



VALTIOVARAINMINISTERIÖ

VALTIONHALLINNON ICT-VARAUTUMINEN

Esitutkimusraportti

Marraskuu 2008



VALTIOVARAINMINISTERIÖ

Valtionhallinnon ICT-varautuminen

Esitutkimusraportti



VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 09 16001 (vaihde)
Internet: www.vm.fi
Taitto: Pirkko Ala-Marttila/VM-julkaisutiimi

Edita Prima Oy
Helsinki 2008

Kuvailulehti

Julkaisija ja julkaisuaika	Valtiovarainministeriö, marraskuu 2008	
Tekijät	Varautumisen esitutkimushanke	
Julkaisun nimi	Valtionhallinnon ICT-varautumisen esitutkimus	
Julkaisun osat/ muut tuotetut versiot	Julkaisu on saatavissa Internetistä osoitteesta www.vm.fi/julkaisut	
Asiasanat	varautuminen, jatkuvuus, riskienhallinta, uhka-analyysi, riskianalyysi, osaa- minen, toimittajaverkosto, vaatimustasot, strategiat, tietoturva, tietotekniik- ka, tietojärjestelmät, tietohallinto, tulosohjaus, ICT, YETTS	
Julkaisusarjan nimi ja numero		
Julkaisun myynti/jakaja		
Painopaikka ja -aika	Edita Prima Oy, Helsinki 2008	
ISBN	Sivuja 92	Kieli Suomi
ISBN	Hinta	
ISSN		
Tiivistelmä	Valtiovarainministeriö asetti 28.9.2007 tekemällään päätöksellä varautumi- sen esitutkimushankkeen 1.11.2007 – 30.6.2008 väliseksi ajaksi. Varautumisen kärkihanke on osa valtionhallinnon kokonaiskehittä- mistä sekä yhteiskunnan elintärkeiden toimintojen strategian (YETTS), Valtioneuvoston päätöksen huoltovarmuuden tavoitteista ja valtioneuvos- ton periaatepäätöksen valtion IT-toimintojen kehittämisestä toimeenpanoa. Siihen sisältyy sekä normaaliolojen häiriötilanteisiin että poikkeusoloihin varautuminen. Asettamiskirjeessä esitutkimuksen ulkopuolelle on rajattu Euroopan unionin ja kuntasektorin varautumisen lähempi tarkastelu. Esitutkimuksen toteuttamista on tukenut ja ohjannut hallinnonaloilta kootut ohjaus-, valmistelu- ja seurantaryhmä sekä Valtionhallinnon tietotur- vallisuuden johtoryhmä (VAHTI). Työhön liittyi laaja nykytilannetta selvittä- nyt kysely kaikille hallinnonaloille. Raporttia on työstetty valmisteluryhmän työkokouksissa ja laajoissa työpajoissa. Esitutkimuksessa esitettävät kehittämistoimenpiteet kohdennetaan orga- nisaatioiden ja toiminnan muutostapahtumiin, hallinnonalojen ja ValtIT:n hankkeisiin sekä esitettäviin uusiin hankkeisiin. Keskeisiä kehittämisalueita ovat ICT-varautumisen vaatimusten täsmentäminen, ohjauksen ja resurssoin- nin tehostaminen, tilannetietojen saatavuuden parantaminen, uhka- ja ris- kianalyysi yhtenäistäminen, osaamisen varmistaminen sekä palveluverkos- ton hallinta ja hyödyntäminen. ICT-varautumisen kehittäminen on edellytys kustannusten, riskien ja priorisointien optimoimiseen. Tällä mahdollistetaan kehittämistä koskeva ennakoiva päätöksenteko ja resurssien yhteiskäyttö. Tavoitteeksi asetetaan, että ICT-varautuminen on kustannustehokas ja koordinoitu osa kunkin hallinnonalan jokapäiväistä toimintaa siten, et- tä palvelujen jatkuvuus kyetään takaamaan toiminnan vaatimusten mu- kaisesti häiriötilanteissa, YETTS-eritystilanteissa ja poikkeusoloissa. ICT- varautuminen ei ole erillinen toiminto, vaan osa tietohallinnon ja yleisen va- rautumisen kokonaisuutta. Tavoitteen saavuttaminen esitetään vaiheistettavaksi siten, että vuoden 2010 loppuun mennessä ICT-varautumisen ohjaus on osana yleisiä ohjaus- menetelmiä ja vaatimustasot on määritelty. Hallinnonalat ovat suunnitel- leet ja käynnistäneet ICT-varautumisen toteuttamisen. Vuoden 2012 lop- puun mennessä hallinnonaloilla ja virastoissa on saavutettu kriittisissä toi- minnoissa ICT-varautumisen perustaso. Kumppanusverkoston vaatimusten hallinta ja sopimusmenettelyt on yhtenäistetty. Vuoden 2016 loppuun men- nessä valtionhallinto on kokonaisuudessaan saavuttanut ja todentanut ICT- varautumisen perustason sekä erikseen määritellyiltä osiltaan korotetun tai korkean tason.	

Presentationsblad

Utgivare och datum	Finansministeriet, November 2008	
Författare	Förhandsundersökningsprojektet för beredskap	
Publikationens titel	Förhandsundersökningsrapport om statsförvaltningens ICT-beredskap	
Publikationens andra versioner	Publikationen finns på finska på Internet-address www.vm.fi/julkaisut	
Nyckelord	-	
Publikationsserie och nummer		
Beställningar/distribution		
Tryckeri/tryckningsort och -år	Edita Prima Ab, Helsingfors 2008	
ISBN ISBN ISSN	Sidor 92	Språk Finska
	Pris	
Sammandrag	Finansministeriet tillsatte genom sitt beslut av den 28 september 2007 förhandsundersökningsprojektet för beredskap för tiden 1.11.2007-30.6.2008. Spetsprojektet för beredskap är en del av statsrådets helhetsutveckling samt av verkställandet av strategin för tryggandet av samhällets livsviktiga funktioner (YETTS), statsrådets beslut om målen för försörjningssäkerheten och statsrådets principbeslut om utvecklandet av statens IT-verksamhet. Det inkluderar förberedelser både inför störningssituationer under normala förhållanden samt beredskap inför exceptionella förhållanden. I beslutet om tillstånd avgränsades noggrannare granskning av Europeiska unionens och kommunsektorns beredskap utanför undersökningen. Genomförandet av förhandsundersökningen har understöts och styrts av styrnings-, berednings- och uppföljningsgruppen samt ledningsgruppen för datasäkerheten inom statsförvaltningen (VAHTI) vilka består av representanter för förvaltningsområdena. I arbetet ingick en omfattande enkät åt samtliga förvaltningsområden om nuläget. Rapporten har bearbetats vid beredningsgruppens arbetsmöten och i omfattande workshops. De utvecklingsåtgärder som presenteras i förhandsundersökningen gäller främst ändringssituationer inom organisationer och verksamheter, förvaltningsområdenas och ValtIT:s projekt samt nya projekt som föreslås. De viktigaste utvecklingsområdena består av specificeringen av kraven för ICT-beredskap, effektivisering av styrningen och resurseringen, förbättring av tillgången på lägesinformation, samordning av hot- och riskanalyserna, säkerställande av kunskanden samt kontroll och utnyttjande av servicenätverket. Utvecklandet av ICT-beredskapen är en förutsättning för optimering av kostnader, risker och prioritering. På så sätt möjliggörs proaktivt beslutsfattande i fråga om utvecklandet samt sammanvändning av resurser. Som mål fastställs att ICT-beredskapen är en kostnadseffektiv och koordinerad del av varje förvaltningsområdes dagliga verksamhet så att servicens kontinuitet kan säkras i enlighet med verksamhetens krav vid störningssituationer, YETTS-undantagssituationer och exceptionella förhållanden. ICT-beredskapen är inte någon skild funktion, utan en del av den helhet som består av informationsförvaltning och allmän beredskap. Det föreslås att uppnåendet av målet ska ske i etapper så att styrningen av ICT-beredskap blivit en del av de allmänna styrmetoderna före utgången av 2010, och så att kravnivåerna fastslagits. Förvaltningsområdena har planerat och inlett beredningen av ICT-beredskapen. Förvaltningsområdena och ämbetsverken har uppnått en grundnivå för ICT-beredskapen för kritiska funktioners del före utgången av 2012. Kraven för kontrollen av samt avtalsförhållanden i fråga om partnerskapsnätverk har harmoniserats. Statsförvaltningen har före utgången av 2016 som helhet uppnått och verifierat en grundnivå för ICT-beredskapen, samt antingen höjd eller hög nivå för skilt definierade delar.	

Description page

Publisher and date	Ministry of Finance, November 2008	
Author(s)	Feasibility study in contingency planning	
Title of publication	Government ICT contingency planning feasibility study	
Parts of publication/ other versions released	The publication is available in Finnish at www.vm.fi	
Keywords	-	
Publication series and number		
Distribution and sale		
Printed by	Edita Prima Ltd, Helsinki 2008	
ISBN ISBN ISSN	No. of pages 92	Language Finnish
	Price	
Abstract	The Ministry of Finance made a decision on 28 Sept. 2007 to set up a feasibility study project from 1 November 2007 to 30 June 2008. The spearhead project on ICT contingency planning related to the implementation of overall development in central government activities, of the strategy on functions vital to society (YETTS), of the Government Decision on security of supply and of the Government Resolution on developing IT activities. It includes contingency plans for abnormalities in ordinary circumstances and provision against emergency conditions. The project declaration specifies that closer examination of contingency plans in the European Union and in local government have been excluded from the study. A task force on steering, preparation and follow-up work was set up from different administrative sectors to lend support and assistance to the study. The Government Information Security Management Board (VAHTI) also collaborated in the work. A broad questionnaire to map out the current situation was sent to the different government sectors. The report was fine-tuned in the task force meetings and in various workshops. The measures for improvement presented in the study focus on periods of change in organizations and activities, on the centralized steering and production of IT services projects (ValtiIT projects) and on forthcoming projects. Key areas of improvement consist of the following: more specific requirements for ICT contingency planning, more effective steering and resourcing, situation information more readily available, more harmonized analysis of threats and risks, safeguarding competence and proper management and exploitation of service networks. ICT contingency planning is essential for optimizing costs, for risk management and for setting priorities. It makes it possible to improve pre-emptive decision-making and joint use of resources. The aim is to ensure that ICT contingency planning is a cost-effective and well coordinated part of the daily activities in each administrative branch, so that the continuity of the services can be secured as specified in abnormal conditions, in situations where the functions vital to society are at risk (YETTS) and in emergency circumstances. ICT contingency is not an isolated function. It is an integral part of overall ICT and contingency planning. To achieve the goals, the process is designed to be implemented in stages, so that by the end of 2010 the steering of ICT contingency planning has become part of overall steering methods and the requirement levels have been specified. By then the administrative branches will have made plans and already set ICT contingency plans in motion. By the end of 2012 the ministries and agencies will have reached a basic ICT contingency level in their critical functions. The requirements for partnership networks can be managed and contract procedures have been harmonized. By the end of 2016 the whole of central government will have reached a basic ICT contingency level and an advanced or higher level where specified.	

Sisältö

1	ICT-varautuminen	9
1.1	ICT-varautumisen esitutkimushanke	9
1.2	ICT-varautumisen sidosryhmät ja siihen liittyvät hankkeet	13
1.3	ICT-varautumisen keskeiset osa-alueet	14
1.3.1	ICT-varautumisen ohjaus	14
1.3.2	Riskienhallinta	16
1.3.3	Jatkuvuuden hallinta	17
1.3.4	ICT-varautumisen osaaminen	18
1.3.5	Tietovarannot ja rekisterit sekä sähköiset palvelut	19
1.3.6	Tietotekniset peruspalvelut, infrastruktuuri ja niitä välittömästi tukevat rakenteet	20
2	Valtion ICT-toiminnan varautumisen nykytila ja tarpeet	21
2.1	ICT-varautumisen toimintaympäristö	21
2.1.1	Turvallisuusympäristö ICT-varautumisen kannalta	21
2.1.2	Arvio tietoyhteiskuntakehityksestä varautumisen näkökulmasta	23
2.2	Valtion ICT-varautumisen ohjaus ja suunnittelu-mekanismit	25
2.2.1	Valtiotason ohjaus	25
2.2.2	ICT-varautumisen ohjaus hallinnonaloilla	29
2.2.3	Sidosryhmäohjaus ja yhteistoiminta	30
2.2.4	ICT-varautumisen tarkastus ja auditointi	32
2.3	Riskienhallinta ja vaatimusten muodostaminen	32
2.3.1	ICT-varautumisen tilannetietoisuus	32
2.3.2	Uhka-arvio ja riskianalyysi	33
2.3.3	Kriittisten toimintojen edellyttämän ICT-tarpeen tunnistaminen	34
2.3.4	ICT-varautumisen vaatimusten asettaminen	35
2.4	Palvelujen ja ICT-infrastruktuurin jatkuvuuden hallinta	36
2.4.1	Sähköiset palvelut, tietovarannot ja rekisterit	37
2.4.2	Tietotekniset peruspalvelut sekä tietotekninen infrastruktuuri ja sitä välittömästi tukevat rakenteet	39

2.5	Osaamisen hallinnan nykytila ja kehittämistarpeet	39
2.5.1	Osaamistarpeet ja nykytila	39
2.6	Keskeisimmät havainnot nykytilasta ja kehittämistarpeista	41
3	ICT-varautumisen kehittäminen	45
3.1	Yleisperiaatteet	45
3.2	ICT-varautumisen vaatimusten kehittäminen.....	49
3.2.1	ICT-varautumisen vaatimusten perusteet	49
3.2.2	ICT-varautumisen vaatimusten kehittämistyö.....	50
3.3	ICT-varautumisen ohjauksen kehittäminen.....	53
3.3.1	Ohjauksen kehittämisen perusteita	53
3.3.2	ICT-varautumisen ohjauksen kehittämistyö.....	54
3.4	ICT-varautumisen tilannetietojen kehittäminen.....	56
3.4.1	ICT-varautumisen tilannetietojen kehittämistyö.....	56
3.5	ICT-varautumisen uhka- ja riskianalyysin kehittäminen	60
3.5.1	Perusteet	60
3.5.2	ICT-varautumisen uhka- ja riskianalyysin kehittämistyö	61
3.6	ICT-varautumisen osaamisen hallinnan kehittäminen	63
3.6.1	Perusteet	63
3.6.2	ICT-varautumisen osaamisen hallinnan kehittämistyö	64
3.7	Palveluverkoston hallinnan ja hyödyntämisen kehittäminen	65
3.7.1	Perusteet	65
3.7.2	Palveluverkoston hallinnan ja hyödyntämisen kehittämistyö	66
4	Hankekartta	69
4.1	ICT-varautumisen kehittämisen organisointi.....	69
4.3	Valtion ICT-varautumishankkeen riskianalyysi	72
4.4	Toteuttamisen välittömät toimenpiteet	73
 LIITE 1:		
	Käsitteet ja määritelmät	75
 LIITE 6:		
	Keskeisimmät ICT-varautumista ohjaavat säädökset ja ohjeet	87

1 ICT-varautuminen

1.1 ICT-varautumisen esitutkimushanke

Valtiovarainministeriö asetti 28.9.2007 tekemällään päätöksellä varautumisen esitutkimushankkeen 1.11.2007 – 30.6.2008 väliseksi ajaksi.

Varautumisen kärkihanke on osa valtionhallinnon kokonaiskehittämistä sekä yhteiskunnan elintärkeiden toimintojen strategian (YETTS), Valtioneuvoston päätöksen huoltovarmuuden tavoitteista ja Valtioneuvoston periaatepäätöksen valtionhallinnon IT-toiminnan kehittämisestä toimeenpanoa. Varautumisen kärkihankkeeseen sisältyy sekä normaaliolojen häiriötilanteisiin että poikkeusoloihin varautuminen.

Valtiovarainministeriö vastaa varautumisen kärkihankkeesta. Esitutkimuksen toteuttamista on tukenut ja ohjannut hallinnonaloilta kootut ohjaus-, valmistelu- ja seurantaryhmä sekä Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI). Työhön liittyi laaja nykytilannetta selvittänyt kysely kaikille hallinnonaloille. Raporttia on työstetty valmisteluryhmän työkokouksissa ja kaikille työryhmille suunnatuissa laajoissa työpajoissa.

Esitutkimuksessa esitettävät kehittämistoimenpiteet kohdennetaan organisaatioiden ja toiminnan muutostapahtumiin, hallinnonalojen ja ValtIT:n hankkeisiin sekä esitettäviin uusiin hankkeisiin.

Kuva 1. ICT-varautumisen hanke

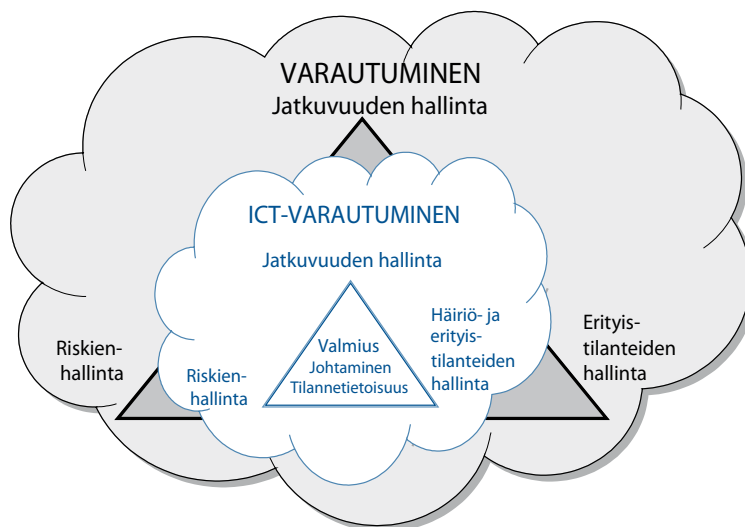


Esitutkimuksen painopiste on valtionhallinnon ICT-toiminnan varautumisessa kaikki hallinnonalat huomioon ottaen. Asettamiskirjeessä esitutkimuksen ulkopuolelle on rajattu Euroopan unionin ja kuntasektorin varautumisen lähempi tarkastelu.

Yhteiskunnan elintärkeiden toimintojen turvaamisen strategian (YETTS) mukaan varautuminen käsittää kaikki ne toimenpiteet, joilla varmistetaan tehävien mahdollisimman häiriötön hoitaminen kaikissa turvallisuustilanteissa. Strategiassa on kuvattu ministeriöiden strategiset tehtävät (50 kappaletta) ja erityistilanteet (60 kappaletta).

ICT-varautuminen on osa organisaation johtamista, yleistä varautumista ja tietohallintoa. Organisaation toiminnan tarpeet häiriötilanteissa ja poikkeusoloissa ohjaavat ICT-varautumisen kehittämistä.

Kuva 2. ICT-varautuminen osana varautumisen kokonaisuutta



Valtionhallinnon keskeiset palvelut ja toiminnot perustuvat sisäisten ja ulkoisten ICT-palvelujen, tietojärjestelmien ja tietoteknisen infrastruktuurin toimivuuteen. Tietojärjestelmäratkaisut ja -palvelut koostuvat sovelluksista, tietovarannoista, tietoverkoista, muusta IT-infrastruktuurista ja niiden oheisjärjestelmistä, tietoturvallisuudesta sekä niihin liittyvästä ylläpidosta, järjestelmähallinnasta ja teknisestä tuesta. Tästä tietohallinnon ja tietotekniikan kokonaisuudesta käytetään lyhennettä ICT (Information and Communication Technology).

Kriittisiä ovat sellaiset ydintoimintoja tukevat ICT-rakenteet, jotka ovat välttämättömiä YETTS:n mukaisen erityistilanteen hoitamisessa ja joiden toimimattomuus estää usean keskeisen organisaation, järjestelmän tai palvelun toiminnan. Kriittisyyttä tarkastellaan yhteiskunnan, valtionhallinnon, hallinnonalan ja viraston näkökulmista.

Keskeisiä ovat sellaiset ICT-rakenteet, joiden toimimattomuus vaikeuttaa merkittävästi organisaation tehtävien suorittamista, aiheuttaa merkittäviä taloudellisia tai muita vahinkoja tai heikentää henkilöstön turvallisuutta.

Raportin keskeisimmät käsitteet ja lyhenteet on esitetty liitteessä 1.

