrastruktuurin suojaamiseen liittyvään yhteistyöhön. Suomi on pitkälti jo toteuttanut EU:n ohjelmassa hahmoteltuja toimenpiteitä.

2.3.1 ECI

Elintärkeät infrastruktuurit, joilla on valtioiden rajat ylittäviä vaikutuksia, määritellään ja nimetään Euroopan elintärkeiksi infrastruktuureiksi (*European Critical Infrastuctures*, ECI). EU-komission hyväksymässä vihreässä kirjassa (marraskuu 2005) esitetyt elintärkeät infrastruktuurit (ECI) tuotteineen ja palveluineen on esitetty liitteessä 2.

Koska elintärkeät infrastruktuurit ulottuvat yli valtioiden rajojen, niiden heikkouksien, haavoittuvuuden ja turvallisuuspuutteiden kartoittamisessa olisi hyötyä koko EU:n laajuisesta yhtenäisestä menettelystä, joka täydentäisi jäsenvaltioissa jo toteutettavia kansallisia suojaamisohjelmia ja toisi niille lisäarvoa. Tällainen menettely vahvistaisi myös EU:n sisämarkkinoiden kykyä turvata yritystoiminnan kannattavuus ja luoda vaurautta jatkuvalta pohjalta.

Kuvassa 2.2 on hallintojen usein esittämä näkemys Euroopan kriittisistä infrastruktuureista (ECI). Koska ICT-järjestelmät ovat strategisia ja integroituja osia muissa kriittisissä infrastruktuureissa, se on kuvassa viety (raportin tekijän toimesta) niihin kaikkiin sisään.



Kuva 2.2
Euroopan unionin määrittelemät elintärkeät infrastruktuurit

2.3.2 ECI/IT

EU:n määrittelemät tietoyhteiskunnan kriittiset viestintäjärjestelmät (ICT-osasektorit) ovat: internet, kiinteät verkot, mobiili verkot, radio- ja navigointijärjestelmät, satelliittijärjestelmät ja yleisradiojärjestelmät. Viestintäjärjestelmien rakenneosat (ICT-kerrokset) ovat: ympäristö, energia, laitteistot, ohjelmistot, verkot, sisällöt, politiikat ja käytännöt, käyttäjät ja lisäarvopalvelut.

2.3.3 CIIP-aloite ja EPCIP

Euroopan unionissa hyväksyttiin 2008 pitkään valmisteilla ollut aloite tietoyhteiskunnan elintärkeiden infrastruktuurien suojaamisesta. Tätä CIIP-aloitetta toteutetaan osana laajempaa Euroopan elintärkeiden infrastruktuurien suojeluohjelmaa (EPCIP, European Programme for Critical Infrastructure Protection) ja sen rinnalla. EPCIP-ohjelmaa johdetaan suoraan DG JLS-pääosastosta (Justice, Freedom and Security)[18]. Euroopan unionin neuvosto hyväksyi EPCIP-ohjelman huhtikuussa 2007.

EPCIP tarkastelee ja tukee keinoja parantaa kriittisten infrastruktuurien suojaamista. Suojauskeinoja tarvitaan erityisesti osana terrorismin torjuntaa, mutta myös muiden syiden kuten luonnonkatastrofien ja teknologisten katastrofien varalta. EU:n terminologiassa kriittiset infrastruktuurit ovat sellaisia yhteiskunnan toiminnan kannalta elintärkeitä järjestelmiä, joiden toiminta vaikuttaa vähintään kahden Euroopan valtion alueella, ja joiden tehokas suojaaminen vaatii yhtenäisiä ja koordinoituja suojausjärjestelyjä ja valtiorajat ylittävää yhteistyötä.

2.3.4 Direktiivi

Yksi EPCIP-ohjelman keskeisistä elementeistä on Euroopan elintärkeiden infrastruktuurien määrittämisestä ja nimeämisestä joulukuussa 2008 annettu direktiivi[19,20]. Toinen ohjelman tärkeä elementti on elintärkeiden infrastruktuurien varoitusjärjestelmä (CIWIN)[21].

Direktiivi 2008/114/EY ”Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista” on ensimmäinen askel kohti ECI-määrittelyitä ja arviointeja. Direktiiviä sovelletaan aluksi energia- ja kuljetusalaan. Direktiiviä arvioidaan kolmen vuoden päästä ja seuraavaan uusittuun direktiiviin on tarkoitus ottaa mukaan ICT-ala.

2.4 Kansainväliset kyberaloitteet

Kansainväliset, lähes jokaviikkoiset verkkohyökkäykset kriittisiä infrastruktuureja vastaan eri puolilla maailmaa ovat aiheuttaneet monien kyberaloitteiden synnyn. Nato pe-

[18] http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm
[19] Direktiivi 2008/114/EY.
[20] http://register.consilium.europa.eu/pdf/fi/08/st16/st16862.fi08.pdf
[21] KOM(2008) 676 lopullinen.

rusti keväällä 2008 Viroon uuden kyberpuolustuskeskuksen[22]. Eritasoisia kyberaloitteita on lukuisia muitakin (mm. Cyber Initiative, USA[23], joka on salainen).

3 YHTEISKUNNAN ELINTÄRKEÄT TOIMINNOT JA UHKAMALLIT

3.1 Toimintojen kokonaisuus

Valtioneuvosto esittää tarvittavat yhteiskunnan elintärkeiden toimintojen[24] turvaamisen poliittiset linjaukset turvallisuus- ja puolustuspoliittisissa selonteoissa, jotka annetaan eduskunnalle hyväksyttäviksi. Selontekokäytäntö antaa valtioneuvostolle ja eduskunnalle mahdollisuuden laajaan turvallisuuteen liittyvien kysymysten säännölliseen ja perusteelliseen käsittelyyn. Selonteoissa arvioidaan turvallisuusympäristön kehittymistä ja määritetään sen perusteella Suomen toimintalinjat.

Elintärkeät toiminnot ovat poikkihallinnollisia yhteiskunnalle välttämättömiä toimintokokonaisuuksia, joiden jatkuvuus on oltava turvattuna joka hetki, kuva 3.1.

Yhteiskunnan elintärkeitä toimintoja ovat:

- valtion johtaminen
- kansainvälinen toiminta
- valtakunnan sotilaallinen puolustaminen
- sisäisen turvallisuuden ylläpitäminen
- talouden ja infrastruktuurin toimivuus
- väestön toimeentuloturva ja toimintakyky sekä
- henkinen kriisinkestävyys.

Kuva 3.1 Yhteiskunnan elintärkeät toiminnot turvataan huolehtimalla strategisista tehtävistä

Kullekin toiminnolle on kuvattu tavoitetila, joka antaa perusteet määrittää ministeriöiden vastuulla olevat strategiset tehtävät sekä näiden ylläpito- ja kehittämistarpeet. Toimintojen ja niiden tavoitetilojen kuvauksissa sekä strategisten tehtävien hoitamisen edellyttämässä kehittämisessä on otettu huomioon Suomen jäsenyys Euroopan unionissa, toiminta Yhdistyneissä kansakunnissa sekä Naton rauhankumppanuusyhteistyössä ja muissa kansainvälisissä yhteyksissä.

3.2 Turvallisuustilanteet ja uhkamallit

Yhteiskunnan elintärkeiden toimintojen turvallisuustilanteet ja niitä uhkaavat uhkakuvat ja -tekijät ovat pääsääntöisesti samat oli sitten kysymyksessä julkishallinnon tai yritysten tai yhteiskunnan kansalaistason toiminta. Ero tulee lähinnä siitä onko kysymyksessä normaali-, poikkeus-, vaiko kriisitilanteiden johtamisolot.

YKÄ-toiminta käsittää ICT-järjestelmien ja niiden energiahuollon käytettävyyden turvaamista kaikissa olosuhteissa.

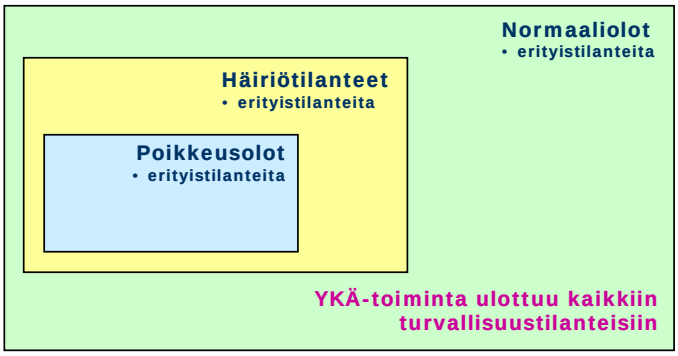
---

[22] Helsingin Sanomat, 11.6.2008.
[23] http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html
[24] Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös, 23.11.2006.

3.2.1 Turvallisuustilanteet

Yhteiskunnan on kyettävä turvaamaan elintärkeät toiminnot kaikissa tilanteissa. Varautumisessa korostetaan normaalioloissa rakennettujen järjestelyjen ja toteutettujen toimenpiteiden tärkeyttä. Erityisesti johtamiseen ja elintärkeiden toimintojen ohjaamiseen tarvittavat sähköisen viestinnän ja tietoliikenteen sekä energiahuollon järjestelmät on suojattava ja varmennettava jo normaalioloissa kestämään myös erilaisten häiriöiden ja poikkeusolojen vaatimukset.

Turvallisuustilanteita ovat normaaliolot, häiriötilanteet, ja poikkeusolot, joissa kaikissa tilanteissa saattaa esiintyä erityistilanteita (kuva 3.2). Yhteiskunnan elintärkeiden toimintojen kannalta välttämättömien tieto- ja viestintäjärjestelmien käytettävyys ulottuu kaikkiin turvallisuustilanteisiin jo pelkästään internetin ja mobiiliverkkojen kautta.



Kuva 3.2 Yhteiskunnan turvallisuustilanteet

Yhteiskunnan eri turvallisuustilanteiden kuvaus, samoin kuin YETT-uhkamallit ja erityistilanteet on esitetty tarkemmin liitteessä 2.

3.2.2 Uhkamallit

Uhkamalli tarkoittaa yleisellä tasolla olevaa kuvausta turvallisuusympäristön häiriöistä, jotka toteutuessaan voivat vaarantaa yhteiskunnan turvallisuuden, väestön elinmahdollisuudet tai valtiollisen itsenäisyyden. Tämän kaltaiset tilanteet voivat sijoittua ensisijaisesti yksilöön kohdistuvien uhkien ja toisaalta globaalien uhkien väliin. Näiden eri tasojen välillä on keskinäisriippuvuutta eikä niiden välistä rajaa pystytä tarkasti määrittelemään.

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategian uhkamallit ovat (YETT):

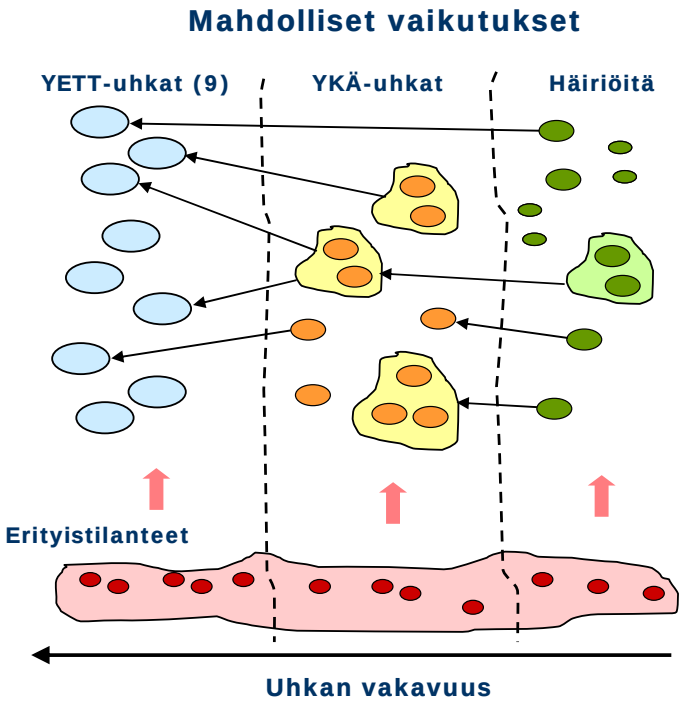
- Sähköisen infrastruktuurin häiriintyminen
- Väestön terveyden ja toimeentuloturvan vakava häiriintyminen
- Taloudellisen toimintakyvyn vakava häiriintyminen
- Suuronnettomuudet ja luonnon aiheuttamat onnettomuudet
- Ympäristöuhkat
- Terrorismi sekä järjestäytynyt ja muu vakava rikollisuus
- Väestöliikkeisiin liittyvät uhkat
- Poliittinen, taloudellinen ja sotilaallinen painostus
- Sotilaallisen voiman käyttö.

3.2.2.1 Uhkien vaikutustasot

Jääkö häiriötapahtuma yksittäisen yrityksen tai organisaation sisäiseksi tai pienen alueen kuluttajien uhkaksi ja toteutuessaan näkyväksi toimintahäiriöksi vai onko sillä toteutuessaan yhteiskunnalle laajempaakin merkitystä normaalioloissa (YKÄ- ja YETT -taso) tai jopa valtion toiminnalle häiriö- ja poikkeusoloissa (YETT-taso), riippuu häiriötapahtuman luonteesta ja laajuudesta.

Eritasoisia ICT-järjestelmissä ja energianhuollossa esiintyviä uhkia ja häiriöiden vaikutuksia on esitetty periaatteellisella tasolla kuvassa 3.3.

YKÄ-toiminnan turvaamisen kannalta olisi löydettävä YKÄ-uhkat ja niitä aiheuttavat häiriöt, joilla voi olla vaikutusta pelkästään paikallisesti mutta myös laajemminkin ja eri turvallisuustilanteisiin.



Kuva 3.3 ICT-järjestelmissä ja/tai energiahuollossa esiintyvistä häiriötapahtumista aiheutuvia uhkia ja vaikutuksia YKÄ- ja YETT-tasolle

Esimerkki: Kaminsky Flaw

Vika voi sijaita internetin infrastruktuurissa, jolloin kaikki liikenne voi olla uhattuna. Tästä on esimerkkinä keväällä 2008 löydetty vakava vika internetin DNS-nimipalvelinjärjestelmässä (*Kaminsky Flaw*)[25]. DNS-haavoittuvuuden vaarana nettikäyttäjille ei ole ainoastaan ohjautuminen haitallisille verkkosivuille. Hyökkääjät voivat myös yrittää sähköpostien kaappaamista. Koska kysymys on liikenteen reitittämisestä, ei ole merkitystä sillä millaista päätelaitetta käyttää (Windows, Linux, Macintosh, kännykkä), joissa on omat tietoturvaongelmansa.

[25] Dan Kaminsky, Black Hat Security Conference, USA, elokuu 2008.

> Kaminsky-virhe on ollut internetissä alusta saakka, eli 25 vuotta. Tätä DNS-haavoittuvuutta ei ole vieläkään kaikista nimipalvelimista korjattu. Viestintäviraston mukaan joka kymmenes nimipalvelin on vieläkin (tammikuu 2009) korjaamatta. Korjaamattomia palvelimia on kaikkialla; julkishallinnossa, yrityksillä, internet-operaattoreilla ja yksityisillä ihmisillä.

DNS-haavoittuvuus on tyyppiesimerkki yhteiskunnan elintärkeiden toimintojen suurista uhkista. Internetiä ei ole aikoinaan rakennettu ns. ”carrier-grade” laatutasolla siten kuin esimerkiksi puhelinverkot tai mobiili verkot on rakennettu. Internetiä on jouduttu paikkaamaan aina kun uusia haavoittuvuuksia on löytynyt. On todennäköistä, että internetissä on vielä lukuisia vakavia aukkoja.

3.2.3 Uhka-analyysi

Taulukossa 3.1 on esitetty pieni osa VARE-hankkeessa[26] tehdystä uhka-analyysista esimerkkinä siitä millaisia vaikutuksia YETT-uhkat ja niiden erityistilanteet voivat aiheuttaa tietoyhteiskunnan toimintaan.

VARE-hankkeessa on tehty laajempi analyysi YETT-uhkamalleista ja niiden erityistilanteista vaikutuksineen tällä hetkellä (2008) sekä VARE-toimenpideohjelman lopussa (2016). Tästä voidaan arvioida toimenpiteiden vaikutusta.

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategian (YETTS) uhkamallit erityistilanteineen ja niiden merkitys valtionhallinnon ICT-varautumiselle (VARE) ovat käytännössä monilta osin samat myös yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta kriittisten ICT-järjestelmien *käytettävyyden* kehittämiselle (YKÄ-toiminta). Sekä valtionhallinnon että koko tietoyhteiskunnan palveluketjut ja palvelutuotanto ovat viime kädessä samojen yksityisten yritysten hoidossa ja vastuulla.

[26] VARE-liite 2, uhka-analyysi ja skenaariot, v05, 28.5.2008. Esimerkkejä erityistilanteiden vaikutuksista ICT-toimintaan ja VARE-kehityksen vaikutuksesta tilanteeseen.

Taulukko 3.1 Esimerkkejä erityistilanteiden vaikutuksista tietoyhteiskunnan toimintaan

YETT-uhka ja sen erityistilanne		Tapahtuma	Vaikutus tietoyhteiskunnan toimintaan / käytettävyyteen
1. Sähköisen infrastruktuurin häiriintyminen			
Yleisiin tieto- ja viestintäjärjestelmiin kohdistunut laaja tuho tai toimintahäiriö	A	Tietoverkkojen ja –järjestelmien kellot menneet sekaisin	Tietojärjestelmien käyttämä kellonaikapalvelu (NTP) ei toimi kunnolla: sähköpostin lähettämis- ja vastaanoton kellonajat eivät täsmää, eräiden tapahtumanhallintaan perustuvien järjestelmien toiminta häiriintyy
	B	Laajat pitkäaikaiset sähkökatkokset myrskyn seurauksena	ICT-järjestelmät siirtyvät varavoimalle, osa varavoimasta ei toimi tai sen kesto on riittämätön, varavoima ei kata erityisesti käyttäjän kaikkia laitteita
	C	Voimakkaat omistusmuutokset	Toimintoja viedään ulkomaille, lakkautetaan ja yrityksiä pilkotaan
	D	Voimajohtoja kaadettu	Aiheuttaa paikallisia häiriöitä sähkönjakelussa
Sähköisen joukkoviestinnän teknisten järjestelmien laaja toimintahäiriö	A	Ohjelmanjakelun siirtoyhteyksissä vakavia vikoja	Joukkoviestintään tarvitaan merkittävästi yleisen televerkon resursseja
Energiaverkon suurhäiriö	A	Loviisan voimalan tuotanto ajetaan alas	Laaja energiajakelun häiriö, joka on kestoltaan varavoimajärjestelyn puskurin ylittävä
	B	Energiahuollon käytönvalvonnan häiriöt jatkuvat	
	D	Muuntoasematuhoja	Paikallisia tarpeita varavoimalle
2. Väestön terveyden ja toimeentulon vakava häiriintyminen			
Sosiaalivakuutuksen palveluverkon vakava toimintahäiriö	A	Palvelun tai perusrekisterien pitkäaikainen käytettävyyden lasku tietojen korrupoitumisen vuoksi	Maksutoimintojen perustietojen saatavuus heikkenee
3. Taloudellisen toimintakyvyn vakava häiriintyminen			
Kansainvälinen ja kotimainen maksujärjestelmien häiriö	A	Suuren pankin verkkotoimintojen sulkeminen vakavien tietoturvahaavoittuvuuksien vuoksi	Laskutuksen ja reskontaran toiminnan heikkenemisestä johtuvat hankintaongelmat
	B	Keskeisellä palveluntuottajalla vakava työvoimaongelma	Palvelutaso romahtaa
Rahoitusmarkkinoiden merkittävä häiriö	A	ICT-osakeiden merkittävä ja pitkäaikainen arvon putoaminen pörssissä, yritysjärjestelyt ja investointilama	Vaikeudet investoinneissa, yritysjärjestelyt
Ulkomaan kaupan häiriintyminen	A	Tietoturvaloukkausten vuoksi Suomen SEPA-toimintoja suljetaan	Varaosien ja kehittämisen edellyttämien materiaalihankintojen vaikeutuminen
4. Suuronnettomuudet ja luonnon aiheuttamat onnettomuudet			
Ydinonnettomuus Suomessa tai lähialueilla	A		EMP:n aiheuttamat suorat ongelmat, huoltojärjestelmän liikkuvuuteen kohdistuvat rajoitukset, työvoiman käytettävyys
	C	Suomen lähialueella vakava ydinonnettomuus	Valtion päätöksenteon ja turvallisuusviranomaisten toiminnan ylläpitäminen
Evakuointeja tai vakavia tuhoja aiheuttavat myrskyt, tulvat tai pato-onnettomuudet	A	Syysmyrskyn seurauksena Helsingin alueella vesi nousee 2,8 m	Helsingin alueella laajalti vesivahinkoja sekä teleoperaattoreiden että asiakasorganisaatioiden laitetiloissa viemärijärjestelmä tukkeuduttua, mikä aiheuttaa sekä tietoliikenteen että tietojärjestelmien infrastruktuurin tuhoutumista. Palvelujen tuotannossa on laajoja keskeytyksiä.
5. Ympäristöuhkat			
Alueen raskasmetalli- tai kemikaalipitoisuuden nousu yli terveydelle sallittujen rajojen	A		Huoltojärjestelmän häiriö liikkumisen rajoittamisen vuoksi
6. Terrorismi sekä järjestäytynyt ja muu vakava rikollisuus			
Valtion ylimpään johtoon ja merkittäviin instituutioihin tai yrityksiin kohdistuvat vakavat rikokset tai niillä uhkaaminen	A	Rikollisjärjestö uhkaa vahingoittaa valtionjohdon henkilöitä, mikäli sen vaatimuksiin ei suostuta	ICT-yrityksiin kohdistunut isku tai väkivaltainen tiedustelu
7. Väestöliikkeisiin liittyvät uhkat			
Laajamittaisen maahantulon tilanne	A		Tiedonsiirtotarpeen paikallinen kasvaminen
	B		Ilkivalta, mellakointi
8. Poliittinen, taloudellinen ja sotilaallinen painostus			
Sähköisen kaupankäynnin ja rahaliikenteen lamauttaminen	A	Luottokunnan varmennejärjestelmiin kohdistuu järjestelmällinen ja pitkävaikutteinen hyökkäys	Tukiresurssien ja varaosien saannin häiriöt
9. Sotilaallisen voiman käyttö			

A = erityistilanteet, jotka kohdistuvat suoraan ICT-infrastruktuuriin
B = erityistilanteet, jotka kohdistuvat ICT-infrastruktuurille välttämättömiin tukirakenteisiin ja heikentävät ICT:n käytettävyyttä
C = erityistilanteet, joiden hoitaminen aiheuttaa merkittäviä erityisvaatimuksia valtiohallinnon ICT:n toiminnalle ja käytettävyydelle
D = erityistilanteet, joista ei aiheudu merkittäviä häiriöitä ICT:lle tai joiden hoitaminen aiheuttaa erityisvaatimuksia vain jonkin hallinnonalan ICT:lle

4 TIETO- JA VIESTINTÄJÄRJESTELMIEN KRIITTISTEN OSIEN MÄÄRITTELY

4.1 Tietoyhteiskunnan kriittinen ICT-infrastruktuuri

4.1.1 ICT-evoluutio, uhkat ja haavoittuvuudet

Paikallinen, kansallinen ja globaali ICT-infrastruktuuri tarjoaa data-, puhe- ja videopalveluita julkisille ja yksityisille käyttäjille monentyyppisistä verkoista, sähköisistä laitteistoista, tietokoneista ja ohjelmistosovelluksista muodostuvissa kompleksisissa järjestelmissä, mitkä muodostuvat lisäksi monentyyppisistä erilaisista teknologioista. Tietoyhteiskunnan ICT-järjestelmiä ja palveluita tarjoavat vapaan kilpailun periaattein verkko- ja palveluoperaattorit sekä järjestelmätoimittajat ja integraattorit sekä yksityiset palveluntuottajat ja toimittajat, jotka voivat olla eri kokoisia aina kansainvälisistä organisaatioista pieniin paikallisiin yrityksiin saakka.

ICT-infrastruktuuri on alituisessa muutosvaiheessa ja murroksessa nopean teknisen kehityksen, uusien liiketoimintavaatimusten sekä liiketoimintaympäristön muutosten ja viranomaisten määräysten ja ohjauksen vuoksi.

Jatkuva evoluutio synnyttää uutta teknologiaa, uusia sovelluksia ja ohjelmistoja sekä uusia laitteita ja uusia toimintamalleja kaikilla ICT-infrastruktuurin eri osa-alueilla. ICT-infrastruktuurin eri osa-alueet ja komponentit riippuvat toisistaan ja kompleksisina järjestelminä ovat siten alttiita erilaisille haavoittuvuuksille ja uhkatekijöille.

4.1.2 Kriittinen ICT-infrastruktuuri

YKÄ-toiminnan kannalta kriittinen ICT-infrastruktuuri voidaan jakaa kriittisiin viestintäjärjestelmiin (osasektoreihin), kriittisiin tietojärjestelmiin sekä näiden rakenneosiin, ”ICT-kerroksiin”. Tätä on hahmoteltu kuvassa 4.1[27,28]. Kriittinen ICT komponentteineen on esitetty lähemmin liitteessä 1.

4.1.2.1 Kriittiset viestintäjärjestelmät

Tietoyhteiskunnan kriittiset viestintäjärjestelmät (viestinnän osasektorit) Euroopan komission esittämänä ovat

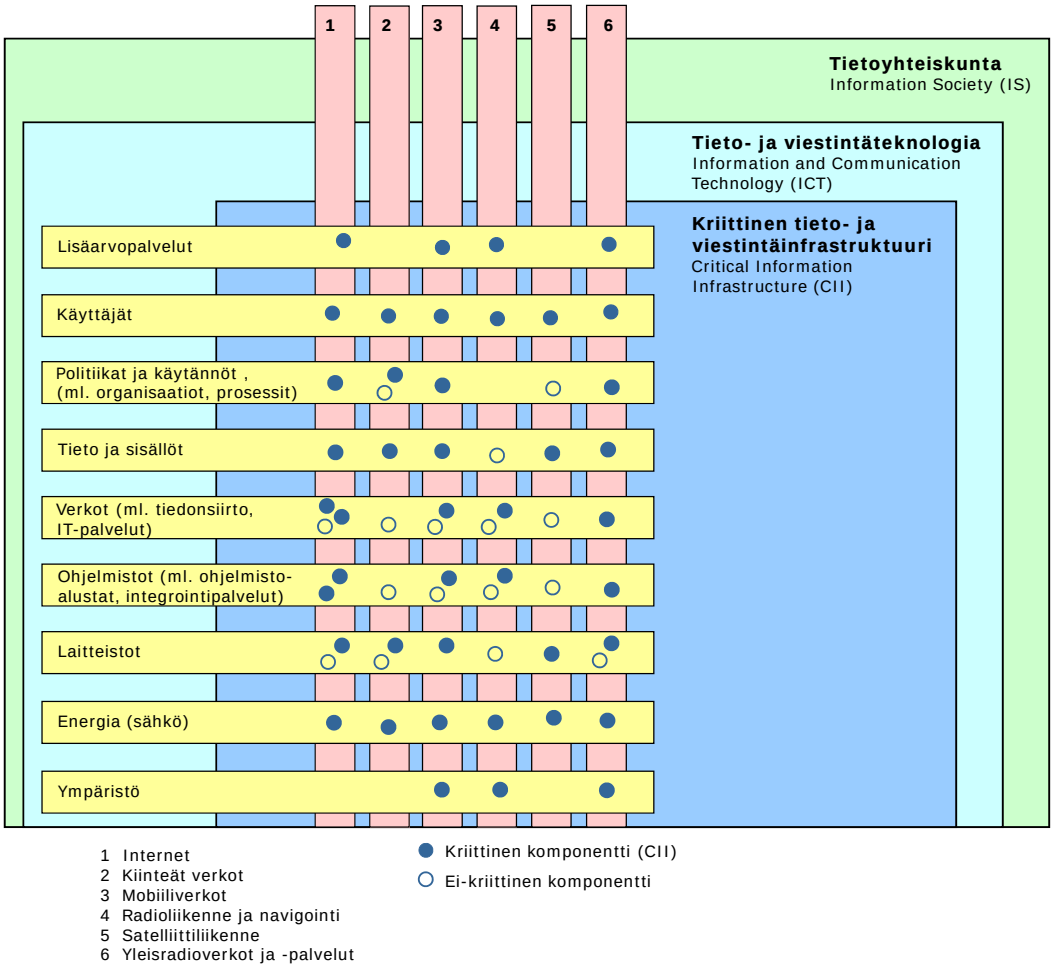
- Internet
- Kiinteät verkot (lanka, langaton)
- Mobiiliverkot
- Radioliikenne ja navigointi
- Satelliittiliikenne
- Yleisradioverkot ja –palvelut

Näiden sisällä voidaan erikseen tarkastella jonkin toimialan omia kriittisiä viestintäjärjestelmiä (esim. Virve).

---

[27] Towards the definition of criteria for the ICT sector, Marcelo Macera, IPSC-JRC, Feb. 2008.

[28] Mukailtu (raportin tekijä) selvityksessä, “The ARECI Study”, Availability and Robustness of Electronic Communications Infrastructures, March 2007, esitetystä.



Kuva 4.1 ICT-kerrokset sekä niiden kriittiset/ei-kriittiset komponentit osana kriittistä tieto- ja viestintäinfrastruktuuria (CII) sekä osana tietoyhteiskuntaa (IS), tunnistettavat kriittiset komponentit esitetty yleisellä tasolla

4.1.2.2 Kriittiset tietojärjestelmät

Tietoyhteiskunta, nimensä mukaisesti, sisältää hyvin monentasoisia ja monia tietojärjestelmiä. Voidaan todeta, että jokainen tietojärjestelmä, iso tai pieni, on kriittinen jollekin taholle sen omassa toiminnassaan. Kriittisen tietojärjestelmän määrittely yksikäsitteisesti on siten hankalaa.

VAHTI-työryhmä on määritellyt keskeiset tietojärjestelmät seuraavasti[29]:

- Keskeiset tietojärjestelmät ovat tietojärjestelmiä, jotka toteuttavat tai tukevat toimintoja, joiden puuttuminen, tietojen virheellisyys tai paljastuminen tuottavat yhteiskunnalle suuria taloudellisia tai muita vahinkoja. Toiminnot voivat olla myös sellaisia, että niiden puuttuminen tai häiriintynyt toiminta vaikuttaa yhteiskuntaa tai organisaation toimintaa lamauttavasti tai henkilöiden turvallisuutta heikentävästi.

[29] Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, Vahti 5/2004.

Keskeinen tietojärjestelmä voi muodostua useasta, keskenään kommunikoivasta tietojärjestelmästä.

Normaalioloissa käytettävien keskeisten tietojärjestelmien lisäksi on olemassa myös keskeisiä tietojärjestelmiä, joita käytetään vain poikkeusoloissa.

YKÄ-toiminnan kannalta kriittisiä tietojärjestelmiä ovat muun muassa
- Kriittisten toimialojen (ks. kohta 2.1.1) omat tietojärjestelmät
- Julkishallinnon rekisterit

Kriittisten toimialojen sisällä on monenlaisia toimialalle tyypillisiä tietojärjestelmiä, kuten finanssialan konesalit laitteistoineen, asiakaspalvelujärjestelmät ja Tupas-tunnistuspalvelu, tai energiansiirron ohjaus- ja valvontajärjestelmät (SCADA[30]), jne.

Julkishallinnon rekisterit voidaan jakaa
- Yhteiskunnan perusrekistereihin
  - Väestötietojärjestelmä (VTJ)
  - Kiinteistötietojärjestelmä (KTJ)
  - Valtakunnallinen yritys- ja yhteisötietojärjestelmä
- Hallinnollisiin rekistereihin
- Paikallisiin ja alueellisiin rekistereihin
- Tilastollisiin järjestelmiin (Tilastokeskus)

Yhteiskunnan perusrekisterien aineiston tuottajat ja ylläpitäjät ovat keskustasolla Väestörekisterikeskus, Maanmittauslaitos ja oikeusministeriö, Tilastokeskus, Verohallitus ja Patentti- ja rekisterihallitus. Perusrekisterijärjestelmät on luotu palvelemaan koko yhteiskuntaa siten, että tiedot olisivat mahdollisimman helposti saatavilla. Eri käyttäjäryhmille luovutetaan vuosittain satoja miljoonia tietoyksiköitä ominaisuustietoineen[31].

Julkishallinnon muut viranomaiset kuten Verohallitus, Kansaneläkelaitos ja työ- ja elinkeinoministeriö keräävät tietoja erilaisiin hallinnollisiin rekistereihin, joita käytetään muun muassa verotuksessa, kansaneläkkeiden määrittelyissä, työvoimapolitiikassa ja sosiaalitoiminnassa.

Julkishallinnon paikallis- ja alueorganisaatioilla on käytössä monenlaisia tietojärjestelmiä ja rekistereitä. Tietosisältö on yleensä laajempi kuin keskustason tietosisältö. Monet paikallis- ja aluehallintoviranomaiset toimivat myös perusrekisterien ylläpitäjinä.