Esitutkimuksessa valtionhallinnon ICT-toimintaa tarkasteltiin kolmessa hallinnon tasossa:

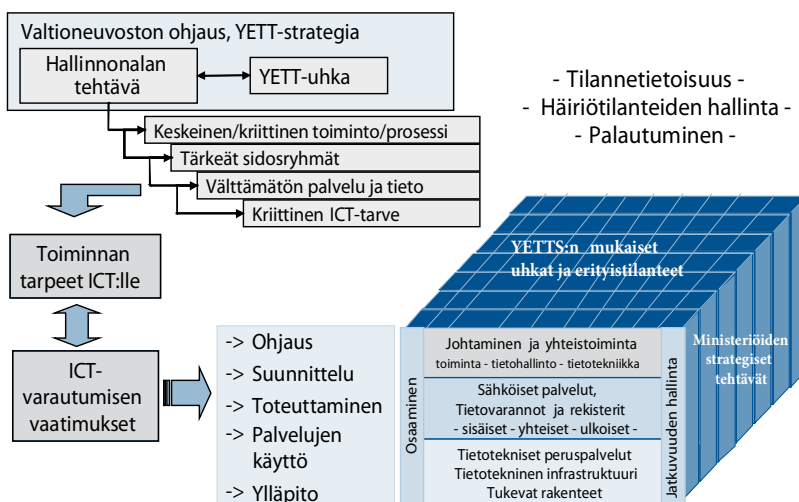
- Valtionhallinnon taso valtioneuvoston sekä valtionhallinnon yhteisten palvelujen ja rakenteiden näkökulmasta
- Hallinnonalojen näkökulma
- Virastojen ja niiden alayksiköiden tarkastelu.

ICT-varautumisen kannalta keskeisiä selvitettäviä kysymyksiä olivat:

- Miten organisaatiossa arvioidaan strategisten tehtävien, kriittisten toimintojen, niiden tarvitsemien tietoteknisten palvelujen ja hallinnonalojen välisten ICT-toimintojen riippuvuuksien kannalta YETTS:n erityistilanteiden hallintakyky?
- Mikä on organisaation toiminnan johdon ja tietohallintojohdon välinen yhteistyö ja vastuunjako määritettäessä organisaation toiminnan tarpeita, ICT-varautumisen vaatimuksia ja tehtäviä sekä varautumisen luomia mahdollisuuksia toiminnalle?
- Miten ICT-varautumista pitäisi toteuttaa hallinnollisessa ja teknisessä rakenteessa ottaen huomioon järjestelmien ja palvelujen elinkaari sekä erityistilanteiden hoitaminen?

Tämä ICT-varautumisen viitekehys on esitetty seuraavassa kuvassa.

Kuva 3. ICT-varautumisen ohjauksen ja toteutuksen viitekehys

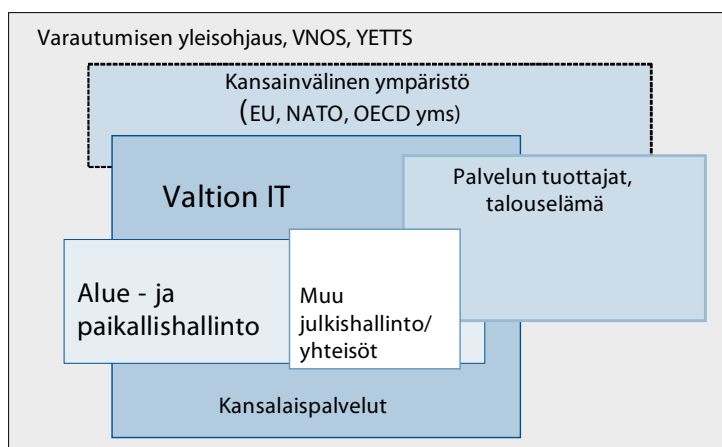


1.2 ICT-varautumisen sidosryhmät ja siihen liittyvät hankkeet

Valtionhallinnon toiminta sisältää useita ulottuvuuksia, joihin liittyy lukuisia eri toimijoita ja niiden välisiä suhteita:

- Suomen ja toisen valtion tai kansainvälisen yhteisön välinen toiminta
- Yksinomaan valtionhallinnon yksiköiden välinen toiminta
- Keskus-, alue- ja paikallishallinnon sekä kuntien välinen toiminta
- Valtionhallinnon sekä valtion ja kuntien liikelaitosten välinen toiminta
- Valtionhallinnon ja kansalaisten tai kansalaisjärjestöjen välinen toiminta

Kuva 4. Valtion ICT-toimintojen varautumisen liittymäalueet



Palvelujen toimivuus häiriötilanteissa ja poikkeusoloissa edellyttää tietotekniikan toiminto- ja vaatimusketjujen katkeamattomuutta. Tässä korostuu kaikkien toimijoiden varautumista tukevien hankkeiden ja kehitystyön koordinoidun yhteistoiminnan merkitys.

Seuraavassa taulukossa on kuvattu keskeisiä valtion ICT-varautumiseen liittyviä hankkeita ja työryhmiä:

Taulukko 1. Valtion ICT-toimintojen varautumiseen liittyviä hankkeita ja työryhmiä

Kohdealue	Vastuu-organisaatiot	Hanke, työryhmä
Valtion ICT-varautumisen yleisohjaus	VNK, VM, PLM, LVM, TEM	Hallitusohjelma, hallituksen strategia-asiakirjat, YETT-strategia, Turvallisuus- ja puolustuspoliittinen selonteko, huoltovarmuuspäätös
Valtion ICT-toiminta	VM, VNK, SM, PLM, LVM, HVK, ValtiJORY, VAHTI, VITKO	Valtion tietoturvan kehittämishankkeet (esim. tietoturvasot-hanke) Yhteinen turvallinen tietoliikennetkaisu-hanke Muut ValtiT-kärkihankkeet, TUVE, VALTU palvelukeskushankkeet, CERT
Kansainvälinen ulottuvuus	VNK, UM, PLM, VM, SM, TEM / HVK, LVM / VIVI, EU, OECD, NATO,	EU-, OECD-, NATO- työryhmät NSA, INFOSEC, CCPC, EPCIP, ECIP, CIWN/ CWCN Turvallinen kansainvälinen tietoliikenne
Alue- ja paikallishallinto	VM, SM, VNK, TEM, JUHTA, KuntaIT	HÄKE, TIVA:t Kriisijohtaminen alue- ja paikallishallinnossa
Talouselämä	TEM, HVK, LVM / VIVI	HV-poolit, Ohjeistus ja määräykset HUOVI, SOPIVA
Muu julkishallinto ja yhdistykset	Eduskunta / KELA, STM	Terveystietojärjestelmien kansalliset tietojärjestelmät (KanTo)
Asiakaspalvelut	LVM, VM, STM, KELA, ValtiIT, KuntaIT	Arjen tietoyhteiskunta / Kriittisen infrastruktuurin käytettävyys, sähköiset asiointipalvelut

1.3 ICT-varautumisen keskeiset osa-alueet

1.3.1 ICT-varautumisen ohjaus

Varautumista ohjataan lainsäädännöllä, normeilla ja ohjeilla, toimilupaehdoilla, teknisillä ohjeilla sekä sopimuksilla. Viranomaisten velvollisuus varautua 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 niin normaaliolojen häiriötilanteissa kuin poikkeusoloissakin.

Ministeriöiden toimialasta ja asioiden jaosta niiden kesken säädetään lailla tai valtioneuvoston asetuksella. Yleiset ministeriöiden toimialasäännökset ja yhteensovittamisvelvollisuudet ovat valtioneuvoston asetuksena annetussa valtioneuvoston ohjesäännössä (VNOS). Ministeriökohtaisissa valtioneuvoston asetuksissa on tarkemmat säännökset ministeriön tehtävistä. Eri alojen lainsäädännössä, laeissa, asetuksissa ja valtioneuvoston periaatepäätöksissä on erityisiä säännöksiä ministeriöiden toimialaan kuuluvista asioista.

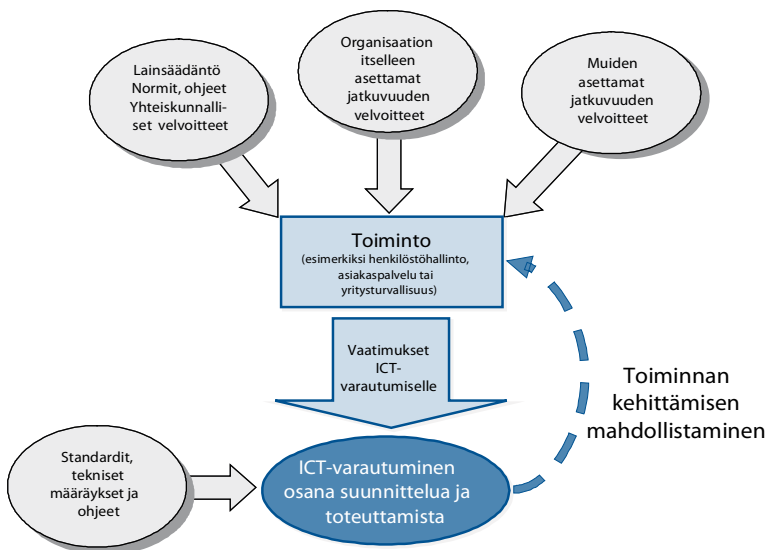
Varautumista johtaa, valvoo ja sovittaa yhteen valtioneuvosto sekä kukin ministeriö hallinnonalallaan. Varautumisen yhteensovittaminen valtioneuvostossa virkamiestasolla tapahtuu viime kädessä ministeriöiden kansliapäällikkö- ja valmiuspäällikkökokouksissa. Valmiuspäällikkökokouksen tehtävänä on sovittaa yhteen ministeriöiden toimet yhteiskuntaa mahdollisesti kohtaavien häiriötilanteiden varalta.

Ministeriössä hallinnonalan varautumisesta vastaa kansliapäällikkö, jonka alaisena toimivaksi valmiuspäälliköksi on usein nimitetty ministeriön ylimpään johtoon kuuluva virkamies. Ministeriössä valmiuspäällikköä avustavat valmiussihteri ja valmiustoimikunta tai sitä vastaava elin. Tietohallintojohto vastaa ICT-varautumisen toteuttamisesta osana tietohallintoa.

Kukin virasto ja laitos vastaavat itse varautumisen toimenpiteistä hallinnonalansa ohjeiden mukaisesti. ICT-varautumisen toteuttamista ohjataan myös virastojen väliseen yhteistoimintaan ja keskinäisiin sopimuksiin perustuen.

Osaamisen ja tiedonkulun varmistamiseksi normaaliolon toimintamalli ei saisi merkittävästi muuttua häiriötilanteiden ja poikkeusolojen johtamisessa. Seuraavassa kuvassa on esitetty ICT-varautumisen ohjausperiaatte.

Kuva 5. ICT-varautumisen ohjausperiaate



Valtion yhteistä IT-toimintaa ohjaa valtiovarainministeriö tukenaan valtion IT-johtoryhmä. KuntaIT –hankkeessa koordinoidaan kuntien välistä yhteistoimintaa kehitettäessä kuntien yhteisiä ICT-ratkaisuja. VAHTI-johtoryhmässä koordinoidaan valtionhallinnon tietoturvallisuuden johtamista ja kehittämistä.

Varautumisen suunnittelua ja toimeenpanoa talouselämässä edistää työ- ja elinkeinoministeriön alaisuudessa toimiva Huoltovarmuusneuvosto (entinen Puolustustaloudellinen Suunnittelukunta). Sen tietoyhteiskuntasektorin kuudessa poolissa edistetään ja koordinoidaan kansallista tietoturvallisuutta sekä tieto- ja viestintäalan yritysten toimintamahdollisuuksia. Tietoyhteiskuntasektorin alueellisena varautumisorganisaationa ovat tietojärjestelmäalan valmius-toimikunnat eli TIVA-toimikunnat.

Kukin ministeriö vastaa lakisääteisin tehtäviinsä liittyen myös talouselämän ohjauksesta. Huoltovarmuuskeskus (HVK) tukee ministeriöitä varautumisen kehittämisessä siltä osin, kuin se koskee elinkeinoelämää, kuten tietoyhteiskuntasektorin, elintarvikehuollon, kuljetuslogistiikan, energiahuollon, terveydenhuollon, rahoitus- ja vakuutussektorin ja kriittisen perusteellisuuden toimintaa. Huoltovarmuuskeskusten, Huoltovarmuusneuvoston ja poolien toiminta painottuu huoltovarmuuskriittisten yritysten varautumisen kehittämisen tukemiseen.

1.3.2 Riskienhallinta

Kiinteänä organisaation varautumisen osana on varautuminen ICT-riskeihin ja niistä aiheutuvien häiriötilanteiden hallintaan. Riskianalyyssissä yhdistyvät uhka-arvio, omien suojattavien toimintojen tarpeet sekä haavoittuvuus- ja vaikuttavuustarkastelut. Riskianalyyssistä voidaan johtaa vaatimukset ICT-varautumiselle sekä määrittää ennalta valmisteltavat suojaustoimenpiteet, toimintatapa häiriötilanteiden hallitsemiseksi sekä toiminnan palauttamiseksi normaaliksi.

Kaikkia toimintaa uhkaavia vakaviakaan riskejä ei voida kokonaan poistaa tai ehkäistä. Vahinkojen pienentämiseksi organisaatio toteuttaa osana toiminnan johtamista jatkuvuussuunnittelua ja luo vaihtoehtoisia menettelytapoja. Jatkuvuussuunnittelun osana poikkeusolojen varalle toteutetaan valmiussuunnitelmia. Käytännön uhkatilanteet poikkeavat todennäköisesti jossain määrin ennakkovalmistelujen perustana olleista malleista. Varautumalla erilaisiin malleihin voidaan kuitenkin todelliseen tilanteeseen reagoida merkittävästi tehokkaammin tekemällä vain pienempiä muutoksia ennalta suunniteltuihin toimenpiteisiin.

1.3.3 Jatkuvuuden hallinta

Jatkuvuuden hallinta on erityisen haasteellista palvelujen koostuessa palvelutuotantoverkostosta. Tällöin erilaisten toimintatapojen, vaatimusmäärittelyjen, rajapintojen sekä epäyhtenäisen henkilöstön ja osaamisen asettamat haasteet ovat merkittäviä. ICT-jatkuvuuden hallinnalla tuetaan toiminnan edellyttämän palvelutason ylläpitämistä häiriötilanteissa. Tärkeää on tarkastella myös erityisesti tietoon ja sen käsittelyyn kohdistuvia käytettävyyss-, luottamuksellisuus-, eheys- ja kiistämättömyystarpeita. Toiminnasta vastaavat osapuolet asettavat ja priorisoivat jatkuvuusvaatimukset ICT-palveluiden tuottaminen tapahtuu myös valtionhallinnossa yhä useammin ulkoistetusti. Korkean käytettävyydestä palveluntarjoajia on markkinoilla vähän ja palvelun hinta nousee usein niin merkittävästi, että joudutaan tyytymään toivottua matalampaan palvelutasoon (klo 9-17).

Priorisoinneista ja työjaosta riippumatta kokonaisvastuu jatkuvuudesta säilyy toiminnasta vastaavalla. Jatkuvuuden hallintaprosessi kattaa toiminnan vaatimukset, riskienhallinnan, ennakoivien toimenpiteiden toteutuksen, häiriötilanteiden hallinnan sekä toiminnan toipumisen toimenpiteet. Ennakoivalla varautumisen kehittämisellä on tavoitteena vähentää häiriön vaikutuksia ja nopeuttaa palautumista.

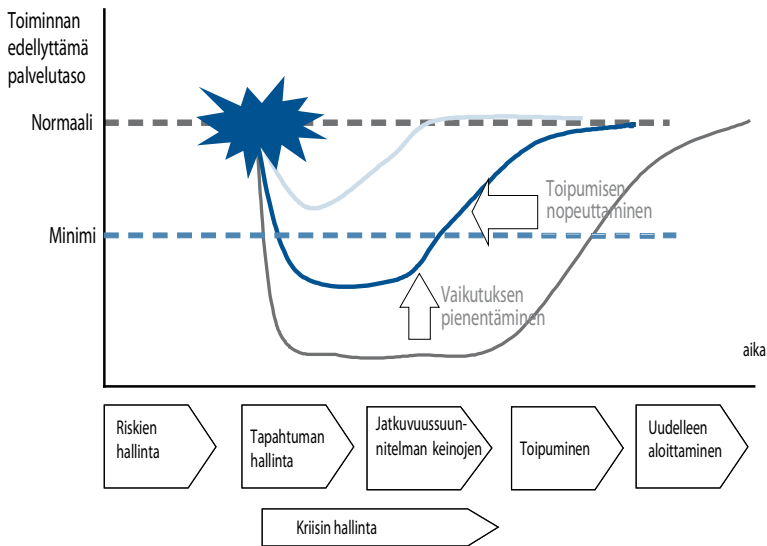
Erityisen tärkeää on suunnitteluvaiheessa määrittää ja palvelujen hankintavaiheessa sopia eri osapuolten varautumiseen liittyvät vastuut ja velvoitteet häiriötilanteissa. Palvelujen hankintaan ja omaan tuottamiseen liittyvissä suunnitelmissa ja sopimuksissa tulee kuvata vaatimukset ja menettelyt palvelujen hallinnalle (ICT-governance):

- ennakoivat palvelutoiminnan riskienhallinnan toimenpiteet
- palvelun käytettävyytasot
- vaihtoehtoiset menettelyt ja toipumistehtävät häiriötilanteissa ja poikkeusoloissa.

Toiminnan jatkuvuuden hallintakykyä organisaatioissa ja palveluverkostoissa arvioidaan jatkuvuussuunnitelmien mukaisten menettelytapojen testauksilla ja harjoituksilla, kuten valmiusharjoituksilla.

Kuvassa 6 alin käyrä esittää vakavan häiriötilanteen vaikutusta palveluun, jossa ei ole huomioitu varautumista. Ylimmällä käyrällä kuvataan kriittistä palvelua, jossa jatkuvuuden hallinnan ja tietoturvan toimenpitein ehkäistään palvelutason laskeminen minimipalvelutason alle ja aikaansadaan nopea palvelutason palautuminen. Keskimmaisella käyrällä kuvataan kustannusoptimoitua palvelua, joka hetkellisesti voi laskea minimitasoon alle. Toiminnan edellyttämä jatkuvuus kyetään kuitenkin takaamaan myös vaikeissa häiriötilanteissa.

Kuva 6. Jatkuvuuden hallinta ICT-varautumisen kannalta



Palvelua tuottavissa organisaatioissa varautumisen ja jatkuvuuden hallinnan suunnittelu sisältää seuraavat asiakokonaisuudet:

- vaatimukset palveluille ja toiminnan toipumiselle
- toiminnalliset prioriteetit palveluille ja riskienhallintapäätökset
- tilannetieto tietoteknisten ratkaisujen nykytilanteesta
- häiriötilanteiden hallinnan prosessien määritykset, resurssit, toimivaltuudet ja päätöksentekomekanismit
- menettelyiden ja vastuiden dokumentointi
- toipumisen toteuttamisen mekanismit ja resurssit
- osaavan, koulutetun ja harjoitelleen henkilöstön.

1.3.4 ICT-varautumisen osaaminen

ICT-palvelujen ja -järjestelmien on mahdollistettava palvelujen jatkuvuus normaaliolon häiriötilanteissa, YETTS –erityistilanteissa ja poikkeusoloissa etukäteen sovitulla käytettävyytasoilla. Tämä edellyttää oikein mitoitettua osaamista kaikilla palveluketjun tasoilla.

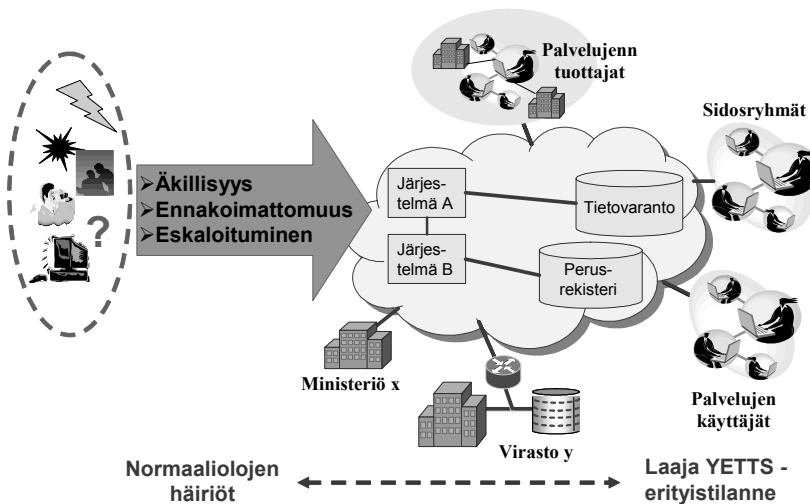
Osaaminen koostuu muun muassa henkilöiden ammattitaidosta, perehtyneisyydestä, organisoinnista ja käytettävyydestä, ohjeistoista, dokumentaatiosta, ongelmanratkaisutiedoista sekä tukijärjestelmien tietämyskannoista.