Tunnistus.fi -palvelun kautta Verohallituksen, Kelan ja TEM:in palveluihin oli elokuun 2009 aikana yhteensä yli 700,000 tunnistusta. Volyymi on koko ajan voimakkaasti kasvanut. Federointiin perustuva, luotettavan henkilö- ja yritystunnistuksen tuottava, sähköisen asioinnin Tunnistus.fi -tukipalvelu on siten hyvä esimerkki julkishallinnon kriittisestä palvelusta.

[30] SCADA (Supervisory Control And Data Acquisition).
[31] Varovaisesti arvioituna perusrekistereistä luovutettiin jo vuonna 2004 yhteensä yli 300 miljoonaa tietoyksikköä ominaisuustietoineen eri käyttäjäryhmille eri menetelmin. Lähde: Esiselvitys asunto-osakkeiden omistuksen sähköisestä rekisteröinnistä, Patentti- ja rekisterihallituksen julkaisuja 1/2004.

4.1.2.3 ICT-kerrokset

Kukin viestinnän osasektori voidaan jakaa seuraaviin toiminnallisesti erillisiin ”ICT-kerroksiin”

- Lisäarvopalvelut (laajasti ymmärrettynä)
- Käyttäjät
- Politiikat ja käytännöt
- Tieto ja sisällöt
- Verkot
- Ohjelmistot ja sovellusalustat, järjestelmäintegrointi
- Laitteistot
- Energia
- Muun infrastruktuurin tuki ja toimivuus

ICT-infrastruktuuri riippuu myös muista kriittisistä infrastruktuureista, erityisesti energiasta (sähköstä).

5 KRIITTISTEN ICT-JÄRJESTELMIEN NYKYTILA JA KRIITTISYYDEN MÄÄRITTELY

5.1 Nykytila

5.1.1 Internetin ja mobiiliverkkojen strateginen merkitys

Internetillä ja mobiiliverkoilla on keskeinen ja kasvava rooli kaikkialla yhteiskunnassa. Molemmat ovat elintärkeitä niin hallinnoille, organisaatioille, yrityksille kuin kansalaisillekin. Käytännössä kaikki yhteiskunnan palvelut siirtyvät ennen pitkää internetiin.

Internetillä on myös kääntöpuolensa. Se tarjoaa järjestäytyneelle rikollisuudelle reaaliaikaisen, helppokäyttöisen ja globaalin markkinointi- ja myynti/osto -kanavan (huumeet, ihmiskauppa, terrorismi). Tietoturvahyökkäykset ovat arkipäivää ja erilaisia haittaohjelmia syntyy päivittäin satoja uusia. Palvelunestohyökkäykset (DoS) aiheuttavat suurta haittaa ja menetyksiä yrityksille.

5.1.2 Internet – kriittinen infrastruktuuri

Internet on tietoyhteiskunnan kriittinen infrastruktuuri. Internetillä tarkoitetaan tässä yhteydessä teknistä infrastruktuuria palveluineen, protokollineen, liitäntöineen ja normeineen, mikä rakentuu IP-protokollien varaan ja päälle. Internet määritellään sen käyttäjäkokemuksen kautta, jonka käyttäjien internet-yhteyspalvelun (operaattoreiden yhdysliikenteen välittämänä) liikenteen sovellukset tarjoavat (data, ääni, video). Internet käsittää siten myös operaattoreiden välisen yhdysliikenteen. Ficix[32] ja TREX[33] ovat siten myös osa kriittistä ICT-infrastruktuuria Suomessa.

---

[32] Vuonna 1993 toimintansa aloittanut FICIX (Finnish Communication and Internet Exchange - FICIX ry) on Internetin suurin solmupiste Suomessa. http://www.ficix.fi/.

[33] TREX (Tampere Region Exchange), the next generation internet exchange point, http://www.trex.fi/.

Internetin yksi pääominaisuus on laajakaista-access. Laajakaistan nopeus ja saatavuus kuvastavat jossain määrin myös koko tietoyhteiskunnan tilaa. Ilman tarpeeksi nopeaa laajakaistaa ei päästä kunnolla hyötymään internetin tuhansista palveluista. Ilman nopeaa laajakaistaa ei myöskään voida rakentaa laadultaan tarpeeksi korkeatasoista infrastruktuuria.

Internetillä on myös valtion tilannekuvan muodostamisessa tärkeä rooli.

Internetin vakavia suoraan infrastruktuuriin tai operointiin liittyviä riskejä ja uhkakuvia on käsitelty lähemmin liitteessä 1.

5.1.3 Mobiiliverkot

5.1.3.1 Tilannearvio

Kriittisenä infrastruktuurina Suomen mobiiliverkot ovat pääsääntöisesti korkealaatuiset ja kilpailun vuoksi palvelujen saatavuus on vähintäänkin kohtuullisella tasolla koko maassa. Palvelujen saatavuudessa, erityisesti joillakin harvaan asutuilla seuduilla on kuitenkin vielä kehittämisen varaa.

5.1.3.2 Riskit ja kehitysmahdollisuudet

Mobiiliverkoissa on omat infrastruktuuririskinsä (liite 1, ei julkinen, JulkL 24.1§ 8,9 k). Yksi riski on yleispalveluksi määritellyn 1 Mbit/s -datayhteyden saatavuuden takaaminen kaikkialla Suomessa (vuonna 2010). Langattomana teknologiana käytetään pääasiassa mobiilipalvelua (UMTS) tai Digitan @450-palvelua.

Toinen riski liittyy hallituksen päätökseen, minkä mukaan lähes kaikkialle Suomessa on tarjottava 100 Mbit/s -liittymä 2015 loppuun mennessä.

5.1.3.3 Normaaliolojen häiriötilanteisiin varautuminen

Suomessa on varauduttu ICT:n osalta poikkeusolojen lisäksi myös normaaliolojen häiriötilanteisiin sektorilainsäädännöllä sekä kaupallisten palvelutasovaatimusten avulla.

5.1.3.4 Poikkeustilanteisiin varautuminen

Sen lisäksi miten yleisesti varaudutaan teleinfrastruktuurin poikkeustilanteissa (luku 9, kohta 9.2.6), tulisi mobiiliverkkojen osalta harkita erityistoimenpiteitä poikkeustiloihin varautumiseksi (kohta 9.2.3).

5.1.4 Kiinteät verkot

Kriittisenä infrastruktuurina Suomen kiinteät verkot ovat korkealaatuiset ja verkkopalvelujen saatavuus on hyvällä tasolla. Varsinkin tulevia laajakaistatarpeita varten, erityisesti harvaan asutuilla seuduilla, kiinteässä verkossa on vielä kuitenkin paljon kehittämisen varaa. Tähän on jo osittain varauduttu, sillä liikenne- ja viestintäministeriössä on laajakaistasuunnitelmat olemassa kuituverkon rakentamiseksi vuoteen 2015 mennessä

lähes jokaisen ulottuville. Ohjelman toteutuksesta vastaa liikenne- ja viestintäministeriö ja käytännön ohjeistamisesta Viestintävirasto[34].

Kiinteän verkon haavoittuvuuksia on käsitelty liitteessä 1.

5.1.5 Public/private -partnership

Kriittinen infrastruktuuri on välttämätön palvelun tai tuotteen tuottamiseksi tai toimittamiseksi. Yhteiskunnan kriittiset tai elintärkeät palvelut, kuten ICT-palvelut tai energian toimitukset, toteutetaan lähes kokonaan yksityisen sektorin tuotteilla ja palveluilla. Tämä koskee sekä julkishallinnon että yksityisen sektorin ICT-palveluita.

5.2 Mikä on kriittistä - tahtotila

5.2.1 Kaikki riippuu kaikesta

Yhteiskunnan elintärkeät toiminnot, ja erityisesti kriittiset infrastruktuurit, ovat kaikki riippuvaisia ICT-järjestelmistä – vallitsee NxN -suhde (riippuvuuksia Nx(N-1)/2), missä N on infrastruktuurien määrä). Kaikki ovat riippuvaisia kaikesta. Käytännössä ei ole viestintäverkkoa /-palvelua, joka ei olisi kriittinen jonkin käyttäjän kannalta.

Kriittisyyden määrittäminen on hyvin haasteellista. Määrittelyyn ja tahtotilaan liittyy seuraavia kysymyksiä:

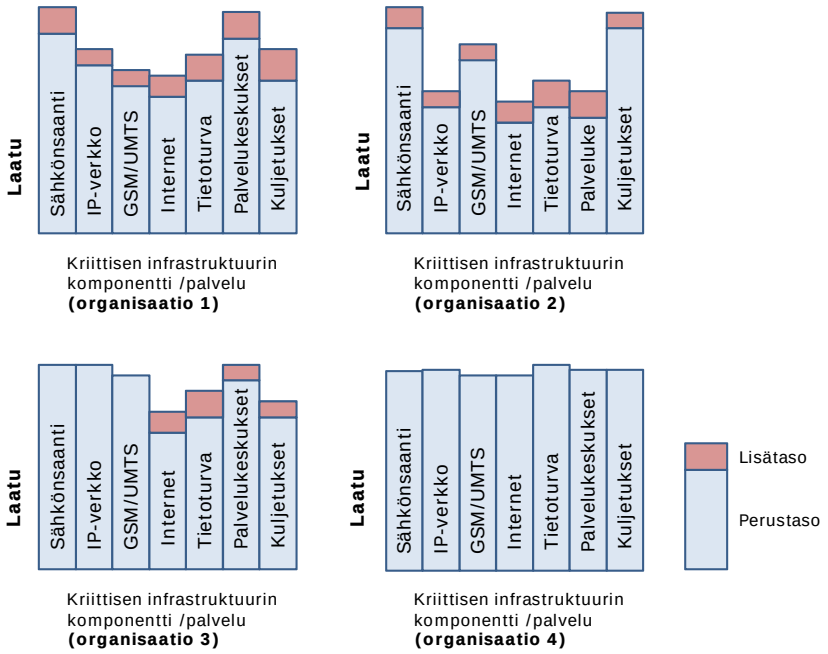
- Onko jokin välttämättömämpää kuin joku muu?
- Kuka määrittelee ja millä kriteerein?
- Missä määrin voidaan määritellä kolmannen osapuolen, esimerkiksi viranomaisen toimesta? Yksi kriteeristö on määritelty Viestintäviraston määräyksessä M54 (Määräys Viestintäverkkojen ja -palvelujen varmistamisesta) – Yleinen käyttäjävaikutusnäkökulma.
- Mille tasolle käytettävyyttä tulisi kehittää?
- Mikä saa olla käytettävyyden alenema?
- Missä määrin voidaan määritellä kolmannen osapuolen, esimerkiksi viranomaisen toimesta?
    - Yleinen määrittely VML 128§:ssä.
    - Viestintäviraston määräystyö M58 käynnissä
- Voidaanko sopia tilaajan ja (viestintäverkon /-palvelun) tarjoajan kesken, SLA:t?
    - Miten verkostoissa, joissa tilaaja – käyttäjäsuhde ei ole selkeä?
    - Entä jos tilaaja ei ymmärrä olevansa elintärkeän toiminnon toteuttaja?
    - Entä jos palveluntarjoajalla ei ole korkeamman käytettävyyden SLA-tuotetta valikoimassaan?
    - Tulisiko vaatimukset sisällyttää aina sopimuksiin?

5.2.2 Elintärkeiden ICT-järjestelmien käytettävyysvaatimukset tapauskohtaisia

Kriittisen infrastruktuurin tai sen jonkun komponentin käytettävyysvaatimukset voivat olla toiselle organisaatiolle elintärkeämpää kuin toiselle, kuva 5.2. Esimerkiksi matkailu- ja majoitusyrittäjälle (organisaatio 1) on-line palvelut ja internet ovat elinehto. Talonraken-

[34] http://www.ficora.fi/index/saadokset/ohjeet/laajakaista2015.html

nusyhtiölle (organisaatio 2) taas polttoaineen saanti ja mobiilipalvelut voivat olla tärkeämmät. Finanssialalla (organisaatio 3) taas televerkot ja palvelukeskukset ovat avainasemassa, mitkä edellyttävät korkeinta laatutasoa. Turva-alan verkko ja palvelut (esim. TUVE) puolestaan edellyttää kaikilta komponenteilta korkeinta laatua (organisaatio 4).



Kuva 5.2 Organisaation/yrityksen kriittisen infrastruktuurin komponentin periaatteellinen laatu – perus- ja lisätaso (riippuu organisaatiosta)

Kuvassa 5.2 on esitetty myös se periaate, että joko viranomaisten asettamien laatukriteerien (esim. televerkoissa Viestintävirasto 54/2008M, sähkön tuotannossa ja jakelussa sähkömarkkinalaki) tai yleisen kilpailun kautta tarjottava perustason laatu sisältyy sovittuun perushintaan kaikille ja kaikkialla, mutta että lisämaksuilla voi saada lisälaatua.

5.3 Käytettävyyskriteerien määrittely

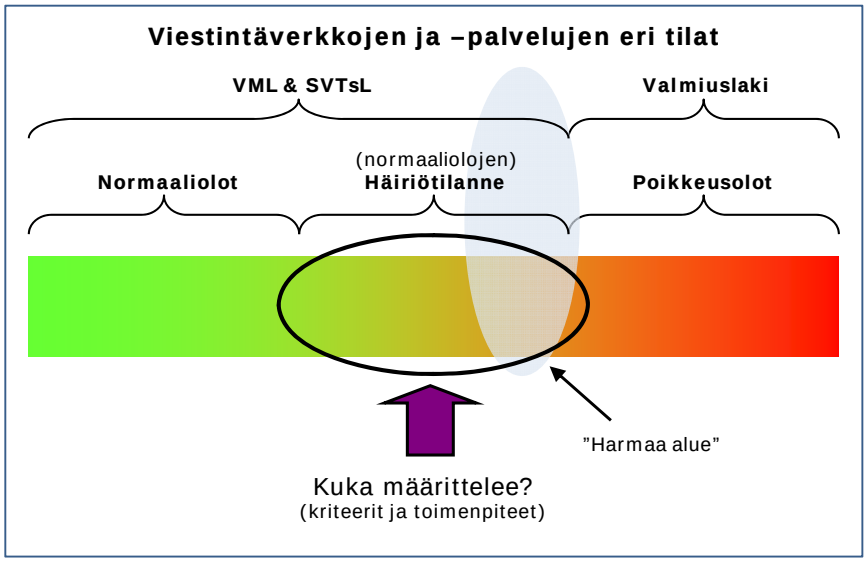
5.3.1 Kansainvälinen näkökulma

Euroopan unioni on todennut, että koska kriittiset ICT-infrastruktuurit (CII) ovat globaaleja ja liittyneet tiiviisti yhteen ja koska ne ovat keskinäisriippuvia muista infrastruktuureista, niiden tietoturvaa ja vioista toipumista ei voida taata pelkästään kansallisesti ja ilman koordinointia. Kriittisten ICT-infrastruktuurien vioista toipuminen on itsessään valtioiden rajat ylittävää, ja joissakin tapauksissa globaalia (internet)[35].

[35] 2.4.2009 EU Commission: Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" Impact Assessment (Part 1).

5.3.2 Harmaan alueen kriteerit

Kuvassa 5.3 on viestintäverkkojen ja -palvelujen eri tilat ja lainsäädännöt, mitkä ovat voimassa normaalioloissa, häiriötilanteissa ja poikkeusoloissa. Viestintävirasto on saanut päätökseen määräystyön koskien viestintäverkkojen ja –palvelujen ylläpitoa ja menettelyitä vika- ja häiriötilanteissa[36]. Harmaan alueen lainsäädäntötyö on käynnissä (kohta 7.2.1).



Lyhenteet: VML (Viestintämarkkinalaki), SVTsL (Sähköisen viestinnän tietosuojalaki)

Kuva 5.3 Viestintäverkkojen ja -palvelujen eri tilojen ja kriteerien ja toimenpiteiden määrittely[37]

Toimenpiteet eivät ole pelkästään tekninen kysymys. Asiaa on tarkasteltava kokonaisvaltaisemmin prosessien, liiketoimintamallien, SLA-sopimusten, omistussuhteiden, jne kautta. Varautuminen on ICT-yrityksille ylimääräinen ponnistus normaali tarjonnan päälle. Viime kädessä varautumisen vaatimukset ja toimenpiteet kulminoituvat kustannuksiin. Maksaako kustannukset CII:n tarjoaja, CII:n käyttäjä, vaiko joku muu.

EU-komissio on antanut kannanoton huhtikuulta 2009, että on yleisesti tunnettua, että markkinavoimat eivät kannusta riittävästi yksityisiä operaattoreita investoimaan kriittisten ICT-järjestelmien (CII) suojaamiseen tasolle mitä hallinnot normaalisti vaativat[38].

[36] Määräys 57/2009M viestintäverkkojen ja –palvelujen ylläpidosta sekä menettelystä vika- ja häiriötilanteissa.
[37] YKÄ-seminaari, 15.4.2009, Sami Kilkkilä, Viestintävirasto.
[38] European Commission statement: “In fact, it is a common perception that market forces do not provide sufficient incentives to private operators for investing to protect CIIs at the level that governments would normally demand – a market failure.”