Varautuminen asettaa vaatimuksia osaamiselle palveluprosessin kaikissa vaiheissa: ohjaus ja johtaminen, suunnittelu, määrittely ja kilpailutus, toteuttaminen, palvelujen käyttö ja ylläpito, häiriötilanteitten hallinta ja palvelun palauttaminen. Kussakin näissä vaiheissa voi toteuttajana olla tulosohtausmielessä eri organisaatio. Osaamista on tarkasteltava koko palveluverkoston muodostamassa kokonaisuudessa.

1.3.5 Tietovarannot ja rekisterit sekä sähköiset palvelut

Hallinnon palvelut ja toiminnot rakentuvat tietovarantojen ja rekisterien varaan. Ne muodostavat perusrakenteen, jonka käytettävyys häiriötilanteissa tulee varmistaa vaihtoehtoisin menetelmin. Sähköiset palvelut muodostuvat organisaatioiden, yritysten ja palvelun käyttäjien välille ja muodostavat toisistaan riippuvaisen verkoston. Osan asioista voi toteuttaa prosessin omistajan sisäinen palveluyksikkö, jokin valtiohallinnon yhteispalveluyksikkö, valtion erillinen yksikkö tai osakeyhtiö (esimerkiksi Hansel Oy, Suomen Erillisverkot Oy, Tietokarhu Oy, CSC-tieteellinen laskenta Oy) tai ulkoinen palveluntuottaja. Verkoston osapuolet voivat sijaita maantieteellisesti missä tahansa.

Kuva 7. Valtion ICT-toiminta on riippuvainen muista toimijoista ja tietotekniikasta



Varautumisen kannalta on keskeistä ymmärtää tämä riippuvuuksien kokonaisuus, jotta vaatimukset ja toimenpiteet kyetään mitoittamaan ja kohdentamaan oikein.

1.3.6 Tietotekniset peruspalvelut, infrastruktuuri ja niitä välittömästi tukevat rakenteet

Tietotekniset peruspalvelut muodostuvat joukosta sähköisten palvelujen toiminnalle välttämättömiä teknisiä palveluja, kuten sähköposti, aika- ja nimi-palvelut, tunnistamispalvelut, reitityspalvelut sekä palomuuuri- ja suodatuspalvelut.

Tietotekninen infrastruktuuri koostuu fyysisistä tietojenkäsittely- ja tiedon-siirtolaitteistoista järjestelmäineen ja palveluineen sekä näiden muodostamista verkostoituneista, kerroksellisista ja keskitetysti hallituista rakenteista. Se vaatii toimiakseen vaatimukset täyttävän ympäristön ja palvelut, kuten sähkö, ilmastointi, jäähdytys, laitetilat, mastorakenteet, turvallisuusrakenteet, ympäristön valvonta- ja hälytysjärjestelmät, varaosat ja laitteet, kuljetukset sekä muut tukipalvelut, kuten vartiointi, siivous ja vesihuolto.

Tietoteknisten peruspalveluja ja infrastruktuuria ylläpitävät sekä organisaation omat osat että ulkoiset kumppanit. Tyypillisesti palvelut tuotetaan verkostomaisena kokonaisuutena. Julkishallinnon hankintoihin sovelletaan JIT-2007 ohjeistusta, joka määrittää palvelun perustason. Mikäli ICT-varautuminen halutaan ottaa korostetummin huomioon, tulee siitä sopia erikseen. Ulkoisten palveluntuottajien toimittamat tietotekniset peruspalvelut on mitoitettu hyvin usein normaaliolojen häiriötilanteisiin ja niitä rajaavat toimitusehtojen force majeure -kohdat. Keskeistä ja haasteellista on palvelukokonaisuuden ja siihen liittyvien vaatimusten kokonaishallinta.

2 Valtion ICT-toiminnan varautumisen nykytila ja tarpeet

2.1 ICT-varautumisen toimintaympäristö

2.1.1 Turvallisuusympäristö ICT-varautumisen kannalta

Valtionhallinnon ja hallinnonalojen toiminnan jatkuvuuden takaaminen edellyttää varautumista normaaliolon ICT-toiminnan häiriötilanteisiin. Normaaliolon ja poikkeusolojen uhkat ovat hyvin samantyyppisiä, mutta niiden kohde, laatu ja vaikutus voivat vaihdella eri turvallisuustilanteissa. Normaaliolon toimintaa ja häiriötilanteita varten toteutetut toimintamallit ja ratkaisut ovat perusta erityistilanteiden hoitamiselle.

Varautumisen kannalta on merkitsevää ICT-toiminnan häiriön aiheuttaja sekä häiriön välittömät ja välilliset vaikutukset. Häiriö voi syntyä luonnonilmiöstä, onnettomuudesta, sähkökatkosta, tietojärjestelmävirheestä, laatuvirheestä, tietoliikennekatkosta, laiteviasta, toiminta- tai käyttövirheestä, tietokatkosta tai väärinymmärryksestä. Häiriö voidaan aiheuttaa myös tahallisesti, kuten tietoverkkoon (ml. laitteisiin, järjestelmiin) kohdistettu vahingonteko, ilkeä tai tietoverkkohyökkäys.

Tietoteknisesti tai fyysisesti heikosti suojattu palvelu (mukaan luettuina järjestelmät, sovellukset, tietoverkot, tieto) voi olla tietojen urkinnan tai muun rikollisen toiminnan kohde; tietojärjestelmän haltuunotonyritys tai palvelun lamauttaminen. Järjestäytyneen tiedustelutoiminnan kohdistamien haittaohjelmien kautta luottamuksellisia tietoja voi joutua asiaankuulumattomille tahoille. Eri uhkatarhojen motiiveja ja vaikutuksia on käsitelty YETTS:n lisäksi muun muassa useissa Huoltovarmuuskeskuksen/puolustustalouden suunnittelukunnan poolien, CERT-FI:n ja tietoturvatyöryhmien raporteissa ja tilastoissa.

Häiriö- ja erityistilanteet voivat vaikuttaa suoraan tietotekniseen kokonaisuuteen tai välillisesti ICT:n tukirakenteisiin (esimerkiksi henkilöstöön). Eri-tyistilanteiden hoitaminen saattaa myös asettaa lisävaatimuksia sähköisille palveluille ja tietojärjestelmille.

YETTS:n uhkia ICT-vaikutuksen näkökulmasta on kuvattu seuraavassa taulukossa.

Taulukko 2. YETTS-uhkamallit ICT-varautumisen kannalta

YETTS uhamalli	ICT-vaikutus
Sähköisen infrastruktuurin häiriintyminen	A
Väestön terveyden ja toimeentulon vakava häiriintyminen	D/C
Taloudellisen toimintakyvyn vakava häiriintyminen	D/C
Suuronnettomuudet ja luonnon aiheuttamat onnettomuudet	B/A
Ympäristöuhkat	C
Terrorismi sekä järjestäytynyt ja muu vakava rikollisuus	B/A
Väestöliikkeisiin liittyvät uhkat	D
Poliittinen, taloudellinen ja sotilaallinen painostus	B
Sotilaallisen voiman käyttö	A

Selite:

A = vaikutus kohdistuu suoraan ICT-infrastruktuuriin

B = vaikutus kohdistuu ICT-infrastruktuurille välttämättömiin tukirakenteisiin ja heikentävät ICT:n käytettävyyttä

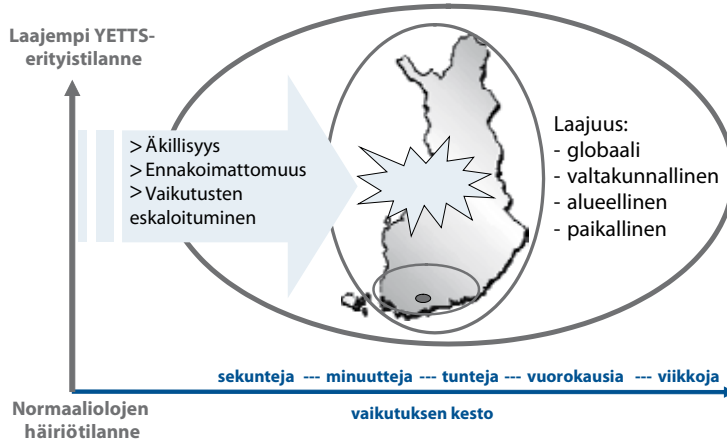
C = Erityistilanteen hoitaminen aiheuttaa merkittäviä erityisvaatimuksia valtiohallinnon ICT:n toiminnalle ja käytettävyydelle

D = Ei merkittäviä häiriöitä ICT:lle tai tilanteen hoitaminen asettaa erityisvaatimuksia hallinnonalan sisäiselle ICT:lle

Liitteessä 2 on kuvattu YETTS-erityistilanteet varautumisen näkökulmasta edellä mainitun luokittelun mukaisesti.

Turvallisuustilanteen tarkasteluun vaikuttavat tilanteen todennäköisyys sekä sen vaikutukset, kuten kesto, laajuus ja aiheutuvat taloudelliset tai henkilöstövahingot. Suuri merkitys on tietoteknisen infrastruktuurin tilanteella ennen uhan kohdistumista. Tällaisia tekijöitä ovat muun muassa olemassa olevat haavoittuvuudet, toiminnan korvattavuus, infrastruktuurin ja ylläpitoresurssien käytettävyys ja käyttöaste, muu tapahtumaympäristö Suomessa ja tietotekniikkatoimittajille oleellisessa kansainvälisessä ympäristössä.

Kuva 8. Esimerkki turvallisuustilanteen ulottuvuuksista



Tämän päivän tietotekniselle toimintaympäristölle on tyypillistä uhkien äkillinen realisoituminen sekä niiden vaikutusten nopea ja ennalta arvaamaton laajentuminen. Tilanteiden ennakointiin tulee varautua toteuttamalla estäviä, paljastavia sekä eskaloitumista rajoittavia ratkaisuja. Häiriöiden vaikutusta rajoittavat toimenpiteet on kyettävä käynnistämään nopeasti. Tähän vaikuttaa keskeisesti päätöksentekokyky ja -rakenne, tilannetietoisuus sekä ennakkovarauminen, dokumentaatio ja ohjeistus.

Organisaation tehtävien ja toiminnan analysointi suhteessa erityistilanteisiin tuottaa vaatimukset ICT-varautumiselle. Varautumisen perustaksi on laadittava uhka-arvio. Perusteita uhka-arvioon saadaan uhkaympäristön tutkimuksesta, jatkuvasta tilanteen seuraamisesta ja sen tuottamasta tilannekuvasta.

2.1.2 Arvio tietoyhteiskuntakehityksestä varautumisen näkökulmasta

Ympäröivän yhteiskunnan, valtionhallinnon sekä uhkaympäristön kehitys vaikuttavat varautumistarpeisiin. ICT-varautumisen näkökulmasta keskeisimmät trendit ovat:

Taulukko 3. Arvio yhteiskunnan kehittymisestä ICT-varautumisen kannalta

Kehityslinja	Kehityspiirteitä
Palvelut, prosessit, ICT-tuotantoketjut ja järjestelmät automatisoituvat, monimutkaistuvat, integroituvat ja verkottuvat voimakkaasti. Tietojen yhteiskäyttö laajenee ja automatisoituu.	- Internetin merkitys myös valtionhallinnossa kasvaa merkittävästi. - Toiminnan tehostaminen tietotekniikan avulla kasvaa – ja myös riippuvuus - Toimittajahallinta sekä resurssien kohdennus ja priorisointi häiriötilanteessa vaikeutuvat. - Vaikeasti ennakoitavia, hallitsemattomia ja laajalle heijastuvia haavoittuvuuksia syntyy yhä enemmän. - Syntyy voimakkaita riippuvuussuhteita, kuten sähkön tuotannon riippuvuus tietoliikenteestä ja päinvastoin sekä organisaatioiden väliset riippuvuudet. - Järjestelmäkokonaisuuksien testaaminen ja auditointi vaikeutuvat. - Osaaminen ei kehity monimutkaistuvien ympäristöjen tahdissa.
Palvelukokonaisuudet hankitaan usean toimittajan palveluverkoston	- Vain pieni osa kyetään hankkimaan omalta sisäiseltä palveluntoimittajalta, joihin tulee kohdistaa samat palveluvaatimukset kuin ulkoisiin toimittajiin. - ICT-palvelutoimittajien alihankinta lisääntyy, myös Suomen ulkopuolelta. - Vaatimusten määrittely ja hallinta sekä hankinta edellyttävät yhä erikoistuvampaa osaamista kaikilla tasoilla. - Verkoston rakentaminen edellyttää toiminta- ja laatu-kriteerejä, jotta keskinäinen luottamus, yhteensopivuus ja tekninen toimivuus voidaan taata.
ICT-palveluketjujen omistussuhteissa ja sopimusvastuissa tulee tapahtumaan jatkuvasti muutoksia	- Osaa kaupallisista palveluista ei voida toteuttaa Suomessa. - Osa perinteisesti Suomessa tuotetuista palveluista siirtyy ulkomaille, jolloin Suomen sääännöllistä kontrollia voidaan saada vain osaan tuotantoketjuista. - Palvelutuotanto, laitteistotoimitus ja komponenttien valmistus globalisoituvat sekä toimittajakentän muutokset yleistyvät. Samalla henkilöstöjohtamisen haasteet lisääntyvät. - Ohjauksessa taloudelliset ja sopimukselliset menetelmät korostuvat. - Sopimusten kattavuuden ja laadun sekä niihin kuvattujen toimintamallien dokumentoinnin merkitys kasvaa.
Uhkaympäristö muuttuu yllätyksellisemmäksi, ammattimaisemmaksi ja vakavammaksi	- Ympäristökatastrofen, suuronnettomuuksien ja laajojen tietoteknisten haavoittuvuuksien monimuotoisuus ja kasaantumisen todennäköisyys kasvavat. - Verkkohyökkäyksistä ja haittaohjelmien kehittämisestä on muodostunut ammattimaista ja hyvin organisoitua palvelutoimintaa. - Kohdistettujen haittaohjelmien käyttö tiedustelutoiminnassa lisääntyy.

Kansainvälisen yhteistoiminnan ja ohjauksen merkitys kasvaa voimakkaasti	• Syntyy uudenlaisia tietohallintoa ja tietotekniikkaa koskevia tarpeita, mahdollisuuksia ja haasteita. • Lisääntyvät tarpeet yhteisiin käytäntöihin ja ohjaukseen • Kansainvälinen säädös- ja standardiohjaus kasvavat (EU, OECD, NATO).
--	---

2.2 Valtion ICT-varautumisen ohjaus ja suunnittelu-mekanismit

2.2.1 Valtiotason ohjaus

Valmiuslaki on keskeisin varautumista ohjaava säädös. Se määrittää yleisen varautumisvelvoitteen:

”Valtioneuvoston, valtion hallintoviranomaisten, valtion liikelaitosten ja muiden valtion viranomaisten sekä kuntien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muin toimenpitein varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa.”

Varautumista säädellään yli 40 laissa tai asetuksessa. Varautumista koskeva säädäntö määrittää selkeästi valtionhallinnon tasoiset ja hallinnonalakohtaiset vastuut sekä eräitä tarpeellisia erityiskysymyksiä, kuten henkilötietojen hallintaa. Säädännössä on tämän lisäksi hajanaisesti asetettu 27 toiminnolle varautumisvelvoitteita. Viranomaismääräyksiä on annettu kuusi kappaletta. ICT-varautumista ei käsitellä säädännössä eikä viranomaisten ohjeistuksissa erilliskysymyksenä. Pääosin säädännössä määrätään varautumisvelvoitteita tai tehtäviä erilaisille toiminnoille tai organisaatioille.

Valmiuslain uudistamisesta on tehty hallituksen esitys eduskunnalle. Uuden valmiuslain mukaan poikkeusoloja olisivat

- ensinnäkin Suomeen kohdistuva aseellinen tai siihen vakavuudeltaan rinnastettava hyökkäys ja sen välitön jälkitila
- toiseksi Suomeen kohdistuva huomattava aseellisen tai siihen vakavuudeltaan rinnastettavan hyökkäyksen uhka, jonka vaikutusten torjuminen vaatii valmiuslain mukaisten toimivaltuuksien välitöntä käyttöönottamista
- kolmanneksi väestön toimeentuloon tai maan talouselämän perusteisiin kohdistuva erityisen vakava tapahtuma tai uhka, jonka seurauksena yhteiskunnan toimivuudelle välttämättömät toiminnot olennaisesti vaarantuvat

- sekä neljänneksi erityisen vakava suuronnettomuus, tällaisen suuronnettomuuden välitön jälkitila ja vaikutuksiltaan erittäin vakavaa suuronnettomuutta vastaava hyvin laajalle levinnyt vaarallinen tartuntatauti.

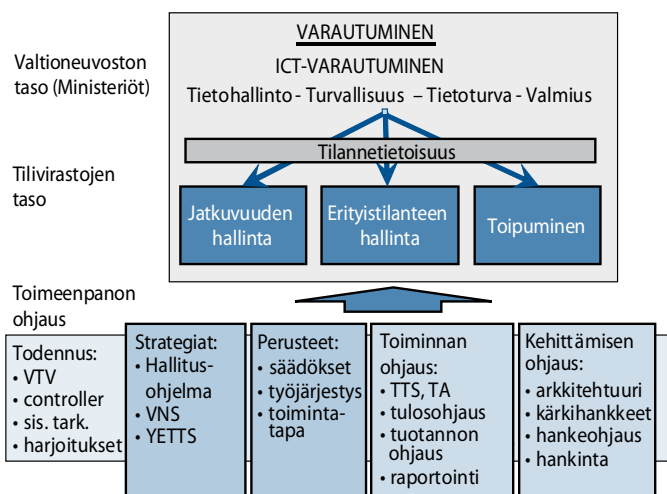
Valmiuslain soveltamisen aloittamista koskevaa päätöksentekomenettelyä ehdotetaan muutettavaksi niin, että valmiuslain mukaisten toimivaltuuksien käyttöönotosta säädettäisiin valtioneuvoston asetuksella eikä tasavallan presidentin asetuksella. Ennen tämän käyttöönottoasetuksen antamista on valtioneuvoston, yhteistoiminnassa tasavallan presidentin kanssa, todettava maassa vallitsevan poikkeusolot. Eduskunta päättäisi viime kädessä käyttöönottoasetuksen voimassaolosta ja voimassaoloajasta. Valmiuslain toimivaltuussäännösten soveltamista täydentävien valtioneuvoston asetusten jälkitarkastuksesta eduskunnassa ehdotetaan luovuttavan. (HE 3/2008)

Myös Huoltovarmuuskeskuksen toiminnan kehittäminen on käynnissä. LVM:n johdolla valmistellaan erityistilanteiden ja poikkeusolojen lainsäädännön kehittämistä.

Varautumisen kokonaisohjaus on määritetty valtioneuvoston kanslian vastuulle ja kullekin ministeriölle oman hallinnonalansa osalta. Yhteiskunnan ICT-varautumisen kehittämisen ja toteuttamisen ohjaus on jakautunut usealle hallinnonalalle. Varautumisen koordinointi on erittäin haastavaa hallinnon toimintojen ja tietotekniikan keskinäisten riippuvuuksien vuoksi. Tällä hetkellä valtionhallinnossa toteuttaminen on tasoltaan vaihtelevaa. Ohjaus ei valtionhallinnossa toteudu yhtenäisesti ja kattavasti valtioneuvoston tasolta toteuttaviin virastoihin asti.

Seuraavassa kuvassa on esitetty varautumisen toteutuksen ohjauksen osalualueita.

Kuva 9. ICT-varautumisen toimeenpanon ohjaus



Kokonaisuutena varautuminen on merkittävän laaja kokonaisuus, jossa ICT-toiminta on luonnollisesti keskeinen tekijä, mutta ei itseisarvo sinänsä. Valtioneuvoston periaatepäätös valtion IT-toiminnan kehittämisestä ja sitä toteuttavat kärkihankkeet huomioivat varautumisen vain vähäisesti. VAHTI-ohjeistossa on huomioitu tietoturvallisuuteen liittyen myös varautumisen näkökulmia. Esille tulleet vaatimukset on tarkoituksenmukaista sisällyttää selkeästi erottuvina elementteinä kaikkiin kärkihankkeisiin ja muihin merkittäviin poikkihallinnollisiin hankkeisiin.

Taulukossa on esitetty ValtIT-kärkihankkeita varautumisen näkökulmasta.

Taulukko 4. ValtIT-kärkihankkeet ICT-varautumisen kannalta

Hankekokonaisuus / hanke	Merkitys varautumiselle	Varautumisen huomioiminen
Sähköinen asiointi (asiointi, palvelualusta, tunnistaminen)	Keskeinen sähköisten palveluiden perusta, toimittava kaikissa tilanteissa	Huomioitu normaali jatkuvuus ja tietoturva. Varautumisen näkökulma tarkennetaan
Yhteentoimivuus (arkkitehtuurit, integraatio ja perustietovarannot)	Keskeinen varautumisen toteutustapaa ohjaava elementti. Edellytys verkostoituneelle toiminnalle.	Huomioitu normaali jatkuvuus ja tietoturva. Varautumisen näkökulma tarkennetaan
Yhteiset tietojärjestelmät (VIRTU, VALDO, KIEKU, talousohjaus)	Poikkihallinnollisia järjestelmiä, varautuminen huomioidava alusta lähtien.	Varautuminen otettu osittain huomioon. Täydennetään.
ICT-infrastruktuuri (tietoliikennematkaisu, käyttöpalvelut)	Valtionhallinnon yhteisissä infrastruktuuripalveluissa on taattava jatkuvuus erityistilanteissa	Suunnitteluvaiheessa – varautuminen tullaan ottamaan huomioon
Tietoturvallisuuden osa-alueet • tietoturvatasot • auditointi, 24/7 • VAHTI	Tehokkaita keinoja toteuttaa varautuminen	Varautuminen on integroitu tiiviisti
Valtion IT-palvelukeskus	Yhteisten palvelujen varautumisen koordinoija ja toteuttaja	Suunnitteluvaiheessa – varautuminen tullaan ottamaan huomioon

ICT-varautumisen ohjaus hallinnonaloilla on epäyhtenäistä ja osittain puutteellista. Tämä johtaa vaikeuksiin toteuttaa kustannustehokkaasti laajan verkottuneen ympäristön varautumista häiriötilanteisiin. Tavoitteiden saavuttaminen edellyttää hallinnonalojen lisäresursointia.

2.2.2 ICT-varautumisen ohjaus hallinnonaloilla

Hallinnonalat ovat sisällyttäneet ICT-varautumisen ohjeistuksen osana varautumisen kokonaisohjausta työjärjestyksiin ja strategia-asiakirjoihin seuraavasti.

Taulukko 5. ICT-varautumisen huomioiminen ministeriöiden ohjauksessa

Hallinnon-ala	Ministeriön työjärjestys	Henkilön tehtäväkuvaus	Strategia-asiakirjat	ICT-varautumisen ohjaus	ICT-varautumisen tulosohjauksessa	Onko strategioissa ja ohjeissa asetettu selkeitä vaatimuksia ICT-varautumiselle
LVM	(x)	X	(x)	(x)	(x)	ei selkeitä vaatimuksia
MMM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
OM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
OPM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
PLM	(x)	X	X	(x)	(x)	ei selkeitä vaatimuksia
SM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
STM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
TEM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
UM	(x)	X	(x)	(x)	(x)	ei selkeitä vaatimuksia
VM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia
VNK	(x)	X	(x)	(x)	(x)	ei selkeitä vaatimuksia
YM	(x)	(x)	(x)	(x)	(x)	ei selkeitä vaatimuksia

Selite: X=tehty (x) = osittain tehty S = suunnitella --- = ei ole tehty

Jokaiselle hallinnonalalle on määrätty varautumista koordinoiva valmiuspäällikkö sekä valmiussihteri. Valmiuspäällikkökokouksen sihteeristönä toimii Turvallisuus- ja puolustusasiain komitean sihteeristö. Valmiuspäällikkökokouksella on havaintojen mukaan ollut suuri merkitys hallinnonalojen varautumisen koordinoinnissa. Valmiuspäälliköiden ja -sihteerien sekä tietoturva-, turvallisuus- ja tietohallintojohdon rooleja ja vastuita ICT-varautumisen johtamisessa tulisi selkeyttää.

Ministeriöiden tasolla nähdään yleisesti varautumista ohjaava säädäntö riittävänä. Viranomaisten varautumista koskeva tarkempi ohjeistus on hallinnonaloittain annettua. Pääosin ICT-varautumista ohjaa hallinnonalojen tietohallintostrategioiden yleiset vaatimukset. Varsinaisia vaatimuksia ei strategioissa juurikaan ole. Virastot toteuttavat varautumista säädännön, yleisten ohjausasiakirjojen sekä omien tarpeittensa ja näkemystensä mukaisesti. Hallinnonalojen ohjaus nähdään riittämättömäksi. Erityisesti virastojen tasolla on tuotu esille ohjauksen ja ohjeistuksen kehittämisen tarve.

2.2.3 Sidosryhmäohjaus ja yhteistoiminta

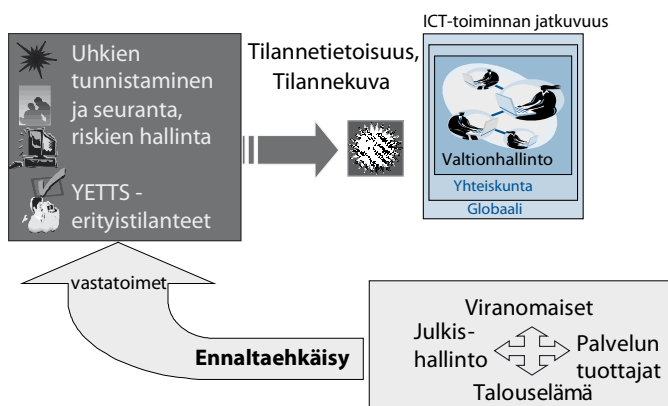
Tietotekniikka ja tietohallinto ovat tärkeässä asemassa tukemassa kaikkea valtionhallinnon keskeistä toimintaa. Valtionhallinnon toiminta on voimakkaasti verkottunutta ulkoisten sidosryhmien kanssa. Myös tietotekninen infrastruktuuri ja palvelut verkottuvat ja rakentuvat muun yhteiskunnan palvelujen varaan.

Esitutkimuksesta rajattiin pois kuntiin ja kansainvälisiin osapuoliin liittyvät tarkastelut. Työn aikana kävi selville, että valtionhallinnon keskeisimpien palvelujen varautuminen edellyttää ICT-varautumisen esitutkimuksen täydentämistä kattamaan myös keskeisimmät kuntasektorin toimialueet ja valtionhallinnon kansainvälisen yhteistyön. Tämän tarvetta korostavat myös käynnissä olevat valtion tuottavuusohjelma sekä julkishallinnon ja tilivirastojen muutokset: julkishallinnon IT-ohjauksen järjestelyt, korkeakouluverkoston uudistaminen, valtionhallinnon toimintojen alueellistaminen ja ulkoistaminen.

Valtionhallinnon palvelut ovat vahvasti riippuvaisia ulkoisista palvelutoimittajista ja näiden tuotantorakenteista sekä palvelutuottajien välisistä verkostoista, alihankintaketjuista ja sopimussuhteista. Nykyinen valtionhallinnon ICT-varautuminen ei ota riittävästi huomioon palveluntuottajien ja muiden sidosryhmien merkitystä eri turvallisuustilanteissa tietotekniset palvelut ovat riippuvaisia. Tämän vuoksi tulisi kehittää menetelmiä ja toimintamuotoja tietojärjestelmien, organisaatioverkostojen ja toimitusketjujen muodostaman kokonaisuuden ymmärtämiseen, hallintaan ja varmistamiseen.

Yritysten varautumisen lähtökohtana ovat liiketoiminnalliset perusteet, sopimukset sekä näihin liittyvä riskienhallinta. Vakavissa erityistilanteissa palvelutoimittajat joutuvat priorisoimaan erityisesti jatkuvuuteen ja palautumiseen liittyviä käyttäjien tarpeita voimakkaasti. Priorisoinnin perustana ovat pääsääntöisesti sopimusehdot ja niistä aiheutuvat sanktiot. Viranomaiset eivät voi tällä hetkellä ohjata priorisointia ilman poikkeusolojen säädännön valtuuksia.

Kuva 11. Sidosryhmien merkitys valtionhallinnon ICT-jatkuvuudelle

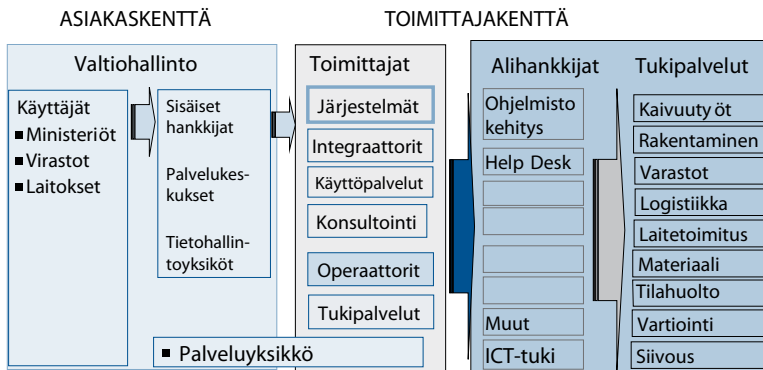


Omistajamuutokset, globalisoituminen sekä EU:n vapaa työvoiman liikkuvuus asettavat erityisiä vaatimuksia sopimusmenettelyille ja yritysverkoston hallinnalle. Voimakkaasti normaalista palvelutuotannosta ja sopimusmenettelyistä poikkeavia kansallisia asiakas- tai toimintokohtaisia vaatimuksia on vaikea asettaa ja hallita.

Palveluketjuissa on useimmiten myös ulkomaisia yrityksiä ja ulkomailla tapahtuvaa palveluntuotantoa. Tällöin varautumisen ohjaaminen kansallisin normein on vaikeaa. Mikäli kriittisten toimintojen jatkuvuus vakavissa turvallisuustilanteissa edellyttää kansallista ohjausta ja osaamista, tulisi palveluketjujen keskeisten osien ja toimintojen olla kattavasti Suomen säädännön ja käytäntöjen piirissä ja useimmiten myös Suomessa toteutettuja. Keskeisten toimintojen ulkomailla toteutettavat palvelut on voitava tarvittaessa siirtää Suomeen olemassa olevia resursseja ja osaamista vahvistamalla.

Palveluiden tuottamisen ja vastuun tulee perustua riskianalyyysiin. Erityisen merkityksellistä tämä on palvelukokonaisuuksia ulkoistettaessa sekä tuotettaessa palveluja Suomen ulkopuolella. Haasteellista on todentaa palveluketjun todellista erityistilanteiden palvelulaatua ja toimituskykyä. Palveluketjuja on esitetty seuraavassa kuvassa.

Kuva 12. Esimerkki palveluketjun rakenteesta



Varautuminen tulee ottaa huomioon kaikissa sopimusmenettelyissä, erityisesti hankinnoissa. Tällä hetkellä palveluketjujen riippuvuudet toimittajaverkostoista, näiden alihankkijoista ja tukipalvelujen toimittajista on tunnistettu puutteellisesti. ICT-varautumista on otettu varsin vaihtelevasti ja rajallisesti huomioon hankintamenettelyissä, palvelusopimuksissa sekä verkostojen muodostamisessa ja hallinnassa. Nykyisellään eri viranomaiset asettavat sopimuksissa kukin omista tarpeista lähteviä ja toisistaan poikkeavia vaatimuksia palvelutoimittajille. Tämä luo epäyhtenäisen ympäristön, aiheuttaa kustannusten

kasvua ja vaikeuttaa erityistilanteissa resurssien ja palvelujen kokonaisuuden kannalta tarkoituksenmukaista kohdentamista. Palvelujentarjoajille ei ole asetettu riittäviä vaatimuksia varautumiseen liittyvien sopimusvelvoitteiden siirtämisestä alihankkijaverkostoonsa. Myös sopimusvelvoitteiden valvonta ja auditointi on puutteellista niin valtionhallinnossa kuin toimittajakentässä.

Varautumisen kannalta on tarkoituksenmukaista luoda yhtenäiset vaatimukset ja sopimusmenettelyt, jotka koskevat sekä sisäisiä että ulkoisia palvelutuottajia. Vaatimukset, sopimukset, tarkastukset ja auditoinnit sekä näiden ylläpito olisi tarkoituksenmukaista toteuttaa yhdenmukaisesti ja tarvittavin osin keskitetysti. Varautumisen kannalta nähdään tarpeelliseksi kehittää Huoltovarmuuskeskuksen roolia talouselämän ICT-varautumiseen liittyvässä ohjauksessa. Tästä on esimerkkinä käynnissä oleva ”Sopimuksiin perustuva varautuminen” -projekti (SOPIVA). Tärkeää on myös varautumisen sisällyttäminen keskitettyihin hankintoihin sekä Hanselin rooli näihin liittyen.

2.2.4 ICT-varautumisen tarkastus ja auditointi

Varautumisen toteutumisen kannalta keskeistä on varmistua, että suunnitellut ja toteutetut toiminnot ja palvelut vastaavat asetettuja vaatimuksia ja solmittuja sopimuksia. Keskeisinä elementteinä tässä ovat controller-toiminta, sisäinen tarkastus sekä kokonaisuuden kaikkiin osa-alueisiin kohdistuva auditoinnit. Tarkastustoiminnan ja auditoinnin on kohdistuttava sekä sisäisiin että ulkoisiin toimintoihin ja ulotuttava syvälle palvelua tuottavaan palveluketjuun tai -verkostoon. Laadusta ja toimivuudesta on kyettävä varmistumaan ennalta. Tätä vaikeuttaa se, että kaikkia mahdollisia riskitekijöitä ja uhkatilanteita ei tunneta.

Yleisenä havaintona voidaan todeta, että ICT-varautumisen tarkastus, controller-toiminta ja auditointi on valtionhallinnossa puutteellista. Tämä johtuu pääsääntöisesti puuttuvista vaatimuksista, ICT-varautumisen puuttumisesta normaaleista laatuikäytännöistä sekä auditointiresurssien vähäisyydestä.

2.3 Riskienhallinta ja vaatimusten muodostaminen

2.3.1 ICT-varautumisen tilannetietoisuus

Keskeistä varautumisessa on tilannetietoisuus ja kuhunkin turvallisuustilanteeseen liittyvä ICT-tilannekuva. Erityistilanteiden johtamisen edellyttämää yhtenäistä tietotekniikan tilannekuvaa kyetään muodostamaan vain hallinnonaloittain rajoitetuilta osin. Viestintäviraston alaisuudessa toimiva CERT-FI muodostaa koko yhteiskuntaa koskevaa tietoteknistä haavoittuvuus- ja uhka-

tilannekuvaa, jossa keskeisinä osina ovat viestintä- ja tietoliikennepalvelujen tilanne, haittaohjelmien ja tietoturvaloukkausten tilastot sekä haavoittuvuudet. Puutteena on tietojärjestelmien ja niiden palvelujen tilannekuvan kokoaminen. CERT-FI:n roolia ja resursointia erityisesti julkishallinnolle suunnatun erikoistuneen ICT-tilannekuvan ja uhkakuvan muodostamisessa tulisi voimakkaasti kehittää.

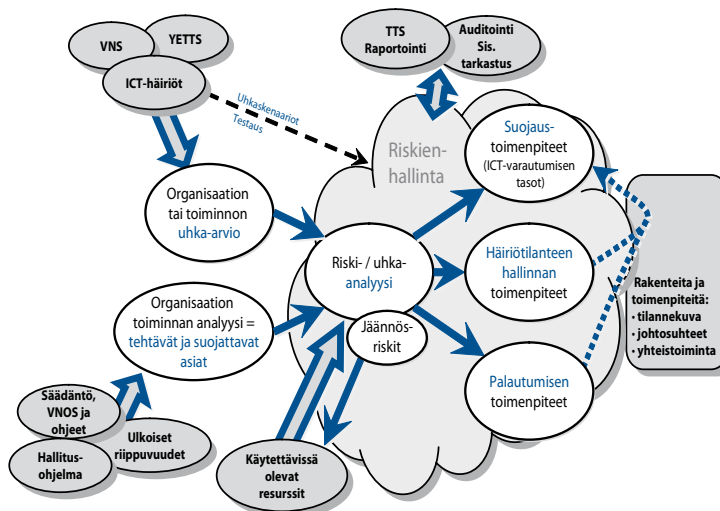
Varautumisen kehittämisen tarvitsema tilannekuva muodostuu hallinnonalojen antamista tiedoista. VALHA- ja TIETO-harjoitukset ovat osoittaneet, että tilannekuva hajautuu hyvin monien eri toimijoiden kesken eikä muodosta yhtenäistä kokonaisuutta, jolle olisi asetettu käyttötärpeiden edellyttämät vaatimukset. Tilannekuvan muodostamista ei myöskään ole organisoitu yhden toimijan vastuulle. Tilannekuvan keräämisen mahdollistamaa rakennetta, kuten yhdenmukaista puitetta ja kirjauskäytäntöä tai tulosraportointikehystä, ei valtionhallinnossa ole.

2.3.2 Uhka-arvio ja riskianalyysi

YETT-strategian toteuttaminen edellyttää valtiohallinnon eri tasoilla yhtenäisiä uhka-arvion perusteita, uhka-arvioita, riskienhallinnan menetelmiä sekä systemaattista prosessia näiden hallintaan. Yhtenäisen uhka-arvion tulee perustua hallitusohjelmaan, hallituksen strategia-asiakirjaan (HSA), valtioneuvoston selontekoon turvallisuus- ja puolustuspolitiikasta, YETT-strategiaan sekä muihin hallinnonaloja ohjaaviin valtioneuvoston periaatepäätöksiin.

Riskienhallinnan kokonaisuutta havainnollistetaan seuraavassa kuvassa.

Kuva 13. Riskien hallinta ICT-varautumisen kannalta



ICT-toiminnan riskienhallintaa ei ole yhtenäistetty valtionhallinnossa. Kytkeä YETT-strategian ja riskienhallinnan välillä on useimmiten puutteellista. Riskianalyysin tekemiseen tarvittavat perusteet siirtyvät usein puutteellisesti ministeriöistä toteuttavien virastojen tasalle. Ongelmana on strategia-asiakirjoissa tuotetun uhka-arvion tarkentaminen sekä yhtenäisten perusteiden jakaminen hallinnonalojen ja virastojen uhka-arvioiden laatimiseksi. Tästä johtuen riskienhallinnan arviot ja ehkäisevät toimenpiteet eivät ole verrattavissa toisiinsa. Poikkihallinnollisten palveluiden muodostaman verkoston riskienhallinta on myös puutteellista. VAHTI-työssä tuotettuja uhka- ja riskienhallintamenetelmiä tulisi voimakkaasti hyödyntää.

Hallinnonaloilla toteutettava uhka-arviointi ja riskienhallinta tulisi yhtenäistää ja integroida osaksi toiminnan ja talouden suunnitteluprosessia sekä tulosohejausta. Riskien ja jatkuvuuden hallintaa käyttäen voidaan kustannustehokkaasti mahdollistaa valtionhallinnon palvelujen jatkuminen ja palautuminen myös YETTS-erityistilanteissa.

2.3.3 Kriittisten toimintojen edellyttämän ICT-tarpeen tunnistaminen

Kokonaisuuden sekä riippuvuuksien tunnistaminen ja arvioiminen luovat perustan vaatimusten asettamiselle, varautumistoimenpiteiden ja rajallisten resurssien suuntaamiselle sekä vaikuttavuuden seuraamiselle. Kaikilta osin valtionhallinnossa ei tunnisteta selkeästi tehtävien toteuttamiselle kriittisiä prosesseja ja näiden riippuvuuksia sidosryhmistä.

Palvelujen jatkuvuus verkostossa on eri turvallisuustilanteissa taattava asetettujen vaatimusten mukaisesti. Vaatimuksia joudutaan asettamaan erittäin usealle toiminnalliselle ja tekniselle osalle kokonaisuudessa.

Toiminnan ja sen prosesseista lähtevien vaatimusten asettaminen ICT-palveluille on myös hajanaista. Merkittävässä osassa hallinnonaloja ja virastoja ei ole toimivaa mekanismia, jolla toiminnan tarpeista tunnistetaan kriittiset tietotekniset ratkaisut ja järjestelmät sekä tästä muodostetaan vaatimukset varautumiselle. Monessa tapauksessa tietohallinto asettaa itselleen vaatimukset. Ne eivät välttämättä ole synkronissa toiminnan tarpeiden kanssa YETTS-erityistilanteiden näkökulmasta.