6 ELINTÄRKEIDEN TOIMINTOJEN TURVAAMINEN JA KÄYTETTÄVYYS

6.1 Motiivi - tietoyhteiskuntakehityksen syventäminen

6.1.1 Luottamuksen takaaminen

Arjen tietoyhteiskunta -ohjelman tavoitteena on tietoyhteiskuntakehityksen syventäminen, mikä lisää kansantalouden tuottavuutta ja kilpailukykyä sekä lisää kansalaisten viihtyvyyttä vertaistalouksiin nähden. Tietoyhteiskuntakehitys voi syventyä vain jos sitä kohtaan kaikki osapuolet tuntevat riittävää perusteltua luottamusta. Kaikilla osapuolilla on luottamukseen oma näkökulmansa; julkishallinnolla, yrityksillä ja kansalaisilla.

Luottamuksen eri näkökulmia on esitetty taulukossa 6.1. Kuluttajan aseman parantaminen edellyttää kaikilta toimijoilta vastuullisuutta, myös kuluttajilta itseltään.

Taulukko 6.1 Eri osapuolten näkökulmia palveluiden luottamuksesta

Ominaisuus	Mittari (esim.)
Pääsy verkkoon (verkon saavutettavuus)	24x7, 8-16, 99,9%
Palvelutaso	Palvelun vasteaika
Yksityisyyden suoja	Ks. taulukko 4.2
Sisältöjen laillisuus	
Palvelujen käytettävyys	24x7, 8-16, 99,9%
Tietoturvallisuus	Vahva, heikko

6.1.1.1 Käytettävyys

Yksi tärkeimmistä tietoyhteiskunnan syventämisen näkökulmista on ICT-järjestelmien *käytettävyyden* takaaminen (taulukko 6.1).

Huom. Käytettävyys on määritelty luvussa 1 (kohta 1.1.1).

6.1.1.2 Yksityisyys - yksityisyyden uhat

Luottamuksen mittaaminen tietoyhteiskunnassa on hyvin haasteellista. Taulukon 6.1 komponenteista käytettävyyden lisäksi toisena komponenttina on taulukossa 6.2 esitetty esimerkkinä yksityisyyden suoja.

Yksityiseen kohdistuu neljä uhkaryhmää[39,40]; tiedon keruu, tiedon käsittely, tiedon välitys ja loukkaus (invaasio) (Solove[39]). Nämä jakautuvat edelleen kuuteentoista alaryhmään. Pelkästään siis yksityisyys on moniselitteinen asia tietoyhteiskunnassa.

[39] Solove, D. J. 2006: A Taxonomy of Privacy. University of Pennsylvania Law Review vol. 154.
[40] Janne Lindqvist, Yksityisyyden suoja verkotetussa yhteiskunnassa, Silmät auki – Tietoyhteiskunnan uhat ja mahdollisuudet, Eduskunnan tulevaisuusvaliokunnan julkaisu 1/2008.

Taulukko 6.2 Yksityisyyteen kohdistuvat uhkat[40]

Pääryhmä	Tiedon keruu	Tiedon käsittely	Tiedon välitys	Loukkaus (invaasio)
Alaryhmät	Valvonta	Yhdistely	Luottamuksen rikkominen	Tunkeutuminen
	Kuulustelu	Tunnistaminen	Paljastaminen	Päätösvaltainen häirintä
		Epäturvallisuus	Julkaiseminen	
		Toissijaiset käyttötarkoitukset	Kohonnut tavoitettavuus	
		Ulkopuolelle jättäminen (ekskluusio)	Kiristys	
			Varastaminen	
			Vääristäminen	

6.1.2 ICT-toiminnan varmistaminen

Luottamusta rakennetaan yhteiskunnan elintärkeiden tieto- ja viestintäjärjestelmien toiminnan varmistamisella

- käytettävyyteen (helppokäyttöisyyteen) panostamalla (palvelutaso)
- tietoturvatoimin
- haitallisiin ja laittomiin sisältöihin puuttumalla
- panostamalla CERT-toimintaan
- varmistamalla verkkopankkitoimintaa
- yksittäisillä suojaushankkeilla
- varautumalla verkkohyökkäyksiin ja haittaohjelmiin

6.1.3 Kriittisten ICT-järjestelmien tunnistaminen

Yhteiskunnan elintärkeiden ICT-järjestelmien toiminnan varmistaminen edellyttää niiden tunnistamista, uhkien ja riskien realistista kartoitusta sekä ratkaisujen hahmottamista. Tämä on erityisen tärkeää infrastruktuuritasolla, missä vaikutukset ovat laajat.

6.2 Kriittisten ICT-järjestelmien toiminnot ja toimijat prosessin osina

6.2.1 Käytettävyys muodostuu palvelun komponenttien käytettävyydestä

ICT-järjestelmien laadun ja sen yhtenä tekijänä *käytettävyyden* määrittely edellyttää tieto- ja viestintäjärjestelmien ”komponenttien” analysointia. Tämä voidaan tehdä joko teknisten tuote/palvelukomponenttien kautta tai tarkastelemalla komponentteja prosessilähtöisesti. Molempia näkökulmia tarvitaan. Prosessiajattelu kertoo mitä ja miten eri vaiheissa ICT-komponentissa tehdään ja toimintaa ohjataan liiketoimintalähtöisesti.

YKÄ-toiminnan kautta ei ole mahdollista määritellä tarkkoja tietoyhteiskunnan kriittisten ICT-järjestelmien eri kerrosten ja niiden komponenttien käytettävyyden mittareita. Käytettävyys ja sen kehittäminen on tuotetta tai palvelua tarjoavan yrityksen liiketoimintaa ja tavoitteet määritellään tilannekohtaisesti ostajan ja toimittajan välisissä sopimuksissa (esim. SOPIVA, liite 2, ei julkinen, JulkL 24.1§ 8,9 k) laatumäärittelyineen (SLA[41]).

[41] SLA (Service Level Agreement).

Taulukossa 6.3 on esitetty esimerkinomaisesti ”ICT-kerrosten” kriittisiä komponentteja ja niiden merkitys ja haavoittuvuus yleisellä tasolla. Todellisuudessa kriittiset komponentit ja niiden haavoittuvuus/merkittävyys analysoidaan kunkin ICT-elementin kohdalla asiakas/organisaatiokohtaisesti.

Taulukko 6.3 Esimerkki ICT-infrastruktuurin tietojärjestelmien tärkeimmistä kriittisistä komponenteista ja komponenttien merkitys ja haavoittuvuus

No	ICT-kerros	Kriittinen komponentti	Merkitys	Haavoittuvuus
9	Lisäarvopalvelut	Asiakasosaaminen	+++	+++
8	Käyttäjät	Käytettävyys	+++++	+++
7	Politiikat ja käytännöt	Sopimusosaaminen	+++	+++
6	Tieto ja sisällöt	Luotettavuus	+++++	++++
5	Verkot	Luotettavuus	+++++	+++++
4	Ohjelmistot	Luotettavuus	++++	+++
3	Laitteistot	Asiantuntemus	++++	++++
2	Energia	Luotettava toimitus	+++	+++
1	Ympäristötekijät	Kuljetukset, maksaminen	+++	+++

(enemmän + -merkkejä, sitä merkittävämpi/haavoittuvampi)

6.2.2 Prosessit liiketoiminnassa

Elintärkeiden ICT-järjestelmien komponenteissa huomioidaan yksittäiset toiminnot ja toimijat prosessin osina

6.2.2.1 Prosessit ja rakenteet

Prosessit ovat määritelmänsä mukaisesti reaaliaikaista toimintaa, miten organisaation henkilöt, tekniset järjestelmät ja vastaavat todellisuudessa toimivat. Siten prosessit tarkoittavat organisaation rakenteelle kohtisuorasti riippumatonta ulottuvuutta.

Liiketoimintaprosessi on joukko toisiinsa liittyviä *tehtäviä* ja niiden toteuttamiseen tarvittavia *resursseja*, joiden avulla saadaan *liiketoiminnan tulokset*. Liitteessä 1 on tarkasteltu yrityksen ydinprosesseja hieman lähemmin.

6.2.2.2 Ulkopuoliset toimijat - jatkuvuuden hallinta

Myös organisaation ulkopuolisia toimijoita (organisaatioita) osallistuu prosessien toimintoihin. Valtionhallinnon kriittisten ICT-toimintojen kohdalla tästä sovitaan vaatimuksineen SOPIVA-menettelyissä. Tilaajan ja toimittajan väliset sopimukset voivat sisältää mm. SLA-asiakirjoja, missä sovitaan palvelutaso- ja muista toimitusten laatuun liittyvistä asioista.

SOPIVA-suositusten keskeisenä tavoitteena on saada organisaation (ylin) johto määrittelemään kyseisen organisaation toiminnan jatkuvuuden hallinnan strategiat ja tavoitteet sekä organisoimaan ja vastuuttamaan jatkuvuuden hallintaan liittyvät asiat.

6.2.2.3 Haasteet

Prosessit tai niiden resurssit voivat sijaita eri puolilla verkossa maailmanlaajuisesti. Kriittisten ICT-järjestelmien *luottamuksen* ja sen osana *käytettävyyden* vaatimukset voivat tästä syystä olla joskus hyvin haasteelliset. Toimintaverkoissa voi olla jopa vihamielisiä osapuolia, jotka omilla – usein myös varsin tehokkailla – prosesseillaan vaikuttavat liiketoimintayhteisöissä omien intressiensä mukaisesti. Uudet verkkomallit voivat jopa edesauttaa tällaista kehitystä, vaikka niissä on kiistatta myös hyvät puolensa (esim. cloud computing).

6.2.3 Kriittisen ICT-ratkaisun käytettävyys suunnitteluvaiheessa

Suunnittelun lähtökohtana on liiketoiminta ja liiketoimintaprosessit. Liiketoimintaprosessit määrittävät järjestelmän vaatimukset. Vaatimukset voivat liittyä esimerkiksi käytettävyyteen tai tietoturvaan. Siten esimerkiksi käytettävyyden suunnittelua johdetaan tiiviisti yhdessä liiketoimintaprosessien johtamisen kanssa.

Turvallista ja luotettavaa tietoyhteiskuntaa normeilla ja säädöksillä suunnittelevan hallinnon osapuolella on oltava samaa asiantuntemusta kuin palveluita tarjoavalla osapuolella, jotta pystytään laatimaan ja ymmärtämään teknisiä sopimuksia.

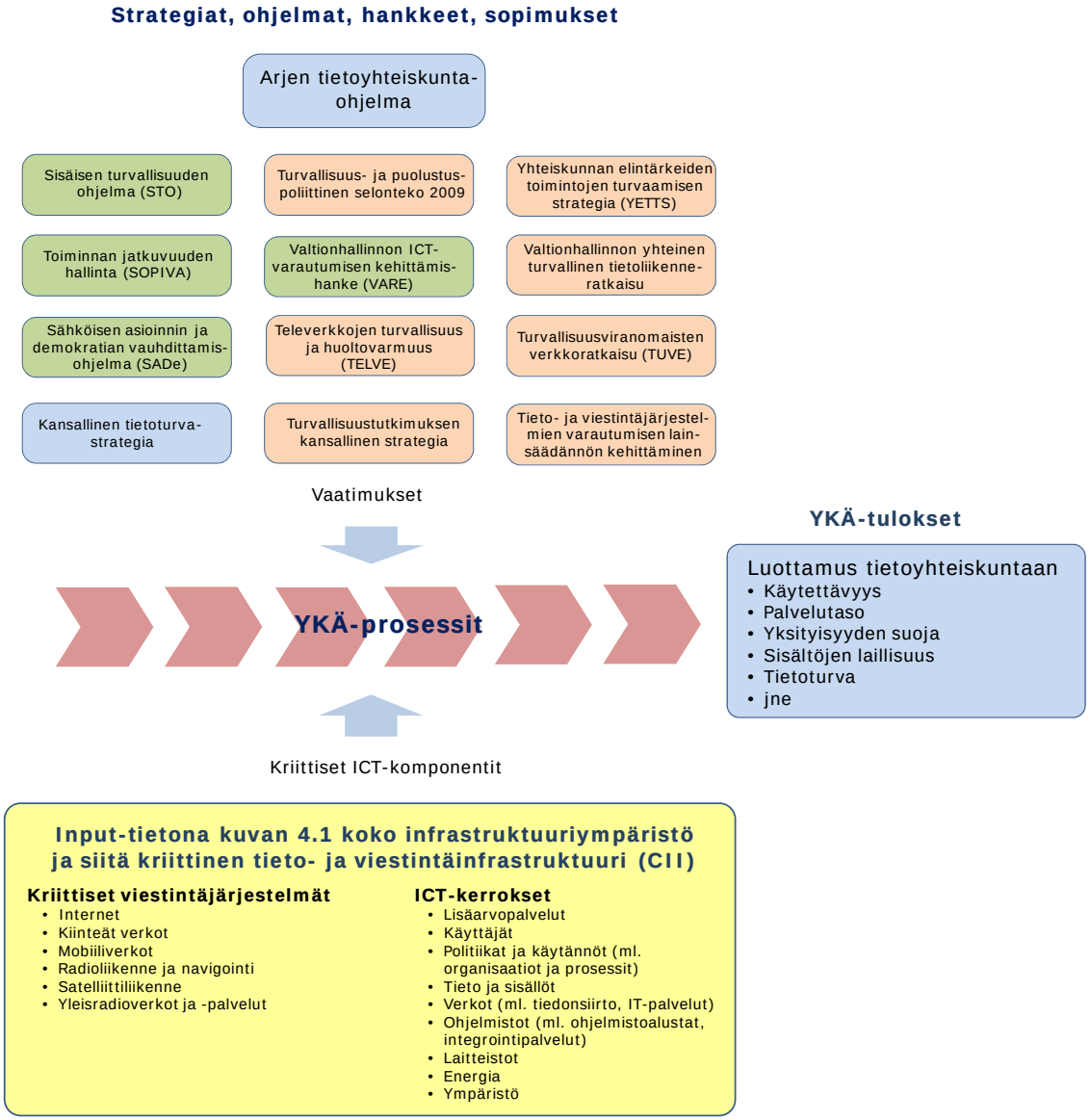
Luottamus tietoyhteiskuntaan – ja siinä yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien tieto- ja viestintäjärjestelmien *käytettävyyden* kehittäminen – voi käytännössä toteutua vain siten, että käytettävyyden vaatimukset viedään mukaan tiiviisti organisaatioiden todelliseen toimintaan eli organisaatioiden liiketoimintaprosesseihin ja niiden johtamiseen. Tämä koskee kaikkia tasoja ja kaikkia turvallisuustilanteita.

6.2.4 YKÄ-prosessit

Elintärkeiden ICT-järjestelmien tunnistamisessa huomioidaan yksittäiset toiminnot ja toimijat prosessin osina. Uhkien ja riskien kartoituksessa pyritään ottamaan realistisesti huomioon niiden todennäköisyydet ja riskien ja uhkien vuorovaikutukset. Hahmoteltujen ratkaisujen tulisi kohdentua toimintoprosessien varmistamiseen, todennäköisimpiin ja vaikuttavimpiin uhkiin ja riskeihin. Tämä on erittäin haasteellinen tehtävä.

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien ICT-järjestelmien *käytettävyyden* kehittäminen (YKÄ-toiminta) on itsessään kokoelma liiketoimintaprosesseja, ns. ”YKÄ-prosesseja”. YKÄ-prosessit ovat korkean tason tehtäviä (määrittely, suunnittelu, julkaiseminen, johtaminen, hallinnon ohjausmekanismit, valvonta). Tehtävät ja määrittelyt vaatimuksineen tulevat valtion- ja kunnallishallinnon sekä yksityisen sektorin (public/private –partnership) strategioista, ohjelmista, hankkeista ja sopimuksista. Prosessit kohdistuvat tunnistettuihin kriittisiin ICT-komponentteihin (kuva 6.1).

YKÄ-prosesseja määrittelevät ja johtavat nimetyt vastuuorganisaatiot (Viestintävirasto, HVK, valtionhallinnon tietoturvallisuuden johtoryhmä, julkisen hallinnon tietohallinnon neuvottelukunta, valtion IT-palvelukeskus, yrityssektori) hallinnon ohjausmekanismien kautta.



Kuva 6.1 Tietoyhteiskunnan syventäminen edellyttää luottamusta - luottamus rakennetaan korkean tason YKÄ-prosesseilla tunnistetuille kriittisille ICT-komponenteille määriteltyjen strategioiden, ohjelmien ja hankkeiden tavoitteiden ja vaatimuksien ohjaamana. Kuvan yläosan strategiat, ohjelmat ja hankkeet on kuvattu liitteessä 2.

6.3 Identiteetin hallinta – uusi CII

6.3.1 Kukin kriittinen infrastruktuuri rakentanut omat identiteetin hallintajärjestelmät

Kriittiset infrastruktuurit ovat teknisiä järjestelmiä, joiden on toimittava kaikissa olosuhteissa, jotta yhteiskunnan elintärkeät toiminnot palveluineen voitaisiin pitää yllä. Tiedetään, että paikalliset, kansalliset ja kansainväliset verkot (esim. sähkö, televiestintä, kuljetukset) kestävät vain lyhyitä katkoksia ja häiriöitä siten, että käyttäjät eivät sitä huomaisi. Sähköinen kaupankäynti, maksaminen, sisäänpääsyt, jne edellyttävät aina tunnistautumista (identiteetin todistamista) olkoot käyttäjänä ihminen, laite, tai verkko tai palvelu.

Miten tietoyhteiskunnassa todistetaan identiteetti, jos muut infrastruktuurit (esim. pankkipalvelut, sähkönsaanti) ovat kaatuneet. Tietoyhteiskunnassa ollaan **tiedon** varassa, ei fyysisten komponenttien tai välineiden varassa – tämä kehitys vain vahvistuu. Tunnistamisongelmat on hoidettu kymmenien vuosien ajan eri kriittisten infrastruktuurien omin keinoin. Kullakin niistä on omat ”kredentiaalinsa”, prosessinsa, passit ja erilaisia testejä, ennen kuin palvelua voi käyttää.

6.3.2 Kymmeniä erilaisia identiteetin todistusmenetelmiä

Pankit ovat perinteisesti olleet etunenässä identiteetin todistamisen kehittämisessä. Lisäksi erilaiset luotto- ja pankkikortit, kansalaiskortit, Kela-kortit, jne ovat toimineet tunnistamisen välineinä toisistaan riippumatta ja yhteensopimattomasti. Monet sähköisessä muodossa olevat identiteetit ovat alttiita identiteettivarkauksille. Tämä on yksi suurimmista tietoturvaongelmista.

6.3.3 Informaation vapautus

Tietoyhteiskunta on kehittymässä ”löyhään liittoon” teknologian kanssa. Hyvin erilaista tietoa liikkuu hyvin kompleksisten järjestelmien ja verkkojen ja kymmenien erilaisten protokollien välittämänä kymmenien erilaisten päätelaitteiden ja sovellusten kautta (mikrot, palvelimet, kännykät, luottokortit, pankki- ja kauppasovellukset, tietokannat, jne).

Monet palvelut ja sovellukset on lisäksi rakennettu siten, että niissä tietoa ei pidetä päätelaitteessa pitkää aikaa. Päinvastoin, tiedosta halutaan päästä mahdollisimman nopeasti eroon, se ei saa palaa ”näpeissä”. Tietoyhteiskuntaan syntyneistä uusista ilmiöistä mainittakoon monet verkkoyhteisöt (Facebook, MySpace, Bebo, LinkedIn, …, Google), joissa on jo kymmenien miljoonien ihmisten ”digitaalielämä”.

Edellä kuvattu kehitys – vain pintaa raapaistuna - heikentää käyttäjien identiteetin turvallisuutta ja luotettavuutta, mikä lisää myös verkkorikollisuuden kasvua. Identiteetin hallinta ei ole kehittynyt toivottuun suuntaan, ei Suomessa eikä muuallakaan.

7 TIETO- JA VIESTINTÄJÄRJESTELMIEN KÄYTETTÄVYYDEN SUHDE VARAUTUMISEEN

7.1 Lähtökohta, nykytila ja normisto

7.1.1 Varautumisen lähtökohta

Huoltovarmuuden yleistavoitteena on kansainvälisiin markkinoihin sekä kansallisiin toimenpiteisiin ja voimavaroihin perustuva huoltovarmuus. Varautumistoimenpiteillä turvataan yhteiskunnan toimivuuden kannalta välttämätön infrastruktuuri ja kriittisen tuotannon jatkuminen kaikissa tilanteissa.

Toimivat markkinat, kansalliset ja kansainväliset yritykset ja verkostot tuottavat merkittävän osan huoltovarmuudesta. Yli kansallisten rajojen hajautetut järjestelmät voivat lisäksi toimia joissakin olosuhteissa toistensa varajärjestelminä. Kaikkia keskeisiä toimintoja ei ole edes mahdollista turvata enää kansallisin järjestelyin. Kansallista huoltovarmuutta on sen vuoksi tarpeen täydentää ja vahvistaa Euroopan unionin jäsenyyden ja muun kehittyvän kansainvälisen huoltovarmuusyhteistyön avulla. Vakavimpiin kriiseihin on kuitenkin aina varauduttava kansallisin toimenpitein.

7.1.1.1 Elinkeinoelämä

Yritysten varautumisen lähtökohtana ovat liiketoiminnalliset perusteet, asiakkaiden kanssa tehdyt sopimukset sekä näihin liittyvä riskienhallinta. Siltä osin, kun tämä ei yhteiskunnan näkökulmasta ole riittävää, täydennetään varautumisvastuita lainsäädännöllisillä velvoitteilla. Lakisääteiset varautumisvelvoitteet eivät saa häiritä markkinoiden toimintaa ja tasapuolisia kilpailuedellytyksiä. Tässä on erityisesti huomioitava sekä kansallinen että Euroopan yhteisön kilpailulainsäädäntö.

Yritykset ja elinkeinoelämän järjestöt osallistuvat sopimusperusteiseen valmiussuunnitteluun Huoltovarmuusorganisaation eri sektoreissa ja pooleissa. Hallinnolle, turvallisuusviranomaisille ja toisilleen palveluita tuottavien poikkeusoloissa tärkeiden yritysten toimintaedellytykset on pyrittävä takaamaan kaikissa turvallisuustilanteissa. Julkisen hallinnon ja yritysten keskinäisriippuvuuden lisääntyessä molemminpuoliset velvoitteet on sisällytettävä palvelusopimuksiin.

Globaaleilla markkinoilla yritysten arvoketjut hajautetaan eri maihin ja mantereille sen mukaan, missä tarvittavat toiminnot pystytään tuottamaan edullisimmin. Tämän kehityksen seurauksena yritysten ja valtioiden menestys on eriytynyt yhä enemmän toisistaan. Kansallisen ohjauksen mahdollisuudet ovat jatkuvasti vähenemässä.

7.1.1.2 Kansalaisjärjestöt

Yhteiskunnan elintärkeitä toimintoja turvattaessa hallinnon, viranomaisten ja elinkeinoelämän yritysten ohella myös vapaaehtoistoimintaan perustuvilla kansalaisjärjestöillä on merkittävä rooli sekä käytännön turvallisuuden toteuttamisessa että kriisinkestokyvyn lisäämisessä. Järjestöjen mukana olo perustuu niiden itselleen asettamiin toimintapäämääriin, mikä on yhteistoimintaa suunniteltaessa otettava huomioon. Nyky-yhteis-

kunnassa myös yksittäiset ihmiset erilaisten verkostojen toimijoina ovat yhä merkittävämmässä roolissa varautumisen ja siihen liittyvän tiedonvälityksen osana.

7.1.2 Normisto

Yhteiskunnan elintärkeiden ICT-järjestelmien käytettävyyden normisto, siltä osin kun se koskee viestintäverkkoja ja -palveluja, on hyvässä kunnossa ja sitä täydennetään ja kehitetään jatkuvasti. Viestintävirasto on laatinut kattavan kokoelman määräyksiä ja ohjeita, joissa on huomioitu myös varautumisen vaatimukset ja ohjeistettu toimenpiteet.

7.1.3 Varautuminen ja YKÄ

Yhteiskunnan elintärkeiden toimintojen turvaamisen (YETT) kannalta välttämättömien ICT-järjestelmien *käytettävyyden* kehittämisellä (YKÄ-toiminta) on selkeä suhde varautumiseen. Yhteisiä tärkeitä ohjelmaelementtejä tässä ovat valtionhallinnon VARE-hanke, sisäisen turvallisuuden ohjelma (STO) sekä huoltovarmuusorganisaatio ja sen varautumissuunnitelmat ja sopimukset (HVK, SOPIVA). Tietoyhteiskunnan syventämisen ja valtionhallinnon ICT-varautumisen käytännön toimenpiteet perustuvat yksityisen sektorin samojen toimijoiden palvelutarjontaan.

YKÄ-toiminnalla on selkeä suhde myös elinkeinoelämän ja kansalaisjärjestöjen varautumiseen.

7.1.4 Haasteet - tietoverkot pysyvässä alivarautumisen tilassa?

Verkostoitumisen tuoma markkinatalouden kilpailupaine yrityksissä näyttää minimoivan varautumista yleensä ja tietoverkoissa erityisesti, esim. varavoiman, varalaitteiston ja varahenkilöstön osalta. Nykyinen tietoverkosto on virittynyt äärimmäisen tehokkaaksi, koska osapuolet luottavat kohtuullisen hyvin verkostoon ja toisiinsa. Kilpailu näyttää pitävän tietoverkot pysyvässä alivarautumisen tilassa. Puuttuu kannustimia. Tarvitaan lainsäätäjän apua.

Kilpailu on myös johtanut yritysten lisääntyvään erikoistumiseen, ja sitä kautta arvoverkkojen laajentumiseen ja arvoketjujen pidentymiseen, mikä lisää systeemin haavoittuvuutta kriisitilanteissa. Yksikään osapuoli ei voi yksipuolisesti saavuttaa merkittävää varautumishyötyä, vaan tarvitaan yhteisiä linjauksia.

Yllä olevan kaltaisia selviä ongelmakohtia voidaan havaita ja korjata, mutta systeemin kompleksisuuden takia on selvää, että kaikkea ei osata ennakoida.

7.2 Lainsäädännön riittävyys varautumiseen

7.2.1 Tieto- ja viestintäjärjestelmien varautumisen lainsäädännön kehittäminen

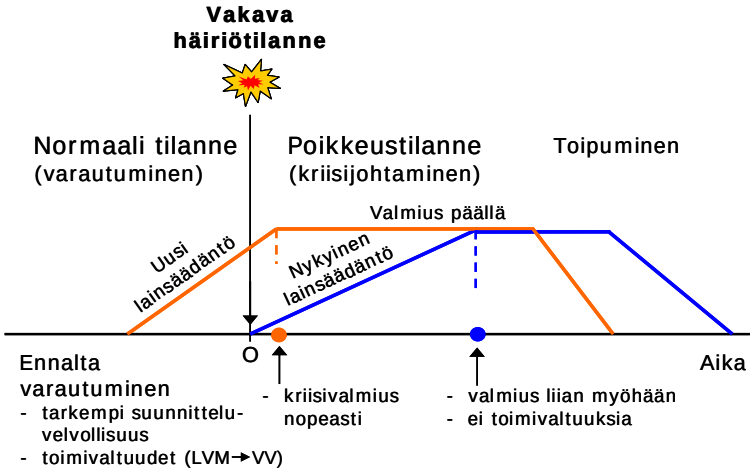
Viestintäministeri asetti 1.11.2007 työryhmän arvioimaan liikenne- ja viestintäministeriön vastuualueella olevien säännösten mahdollisia muutostarpeita varautumisen näkökulmasta ottaen huomioon muun muassa YETT-strategian edellyttämät toimet. Lisäksi työryhmän tulisi arvioida lainsäädännöllisten keinojen tarpeita ja mahdollisuuksia te-

hostaa teleyritysten ja energian jakelusta vastaavien yritysten välistä yhteistyötä. Työryhmä jatkaa marraskuun 2009 lopulle.

Teleyritykset (verkkoyritykset ja viestintäpalvelun tarjoajat) pystyvät usein sopimusteitse hallitsemaan ja kattamaan erilaiset ongelmalliset häiriötilanteet. Tiettyjä vakavia häiriötilanteita ei välttämättä kuitenkaan pystytä hallitsemaan toimijoiden keskinäisin sopimuksin. Työryhmän tavoitteena on löytää ne yhteiskunnassa havaittavissa olevat häiriö- tms. tilanteet, jotka eivät kuulu valmiuslain tarkoittaman poikkeusolon käsitteen piiriin, mutta jolloin valtiovallan olisi tarpeen tukea markkinoiden häiriötöntä toimintaa.

Luonnonilmiöt, erityisesti tietoturvaa koskevat häiriötilanteet, sähköverkon ja energianjakelun häiriöt, varaosien saantiin liittyvät häiriöt ja markkinahäiriöt sekä muut häiriöt tietoliikenteessä ja verkkopalveluissa voivat aiheuttaa sellaisia vakavia tilanteita, että yhteiskunnan elintärkeiden toimintojen toimivuutta ei enää kyetä takaamaan. Näihin tilanteisiin on pystyttävä reagoimaan–usein nopeastikin–ja riittävillä toimivaltuuksilla. Myös yhteistyön kehittäminen lainsäädännöllisin keinoin eri toimijoiden välillä saattaisi edistää vakavista häiriötilanteista toipumista.

Tätä varten tarvitaan avuksi lainsäädännöllisiä valtuuksia, jotta päästään nopeammin kriisijohtamiseen ja tilanteen lauettua taas normaalioloihin (kuva 7.1).



Kuva 7.1 Varautumislainsäädännöllä parannetaan ennalta varautumista

7.2.2 Varautumisohjeet

Yhteiskunnan elintärkeät toiminnot ovat entistä haavoittuvampia laajan ICT- ja sähkönsaannin riippuvuuden vuoksi. Kansalliset palvelut riippuvat yhä enemmän myös kansainvälisistä verkoista ja palveluista (esim. pankkipalvelut). Yhteiskunnan elintärkeät toiminnot ovat siten entistä haavoittuvampia paitsi kansallisille, myös kansainvälisille verkkohyökkäyksille.

Pitäisikö siten varautumisen toimivaltuudet olla käytössä jo laajoissa katastrofitilanteissa?

8 TELEVERKKOJEN ENERGIAHUOLTO JA SUOJAUSTEN RIITTÄVYYS

Tietoyhteiskunta ei toimi ilman sähköä. Joissakin päätelaitteissa voidaan käyttää paristoja, tukiasemilla on varavoimaa muutamaksi tunniksi, perinteisellä lankapuhelimella voidaan soittaa hätäpuhelu vaikka kotona on sähkökatko. Tässä on joitakin esimerkkejä miten sähkökatkoksen aikana voidaan toimia.

YKÄ-toiminta elää siten rinnan sähkön saannin kanssa.

8.1 Suomen sähköverkko

Suomen sähköverkkoon kuuluvat kantaverkko, alueverkot ja jakeluverkot. Kantaverkossa sähköenergia siirretään voimantuotantoalueilta ja ulkomailta kulutuskeskittymiin. Valtaosa Suomessa käytettävästä sähköstä kulkee kantaverkon kautta. Osa sähköä tuottavista voimalaitoksista on liittynyt suoraan kantaverkkoon samoin kuin suuret kuluttajat, esimerkiksi isot tehtaat. Voimalaitokset voivat liittyä myös alue- tai jakeluverkkoon. Esimerkiksi sähköistetyt rautatieosuudet ottavat ajosähkön kantaverkosta, samoin Helsinki-Vantaan lentokenttä.

Alue- ja jakeluverkot siirtävät sähköä omalla alueellaan. Koteihin sähkö tulee jakeluverkoista. Teollisuus, kauppa, palvelut ja maatalous taas saavat sähkön jakelu-, alue- tai kantaverkosta käyttämänsä energiamäärän mukaan.

Kantaverkko kulkee pääosin ulkoilmassa. Keskijänniteverkosta kymmenesosa ja pienjänniteverkoista kolmasosa kulkee kaapeleissa. Etenkin kaupunkien keskustoissa johdot on kaapeloitu maan alle. Pienjänniteverkko pyritään kaapeloimaan entistä useammin, mutta esimerkiksi kantaverkon kaapelointi olisi hyvin kallista.

8.2 Sähkön merkitys

8.2.1 Sähkökatkokset

Yhteiskunnan sähköriippuvuus on kasvanut niin suureksi, että häiriöt sähkönjakelussa voivat lamauttaa arjen toiminnot täysin. Veden jakelu, viemäreiden toiminta, polttonesteiden jakelu, kauppojen ja pankkiautomaattien toiminta, tietoliikenne ja lämmitys ovat täysin sähkön varassa. Myrskyn tai teknisen häiriön aiheuttaman sähkökatkon aiheuttamana kaikki nämä toiminnot pysähtyvät. Teknistyneen yhteiskunnan sähköriippuvuus aiheuttaa riskejä, jotka tulisi ottaa valmiussuunnittelussa entistä tarkemmin huomioon niin hallinnossa kuin yrityksissäkin.