Kriittisen toiminnan edellyttämän tietotekniikan jäädessä määrittämättä, häiriötilanteiden hoitamisen edellyttämiä resursseja ei ole osoitettu. Vaatimusten puuttuessa ICT-varautumiseen käytettyjen resurssien käytön optimointi on vaikeaa. Tämä on johtanut kokonaisuuden kannalta jopa epätarkoituksenmukaisiin investointeihin.

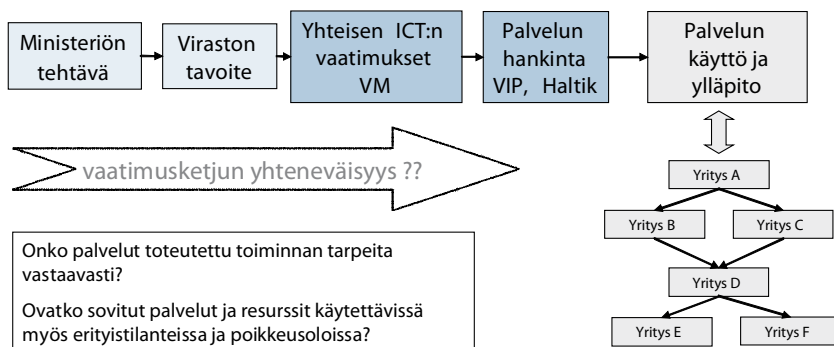
2.3.4 ICT-varautumisen vaatimusten asettaminen

Kriittisimmät ja keskeisimmät tietotekniikan varassa olevat yhteiskunnan toiminnot tulee tunnistaa ja niihin liittyvät tietojärjestelmäratkaisut ja -palvelut tulee varmistaa erilaisia vakavia häiriöitä ja poikkeusoloja kestäväillä järjestelyillä. Valtionhallinnon kriittisten toimintojen jatkuvuusvaatimukset edellyttävät toiminnallisten ja teknisten vaatimusten asettamista tietotekniikalle ja tietohallinnolle häiriö- ja erityistilanteiden sekä poikkeusolojen varalle. Varautuminen on otettu vain vähäisesti huomioon valtionhallinnon ICT-toimintaa ohjaavissa teknisissä arkkitehtuureissa, spesifikaatioissa, laatuja järjestelmissä, hankeohjauksella, sopimusmalleissa sekä toteutus- ja auditointiohjeistoissa. Jonkin verran teknisiä vaatimuksia asettavat yleiset standardit, hyvät käytännöt, Viestintäviraston tekniset määräykset sekä valtionhallinnon suositukset.

Tällä hetkellä vaatimusten asettaminen erityisesti poikkihallinnollisissa ja valtionhallinnon ulkopuolelle ulottuvissa prosesseissa on erittäin haastavaa. Toiminnot ja niiden prosessien jatkuvuusvaatimukset ovat keskeisessä osassa määrittäessä niitä tukevalle tietotekniikalle varautumisvaatimuksia. Vaatimusten tulee kattaa koko verkostoitunut toimintaprosessi. Valtiohallinnossa ei aseteta näitä vaatimuksia yhtenäisesti.

Haasteellista on varmistaa vaatimusten periytyminen hallinnonalan sisällä ja ulottaminen katkeamattomana palveluja tuottaviin sisäisiin ja ulkoisiin toimijoihin. Tällä hetkellä vaatimusten periytymistä ja toteutumista ei pääosin kyetä varmistamaan. Myös sopimusmenettely on varautumisen kannalta epäyhtenäistä ja puutteellista.

Kuva 14. ICT-varautumisen vaatimusten hallinta



Varautumiseen liittyvää yhtenäistä vaatimusten hallintaa valtionhallinnossa tulee kehittää. Vaatimukset tulisi mahdollisuuksien mukaan sovittaa palvelun tuottajien jo olemassa oleviin palvelutasovaihtoehtoihin ja toimintamalliin. Vaatimukset on tarkoituksenmukaista koota muutamaaan vaatimustasoon, jotta niiden toteuttaminen ja valvonta olisi mahdollista. Vaatimustasojen perusteella voidaan määrittää malleihin perustuen palvelutasosopimukset ja auditoitavat palvelutasomittarit. Vaatimusten puuttuessa joudutaan usein määrittämään, sopimaan ja auditoimaan kaikki yksityiskohtaiset menettelyt erikseen.

Tällä hetkellä valtionhallinnossa ei varmistuta asetettujen vaatimusten siirtymisestä verkostojen sopimusmenettelyyn ja toteutumisesta palvelutuotannossa erityistilanteissa.

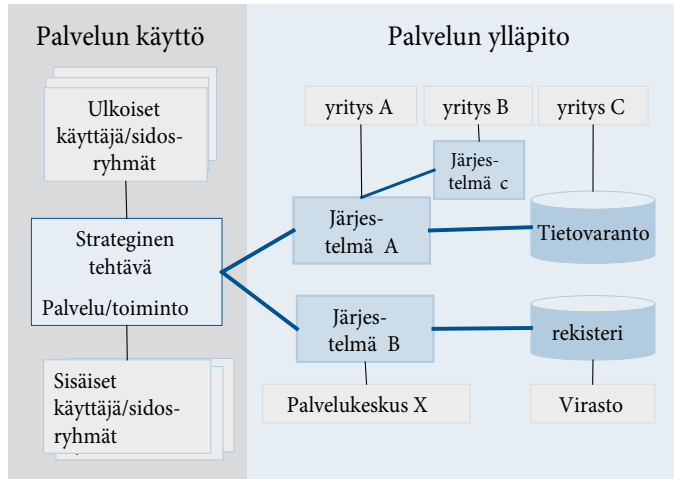
2.4 Palvelujen ja ICT-infrastruktuurin jatkuvuuden hallinta

Kriittiseksi määritelty toiminta vaatii erityisratkaisuja kaikkien sitä tukevien resurssien osalta, myös tietoteknisten palvelujen osalta. Tässä tulee ottaa huomioon kaikki toimijat ja tekniset rakenteet.

Hallinnonalojen keskeisten tehtävien suorittamisen kannalta voidaan erottaa kolme kokonaisuutta:

- sisäiset ja ulkoiset käyttäjä- ja sidosryhmät
- toimintaa tukeva omassa hallussa oleva ja ulkoistettu tietotekninen infrastruktuuri palveluineen, erityisesti tietoliikenne, rekisterit ja tietovarannot
- infrastruktuuria ylläpitävät ja palveluja tuottavat ulkoiset ja sisäiset palveluntuottajat

Kuva 15. Esimerkki kriittisen toiminnan ICT-ympäristöstä



Valtionhallinnossa palveluja hankkivat, tuottavat ja integroivat hallinnonaloja palvelevat ICT-palvelukeskukset. Tällaisia ovat muun muassa sisäasiainministeriön Hallinnon tietotekniikkakeskus (HALTIK), Puolustusvoimien J ohd tamisjärjestelmäkeskus (PVJJK), Valtion IT-palvelukeskus (VIP) ja Oikeushal linnon tietotekniikkakeskus (OTTK).

HALTIK tuottaa usean hallinnonalan turvallisuudesta vastaaville viran omaisille tietotekniikkapalveluja. Valtion IT-palvelukeskus tulee koordinoi maan valtion yhteisten tietotekniikkapalvelujen hankintaa, kehittämistä ja ylläpitoa.

2.4.1 Sähköiset palvelut, tietovarannot ja rekisterit

Kriittisissä ja keskeisissä valtakunnallisissa tieto- ja viestintäjärjestelmissä yksittäisen kohteen lamautuminen tai vaurio ei saa lamauttaa koko järjes telmää. Tietojärjestelmät ja tietovarannot on hajautettava maantieteellisesti vähintään kahteen paikkaan. Yhteiskunnan toimivuudelle kriittisiä tietojär jestelmiä suunniteltaessa ja rakennettaessa on varmistettava, että niihin liit tyvän ohjauksen, ylläpidon, järjestelmähallinnan ja teknisen tuen osaaminen säilyy Suomessa tai ohjaus- ja hallintakyky on oltava mahdollista palauttaa Suomeen. Sovellusten tietovarantojen tulee olla Suomessa. Tietojärjestelmät ja niiden muodostamat kokonaisuudet tulee dokumentoida.

Sähköisten palvelujen ja tietovarantojen varautumisen vaatimuksista ja nii den toteuttamisesta ovat vastuussa kaikki palvelujen käyttöön, ylläpitoon ja tuottamiseen osallistuvat tahot. Valtionhallinnon verkostoituneessa toimin

nassa on päästävä yhtenäisiin toimintatapoihin vaatimusten asettamisessa ja palvelusopimuksissa.

Sähköisten palvelujen ja tietovarantojen käytön edellyttämät varautumisen vaatimukset tulee sisällyttää palvelutasosopimuksiin. Kehitysvaiheessa vaatimukset tulee määritellä, suunnitella, toteuttaa ja dokumentoida. Käyttövaiheessa on huolehdittava vaatimusten ylläpidosta ja toteutumisen todentamisesta. Joissain tapauksissa palveluntarjoaja määrittää saatavissa olevat palvelutasovaihtoehdot, jolloin tyypillinen palvelujen jatkuvuutta rajoittava tekijä on force majeure -ehto.

Palvelutasoja ja -vaatimuksia määritettäessä tulee ottaa huomioon tuki- ja palveluvuoroitukset kaikille osapuolille. Poikkihallinnollisissa toiminnoissa ja palveluissa on tunnistettava jokaisen organisaation sille asettamat tarpeet ja vaatimukset. Tämä toteutuu useimmiten ainoastaan toimijoiden kahdenvälisin sopimuksin. Useimmissa tapauksissa sähköisten palvelujen erityistilanteisiin liittyvää varautumisen tasoa ei ole määritetty ja julkaistu.

Kaikilla virastoilla ei välttämättä ole valtiohallinnon kokonaisuuden kannalta kriittisiä toimintoja ja palveluja. Toiminnot voivat kuitenkin olla kyseisen viraston päätehtävien ja tuotettavien palvelujen kannalta hyvinkin tärkeitä. Toiminnot voivat perustua ulkoistettuihin palveluihin, joissa palvelun jatkuvuuden vaatimukset sisällytetään normaaleihin kaupallisiin sopimuksiin.

Valtiohallinnon yhteisiä keskeisiä tietovarantoja ja perusrekistereitä ovat muun muassa väestö-, kiinteistö- sekä yritys- ja yhteisötietojärjestelmä, paikatietoa koskevat tietovarannot sekä sää- ja olosuhdepalvelut. Näiden lisäksi on joukko eri organisaatioiden itselleen ja muiden käyttöön tuottamia palveluja, joista muut organisaatiot ovat riippuvaisia.

Yhteisille tietovarannoille, perusrekistereille ja niitä tukeville palveluille on valtionhallinnossa asetettu yleisellä tasolla vaatimuksia. Näitä on täydennetty kahdenvälisillä sopimuksilla. Vaatimuksien tulisi koostua käyttäjien esittämistä tarpeista, joiden toteuttamisesta ja raportoinnista vastaavat toteuttajat. Erityistä huomiota tulee kiinnittää valtionhallinnon yhteisten ja hallinnonalojen sisäisten kriittisten tietovarantojen ja palvelinten sekä näiden välisen tietoliikenteen suojaamiseen. Tätä ei kaikilta osin ole toteutettu riittävällä tasolla.

Normaalioloissa sähköisten palvelujen ja niitä tuottavien tietojärjestelmien tärkeys ilmaistaan palvelusopimuksen käytettävyyksivaatimuksina ja asetettuina sanktioina. Erityistilanteissa palvelujen ja tietojärjestelmien toiminnan palauttamisjärjestys määräytyy niille luotavan tärkeysluokituksen mukaan. Tärkeysluokitus voi pohjautua ennalta tehtyyn luokitukseen, mutta jokaisen erityistilanteen hoitaminen saattaa edellyttää tärkeysjärjestyksen tarkistamista tilannetta vastaavaksi. Tällä hetkellä yhtenäistä palvelujen ja tietojärjestelmien tärkeysluokittelua ja siihen liittyvää päätöksentekojärjestelmää ei valtionhallinnossa ole.

Raportointi- ja tarkastusmenettelyillä on varmistuttava, että tietovarantojen toteutus vastaa asetettuja ICT-varautumisen vaatimuksia.

2.4.2 Tietotekniset peruspalvelut sekä tietotekninen infrastruktuuri ja sitä välittömästi tukevat rakenteet

Valtionhallinnon palveluista sisäiset palveluyksiköt voivat tuottaa vain osan. Suuri osa palveluista on ulkoistettua ja toimittajaverkostoista riippuvaista. Valtionhallinnon sisäiset palveluyksiköt ovat palvelun jatkuvuuden kannalta osa tätä verkostoa. Verkoston toimintaa varautumismielessä tulee kehittää.

Palvelut ja niitä tukeva tietotekninen infrastruktuuri muodostuu kerroksellisesta rakenteesta, jossa kullakin kerroksella on omat suojauksensa ja haavoittuvuutensa. Näistä muodostuu monimutkainen ja vaikeasti hallittava kokonaisuus, jonka varautumisen kannalta eräitä keskeisiä osia ovat muun muassa konesalit, kaapelireitit ja laitetilat, protokollat, verkon ja järjestelmien hallinta sekä tukitoiminnot. Valtionhallinnon kriittisissä toiminnoissa on noussut esille erityisesti tietoliikenteen sekä käyttö- ja konesalipalvelujen varmentamisen merkitys vakavia erityistilanteita varten. Varautumisen toteuttamisesta vastaa infrastruktuurin kehittäjä ja ylläpitäjä.

Kokonaisuuden yhteisvaikutuksen ja jatkuvuuden tason arviointi sekä varautumisen koordinointi tietotekniseen kokonaisuuteen kohdistuvan vakavan erityistilanteen näkökulmasta on vaikeaa. Kokonaisuuden tukemiseksi tarvitaan myös yksityiskohtiin meneviä vaatimuksia ja toteutusmalleja.

2.5 Osaamisen hallinnan nykytila ja kehittämistarpeet

2.5.1 Osaamistarpeet ja nykytila

Organisaatioissa oleva henkilöstön osaaminen yhdessä palvelua tuottavan toimittajaverkoston osaamisen kanssa muodostavat perustan varautumiselle. Erityistilanteissa ja poikkeusoloissa tarvittavan osaamisen määrän ja laadun määrittely sekä käyttö ja ylläpito ovat keskeisiä, mutta haasteellisia tehtäviä. ICT-varautumisen kannalta tärkeää on osaamisen todellinen käytettävyys ja hallinta pitkissä palveluketjuissa.

Nykyisin osaamista hallitaan hallinnonalojen ja virastojen tai erillisten yksiköiden puitteissa. ICT-varautumisen osaamista ei ole yleensä erityisesti huomioitu osaamisen hallinnassa. ICT-varautumisen osa-alueiden, kuten jatkuvuuden hallinnan, riskienhallinnan, häiriötilanteiden hallinnan ja palautumisen, osaamista organisaatioissa kuitenkin on merkittävästi.

Tyypillisesti merkittäviä osia palvelusta ja niiden edellyttämästä osaamisesta hankitaan valtionhallinnon ulkopuolelta. Usein tukijärjestelmän ja erikoiskomponenttien edellyttämä syvä osaaminen on saatavissa vain valmistajan asiantuntijoilta ulkomailta. Palvelujen tuottajat ja infrastruktuurin ylläpitäjät

mitoittavat osaamistarpeensa ainoastaan palvelutasosopimuksissa olevien vaatimusten sekä oman tarpeensa mukaisesti. ICT-varautumisen huomioon ottaminen vaatii ulkoistettujen palvelujen määrittelyssä, hankinnassa, sopimushallinnassa ja tuotannon valvonnassa tilaajalta erityisosaamista.

Seuraavassa taulukossa on kuvattu yleisellä tasolla eri henkilöstöryhmille asetettavia osaamistarpeita.

Taulukko 6. Esimerkki henkilöstöryhmille asetettavista osaamistarpeista

	Toiminto/ prosessi	Yleinen varautu- minen	ICT- varautu- minen	Tietohal- linnon johtaminen	Tietotek- niikan johtaminen	Tietotekniikan ja -turvalli- suuden erityis- kysymykset	Turvalli- suus ja tietoturva
Valtionhallinto							
Ylin johto							
Yleisjohto							
ICT-johto							
Valmiusjohto							
Palveluyksikkö							
Palvelutoimittaja							
Konsultointi							
Järjestelmätuotanto							
Käyttöpalvelu							
Selite:							
	Syvä asiantuntemus, mahdollistaa substanssin suunnittelun ja ohjauksen						
	Hyvät perustiedot, mahdollistaa hyödyntämisen ja toimintojen suunnittelun ja ohjauksen						
	Yleiskäsitys, mahdollistaa hyödyntämiseen osallistumisen						
	Ei erityisvaatimuksia						

Osaamisen haasteet kohdistuvat myös itse ICT-varautumisen perusteiden ja keinojen tuntemiseen sekä rekrytointiin ja työvoiman pysyvyyteen rajusti kilpailuilla työmarkkinoilla.

ICT-varautumiseen ei ole erityiskoulusta. Tukena ovat tietoturvan, yritysturvallisuuden ja informaationsodankäynnin koulutukset. ICT-varautumista käsitellään vähäisesti myös erilaisissa yleiskoulutuksissa. ICT-varautumisen näkökulmasta tulisi määrittää koulutussisällöt ja oppimiskokonaisuudet sekä täydentää olemassa olevia ulkopuolisten tahojen ja valtionhallinnon kursseja vastaamaan koulutustarvetta.

ICT-varautumiseen liittyviä asioita harjoitellaan eriasteisissa valmiusharjoituksissa, kuten valtionhallinnon VALHA- ja TIETO-harjoitukset sekä hallinnonalakohtaiset yksittäiset harjoitukset. Varautumiselle olisi eduksi muodostaa

olemassa olevia harjoituksia täydentäen yhtenäinen ja YETT-strategiaa tukeva kokonaisuus. Harjoitustoimintaan on tarkoituksenmukaista liittää kriittisten palvelujen todelliseen toteutumiseen liittyvä tutkimus- ja testaustoiminta.

2.6 Keskeisimmät havainnot nykytilasta ja kehittämistarpeista

Valtionhallinnossa kaikki hallinnonalat ovat käynnistäneet ICT-varautumiseen liittyviä toimenpiteitä. Hyvää viranomaisyhteistyötä tehdään monissa kohteissa ja valmius hallinnonalojen väliseen yhteistyön edelleen kehittämiseen on hyvä. Valtionhallinnon ja elinkeinoelämän välillä on varautumiseen liittyen syvä yhteistoiminta, jossa keskeisenä toimijana on jo pitkään ollut Huoltovarmuuskeskus. Varautumisen toteuttaminen Suomessa kestää hyvin kansainvälisen vertailun.

Toimintaympäristön ja valtionhallinnon muutokset luovat uusia haasteita ICT-varautumiselle. Yhteiskunnan riippuvuus tietotekniikasta lisääntyy edelleen voimakkaasti. Todennäköisyys tilanteelle, jossa ympäristökatastrofi, suur-onnettomuus ja inhimillisestä virheestä johtuva tai tahallisesti aiheutettuna laaja tietotekniikkahäiriö sekoittavat valtionhallinnon toimintakyvyn lisääntyy. Tällaisen tilanteen vaikutusten minimoiminen ja toimintojen nopea vakauttaminen edellyttävät valtionhallinnossa ennalta tehtyjä, yhtenäisiä ICT-varautumisen toimenpiteitä. ICT-varautumisen toteuttamisen taso ministeriöissä ja muissa virastoissa vaihtelee.

Havainnot ICT-varautumisen haasteista ja kehittämistarpeista on esitetty seuraavassa taulukossa.