Pitkä sähkökatko kestää viranomaisten määritelmän mukaan yli kolme minuuttia[42]. Silloin sähköt eivät palaudu automaattisesti hetkessä takaisin. Pitkä sähkökatko voidaan määritellä myös sillä perusteella, että kuluttajille maksetaan vakiokorvausta yli 12 tunnin sähkökatkoista. Vakiokorvauksista määrätään sähkömarkkinalaissa.

Yksittäinen vika Suomen kantaverkossa, esimerkiksi voimalan putoaminen pois tuotannosta, ei vielä aiheuta pitkiä sähkökatkoksia kuluttajille. Kuitenkin kaksi samanaikaista

[42] Pitkä sähkökatko ja yhteiskunnan elintärkeiden toimintojen turvaaminen, Puolustusministeriö 28.5.2009.

merkittävää vikaa tai vian ilmeneminen korkean kulutuksen ja alhaisen tuotannon tilanteessa voivat johtaa jopa koko Suomen laajuiseen sähkökatkoon. Jos Suomen kantaverkosta johtuva vika aiheuttaa koko maan laajuisen sähkökatkon, sen kesto on etelässä pisin. Sähkön palauttaminen aloitetaan tällaisessa tilanteessa Pohjois-Suomesta[42].

8.3 Varavoima

8.3.1 Normit

Viestintäviraston määräys 54/2008M[43] ”Viestintäverkkojen ja –palvelujen varmistamisesta” sisältää määräykset viestintäverkkojen ja –palveluiden komponenttien varavoiman tarpeesta. Viestintäverkon tai -palvelun komponentit luokitellaan merkittävyyden perusteella alenevassa tärkeysjärjestyksessä tärkeysluokkiin 1-5. Tärkeysluokkien määräytymiskriteerit on kuvattu samassa määräyksessä. Tärkeysluokat koskevat puhelinpalveluita, laajakaistapalveluita, sähköpostipalveluita, joukkoviestintäpalveluita ja muita viestintäpalveluita.

Esimerkiksi komponentti, joka vaikuttaa viestintäpalveluihin suurella maantieteellisellä alueella (yli 20,000 km^2) tai komponentti, joka vaikuttaa suuruusluokaltaan

≥ 50 000 käyttäjän puhelinpalveluun, tai
≥ 50 000 käyttäjän laajakaistapalveluun, tai
≥ 200 000 käyttäjän sähköpostipalveluun, tai
≥ 100 000 käyttäjän joukkoviestintäpalveluun, tai
≥ 200 000 käyttäjän muuhun viestintäpalveluun,

on tärkeysluokan 2 tilanne, mikä edellyttää vähintään 6 tunnin vara-akustot (jos viestintäverkon tai -palvelun komponentti on kytketty voimalaitejärjestelmään, jossa tehonsyötön varmistuksena on kiinteä varavoimalaitos, akuston minimivarmistusajaksi riittää 3 tuntia)[43].

Vara-akustojen minivarmistusajat ovat riittävät tietoyhteiskunnan perustarpeisiin ja normaalioloissa. Suomessakin on kuitenkin silloin tällöin pidempiä suurten myrskyjen aiheuttamia katkoksia, missä 6 tunnin varmistukset eivät riitä.

Myrskytuhojen korjaaminen edellyttää kaiken lisäksi kenttähenkilökunnalta, että heillä on käytössään toimivat mobiiliyhteydet. Tässä on selkeä riippuvuussuhde sähkö- ja mobiiliverkkojen kesken.

[43] Määräys 54/2008M, Viestintävirasto.

8.4 Nykyisten suojausjärjestelmien riittävyys

8.4.1 Tilanne

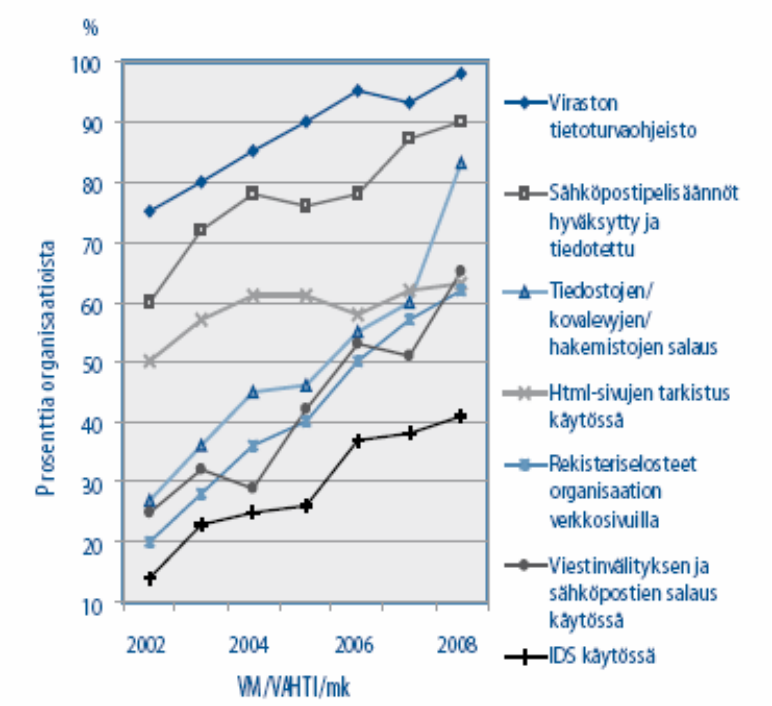
ICT-järjestelmiä suojataan useilla tasoilla. Viranomaiset antavat määräyksiä (esim. Viestintävirasto televiestinnässä ja VAHTI tietoturvallisuuden osalta valtionhallintoon), teollisuudella on omat määräyksensä, kiinteistöillä omat määräykset (esim. kaapeloinnista).

Tämän lisäksi käyttäjillä on monenkirjavaa käytäntöä suojautua esimerkiksi haittaohjelmia vastaan ja salata siirrettävää tietoa tai kryptata tiedostoja tietokoneellaan.

Seuraavassa suojausjärjestelmien riittävyyttä on käsitelty valtionhallinnon elintärkeissä tietojärjestelmissä, kuntien ICT-palveluissa sekä viestintäjärjestelmissä.

8.4.2 Valtionhallinnon tietojärjestelmät – tilanne 2008

Valtionhallinnon tietoturvan tilan kehitystä on seurattu systemaattisesti 2000-luvulla. Kuvassa 8.1[44] on kyselyiden perusteella laadittu tilastokuva 2002–2008. Kuvassa ei ole esitetty sellaisia tietoturvatoiminnan alueita, joissa käytännössä lähes 100 % virastoista on toteuttanut perustavoitteiden mukaisen toiminnan. Tällaisia ovat esimerkkinä tietoteknisestä tietoturvallisuudesta haittaohjelmatorjunta ennen sähköpostien jakelua ja työasemissa sekä esimerkkinä hallinnollisesta tietoturvallisuudesta vähintään osapäiväisen, ylimmälle johdolle raportoivan tietoturvavastaavan toiminta organisaatiossa.



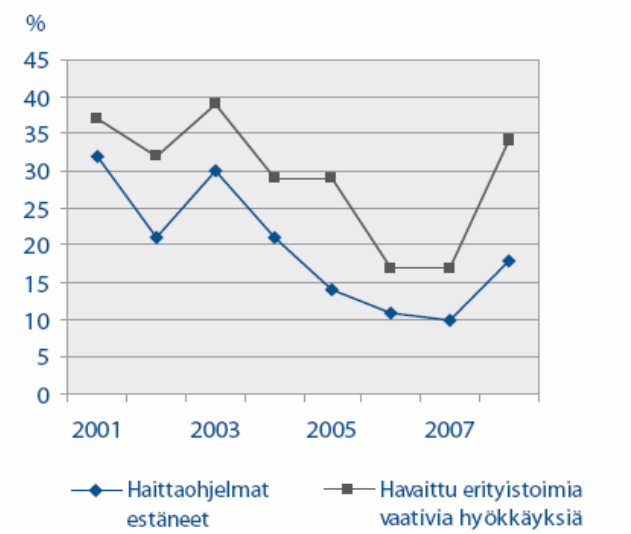
Kuva 8.1 Tietoturvallisuuden kehittyminen. Tiedot on kerätty valtionhallinnon tietoturvallisuuden teemapäivissä, jotka VAHTI on järjestänyt vuosittain joulukuussa.

[44] VAHTIn toimintakertomus vuodelta 2008, Vahti 1/2009, VM.

Ministeriöt ja virastot ovat panostaneet laajasti muun muassa tietoturvatyön organisointien ja eri yksiköt kattavan tietoturvayhteistyön, poikkeama- ja häiriötilanteisiin ja poikkeusoloihin varautumisen ja tietosuojan kehittämiseen sekä virastotason suunnitelmien ja ohjeistojen kehittämiseen. Haittaohjelmilta ja tietoturvahyökkäyksiltä suojautuminen sekä muu tietotekninen turvallisuuden kehittäminen on ollut keskeinen osa jatkuvaa jokaisessa valtion organisaatiossa toteutettavaa tietoturvatyötä.

Kuvassa 8.2 on esitetty haittaohjelmista aiheutuneen järjestelmien käytön estymisen ja erityistoimia vaatineiden tietoturvahyökkäysten yleisyyden kehitys[70]. Haittaohjelmien ja tietoturvahyökkäysten haitat ovat lisääntymässä. Noin 16 % valtionhallinnon organisaatioista on havainnut olleensa kohdistetun hyökkäyksen kohteena vuonna 2008.

Toimintojen riskien hallitsemiseksi ja jatkuvuuden varmistamiseksi valtionhallinnon on jatkossa merkittävästi pystyttävä edelleen parantamaan tietoturvaongelmiin varautumista ja poikkeamatilanteiden hallintaa sekä tietojärjestelmiensä ja - verkkojensa tilanteiden tuntemista ja hallintaa.



Kuva 8.2 Tietoturvaongelmien vaikutuksia valtionhallinnossa 2001–2008

Tilanne valtionhallinnon tietojärjestelmien suojauksen riittävyydestä on hyvä ja kehittyy edelleen.

8.4.3 Yksityinen sektori

Palveluntarjoajien suojausvaatimukset on määritelty palvelun ostajan ja toimittajan välisissä sopimuksissa. Julkisen hallinnon tietopalveluiden suurimmat yksityisen sektorin tarjoajat ovat Tietoenator, Logica sekä Fujitsu. Näiden suojausmenetelmät ovat korkealla tasolla. Pienempien palveluntarjoajien sekä palveluketjujen suojausmenetelmissä voi olla parantamisen varaa. Nämäkin kohteet sovitaan sopimuksissa ja sopimuksia valvotaan.

8.4.4 Viestintäjärjestelmät

Viestintäjärjestelmien suojausnormistosta vastaa Viestintävirasto. Lukuisat suojausmääräykset[45] perustuvat viestintämarkkinalakiin (VML) sekä sähköisen viestinnän tietosuojalakiin (SVTsL).

8.4.4.1 Määräys 54/2008 M[46]

Viestintäviraston määräys 54/2008M[43] koskee yleisten viestintäverkkojen ja viranomaisverkkojen sekä niissä tarjottavien viestintäpalveluiden tärkeysluokittelua, laitteistovarmistuksia ja varatiejärjestelyitä, tehonsyöttöä ja tehonsyötön varmistamista sekä fyysistä suojaamista. Määräys ei koske viestintäverkkojen tai -palvelujen väliaikaista tarjontaa tai väliaikaista kapasiteettia, DVB-H-verkon lähettimiä tai radiotoiminnan harjoittajia, joiden toimiluvan mukainen väestöpeitto on alle 85 %.

Viestintäverkon tai -palvelun komponentit luokitellaan merkittävyyden perusteella alenevassa tärkeysjärjestyksessä tärkeysluokkiin 1-5, esimerkki edellä kohdassa 8.3.1 (ks. myös liite 2, kohta 3.1.3.1, ei julkinen, JulkL 24.1§ 8,9 k).

Teleyrityksen on huolehdittava siitä, että sen yleiseen teletoimintaan käyttämät laitetilat täyttävät fyysisen suojaamisen minimi vaatimukset. Teleyrityksen on huolehdittava myös siitä, että tärkeysluokittelun ulkopuolelle jäävät viestintäverkon tai -palvelun komponentit on suojattu fyysisesti siten, että asiaankuulumattomat eivät pääse niihin helposti käsiksi.

Myös siirtojärjestelmän komponenttien suojaukselle on omat vaatimukset määräyksessä 54/2008 M.

[45] http://www.ficora.fi/index/saadokset/maaraykset/teletoiminta.html
[46] Viestintävirasto 54/2008 M.

9 JOHTOPÄÄTÖKSET JA TOIMENPIDE-EHDOTUKSET

9.1 Johtopäätökset nykytilasta yleisesti ja toimenpide-ehdotukset

9.1.1 Televiestinnän lainsäädäntö, normit, rakenne, hinnoittelu

Tietoyhteiskunnan televiestinnän lainsäädäntö, säädösten valvonta ja norminanto sekä verkkojen ja palvelujen rakenne, suojaukset ja operointi ovat Suomessa käytettävyyttä silmällä pitäen kansainvälisesti hyvällä tasolla. Rakennemääräykset, turvaluokitukset ja muut normit ovat korkealla tasolla. Yhdysliikenne on toimivaa ja yksinkertaista. Viestintävirasto seuraa aktiivisesti alan kehitystä ja kehittää normeja vastaamaan toimialalla tapahtuvia muutoksia.

Julkisen puhelinverkon yhdysliikenne on toteutettu operaattorien keskinäisin järjestelyin. IP-yhdysliikenne on järjestetty keskitetysti alan toimijoiden kesken. VoIP-yhdysliikenne on vielä muotoutumaton. Tunnushallinto on järjestetty erittäin hyvin niissä kohdissa, joissa on kansallista toimivaltaa. IP-osoitteet ja reittitietokannat tuottaa RIR – yhteisö (Euroopassa RIPE NCC). .fi-juuri on hajautettu asiantuntevasti. Suomen rajojen sisäpuolella on kolme juurinimipalvelinta. E.164-numeroiden (puhelinnumerot) osalta mekanismi on erilainen ja kansallinen rooli suurempi.

Eri verkkojen haavoittuvuuksia on käsitelty liitteessä 1.

9.1.1.1 Toimenpide-ehdotukset

ICT-toiminnan, erityisesti televerkkojen ja palvelujen, liiketoimintaa ja markkinoita tulisi ohjata vain siinä määrin kuin se on välttämätöntä markkinoiden ja palvelujen pitämiseksi saatavilla monipuolisina ja riittävinä. Ohjausvälineinä ovat normit, toimilupaehdot ja rahoitus. Kilpailu lisää vaihtoehtoja, myös käytettävyyden kannalta.

Infrastruktuuri

Infrastruktuurin johdinverkosto (ja radiotaajuudet) pidetään kunnossa, tiheänä, joustavana, ajanmukaisena ja kehittyvänä. Suoritetaan jatkuvaa vikakomponenttien (SPOF, Single Point of Failure) etsintää ja minimointia. Tarvittavaa laitteistoa ja energiaa on saatavilla.

Syntyy kustannusvaikutuksia alan toimijoille.

Tietoliikenne

Liikenteen (operoinnin) tavoitteisiin kuuluu, että LVM ja Viestintävirasto toimivat kansallisesti ja kansainvälisesti vireästi ja vahvalla mandaatilla. Tämä on turvattava koko CIIP-tasolla.

Ei kustannusvaikutuksia.

Loppukäyttäjä

Käyttäjätasolla on turvattava päätelaitemarkkinat, käyttöjärjestelmä- ja varusohjelmistomarkkinat, salaustuotemarkkinat, suojaohjelmamarkkinat (virustorjunta, IPS[47], jne). On pyrittävä huolehtimaan siitä, ettei päätelaite- tai ohjelmistomarkkinoille synny liian vaarallisia yhdistelmiä taikka riippuvuuksia yhteydestä valmistajan online-palveluihin valtiollisen sääntelyn ulottumattomissa.

Ei kustannusvaikutuksia.

Hinnoittelu

Suomen telepalvelujen hinnoittelu on vähintäänkin kohtuullisella tasolla. Onko viime vuosina osittain rajukin hintakilpailu aiheuttanut sen, että palvelujen laatuun ja saatavuuteen (mm. mobiiliverkoissa heikkoja peittoja) ja kehitystoimintaan ei ole voitu panostaa tarpeeksi? Tästä kysymyksestä on käyty yleistä keskustelua.

Asian omistus

Valtiolla IT-omistajuus on VM:llä. Televiestintäasiat, mukaan lukien internet, ovat LVM:ssä ja Viestintävirastossa ja varautumisen osalta LVM:ssä ja HVK:ssa (sektorit, poolit). Tapauksesta ja tilanteesta riippuen asioiden hoito voi vaatia myös yleisiä valtioneuvostotasoisia kannanottoja. Käytännössä kyse on kaupallisten toimijoiden motivoinnista ja toteutuksen seurannasta.

Ei kustannusvaikutuksia.

Osapuolten välinen yhteistyö

Operaattoreiden (tele, energia) välistä yhteistyötä on edelleen lisättävä erityisesti verkkojen ja palvelujen häiriöiden selvittämisessä ja vikojen korjaamisessa ja sekä varautumisen suunnittelussa. Tämä parantaa palvelujen käytettävyyttä.

Käytettävyyden kehittäminen edellyttää asiantuntijaosaamisen vahvistamista ja koulutukseen panostamista. Kansallisten elintärkeiden ICT-järjestelmien ja palveluiden ylläpitäminen sekä korkealaatuisten hankinta- ja käyttösopimuksien laatiminen edellyttää oman osaamisen vahvistamista normaalioloissa. Osaamisen kehittäminen edellyttää myös tämän alueen t&k-hankkeisiin lisäpanostuksia sekä hallinnossa että vastuu- ja omistajaorganisaatioissa.

Eri osapuolille syntyy kustannusvaikutuksia. Suuruutta ei voida arvioida.

[47] IPS (Intrusion Prevention System).

9.1.2 ICT-järjestelmien suojaus

9.1.2.1 Johtopäätökset

ICT-järjestelmiä suojataan useilla tasoilla. Viranomaiset antavat määräyksiä (esim. Viestintävirasto televiestinnässä ja VAHTI tietoturvallisuuden osalta valtionhallintoon), teollisuudella on omat määräyksensä, kiinteistöillä omat määräykset (esim. kaapeloinnista).

Tämän lisäksi käyttäjillä on monenkirjavaa käytäntöä suojautua esimerkiksi haittaohjelmia vastaan ja salata siirrettävää tietoa tai kryptata tiedostoja tietokoneellaan.

9.2 Kriittiset viestintäjärjestelmät

9.2.1 Kriittisten ICT-järjestelmien käytettävyys – yleiset johtopäätökset

Suomessa yhteiskunnan elintärkeiden toimintojen kannalta välttämättömien

- viestintä- ja tietoliikennejärjestelmien *käytettävyyden varmistaminen* on hallinnoltaan, organisaatioltaan, lainsäädännöltään ja tuotteiltaan/palveluiltaan pääsääntöisesti hyvässä kunnossa.
- Tietojärjestelmien ja -palvelujen *käytettävyydessä* on kehittämisen varaa. Tietojärjestelmä- ja palvelusektorilla ei ole kuitenkaan kattavia normeihin perustuvia säätelymekanismeja kuten sähköisen viestinnän alueella.
- ICT-järjestelmien ja –palvelujen *käytettävyys* suunnitellaan, toteutetaan ja johdetaan liiketoimintaprosessien sisällä. Pelkät tekniset ratkaisut ja normit eivät riitä.
- Suomessa on varauduttu ICT:n osalta poikkeusolojen lisäksi myös normaaliolojen häiriötilanteisiin sektorilainsäädännöllä sekä kaupallisten palvelutasovaatimusten avulla.
- Julkisen ja yksityisen sektorin välinen varautumisen yhteistoiminta toimii hyvin ja on kustannusten jaoltaan vakiintunutta.

Tietoyhteiskunnan verkkoon syntyy perinteisen televiestinnän lisäksi liikennettä myös erilaisista uusista lähteistä, kuten viihdeteollisuudesta ja maksupalveluista. Näiden ohjaus perustuu erilaisiin tarpeisiin kuin mitä ICT-toiminnalla on (esim. suodatus, tallennusvelvoite). Tästä on seurauksena, että verkkojen ja palveluiden käytettävyysvaatimukset voivat olla ristiriitaisia (laatuluokittelu, hinnoittelu).

9.2.2 Kiinteät verkot

9.2.2.1 Johtopäätökset

Kriittisenä infrastruktuurina Suomen kiinteät verkot ovat korkealaatuiset ja verkkopalvelujen saatavuus on hyvällä tasolla. Varsinkin tulevia laajakaistatarpeita varten, erityisesti harvaan asutuilla seuduilla, kiinteässä verkossa on vielä kuitenkin paljon kehittämisen varaa. Tähän on jo osittain varauduttu, sillä liikenne- ja viestintäministeriössä on laajakaistasuunnitelmat olemassa kuituverkon rakentamiseksi vuoteen 2015 mennessä lähes jokaisen ulottuville. Ohjelman käytännön ohjeistuksesta vastaa Viestintävirasto.

9.2.3 Mobiiliverkot

9.2.3.1 Johtopäätökset

Kriittisenä infrastruktuurina Suomen mobiiliverkot ovat pääsääntöisesti korkealaatuiset ja kilpailun vuoksi palvelujen saatavuus on vähintäänkin kohtuullisella tasolla koko maassa. Palvelujen saatavuudessa, erityisesti joillakin harvaan asutuilla seuduilla (mutta myös paikoin jopa pääkaupunkiseudulla) on kuitenkin vielä kehittämisen varaa.

9.2.3.2 Toimenpide-ehdotukset

Sen lisäksi miten yleisesti varaudutaan teleinfrastruktuurin poikkeustilanteissa, tulisi mobiiliverkkojen osalta harkita seuraavia erityistoimenpiteitä

- ”etuoikeustilaaja”-toiminteen toteuttaminen
- yhteis-SIM –toiminne (oma SIM-kortti toimii missä tahansa suomalaisessa verkossa, mikä on toiminnassa oman verkon kaaduttua).

Kustannusvaikutuksia ei arvioitu.

9.2.4 Internet

9.2.4.1 Tilannearvio ja yleiset toimenpiteet[48]

Ei voida tarkalleen luetteloida eikä tietää yhteiskunnalle välttämättömiä palveluja useiden vuosien perspektiivillä (vrt. kehitys viimeisen 15 vuoden aikana). Kaikki tarvitsevat internetiä johonkin, yhteiskunta tarvitsee kaikkia palveluita ja verkkoja johonkin.

Internetistä on tullut kriittinen infrastruktuuri. Internetin kautta saatavat elinkeinoelämän ja kansalaisten palvelut ovat elintärkeitä. Internetin Suomessa sijaitsevat osat ja Suomessa saatavilla olevat palvelut ovat osa yhteiskuntarakennetta.

9.2.4.2 Toimenpide-ehdotukset

Internetin toimivuus neutraalina ja kehittyvänä kriittisenä tiedonsiirtoalustana on turvattava kansainvälisen yhteistyön, säännösten ja teknisten ratkaisujen avulla siten, että se palvelee koko yhteiskuntaa riittävästi ja luotettavasti seuraavasti:

- huomioidaan, että sekä runkoliikennetasolla että päätelaitetasolla eri verkot yhdistyvät yhdeksi, tarpeeksi silmukoiduksi viestintäinfrastruktuuriksi, joka käyttäjälle näkymättömästi hyödyntää eri protokollia tai eri verkkoja tiedon välittämiseen,
- huolehditaan, että internetin viestintäsalaisuus turvataan,
- huolehditaan, että Suomella on jatkuva ja aktiivinen rooli internetin kansainvälisessä hallinnossa ja kehittämisessä (ICANN),
- käynnistetään internetin suojaamisesta erillinen selvitystyö.

Näihin tehtäviin hallinnon tulee varata riittävät resurssit.

[48] YKÄ-seminaari, 15.4.2009. Internet-työryhmän johtopäätökset.

9.2.4.3 Riskit ja kehitysmahdollisuudet

Taulukossa 9.1 on esitetty mitä uhkakuvia (esimerkkejä) internetissä voi esiintyä ja miten kyseisiä uhkia voidaan torjua kokonaan tai osittain ja vastuuorganisaatiot.

Taulukko 9.1 Internetin uhkakuvia ja torjunta/ehkäisykeinoja.

Uhka	Torjunta / ehkäisykeinoja	Vastuuorganisaatio

Kansainväliset tietokannat tai operatiiviset (tieto) turvajärjestelmät voivat pettää	• peilataan palvelut Suomeen ja luodaan
	  • joko kokonaan omat, kansalliset (tieto)turvajärjestelmät, tai
	  • luodaan kansalliset varajärjestelmät yhteistyössä alan organisaatioiden kanssa.
		• CERT-FI
		• operaattorit
		• FICIX

Internetin nimipalvelintietoja voidaan massaväärentää tai väärentää kokonaisia palvelimia.	• otetaan käyttöön kriittisiin käyttökohteisiin soveltuvin osin DNSsec –järjestelmä, ja • ENUM[49] (tai DNSxxx)	• FICIX • operaattorit • Viestintävirasto
Suomeen rekisteröidyt IP-osoitteet voidaan kaapata joko tahallisesti tai tahattomasti.	• luodaan kansallinen varoitusjärjestelmä, sekä • sovitaan EU-yhteistyön kautta vaikutusten minimoinnista uhan realisoituessa	• CERT-FI • LVM
Muita internetin käytettävyyttä, luotettavuutta ja kansainvälistä saatavuutta parantavia toimenpiteitä		
Uusien televerkkojen kellotus ja NTP (Network Time Protocol) -jakelu (cesium- tai GPS-kello).		• FICIX
Teleyritysten reittiheijastimien käytön ohjeistaminen sekä yhdysliikenteeseen harkittavaksi RouteServer –optio		• Viestintävirasto • operaattorit
Suomen edustuksen turvaaminen ja jatkumo globaalissa Internetin hallinnossa (ICANN[50], IGF[51] ja IANA[52]).		• LVM/Viestintävirasto • UM
Yhdysvalloissa on tekeillä laki tietoverkkoturvasta (cybersecurity). Laki on kehittymässä siihen suuntaan, ettei presidentillä olisikaan oikeutta katkaista minkä tahansa organisaation tai palvelun internet-yhteyksiä[53]. Lain ensimmäisen luonnoksen mukaan "presidentti voi määrätä katkaistavaksi minkä tahansa liittovaltion hallitukselle tai Yhdysvalloille olennaisen informaatiojärjestelmän tai verkon yhteydet".		• Lain kehittymistä tulee seurata sekä kansallisella että EU-tasolla • LVM • UM

Normaaliolojen häiriötilanteisiin varautuminen

Internetissä voi normaalioloissa esiintyä erilaisia häiriötilanteita, joihin pitää pystyä varautumaan. Näitä on esitetty taulukossa 9.2. Suomeen voi kohdistua esimerkiksi maan ulkopuolinen häiriötekijä (esim. DDoS[54]-hyökkäys). Tämä on erittäin vakava uhkakuva. Suomesta voi kohdistua häiriötekijä myös ulospäin (esim. DDoS-hyökkäys, IP-kaappaus).

[49] ENUM (from **E**.164 **NU**mber **M**apping). ENUM on teknologia, jossa perinteisestä puhelinnumerosta (E.164-standardin mukainen) muodostetaan internetin nimipalvelinjärjestelmän mukainen verkkotunnus eli niin kutsuttu ENUM-tunnus. Sen avulla numeroon voidaan osoittaa useita viestintäpalveluita, kuten internet-puheluja ja sähköpostia. Vaikka ENUM tukee erilaisia palveluita kuten pikaviestejä tai sähköpostia, sen tärkein käyttökohde on VoIP-puhelujen ohjaaminen (http://www.ficora.fi/index/palvelut/palvelutaiheittain/enum/mikaenumon.html).
[50] ICANN (Internet Corporation for Assigned Names and Numbers). Ks. Liite 2.
[51] IGF (Internet Governance Forum). Ks. Liite 2
[52] IANA (Internet Assigned Numbers Authority). Ks. Liite 2.
[53] TIVI.fi, 1.9.2009. http://www.tietoviikko.fi/kaikki_uutiset/article323975.ece?s=l&wtm=tietoviikko/-01092009
[54] DDoS (Distributed Denial of Service). Useista lähteistä tapahtuva samanaikainen hyökkäys tiettyä järjestelmää kohtaan, hajautettu palvelunestohyökkäys (DDoS).

Taulukko 9.2 Internetin normaaliolojen häiriötilanteisiin varautuminen

Häiriötilanne	Torjunta / ehkäisykeinoja	Vastuuorganisaatio
Teleyritysten yhteistoiminnan lamaantuminen (esim. yritysoston seurauksena)	• Turvaamalla hätärahoitus • Ottamalla yrityksen operatiivinen toiminta haltuun • Järjestämällä toiminta väliaikaisin ratkaisuin	• HVK • LVM • Viestintävirasto

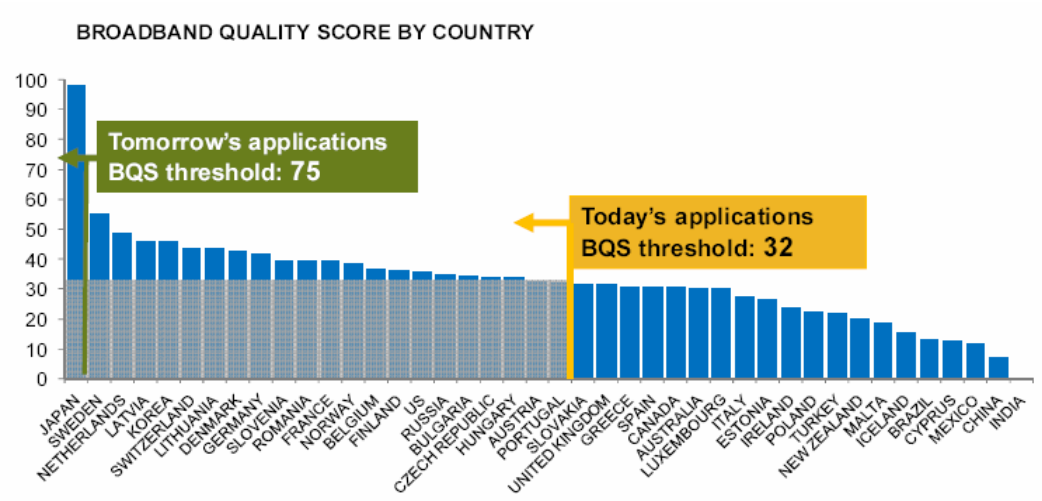
Suomeen voi kohdistua maan ulkopuolinen häiriötekijä (esim. DDoS-hyökkäys).	• Preferoimalla maan sisäistä liikennettä, esim.
	  • ottamalla käyttöön white-listatut postipalvelimet, nimipalvelimet ja ”etuoikeustilaaja-toiminne”.
	  • ”Etuoikeustilaaja”-toiminne tulisi standardoida kansallisesti.
		• LVM
		• Viestintävirasto
		• Operaattorit

Suomesta voi kohdistua häiriötekijä myös maailmalle (esim. DDoS-hyökkäys, IP-kaappaus), jolloin uhkana voisi olla • Suomi eristetään ulkomaista, ja • mahdollisesti jopa kansallisen infrastruktuurin alasajo	• Pyrittävä välttämään yhteiskunnan suojatointen (suodatukset, televalvonta) kohdistamista kriittisiin elementteihin. • Suojatoimet tulisi toteuttaa niistä erillään	• LVM • Viestintävirasto • Operaattorit

9.2.5 Laajakaistan laatu

9.2.5.1 Johtopäätökset

Suomen laajakaistan ”laatu” (BQS) on jäänyt viime vuosina jälkeen muiden kehittyneiden maiden laajakaistapalveluista. Tätä on esitetty kuvan 9.1 mukaisella laajalla selvityksellä. Kuvan BQS (Broadband Quality Score) mittaa sekä downlink- että uplink-nopeuksia ja liikenteen latenssia (viivettä) painotettuna eri liikenneprofiileilla tällä hetkellä sekä tulevaisuuden sovellusskenaarioiden mukaisesti.



Kuva 9.1 Laajakaistan laatumitta (BQS) eri maissa[55]

[55] Broadband Quality Score – A global study of broadband quality, September 2008 (sponsored by Cisco).

Laajakaistan laatu korreloi ICT-tuotteiden ja palveluiden yleisyyden, osaamistalouden ja web-käytön kanssa. Kuituverkon tiheys ja kaapeliverkkojen päivitykset nostavat BQS-arvoa.

Viestintävirastossa on käynnissä määräystyö M58 viestintäverkkojen ja palvelujen laadusta. Määräystyö on loppusuoralla ja tulee voimaan 1.1.2010.

9.2.5.2 Toimenpide-ehdotukset

Panostukset kuituinfrastruktuuriin

Jotta Suomi taas pääsisi tietoyhteiskunnassa sille tasolle mille se kuuluisi kokemuksensa ja sekä ekonomisen ja teknologisen osaamisensa vuoksi ja jotta internetin rooliin kriittisenä infrastruktuurina luotettaisiin enemmän, Suomessa tulisi panostaa laajakaistan saatavuuteen, penetraation lisäämiseen ja laatuun enemmän. Infrastruktuuritasolla tämä tarkoittaa suurempia panostuksia kuituyhteyksiin.