Taulukko 7. Havainnot valtionhallinnon ICT-varautumisen nykytilasta ja kehittämistarpeista

ICT-VARAUTUMISEN NYKYTILA JA KEHITTÄMISTARPEET		
Havainto	Kehittämistarve	Kehitysvastuu
ICT-VARAUTUMISEN OHJAUS JA VAATIMUSTENHALLINTA		
ICT-varautumiselle ei aseteta selkeästi velvoittavia vaatimuksia, jotka ulottuvat ministeriöistä virastoihin. Resursointi ei vastaa tavoitteita eikä vaikutuksia kyetä seuraamaan.	- CT-varautumisen tulee olla sisäänrakennettuna ydintoimintaprosesseihin ja niitä tukevaan muuhun varautumiseen, koska tietoteknologia on keskeinen tekijä yhteiskunnan toiminnassa. - ICT-varautumisen keskeisimpien kehitystarpeiden, resurssien ja muiden toimintaedellytysten tulee näkyä valtioneuvoston selonteissa, hallitusohjelmassa sekä hallinnonalojen ja virastojen strategioissa ja tulosohjauksessa. YETT-strategiaa tulee uudistaa ICT-varautumisen toteuttamista konkreettisesti linjaavaksi asiakirjaksi. - ICT-varautumisen vastuut ja tehtävät on liitettävä kaikkien hallinnon tasojen TTS-prosessiin ja tulosohjaukseen (tavoitteet, resurssit, mittarit, raportointi), ministeriöiden ja virastojen työjärjestyksiin sekä johdon ja asiantuntijoiden tehtäväkuvauksiin.	VNK VM TPAK ministeriöt
Kriittisten toimintojen ja kriittisen tietoteknologian tunnistaminen on epäyhtenäistä.	- Toimintojen, palvelujen ja järjestelmien merkitys eri turvallisuustilanteissa on tunnistettava. Palvelujen ja tietojärjestelmien tärkeysluokitukset on laadittava tukemaan kehittämistä ja erityistilannekohtaista jatkuvuuden hallintaa. Jatkossa tulee keskittyä varautumisen kannalta kriittisten toimintaprosessien tunnistamiseen ja turvaamiseen. - Luotava malli ja työväline kriittisen ICT:n ja kriittisimpien yksittäisten osien tunnistamiselle ja kuvaamiselle. - Virastojen palveluille ja järjestelmille määritettävä palvelutasovaatimukset myös YETTS-erityistilanteisiin ja määritettävä varautumisen tavoitetaso. - Määritettävä kriittisten toimintojen ja järjestelmien ylläpito- ja resursointivastuut. Tehtävä tarvittavat varaukset omista resursseista sekä toimittajien osalta täydennettävä sopimukset ottamaan huomioon erityistilanteiden edellyttämät vastuu- ja priorisointivaraukset.	VM ministeriöt HVK, poolit IT-palvelukeskukset
Ohjaavan ohjeistuksen puutteellisuus ja noudattaminen; riittävyys vakavissa erityistilanteissa on epävarmaa	- Lainsäädäntöä, normeja ja ohjeistusta on kehitettävä YETTS-erityistilanteiden hoitamisen (toimivaltuudet, resurssien käyttö) näkökulmasta. Ohjeistuksessa tulee huomioida myös nykyisistä YETTS-malleista poikkeavat häiriötilanteet. - ICT-varautumisen huomioon ottaminen valtionhallinnon tietohallintoa koskevissa ohjeistuksessa, standardeissa ja teknisissä määräyksissä sekä niiden käytössä. - Jokaisen ministeriön ja viraston on varmistettava varautumissuunnitelmansa dokumentointi ja toteutettavuus.	VM VNK LVM Ministeriöt
ICT-varautumisen tarkastus, auditointi ja controller-toiminta on puutteellista	On luotava vaatimuksia vastaavat tarkastusluettelot ja ohjeistot olemassa olevan tarkastus- ja controller-toiminnan osaksi. On kehitettävä koko palveluntuotantoketjuun ulottuvat oikein mitoitettavat auditointi- ja arviointimenettelyt.	VM VTV HVK VIVI

TILANNEKUVA, RISKIENHALLINTA JA JATKUVUUS		
ICT-varautumisen kehittämisen ja häiriötilanteiden hoitamisen tilannekuva on puutteellinen.	- On määritettävä ICT-varautumisen kehittämisen edellyttämät tilannetiedot ja niiden tuottamisvastuut hallinnonaloilla ja kansainvälisestä ympäristöstä noudattaen muunkin tiedon tuottamiseen luotua vastuujakomallia. - Hallinnonaloilta, yhteistoimintakumppaneilta ja kansainväliseltä yhteisöltä tarvittava ICT-toimintaan liittyvä tieto YETTS-erityistilanteiden hoitamisessa ja tietojen esittäminen osana tilannekuvajärjestelmiä on kuvattava. - Luotava ughiin ja haavoittuvuuksiin liittyvä kokoava tutkimusstrategia ja -koordinaatio.	VM, VNK ministeriöt, ViVi HVK, poolit
Riskien hallinnan menetelmät hallinnonaloilla ja virastoissa ovat epäyhtenäisiä	- On luotava toimintaa tukevan ICT:n uhka- ja turvallisuustilannearvioiden ja riskianalysien laatimiseen yhtenäiset perusteet, menettelytavat, työkalut ja resurssit. - huomioitava muiden verkoston osapuolien suorituskyky- ja jatkuvuusvaatimukset.	VM ministeriöt
Tietovarantojen ja tietoliikenteen merkitys sähköisten palvelujen perustana on erittäin suuri ja sen suojaamisessa on puutteita	- Kriittisille tietojärjestelmille, -tietokannoille, rekistereille ja tietoliikenteelle on määriteltävä jatkuvasti ylläpidettävät palvelukohtaiset eri turvallisuustilanteiden käytettävyyssvaatimukset sekä huomioitava ne sopimusrakenteissa. Palvelutasovaatimusten ja tärkeysluokittelujen mukaiset jatkuvuuden hallinnan toimintaohjeet, menettelytavat ja tietotekniset ratkaisut on toteutettava. - Kriittisten tietojärjestelmien toiminta tulee varmistaa siten, että ne on sijoitettu sellaiseen tuotantoympäristöön, jossa rakenteet on suunniteltu ja toteutettu häiriö- ja erityistilanteita sekä poikkeusoloja varten. - Valtion hallitsemien suojattujen ja rakennettujen laitetojen yhteiskäyttöä on tehostettava sijoittamalla niihin kriittisiä palveluja tuottavia tietojärjestelmiä, tietovarantoja ja tietoliikenneverkon laitteita sekä tarvittaessa käyttöön otettavaa lisäkapasiteettia. Kehitettävä ja ylläpidettävä valmiutta varajärjestelyjen käyttöönottoon.	VM LVM VNK OPM. HVK PV HALTIK Muut IT-palvelukeskukset
TOIMITTAJAVERKOSTON HALLINTA JA HYÖDYNTÄMINEN		
Sopimusmenettelyissä ja vaatimusten asettamisessa toimittajille on epäyhtenäisyyttä	- On luotava yhtenäiset ICT-varautumisen vaatimukset julkishallinnon hankintaehtoihin, tarjouspyyntöihin ja sopimuksiin. - Sisäisille palveluntuottajille on asetettava yhtäläiset vaatimukset muiden palveluntuottajien kanssa. Hallinnon palvelukeskukset on mitoitettava tuottamaan myös kriittisiä yhteisiä palveluja. - Turvallisuussopimukset yritysten kanssa tulee laatia ja auditoida systemaattisesti	TEM, VM, LVM, PLM HVK, ViVi, VIP, Hansel,
Palvelujen tuottaminen verkostoituu ja niiden tuottaminen ulkomailla lisääntyy.	- Palveluverkoston ja alihankintaketjujen hallinta korostuu. - Palvelujen ulkoistamisessa on varauduttava siihen, että osa tuotannosta tapahtuu ulkomailla. - Valtionhallintoon on luotava yhtenäiset kriteerit sekä sopimusmallit mitä palveluja ja miten voidaan tuottaa ulkomailla. On määritettävä mille kriittisen palvelun osille asetetaan erityisvaatimuksia; esimerkkinä käyttäjähallinnan toteutus Suomessa suomalaisella henkilökunnalla..	TEM, VNK, VM, SM, PLM, LVM, UM HVK, VIP, Hansel

OSAAMINEN, KOULUTUS JA HARJOITTELU		
ICT-varautumisen osaamistarpeen tunnistaminen on haasteellista ja koulutustarjonta vähäistä	- Hallinnon on tunnistettava kriittiset osaamistarpeet ja luotava ICT-varautumisen osaamisprofiilit, joita hyödynnetään rekrytoinnissa, tehtäväkierrossa, koulutuksessa ja erityistilanteiden hallinnassa. - On muodostettava kartoitettava olemassa oleva soveltuva koulutus ja kehitettävä opetuslaitosten ICT-varautumista tukevaa koulutustarjontaa. Myös vapaaehtoisen maanpuolustuksen harjoitusrakenteita voidaan hyödyntää.	OPM, VM, ministeriöt, HVK
ICT-varautumiseen liittyvä harjoitustoimintaa tulee kehittää vastaamaan paremmin tulevaisuuden tarpeita.	- ICT-varautuminen on saatava tiiviimmin osaksi valtiohallinnon harjoituskokonaisuutta. - On kehitettävä tilannekuvausten yhteiskäyttöä ja yhteisten harjoituskehysten luomista järjestettävissä varautumis- ja valmiusharjoituksissa. - Palveluketjun ja -verkon toimintakykyä tulee testata säännöllisesti. - Harjoituksissa on hyödynnettävä poikkeusoloja varten luotuja toimitila ja muita järjestelyjä.	VNK, VM LVM, PLM ministeriöt, Pv, HVK

Hallinnonaloilla ja niiden noin 120 virastossa ICT-varautumisen tarve, ohjausmekanismit, taso ja keinot vaihtelevat varsin paljon. Yhtenäistämällä toimintatapoja, tuottamalla keskitetyksi perusteita ja menetelmiä, kehittämällä tulosojausta ja-raportointia sekä vahvistamalla valtionhallintoa voidaan käytettävillä resursseilla saada huomattavasti enemmän vaikuttavuutta ICT-varautumiseen.

3 ICT-varautumisen kehittäminen

3.1 Yleisperiaatteet

ICT-varautumisen kehittämisen tavoite

Hankkeessa määritetään vaatimukset, keinot ja menetelmät, joilla ICT-varautuminen saadaan kustannustehokkaaksi ja koordinoituksi osaksi kunkin hallinnonalan jokapäiväistä toimintaa. Palvelujen jatkuvuus on kyettävä takaamaan toiminnan vaatimusten mukaisesti häiriötilanteissa, YETTS-erityistilanteissa ja poikkeusoloissa. ICT-varautuminen ei ole erillinen toiminto, vaan osa tietohallinnon ja yleisen varautumisen kokonaisuutta.

Vuoden 2010 loppuun mennessä ICT-varautumisen ohjaus on osana yleisiä ohjausmenetelmiä ja vaatimustasot on määritelty. Hallinnonalat ovat suunnitelleet ja käynnistäneet ICT-varautumisen toteuttamisen.

Vuoden 2012 loppuun mennessä ministeriöissä ja virastoissa on saavutettu kriittisissä toiminnoissa ICT-varautumisen perustaso. Kumppanusverkoston vaatimusten hallinta ja sopimusmenettelyt on yhtenäistetty.

Vuoden 2016 loppuun mennessä valtionhallinto on kokonaisuudessaan saavuttanut ja todentanut ICT-varautumisen perustason sekä erikseen määritellyiltä osiltaan korotetun tai korkean tason.

ICT-varautumista kehitetään siten, että:

1. ICT-varautuminen on kaikilla tasoilla osa TTS- ja tulosohtausprosessia. Ministeriöt ja virastot rahoittavat toimintansa edellyttämän varautumisen normaalista kehiksestään. ICT-varautuminen toteutetaan osana yleistä ohjausta ja ICT-toteutusta.
2. ICT-varautumisen johtosuhteet ja tehtävät määritetään työjärjestyksiin ja tehtäväkuvauksiin kaikilla hallinnon tasoilla.
3. Uhka-arvio, riskianalyysi ja ICT-varautuminen otetaan alusta lähtien huomioon kaikessa kehittämis- ja tuotantotoiminnassa.
4. ICT-varautumisen osahankkeissa luodaan valtion, ministeriöiden ja virastojen tasojen ratkaisut ja toimintamallit. Mahdollisimman aikaisessa vaiheessa tuotetaan virastojen ja ministeriöiden ICT-varautumisen ja

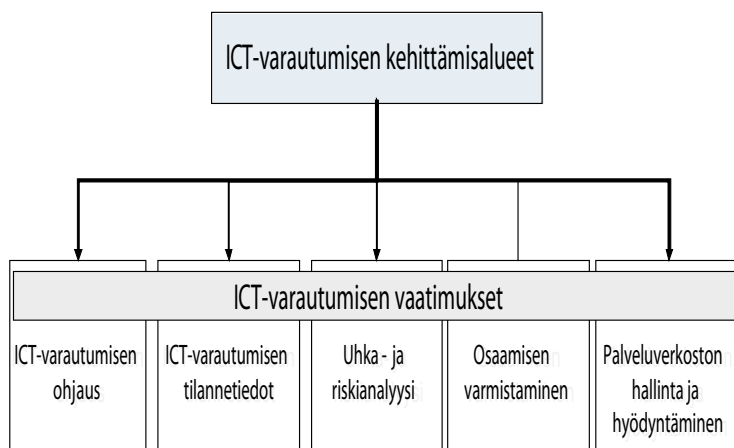
jatkuvuuden hallinnan käytännön toteuttamista tukevat yhtenäiset suunnittelumallit ja tarkistuslistat.

5. Keskeisimmät valtionhallinnon yhteiset kehittämistoimet ja palvelut toteutetaan keskitetysti. Hallinnonalat vastaavat itsenäisesti omien palveluiden varautumisesta.
6. ICT-varautumisen periaatteet ja varautumistasot ulotetaan toiminnan vaatimusten mukaisesti kaikkiin tuotantotapoihin ja tuottajiin.
7. Ylläpidetään tiivis yhteistyö muiden hallinnonalojen ohjaamien varautumishankkeiden kanssa, erityisesti LVM:n yhteiskuntaan ja kansalaisiin sekä HVK:n talouselämään suuntautuneiden hankkeiden kanssa.

Varautumisen kehittäminen tulee toteuttaa keskitetysti ohjattuna. Hyötyjen saavuttaminen edellyttää toteutuakseen sekä valtionjohdon että hallinnonalojen sitoutumista yhteisesti tehtyihin linjauksiin, ratkaisuihin ja resursointiin.

Valtioneuvoston kanslialle kuuluu valtioneuvoston yhteinen varautuminen. Julkishallinnon ICT-varautumisen kehittämisestä vastaa valtiovarainministeriö. ICT-varautumisen kehittämiseksi muodostetaan hanke, jonka osa-alueet on esitetty seuraavassa kuvassa.

Kuva 16. ICT-varautumisen kehittämisalueet



ICT-varautumisen kehittämisen kokonaisohjaus tulee valtionhallinnossa olla selkeästi vastuutettu.

Taulukko 8. ICT-varautumisen ohjaus valtionhallinnossa

ICT-varautumisen ohjaus	
Valtioneuvoston kanslia (VNK)	Ohjaa valtionhallinnon johtamisen ja hallinnon kokonaisvarautumista ja näihin sisältyen ICT- varautumista
Turvallisuus- ja puolustusasiantuntemusta (TPAK)	- ICT-varautumisen kytkeminen YETT-strategiaan - Toteutumisen seuranta osana YETTS:n toteumaa
Valtiovarainministeriö (VM) Valtion IT-toiminnan johtamisyksikkö (ValtiT)	- Valtion ICT-varautumisen suunnittelun ja toteuttamisen johtaminen - Kuntien ICT-varautumisen ohjaus
Liikenne- ja viestintäministeriö (LVM) Viestintävirasto (VIVI)	- Yhteiskunnan tietoteknisen infrastruktuurin toimivuus - Poikkeusolojen säädännön kehittäminen - Teletoiminnan sääntely, regulaatio ja valvonta - CERT-FI toiminta
Ministeriöt, virastot, Tietohallintojohto	- Hallinnonalan ICT-varautumisen toteutus - Erikseen sovittujen yhteisten ICT-varautumisen projektien johtaminen / pilotoint - ICT-varautumisen toimeenpano
Valmiuspäällikkökokoukset	Varautumisen eri osa-alueiden toteuttamisen koordinointi valtioneuvoston ja hallinnonalojen tasolla

Toteutus jakautuu keskitetysti toteutettaviin, keskitetysti ohjattuihin, mutta hallinnonaloilla tai kärkihankkeissa toteutettaviin sekä hallinnonaloilla itsenäisesti toteutettaviin toiminnan kehittämisprojekteihin ja hankkeisiin.

Taulukko 9. ICT-varautumisen toteutuksen ohjaustavat

Ohjaustapa	Kriteerit	Koordinoitavastuu
Keskitetysti toteutettavat	- Välttämätön erityistilanteissa usealle hallinnonalalle - Keskitetty resurssien hallinnan tarve erityistilanteissa - Poikkihallinnollinen koko valtionhallintoa varten	ValtiT tai erikseen määrätty ministeriö/ virasto
Keskitetysti ohjattavat, hallinnonalojen toteuttamat	- Yhtenäisyys takaa erityistilanteissa paremman tilannekuvan ja resurssien kohdentamisen - Tarjoaa hallinnonaloille valmiin ratkaisun ja yhtenäisen toteuttamistavan (vaatimukset, sopimukset, auditoinnit ...)	ValtiT / Valtion IT-palvelukeskus
Hallinnonalan sisäiset	- Hallinnonaloilla mahdollisuus räätälöidä toimintaa tarpeiden mukaan - Häiriöt palvelussa vaikuttavat vain hallinnonalan toimintaan	Hallinnonalat / virastot

Valtionhallinnon yhdenmukainen ICT-varautuminen mahdollistaa merkittävien toiminnallisten hyötyjen saavuttamisen.

- Turvalliset poikkihallinnollisesti verkottuneet palvelut ja ratkaisut mahdollistuvat tuottamalla yhtenäisillä perusteilla luodut ja selkeästi viestityt jatkuvuuden, häiriötilanteiden hallinnan ja toipumisen toimintamallit (yhtenäinen uhka-arvio, riskienhallinta, tilannekuva, suojautumistavat ja -toteutukset).
- Yhden osapuolen tutkittujen ja laadukkaiden ratkaisujen käyttöönotto, resurssien poikkihallinnollinen hyödyntäminen ja volyymietujen saavuttaminen mahdollistuu. Saavutetaan työmääräsäästöjä.
- Yhtenäisten sopimus-, toimitus- ja auditointimallien sekä palvelurakenteiden hyödyntäminen mahdollistaa asetettujen vaatimusten mukaisen palvelun jatkuvuuden optimoiduilla resursseilla ja erikoistuneiden palveluyksiköiden tuella (muun muassa HANSEL, HVK, Valtion IT-palvelukeskus, HALTIK, PVJJK)
- ICT-tilannekuvan ylläpito selkiytyy. Erityisesti uusissa uhkatilanteissa riskiarviointi, toiminnan ja resurssien käytön priorisointi sekä oikea reagointi valtionhallinnon yhteisen ja hallinnonalojen ICT-toiminnan jatkuvuuden takaamiseksi on mahdollista.
- Hallinnonalojen ja muiden toimijoiden ICT-varautumisen kokonaistilannetta kyetään ohjaamaan, resursoimaan ja seuraamaan kattavasti.

Yhdenmukainen varautuminen ja hyötyjen saavuttaminen edellyttävät toteutuakseen sekä valtionjohdon että hallinnonalojen sitoutumista yhteisesti tehtyihin linjauksiin, ratkaisuihin ja resurssitarpeisiin. Yhtenäinen ratkaisu ei aina tarjoa hallinnonalalle kaikkia sen toiminnan edellyttämiä ominaisuuksia. Tällöin toimintaa on sopeuttava tarjottuun palveluun tai otettava käyttöön hyväksyttyjä erillisratkaisuja. Varautumisen hyötytarkastelu on tehtävä riittävän pitkällä aikajänteellä ja tarvittaessa yhtenäisten ratkaisujen tuottamista on tuettava keskitetyin resurssein.

ICT-varautumisen kehittämisen kustannukset voidaan saada takaisin pienentämällä merkittävästi erityistilanteiden vaikutuksia toimintaan ja nopeuttamalla palauttamista. Hyödyt realisoituvat vakavan erityistilanteen sattuessa. Todennäköisyys vakavalle erityistilanteelle kasvaa jatkuvasti. Saavutettavat hyödyt vakavassa erityistilanteessa ovat monikymmenkertaiset kustannuksiin nähden. Tällä hetkellä ICT- varautuminen ja sen resurssit eivät vastaa uhkaympäristön asettamia vaatimuksia.