Laajakaistan saatavuus syventää tietoyhteiskuntaa ja on siten YKÄ-tavoitteiden mukainen. Tätä tehtävää edesauttaa hallituksen laajakaistastrategia.

Kustannusvaikutukset ovat suuret ja kohdistuvat lähinnä verkkoinvestointeihin.

9.2.6 Poikkeustilanteisiin varautuminen yleisesti

Tieto- ja viestintäpalvelujen poikkeustilanne voi syntyä esimerkiksi suuremmista markkinahäiriöistä johtuen tai ulkopuolisen vakavan uhkan toteuduttua. Telepalvelujen saatavuus voi estyä tällöin joko kokonaan tai osittain, taulukko 9.3.

Taulukko 9.2 Poikkeustilanteisiin varautuminen

Poikkeustilanne	Toimenpide	Vastuuorganisaatio
Teleyritysten yhteistoiminta voi lamaantua isojen markkinahäiriöiden seurauksena • konkurssit • ei huolehdita resurssoinnista	• Sopimalla teleyrityksen operatiivisen toiminnan haltuunottamisesta valtion, tai jonkin muun valtion sopiman tahon toimesta	• VM • LVM
Teleyritysten oma toiminta voi lamaantua • esim. sotilaalliset iskut	• Viranomaisjärjestelmiin siirtyminen	• VM • LVM

9.2.7 Muita yleisiä haasteita ja toimenpiteitä

9.2.7.1 Valmiuslainsäädäntö – varautumisohjeet

Pitäisikö toimivaltuuksia olla käytössä jo laajoissa katastrofitilanteissa, eikä pelkästään poikkeusoloissa (ks. kohta 7.2).

9.2.7.2 Palvelujen sovittaminen EU-tason kehityksen kanssa

Tulee huolehtia siitä, että EU-tasolla tapahtuva palvelurakenteiden kehitys ja kotimaisten elintärkeiden toimintojen turvaamistoimenpiteet saadaan sovitettua yhteen ja keskenään. Esimerkkinä voidaan mainita finanssitoimialan maksuliikkeen kehitys, tai toimijoiden yhteiset rakenteet (energia, tietoliikenne). Kehitystä tulee edesauttaa siten, että Suomesta viedään hyviä ratkaisumalleja myös EU-tasolle sen rinnalla, kun sieltä tuodaan ratkaisuja Suomeen.

9.2.7.3 Verkottuvan elinkeinotoiminnan hallittavuus

Lähes koko tietoyhteiskunnan palvelutuotanto hoidetaan yksityisen sektorin toimesta. Palveluntuottajien omat suorat kumppanit ovat hallittavissa sopimuksin. Ketjuuntuvat palvelurakenteet ja siinä tapahtuvat muutokset ja vastuut ovat hankalammin hallittava ja valvottava alue.

9.2.7.4 Poliittisen päätöksenteon, lain valmistelun ja elinkeinoelämän yhteistyö

Tietoyhteiskunnassa on lukuisia yhteishankkeita, missä on mukana poliittista päätöksentekoa, lainvalmistelua ja elinkeinoelämän edustusta. Aina nämä hankkeet eivät ole tuottaneet parhaita mahdollisia tuloksia. Esimerkiksi, voiko tavoite lukuisista rinnakkaisista sähköisen tunnistuksen menetelmistä nousta uudeksi uhaksi palvelujen tuottamisen jatkuvuudelle. Ks. kohdat 6.3 ja 9.6.

Onko pienillä ja keskisuurilla yrityksellä ylipäätään edellytyksiä ylläpitää ja hallita lukuisia rinnakkaisia tunnistus- ja tietoturvateknologioita.

Eri osapuolten välistä yhteistyötä tulee jäntevöittää ja käyttäjien (yritykset, kuluttajat) tarpeita ja mahdollisuuksia hyödyntää syntyviä päätöksiä ja ratkaisuja selvittää enemmän.

9.3 Omistaja- ja teollisuuspoliittiset kysymykset

9.3.1 Muuttuva tilanne – haasteet kasvavat

Tieto- ja viestintäjärjestelmistä (ICT) on tullut nopeasti strategisin kriittinen infrastruktuuri yhdessä energian saannin kanssa. Tämä tunnustetaan kansainvälisesti yhteiskunnan kaikilla alueilla, niin volyymeissa kuin merkityksessä esimerkiksi yhteiskunnan tuottavuuteen.

Suomi on turvallisimpia valtioita maailmassa. Suomea ei uhkaa välittömästi mitkään selkkaukset eikä konfliktit. Maailma kuitenkin kutistuu. Globalisaatio, taloudelliset käänteet ja verkkojen kautta tulevat uhkakuvat ovat aiheuttaneet pyrkimyksiä kriittisten elintärkeiden ICT-toimintojen varmistamiseen kansallisin resurssein.

Kansainvälisen yhteistyön seurauksena on syntynyt uusia, kompleksisista arvoverkoista muodostuneita toimintamalleja. Organisaation toimintaprosessit voivat sijaita osittain tai kokonaan maan rajojen ulkopuolella, jolloin toiminnan turvallisuus ja luotettavuus ovat vaikeammin hallittavissa.

9.3.2 Uhka - markkinahäiriöt

ICT-palvelujen viime vuosien kehitykselle on ollut ominaista tarjonnan globalisoituminen ja toimintojen ulkoistaminen, mihin liittyvistä mahdollisista lieveilmiöistä voi aiheutua vakavia markkinahäiriöitä ja ongelmia ICT-palvelujen saatavuudelle.

Markkinat eivät välttämättä kannusta yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien suojaamiseen yhteiskunnan varautumisen edellyttämälle tasolle. Tämän on todennut myös EU-komissio.

ICT-palvelujen **käytettävyyttä** ei kaikissa tapauksissa pystytä takaamaan, mikä vaikuttaa yhteiskunnan varautumiseen. ICT-yritys tai sitä palveleva kriittinen alihankintayritys voi esimerkiksi irtisanoa suuren osan henkilöresursseistaan, lopettaa joidenkin palveluiden tarjoamisen tai mennä jopa konkurssiin.

Nykymuotoinen tiukka kilpailu ei jätä yritykseen vararesursseja, mikä voi heikentää yrityksen riskinkantokykyä ja sitä kautta tehdä yrityksen toiminnan haavoittuvammaksi erilaisille uhkille kriisitilanteissa.

9.3.3 Työryhmän toteamukset

Kriittisten ICT-järjestelmien ja niiden komponenttien omistus ja valvonta on aiheuttanut työryhmässä vilkasta keskustelua.

9.3.3.1 Toimenpiteet

Yhteiskunnalle elintärkeiden tietovarantojen ja datan varmistaminen ja saatavuus tulee olla taattu kaikissa turvallisuustilanteissa. Esimerkiksi tietovuotojen ja palvelunestohyökkäysten torjumiseksi olisi hyvä mikäli tietovarannot olisi hajautettu laajalle. Yhteiskunnan toiminnan kannalta kriittisten tietojärjestelmien hallinta tulee järjestää siten, että siihen voidaan vaikuttaa kansallisin säädöksin ja päätöksin.

Yhteiskunnan tulee edesauttaa kriittisten ICT-järjestelmien suojausintressin luomisessa niitä tilanteita varten, missä markkinat eivät kannusta riittävästi yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien suojaamiseen yhteiskunnan varautumisen edellyttämälle tasolle.

9.3.4 Huoltovarmuusorganisaatio

9.3.4.1 Taustaa

Huoltovarmuuskeskuksen tase on noin 1,2 miljardia euroa[56]. Pääosa varoista on sidottu varastomateriaaleihin. Selvästi suurin tuoteryhmä on nestemäiset polttoaineet, joissa on 80 prosenttia Huoltovarmuuskeskuksen omaisuudesta. Muita isoja tuoteryhmiä ovat vilja ja siemenvilja, lääkintämateriaalit ja erilaiset teollisuuden tarvitsemat materiaalit.

[56] http://www.huoltovarmuus.fi/organisaatio/talous-ja-lainsaadanto/huoltovarmuuden-rahoitus/

Tietoyhteiskuntatoimialan huoltovarmuutta koordinoivat Huoltovarmuuskeskuksen infrastruktuuriosasto, tietoyhteiskuntasektori sekä sektorin alaiset poolit. Lisäksi tietoyhteiskuntasektorilla on oma alueorganisaatio, aluepooli, jonka muodostavat tietojärjestelmäalan valmiustoimikunnat eli ns. TIVA-toimikunnat. HVK:n tietoyhteiskuntasektori on strateginen YKÄ-toiminnan kannalta.

ICT-toiminnan ja logistiikan osuus huoltovarmuuden ylläpitämisessä on strateginen ja sen merkitys koko ajan kasvaa. Tämän lisäksi tietoyhteiskunnan syventynyt merkitys yhteiskunnan elintärkeiden toimintojen varmistamisessa jo normaalioloissa on entisestään tärkeämpää.

9.3.4.2 Työryhmän ehdotus

Huoltovarmuusorganisaation roolia tulisi vahvistaa ja laajentaa ICT-alueella.

Kustannusvaikutuksia ei arvioitu.

9.3.5 Huoltovarmuusbudjetin laajentaminen

9.3.5.1 Ongelma ja mallit

Tietoyhteiskunnan syventäminen elintärkeiden toimintojen kriittisten ICT-järjestelmien varmistuksilla yli normaalitason tulee edellyttämään ICT-toimijoilta ylimääräisiä panostuksia. Myös CIIP-toiminnan kehittäminen vaatii lisäpanostuksia.

EU-komissio on julkaissut kannanoton (huhtikuu 2009), minkä mukaan on yleisesti tunnustettua, että markkinat eivät välttämättä kannusta yksityisiä toimijoita investoimaan kriittisten ICT-järjestelmien (CII) suojaamiseen yhteiskunnan varautumisen edellyttämälle tasolle.

CIIP-rahoituksella on kaksi päävaihtoehtoa

- Erillinen CIIP-budjetti, josta valtion osuus on esimerkiksi 50 % ja teleyritykset maksavat yhteensä toisen 50 %.
- Teleyritykset keräävät ”CIIP-senttejä” suoraan tilaajilta ja tulouttavat sen CIIP-budjettiin.

Molemmissa malleissa teleyrityksille on asetettu velvoitteita ja periaatteet siitä kuka maksaa, jos pitää suorittaa välttämättömiä normaalitason ylittäviä CIIP-investointeja.

Ensimmäinen malli on käytössä Ruotsissa. Jälkimmäinen periaate on sama kuin nykyinen ns. huoltovarmuusmaksun kerääminen energiaverojen yhteydessä. Huoltovarmuusrahastoa kartutetaan energiankäytön kautta, mutta varoja suunnataan mm. lääkkeiden ja ICT-rakenteiden suuntaan.

Oma kysymyksensä on yhteiskunnallisesti merkittävien verkkojen ja palveluntuottajien (joukkoviestintä, rahoitus, kauppa, …) rooli CIIP-rahoituksen keräämisessä/investointien maksatuksissa.

Esimerkiksi teleyritysten liikevaihto oli vuonna 2008 yhteensä 4262,6 milj. euroa[57]. Jos tästä kerättäisiin 0,6 % varautumiseen, tarkoittaisi se noin 25 miljoonan euron lisää nykyiseen varautumisbudjettiin.

Rahoituksen tasoa pitää säätää vastaamaan kokonaistarvetta ja suunnata kriittisen infrastruktuurin tarpeiden mukaisesti siten kuin parlamentaarisesti VNp:ssä on linjattu.

Kysynnän ja tarjonnan tulisi kuitenkin itsessään taata yrityksille tarkoituksenmukainen jatkuvuuden hallinta. Mikäli tarpeet menevät tämän yli, viranomaiset maksavat sen budjettivaroin.

9.3.5.2 Työryhmän toteamus

Työryhmä on käynyt keskustelua uusien varautumishaasteiden rahoittamisesta.

9.4 YKÄ-toiminnan kehittäminen

9.4.1 YKÄ-prosessin jatkuvuuden takaaminen

Yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta välttämättömien ICT-järjestelmien *käytettävyyden* kehittäminen (YKÄ-toiminta) on tällä hetkellä vastuutettu hallinnossa eri ministeriöihin ja organisaatioihin ja moniin hankkeisiin. Päättyvässä YKÄ-hankkeessa sitä selvitetään nyt liikenne- ja viestintäministeriön johdolla. YKÄ-toiminta edellyttää jatkuvuutta ja liiketoimintaprosesseihin ja niiden pohjalta sovittuihin käytäntöihin ulottuvaa kehittämistä (ks. kohta 6.2.4). Työryhmä toteaa, että

- YKÄ-tavoitteisiin ei ole oikotietä, kaikki vaadittavat toimenpiteet on tehtävä huolellisesti
- YKÄ-toimintaa pitää ohjata ja seurata aktiivisesti, jottei vahingossa vakiinnu rapauttavia käytäntöjä
- Monisyisyyden vuoksi YKÄ-toiminnan strategiaa ja linjauksia tulisi ohjata sekä seurantaa hoitaa keskitetysti, mutta toimenpiteiden toteutus on hajautettua.

YKÄ-toimintaan liittyy tärkeänä elementtinä kansainvälinen CII- ja CIIP-ulottuvuus, lähinnä Euroopan unionin taholta. Nämä aktiviteetit edellyttävät jatkuvaa seurantaa ja hallinnon laajasti perusteltuja kannanottoja.

9.4.1.1 Työryhmän ehdotus

Työryhmä kokee tärkeänä, että YKÄ-toimintaa kehitetään edelleen ja sen jatkamisen muotoja valmistellaan. Valmistelutyön omistajaksi ehdotetaan Huoltovarmuusorganisaation tietoyhteiskuntasektoria. Valmistelutyöhön kuuluu myös YKÄ-alueen t&k-toiminta.

YKÄ-toiminnan kehittämiseen on osoitettava riittävät resurssit.

[57] http://www.stat.fi/til/tvie/2008/tvie_2008_2009-06-09_tau_011_fi.html

9.5 Palveluihin ja tekniikkaan liittyvät toimenpiteet

9.5.1 Häiriötapahtumarekisterin perustaminen

9.5.1.1 Taustaa

Kriittiset infrastruktuurit (CI) riippuvat monella tavalla toisistaan, erityisesti ICT:stä ja energian saannista. Keskinäisiä riippuvuuksia on mallinnettu lukuisissa kansainvälisissä tutkimuksissa. Kyseiset tutkimukset ovat kuitenkin pääsääntöisesti kaikki teoreettisia ja niistä puuttuu lähes poikkeuksetta käytännön reaalidata. Tarvittaisiin käytännön havaintoihin perustuva häiriörekisteri.

Rekisteri voisi toimia käytännössä esimerkiksi siten että kukin CI-sektori kerää omassa toiminnassaan esiintyneet häiriöt luokiteltuna sovitusti, joista tehdään keskitetysti tilastot myöhemmin suoritettavan mallinnuksen edellyttämällä tavalla automaattisesti.

Rekisteri voisi palvella

1. *Kriittisten CI-komponenttien (ainakin ICT, energia) tunnistamisessa*
   a) kriittisten komponenttien tunnistaminen,
   b) häiriöiden **todellisen** alkuperän ja merkityksen selvittäminen ja häiriöiden leviäminen (cascading) CI:stä toiseen ja kolmanteen,
   c) mallintaminen ja ennustaminen.
2. *Laadun kehittämisessä*
   a) käytettävyyden/ varautumisen ICT-resurssien ja organisoinnin suunnittelu ja allokointi,
   b) ICT-järjestelmien SLA-sopimusten valvonta,
   c) tilannekuvan muodostaminen (esim. energia, ICT).

9.5.1.2 Työryhmän ehdotus

Tehdään erillinen selvitys kuvatun häiriörekisterin perustamisesta. Hankkeen omistajana voisi olla Huoltovarmuusorganisaatio/tietoyhteiskuntasektori.

Hankkeen arvioidut kustannusvaikutukset ovat **400,000 euroa** vuodessa.

9.6 Muut toimenpide-ehdotukset

9.6.1 Identiteetin hallinta

Identiteetin arvo ja sen todistaminen tulisi nostaa tietoyhteiskunnassa omaksi kriittiseksi infrastruktuuriksi. Tämä huoli tulisi lisäksi nostaa CII-tasolle myös Euroopan unionissa.

Tietoyhteiskunnassa tulee olla käytettävissä toimiva, luotettava ja tarpeeksi laajasti hyväksytty ja yksinkertainen identiteetin tunnistusmenetelmä.

9.6.1.1 Työryhmän ehdotus

Työryhmä ehdottaa, että identiteetin hallinnasta muodostettaisiin kriittisen infrastruktuurin tasoinen konsepti. Konseptin kehittämiseksi tulee selvittää voidaanko se kytkeä osaksi jo jotain meneillään olevaa tarpeeksi laajaa identiteetin hallinnan kehityshanketta.

Hallinnon tulee varata tähän riittävät resurssit.