3.2 ICT-varautumisen vaatimusten kehittäminen

3.2.1 ICT-varautumisen vaatimusten perusteet

Palveluiden kriittisyys määrittää selkeät jatkuvuusvaatimukset niiden toteutamiselle. Varautumisen kustannustehokkuus edellyttää ennakoivien toimenpiteiden mitoittamista hallinnonalan ja valtionhallinnon kokonaisuuden kannalta oikein. Varautumisen toteutus tulee sisällyttää palvelun ja järjestelmän kehittämisen kaikkiin vaiheisiin. Tämän mahdollistavat valtionhallinnolle luotavat yhtenäiset ICT-varautumisen vaatimukset ja vaatimustasot.

ICT-varautumisen perustan luovat toiminnan sille asettamat toiminnalliset vaatimukset. Näiden tulee perustua YETT-strategiassa kuvattuihin erityistilanteisiin. ICT-varautumisen vaatimukset kohdistuvat kolmeen kokonaisuuteen: organisaation kypsyys, toiminnalliset rakenteet sekä tietotekniikka.

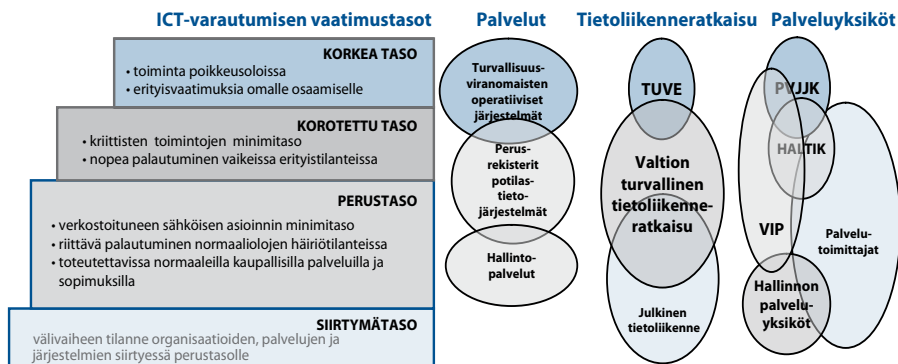
Vaativuustasot muodostetaan kansainvälisen vakiintuneen käytännön mukaisesti viisiportaiseksi, joista varautumisen kannalta merkityksellisiä ovat perus-, korotettu ja korkea taso. Tasojen sisältö yhdennetään Tietoturvasojen ja HVK:n HUOVI -hankkeen talouselämän organisaatioiden kypsyyttä mitaavien tasojen kanssa.

Perustasolla voidaan normaali hallinnon toiminta toteuttaa myös voimakkaasti verkostoituneena turvallisesti. Taso mahdollistaa normaaliolojen häiriötilanteista selviytymisen normaaleilla palvelusopimuksilla. Erityistilanteet aiheuttavat palvelukatkoja, joista toiminta ei kuitenkaan kärsi kohtuuttomasti. Taso vastaa laadukasta normaalin liikeyrityksen toimintaa. Perustasolle valtionhallinnossa sijoittuvat esimerkiksi sähköposti, asianhallinnan ja henkilöstöhallinnon järjestelmät. Liitteessä 3 on esitetty perustasolle asetettavia varautumisvaatimuksia, joita täydennetään yhteistyössä Tietoturvasot -hankkeen kanssa.

Korotetulla tasolla osa perustason vaatimuksista on tiukennettu vastaamaan kriittisten toimintojen sekä niiden verkostoitumisen asettamia vaatimuksia. Vain osa organisaation tai toimintayksikön toiminnasta ja palveluista on tarkoituksen mukaista toteuttaa tällä tasolla. Korotetun tason järjestelmiä ovat esimerkiksi potilastietojärjestelmä ja perusrekisterit.

Korkealle tasolle asetetaan vaatimukset poikkeusolojen ja laajojen vaikeiden erityistilanteiden mukaisesti. Vaatimukset asetetaan samoille asioille kuin alemmilla tasoilla, mutta pääsääntöisesti merkittävästi tiukempina. Korkean vaatimustason järjestelmiä ovat esimerkiksi turvallisuusviranomaisten operatiiviset järjestelmät.

Kuva 17. Esimerkki ICT-varautumisen vaatimustasoista, sekä niitä tukevat tietoliikenne- ja palveluyksiköistä ja palveluista



Palvelujen ja järjestelmien sijoittumista korkealle tai korotetulle tasolle valmistellaan hallinnonalojen sisällä ja hallinnonalojen välillä hyödyntäen olemassa olevia työryhmiä, kuten tietohallintotyöryhmät ja valmiuspäällikkökokoukset.

Valtionhallinnon yhteisten palvelujen ja järjestelmien sijoittaminen korkealle ja korotetulle tasolle koordinoidaan keskitetysti. Ministeriöt päättävät hallinnonalansa korkean ja korotetun tason järjestelmistä.

3.2.2 ICT-varautumisen vaatimusten kehittämistyö

Tavoite ICT-varautumisen vaatimusten kehittämisessä:

ICT-varautumiselle on määritetty vaatimukset, jotka vastaavat normaaliolojen häiriötilanteiden ja erityistilanteiden ja poikkeusolojen tarpeisiin. Hallinnonalan tunnistavat osana omia prosessejaan palvelujensa kriittisyyden ja niiden sijoittumisen eri vaatimustasoille. Valtionhallinnon palvelut on toteutettu vaatimustasojen mukaisesti.

Vaatimukset, vaatimustasot ja niiden noudattaminen tarkastetaan YETTS:n tarkastamiseen liittyen säännöllisesti.

Vuoden 2010 loppuun mennessä tarkka perustason vaatimusmäärittely, kuvaukset ja mittaaminen on määritelty ja testattu sekä runkovaatimukset korotetulle ja korkealle tasolle. Kukin hallinnonala on määrittänyt aikataulun, jonka kuluessa palvelut toteutetaan ICT-varautumisen vaatimustasojen mukaisesti.

Vuoden 2012 loppuun mennessä hallinnonaloilla ja virastoissa saavutetaan kriittisissä toiminnoissa ICT-varautumisen perustaso. Korotetun ja korkean tason vaatimusmäärittely, kuvaukset ja mittaaminen on määritelty ja testattu.

Vuoden 2016 loppuun mennessä valtionhallinto on kokonaisuudessaan saavuttanut ja todentanut ICT-varautumisen perustason sekä erikseen määriteltyiltä osiltaan korotetun tai korkean tason.

ICT-varautumisen tasojen eri osakokonaisuuksille laaditaan niin tarkat toiminnalliset ja tekniset vaatimukset, että niiden suunnittelu ja toteutus valtionhallinnon kokonaisuuden, hallinnonalojen, virastojen ja hankkeiden tasolla sekä erilaisissa tietoteknisissä palveluympäristöissä tuottaa yhdenmukaisen ja todennettavan tuloksen. Kehittämisalueen sisältö ja päätoimijat on esitetty seuraavassa kuvassa.

Kuva 18. ICT-varautumisen vaatimusten kehittämisen kohdealueet, sisältö ja päätoimijat



Saavutettavat hyödyt:

Vaativustasot ovat ICT-varautumisen toteuttamisen keskeisin väline. Ne yhdenmukaistavat ICT:n toteuttamista ja mahdollistavat yhteismitallisten tavoitteiden ja resurssien kohdentamisen ja varautumisen toteutuksen seurannan. Verkostoituneessa ympäristössä vaatimusten noudattaminen mahdollistaa tehtyjen ratkaisujen monistamisen sekä resurssien kustannustehokkaan käytön ja erityistilanteiden hallinnan.

ICT-varautumisen vaatimukset -osahankkeeseen sisältyvät seuraavat linjaorganisaatiossa toteutettavat hallinnon kehittämistoimenpiteet sekä muissa hankkeissa huomioon otettavat ja toteutettavat ICT-varautumisen kehittämistarpeet.

Taulukko 10. ICT-varautumisen vaatimusten kehittämistoimenpiteitä

ICT-varautumisen vaatimukset	Tulos / sisältö	Tekijä	Valmis
Linjaorganisaation kehittämistoimenpiteet			
Eri hankkeiden vaatimustasojen sisällön koordinointi	Koordinoidaan tietoturvaan, varautumiseen ja jatkuvuuden hallintaan liittyvien vaatimustasojen yhteneväisyys	VM VARE, TTT, TUVE, HUOVI, VIP	2008 – 2012
ICT-varautumisen perustaso	Perustaso ja mittarit määritetty, korotetun ja korkean tason runkomääritykset tehty	VARE Hallinnonalat	Q2/2009
	Perustason keskitetysti ohjattu ja hallinnonalakohtainen toteutus aikataulutettu	VM Ministeriöt	2009
	Perustason ensimmäiset vaatimukset toteutettu	Hallinnonalat	2012
	Perustason vaatimukset toteutettu	Hallinnonalat	2016
	Perustason toteutus on todennettu	VM Ministeriöt	2013/ 2017
ICT-varautumisen korotettu ja korkea taso	Korotetun ja korkean taso sekä mittarit on määritetty	VARE Hallinnonalat	2012
	Palvelut ja järjestelmät korotetulle ja korkealle tasolle määritetty	Ministeriöt Järjestelmien omistajat	2012
	Korotetun ja korkean tason toteutus aikataulutettu	Ministeriöt Järjestelmien omistajat	2010
	Keskeisimmät korotetun ja korkean tason toteutukset on otettu käyttöön ja todennettu	Hallinnonalat	2012 (perustaso) 2016
Tulosohjaus ja raportointi	ICT-varautumisen kehittämistä ohjataan tulostavoitteilla ja -mittareilla	VM Ministeriöt Virastot	2012
Kehittämistarpeet hankkeissa			
Perustaso	Tarkkojen vaatimusten määrittely ja testaus	Tietoturvasot ValtIT	2009
Korotettu ja korkea taso	Tarkkojen vaatimusten ja mittarien määrittely sekä testaus	TUVE PLM	2011
Todentaminen	Raportointi, mittaus ja auditointi: kohteet, mallit, menetelmät, käytännöt ja testaus	VARE ValtIT	2009 – 2011

3.3 ICT-varautumisen ohjauksen kehittäminen

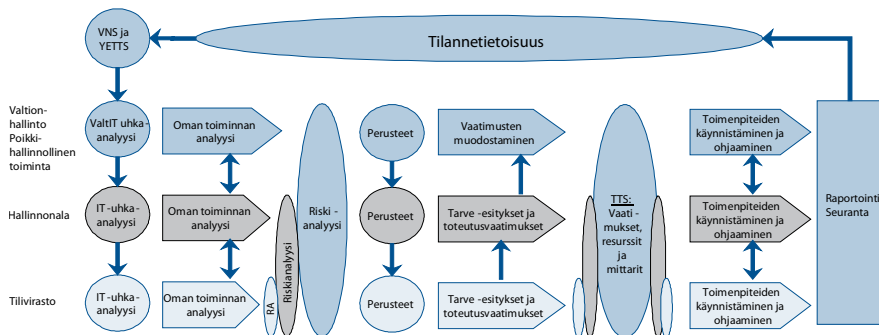
ICT-varautumisen ohjaus perustuu toiminnan tarpeista lähtevien vaatimusten asettamiseen ja niiden toteuttamisen todentamiseen. ICT-varautumisen ohjaus on saatava entistä tehokkaammin osaksi normaalia toiminta- ja taloussuunnittelua sekä tulosohjausprosessia ja raportointia.

3.3.1 Ohjauksen kehittämisen perusteita

Varautumista ohjaavat ja priorisoivat valtioneuvoston periaatepäätökset. YETT-strategia asettaa yleistavoitteita. VAHTI-ohjeistossa määritetään keinoja ICT-varautumisen toteuttamiseen tietoturvallisuuden alalla. Keskeisiä haasteita ohjauksessa ovat strategiaan perustuvien varautumisen toimenpiteiden ohjeiston ja toimintamekanismin, valtionhallinnon tason päätöksenteon ja koordinaation epäyhtenäisyys sekä puutteellisuudet. Toimenpiteiden kytkeytyminen toteutusohjelmiin ja varautumisen tarkastelun mahdollistava raportointi on puutteellista.

Varautumisen vaatimukset muodostetaan prosessissa, johon osallistuvat hallinnonalat ja virastot osallistuvat. Toimenpiteiden ohjaaminen ja raportointi toteutetaan normaalin toiminnanohjauksen yhteydessä. Näitä ovat muun muassa strateginen suunnittelu, arkkitehtuurien määrittäminen, TTS-suunnittelu, laatu järjestelmä, hankeohjaus ja hankintojen ohjaus. Tukevia toimintoja ovat muun muassa raportointi sekä tarkastustoiminta, kuten controller-toiminta, sisäinen tarkastus ja erilaiset auditoinnit.

Kuva 19. ICT-varautumisen ohjauksen kehittämisen kohdealueet, sisältö ja päätoimijat



Varautumisen toimenpiteiden käynnistäminen, ohjaus ja raportointi tulee sisällyttää kaikkiin keskeisiin suunnittelu- ja toteutusvaiheisiin omaksi kohdakseen. Kaikilla vaiheilla tulee olla selkeä omistaja ja päätöksentekomenettely. Prosessia on kyettävä tarkastelemaan vaatimuksien asettamisesta raportointiin sekä poikkihallinnollisesti että hallinnonaloittain.

3.3.2 ICT-varautumisen ohjauksen kehittämistyö

Tavoite ICT-varautumisen ohjauksen kehittämisessä:

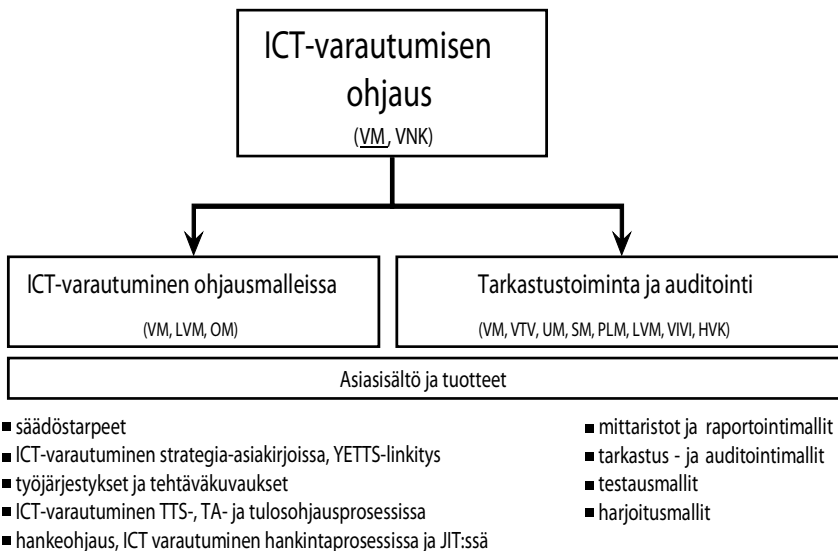
ICT-varautuminen on kiinteä osa valtion tietohallinnon kehittämistä ja toteuttamista ohjaavissa strategioissa ja muissa asiakirjoissa. ICT-varautumiselle asetetaan kaikilla tasoilla selkeät tavoitteet, resurssit ja mittarit osana normaalia tulosohtausprosessia ja tarkastustoimintaa.

Vuoden 2010 loppuun mennessä ICT-varautuminen on osa strategia- ja tulosohtausprosessia sekä organisaatioiden ja henkilöstön tehtäviä. Valtionhallintoon on laadittu yhtenäiset ICT-varautumisen suunnittelumallit ja tarkistuslistat.

Vuoden 2012 loppuun mennessä ICT-varautumisen tulostavoitteiden mukaista toteuttamista mitataan ja raportoidaan hallinnonaloittain.

ICT-varautumisen vaatimustenhallinta, erilaiset ohjausmekanismit ja raportointi on kytkettävä yhdeksi saumattomasti hallinnon eri tasojen välillä toimivaksi kokonaisuudeksi. Erityisesti ohjauksessa ja raportoinnissa on hyödynnettävä mahdollisimman hyvin nykyisiä mekanismeja ja lähinnä tarkennettava niiden toimintaa. Prosessista on luotava sellainen, että sen avulla voidaan muodostaa nykyisestä hajanaisesta tilanteesta yhtenäinen ja myös ylläpitää määriteltä ICT-varautumista. Kehittämisaalueen sisältö ja päätoimijat on esitetty seuraavassa kuvassa.

Kuva 20. ICT-varautumisen ohjauksen kehittämisen kohdealueet, sisältö ja päätoimijat



Saavutettavat hyödyt:

ICT-varautumisen kytkeminen tiiviisti tulosohjausprosessiin mahdollistaa tarpeisiin perustuvien tavoitteiden asettamisen, oikein mitoitettujen resurssien osoittamisen sekä saavutettujen tulosten todentamisen. Tämä mahdollistaa järjestelmien toteuttamisen hallinnonaloilla kokonaistaloudellisesti siten, että niiden toiminta jatkuu hallitusti sekä häiriötilanteissa että vaikeissa erityistilanteissa.

ICT-varautumisen ohjaus -osahankkeeseen sisältyvät seuraavat linjaorganisaatiossa toteutettavat hallinnon kehittämistoimenpiteet sekä muissa hankkeissa huomioon otettavat ja toteutettavat ICT-varautumisen kehittämistarpeet.

Taulukko 11. ICT-varautumisen ohjauksen kehittämistoimenpiteitä

ICT-varautumisen ohjaus	Tulos / sisältö	Tekijä	Valmis
Linjaorganisaation kehittämistoimenpiteet			
Tehtävät ja vastuut	ICT-varautumisen tehtävät ja vastuut näkyvät organisaatioiden työjärjestyksissä kaikilla tasoilla	VNK, VM Ministeriöt, virastot	2009
	ICT-varautuminen näkyy henkilöstön tehtäväkuvauksissa	Ministeriöt ja virastot	2010
Strategiat ja suunnittelu	ICT-varautumiselle on asetettu tavoitteet strategia-asiakirjoissa	VNK, VM Ministeriöt, virastot	2010
	ICT-varautumisen suunnittelu-, työjärjestys- ja tehtäväkuvausmallit ja tarkistuslistat	VM, ministeriöt, virastot	2009
Tulosohjaus	ICT-varautumisen tavoitteet ohjaavat toimintaa virastojen tasolle asti osana tulosohjausprosessia	Hallinnonalat	2011
Raportointi ja tarkastustoiminta	ICT-varautumisen toteuttamista seurataan osana muuta raportointia ja tarkastustoimintaa	Hallinnonalat	2011
Kehittämistarpeet hankkeissa			
Raportointi-, tarkastus- ja auditointikäytännöt	Määritellään sisältö, prosessit ja vastuut toteutuksen organisoimille. Otetaan huomioon sisäiset ja ulkoiset toimijat sekä kohteina että toteuttajina		2009 – 2011

3.4 ICT-varautumisen tilannetietojen kehittäminen

Toimintaa tukevan ICT-varautumisen kehittäminen edellyttää laajaa ICT-tilanteen ja sen kehityslinjausten tuntemista. Erityistilanteiden hoitamista varten tulee kyetä muodostamaan lähes reaaliaikaisista tilannetiedoista valtion ICT-toiminnan tilannekuva, joka on kyettävä esittämään ja jakamaan valtionhallinnon sisällä eri tilannekuvajärjestelmissä. Tilannetietoisuus on myös perusedellytys totuudenmukaiselle ja oikea-aikaiselle sisäiselle ja ulkoiselle viestinnälle.

3.4.1 ICT-varautumisen tilannetietojen kehittämistyö

Osittain reaaliaikaisen tilannekuvajärjestelyn tulee tukea häiriö- ja erityistilanteiden analysointia, päätöksentekoa, toimenpiteiden vastuutusta ja ohjausta sekä priorisoidun tiedon jakelujärjestelyjä.

Kehittämisen tilannekuvaa valtionhallinnon käytössä olevasta tietotekniikasta ja sen käyttötavoista tulee kerätä myös analyysissä syvemmälle ulottuvana. Tämän on mahdollistettava toimintojen, järjestelmien ja palvelujen, sekä näiden suojaamis-, toipumis- ja vastatoimenpiteiden kehittäminen. Kehittämiseen tarvittavien tietojen tuottamiseen osallistuvat käyttäjäorganisaatiot, erilaiset toimittajaosapuolet, palveluyksiköt sekä ohjausta, kehittämistä ja tutkimusta suorittavat organisaatiot. Tiedot tulee kerätä pääosin nykyisten raportointijärjestelmien avulla.

Tavoite ICT-varautumisen tilannetietojen kehittämisessä:

Hallinnonaloilta saadaan yhdenmukainen ICT-tilannetieto osana normaalia raportointia ja tilastointia. Tämä mahdollistaa valtionhallinnon kokonaisuudessa ja hallinnonaloilla varautumisen kustannustehokkaan ja tarkoituksenmukaisen kehittämisen.

Kyetään tuottamaan päätöksenteon perustaksi häiriö- ja erityistilanteiden hallinnan edellyttämä tieto hallinnonalojen järjestelmistä ja niiden merkityksestä erityistilanteessa sekä käyttöön saatavista resursseista.

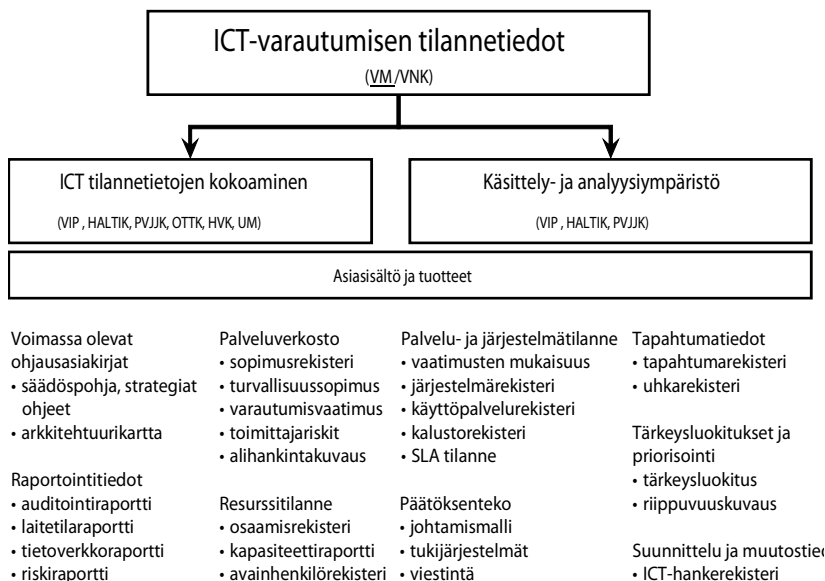
Vuoden 2010 loppuun mennessä on määritetty tietotarpeet ja raportointimenettelyt osaksi hallinnonalojen ja virastojen normaalia raportointia ja tilastointia.

Vuoden 2012 loppuun mennessä raportointiin perustuen on luotu ja otettu käyttöön tiedon hallinta-, analysointi- ja esittämismenetelmät ICT-varautumisen kehittämisen tueksi.

Vuoden 2016 loppuun mennessä YETTS-erityistilanteiden hoitamisen edellyttämä varautumisen tilannetieto kyetään keräämään hallinnonaloilta ja niiden järjestelmistä sekä esittämään tilannekuvajärjestelmissä.

ICT-varautumisen tilannetiedot -osahankkeen rakenne ja päätoimijat on esitetty seuraavassa kuvassa.

Kuva 21. ICT-varautumisen tilannetiedot –osahanke



Saavutettavat hyödyt

Tilannetietojen kokoamisella ja analysoinnilla mahdollistetaan hallinnonaloilta ja ulkopuolisilta toimijoilta saatavan tilannetiedon yhdistely, analysointi ja jakaminen ICT-varautumisen kehittämisen ohjauksen ja häiriötilanteisiin liittyvän päätöksenteon tueksi.

Tilannekuvan keräämisellä parannetaan tietohallinnon ja tietotekniikan suunnittelua siten, että varautumiseen ja jatkuvuuteen liittyviä tekijöitä kehitetään riittävän aikaisessa vaiheessa ja kokonaisuutena. Tämä mahdollistaa laadukkaan ja kustannustehokkaan lopputuloksen käytettävissä olevilla resursseilla.

ICT-varautumisen tilannetiedot -osahankkeeseen sisältyvät seuraavat linjaorganisaatioissa toteutettavat hallinnon kehittämistoimenpiteet sekä muissa hankkeissa huomioon otettavat ja toteutettavat ICT-varautumisen kehittämistarpeet.

Taulukko 12. ICT-varautumisen tilannetietojen kehittämistoimenpiteitä

ICT-varautumisen tilannetiedot	Tulos / sisältö	Tekijä	Valmis
Linjaorganisaation kehittämistoimenpiteet			
Tilannetiedot	Kehittämisen edellyttämien tietosisältöjen ja tuottamisen hallinnonalakohtainen määrittäminen	Ministeriöt Virastot	2010
	Häiriö- ja erityistilanteiden hoitamisen edellyttämän ICT:n tietosisältöjen määrittäminen	Ministeriöt	2010
Keräämis-, analysointi- ja esittämismenetelmät	Tietojen keräämis-, analysointi- ja esittämistarpeiden määrittely	VNK Ministeriöt Virastot	2011
	Häiriö- ja erityistilanteiden hoitamisen edellyttämän ICT:n tilannetietojen keräämis-, analysointi- ja esittämismenetelmien käyttöönoton suunnittelu	VNK / VARE Hallinnonalat	2012
Kehittämistarpeet hankkeissa			
ValtIT/VAHTI 24/7 -hanke	Valtionhallinnon ICT-palvelujen ympärivuorokautinen päivystys ja valvonta	VM/VAHTI	2009 - 2012
Kehittämisen tilannetiedot	Prosessit ja raportointimallit kehittämisen tietojen kokoamiseksi ja esittämiseksi olemassa olevia järjestelmiä käyttäen		2009 - 2010
Eryitystilanteiden hallinnan tilannekuva	Prosessit ja raportointimallit kehittämisen tietojen kokoamiseksi eri järjestelmistä ja esittämiseksi olemassa olevia järjestelmiä käyttäen		2009 - 2012
Käsittely- ja analysointiympäristöt	Normaaliolojen suunnittelussa ja erityistilanteiden hallinnassa tarvittava turvaluokiteltu yhteistoimintaympäristö	2009 - 2012	

3.5 ICT-varautumisen uhka- ja riskianalyysin kehittäminen

3.5.1 Perusteet

Uhka-arvio on edellytys riskianalyysin sekä valmius- ja jatkuvuussuunnittelun toteuttamiselle. Yhtenäisellä uhka-arviorakenteella mahdollistetaan toimenpiteiden oikea ja kustannustehokas kohdentaminen.

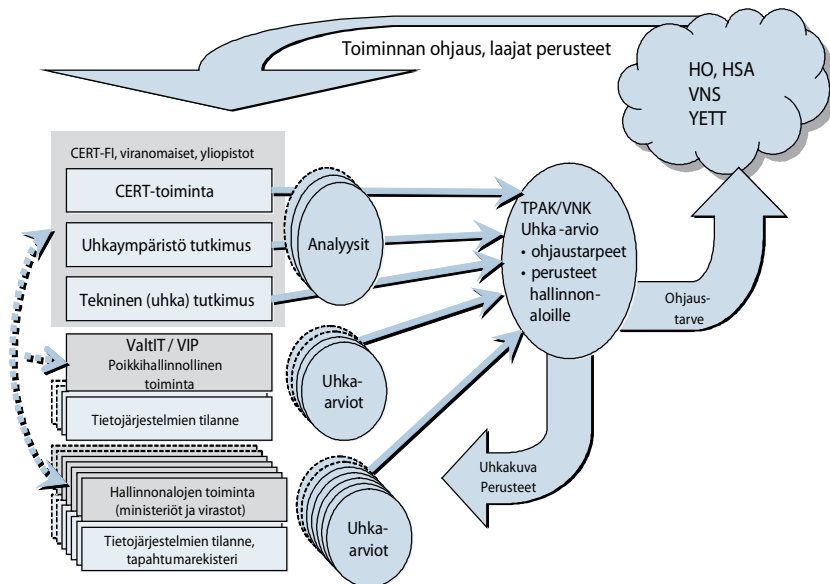
Yhteisen prosessin tulee käyttää perusteinaan YETT-strategian mukaisia erityistilanteita ja hallinnonalojen erityistehtäviä sekä sitoa nämä hallinnonaloilla toteutettaviin jatkuvuuden ja häiriötilanteiden hallinnan sekä palautumisen toimenpiteisiin.

Uhka-arvion tulee perustua ajantasaiseen tietoon uhka-ympäristöstä, uhkien kohdistumisesta suojattavaan toimintaan, haavoittuvuuksista sekä mahdollisuuksista suojautua uhkia vastaan. Sen tulee huomioida toimintaan kohdistuvan uhan vaikutukset tietoteknisiin järjestelmiin.

Uhka-arvio on kytkettävä riskianalyysin osaksi. Näiden tulee olla kaikilla hallinnon tasoilla säännönmukaisesti toistettava prosessi. Prosessin aikataulutus on kytkettävä strategia-asiakirjojen valmisteluun, TTS-suunnitelman laatimiseen, vuotuisen budjetointiin sekä hankehallintaan.

Seuraavassa kuvassa on esitetty malli uhkatilanteen ja -arvion tuottamisesta.

Kuva 22. Uhka-arvioprosessi



3.5.2 ICT-varautumisen uhka- ja riskianalyysin kehittämistyö

Luodaan yhtenäinen prosessi valtionhallinnon kokonaisuuden, hallinnonalojen ja poikkihallinnollisten tietohallinnollisten ja tietoteknisten ympäristöjen kokonaisriskinhallintaan. Ajantasaisen uhka-analyysin tuottaminen on oltava jatkuvaa virastojen riskikartoitusten ja ennakoivan varautumisen tarpeisiin.

Tavoite ICT-varautumisen uhka- ja riskianalyysin kehittämisessä:

Uhka-arvion ja riskienhallinnan yhtenäistämiseksi on käytössä yhteinen prosessi ja ohjeistus, jotka palvelevat valtionhallinnon, virastojen sekä poikkihallinnollisten toimintojen tasoa.

Uhka-arvioon liittyvien tietojen jatkuva systemaattinen kerääminen ja analysointi sekä riskienhallintaa että oman toiminnan kehittämistä varten on toteutettu.

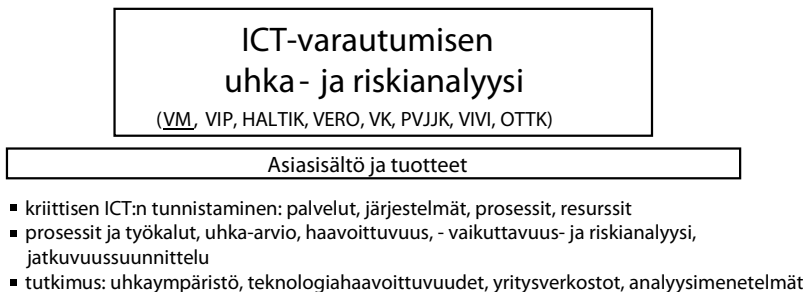
Vuoden 2010 loppuun mennessä on luotu ja testattu menettelyt uhka-arvion tuottamiseksi yhdenmukaisesti valtioneuvoston tasolta viraston tasolle. On laadittu ICT varautumisen tutkimusstrategia.

Vuoden 2012 loppuun mennessä uhka-arviomenettely on ulotettu koko palveluntuotantoketjuun. ICT-varautumisen riskienhallinta on määritetty ja pilotoitu. Koordinoitu tutkimustoiminta on käynnistetty.

Vuoden 2016 loppuun mennessä ICT-varautumisen riskienhallintaprosessi ja sitä tukevat työkalut on otettu käyttöön koko palveluverkossa.

Kehittämisalueen sisältö ja päätoimijat on esitetty seuraavassa kuvassa.

Kuva 23. ICT-varautumisen uhka- ja riskianalyysi –osahankkeen resurssitarve ja aikataulu



Saavutettavat hyödyt:

Yhtenäistämällä uhka- ja riskiarviointimenettelyjä säästetään suunnittelutyötä, yhtenäistetään toimintamalleja, kohdennetaan varautumisen toimenpiteet ja resurssit kokonaisuuden kannalta tasapainoisesti ja tarkoituksenmukaisesti sekä mahdollistetaan myös kansainvälisesti verkostoituneet palvelut tunnistetulla ja hyväksyttävällä riskitasolla.

ICT-varautumisen uhka- ja riskianalyysi -osahankkeeseen sisältyvät seuraavat linjaorganisaatiossa toteutettavat hallinnon kehittämistoimenpiteet sekä muissa hankkeissa huomioon otettavat ja toteutettavat ICT-varautumisen kehittämistarpeet.

Taulukko 13. ICT-varautumisen uhka- ja riskianalyysiin liittyviä kehittämis-toimenpiteitä

ICT-varautumisen uhka- ja riskianalyysi	Tulos / sisältö	Tekijä	Valmis
Linjaorganisaation kehittämistoimenpiteet			
Kriittisen ICT:n tunnistaminen	Määritetään keskeisimpiä toimintoprosesseja tukeva organisaatiolle välttämätön kriittinen ICT	VNK /VARE Hallinnonalat	2009
Uhkamallit	Täydennetään YETTS:an pohjautuvat yhteiset ICT-varautumisen uhkamallit	VM / VNK	2009
Tutkimus	Laaditaan tutkimusstrategia ja -suunnitelma	VM/HVK	2010
Riskienhallinta	Tarkennetaan ICT-varautumisen kannalta jatkuvuussuunnitelmien mallit virastotasoille	VIP Hallinnonalat	2010
	Toteutetaan hallinnonalojen ICT-varautumisen uhka- ja riskiarviot sekä toistetaan ne säännöllisesti	Hallinnonalat	2012
Kehittämistarpeet hankkeissa			
	Yhteistoiminta VERO:n riskienhallinta-hankkeen kanssa		

3.6 ICT-varautumisen osaamisen hallinnan kehittäminen

3.6.1 Perusteet

Osaaminen muodostaa keskeisen voimavaran ICT-varautumisessa. Jatkuvuuden takaaminen edellyttää palvelujen tuottamisessa ja käyttämisessä keskeisten osaamistarpeiden tunnistamista. Palvelujen edellyttämät käytössä olevat ja käyttöön saatavat osaamisresurssit on hallittava eri turvallisuustilanteissa. Vaikeissa erityistilanteissa käyttöön saatavat henkilöresurssit ovat usein huomattavasti normaalitilannetta vähäisemmät. Osaamisen hankkiminen, kehittäminen ja ylläpitäminen sekä valtionhallinnon sisällä että toimittajaketjussa on mitoitettava oikein.

Osaaminen voidaan erotella koskemaan varautumisen perusteita ja mekanismeja, varautumisen tavoitteita ja toteutusta sekä teknisiä toteutustapoja. Osaaminen ja sille kohdistettavat vaatimukset ovat myös varsin erilaisia riippuen hallinnon tasosta ja toimialasta. Vaatimukset ulottuvat tietohallinnon henkilöstön lisäksi myös ylimpään johtoon ja tietotekniikan käyttäjiin.

Valtionhallinnon omaa osaamista täydentää palvelutoimittajien verkostossa oleva osaaminen. Myös tälle on asetettava yhtenevät osaamistarpeet ja -vaatimukset erityistilanteiden ja poikkeusolojen näkökulmasta.

Määrittämisellä ja yhtenäistämällä mahdollistetaan osaamisen voimavarojen keskittäminen ja yhteiskäyttö, vaatimusten asettaminen palvelutoimittajille ja siten oman osaamisen järjestelmällinen täydentäminen sekä osaamisen tarkoituksenmukainen kehittäminen henkilöstön koulutuksella, harjoitustoiminnalla, rekrytoinnilla sekä osaamista tukevien järjestelmien ja toimintamallien kehittämisellä. Osaamisen hallinnan on otettava huomioon myös erityistilanteissa tarvittava ja poikkeussäännöksillä mahdollisesti käyttöön saatava osaaminen.

Osaamisen hallinnan on oltava jatkuva prosessi, jonka avulla osaaminen kyetään sopeuttamaan riittävän aikaisessa vaiheessa muun muassa ICT-varautumisen edellyttämiin osaamistarpeisiin. ICT-varautumisen osaamista tulee kehittää saman prosessin yhteydessä kuin muutakin osaamista.

3.6.2 ICT-varautumisen osaamisen hallinnan kehittämistyö

Tavoite osaamisen hallinnan kehittämisessä:

Palvelujen jatkuvuuden edellyttämä osaaminen varautumisen kehittämisessä sekä häiriö- ja erityistilanteiden hoitamisessa kyetään varmistamaan asetettujen vaatimusten mukaisesti koko palveluntuotantoverkoston resursseja hyödyntäen. Kriittisten toimintojen osaamistarpeet on tunnistettu, henkilöstöön kohdistuvat vaatimukset on määritetty ja nämä on huomioitu tehtäväkuvauksissa, tehtäväkierrossa, rekrytoinnissa sekä koulutusjärjestelyissä.

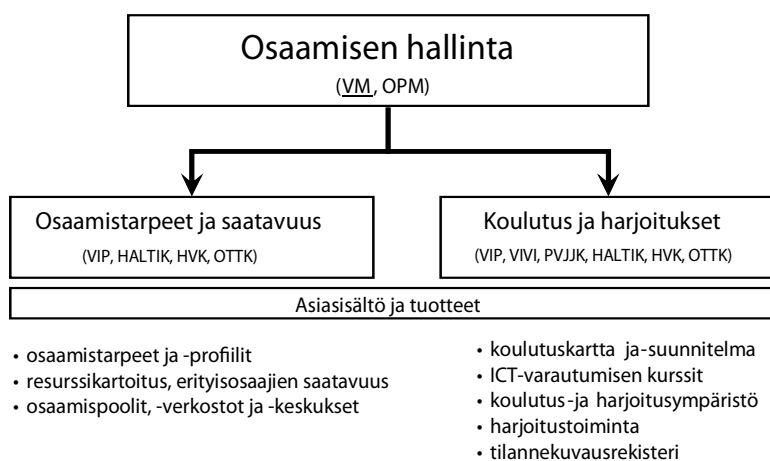
Vuoden 2010 loppuun mennessä hallinnonaloittain on kartoitettu kriittiset osaamistarpeet ja niiden edellyttämät osaamisresurssit sekä keskitetysti määritetty ICT-varautumisen toteuttamista tukeva harjoitusrakenne.

Vuoden 2012 loppuun mennessä ICT-varautumisen edellyttämät koulutusjärjestelyt on toteutettu ja ICT-varautumisen osaamisen hallinta on osana muuta osaamisen hallintaa.

Vuoden 2016 loppuun mennessä on luotu tarvittavat osaamiskeskukset valti-onhallintoon ja palveluyrityksiin sekä luotu koko palveluverkostoon ulottuvat osaamispoolit.

Hankkeessa on määritettävä eri tehtävätasojille ja osaamisalueille osaamistarpeet ja vaatimukset, kuten määrä, laatu, tekninen tukeminen, palveluverkostolta edellytettävä osaaminen ja osaamisen täydentäminen erilaisissa tilanteissa. Erityinen painopiste on kriittisimpien osaamistarpeiden määrittäminen koko palveluketjuun. Kehittämisaalueen sisältö ja päätoimijat on esitetty seuraavassa kuvassa.

Kuva 24. ICT-varautumisen osaamisen hallinnan kehittämisen kohdealueet, sisältö ja päätoimijat



Saavutettavat hyödyt:

Kriittisen toiminnan edellyttämä osaaminen on käytettävissä häiriö- ja erityis-tilanteissa. Kyetään hyödyntämään valtionhallinnon organisaatioissa ja palveluntoimittajilla olevaa erityisosaamista poikkihallinnollisesti. Osaamista kyetään varmistaa ja kehittää henkilöstömuutosten sekä muuttuvien uhkakuvien ja vaatimusten mukaisesti. Harjoitustoiminnalla kyetään kehittämään ja varmentamaan palveluketjun toimivuutta erityistilanteissa.

ICT-varautumisen osaamisen hallinta -osahankkeeseen sisältyvät seuraavat linjaorganisaatiossa toteutettavat hallinnon kehittämistoimenpiteet sekä muissa hankkeissa huomioon otettavat ja toteutettavat ICT-varautumisen kehittämistarpeet.

Taulukko 14. ICT-varautumisen osaamisen hallinnan kehittämistoimenpiteitä

ICT-varautumisen osaamisen hallinta	Tulos / sisältö	Tekijä	Valmis
Linjaorganisaation kehittämistoimenpiteet			
Osaamisen hallinta	Keskeisten palvelujen kriittisten osaamistarpeiden kartoittaminen	Ministeriöt Virastot	2009
	Tarvittavien kriittisten osaamisresurssien palvelukohtainen määrittely	Ministeriöt Virastot	2010
	Kriittisen toiminnan edellyttämä ICT-varautumisen osaamisen hallinta on toteutettu osana henkilöstöhallintoa	Ministeriöt Virastot	2012
Koulutus	Koulutustarpeet on määritetty ja koulutussuunnitelmat on tehty	Ministeriöt Virastot	2011
Harjoitukset	ICT-varautumisen harjoitusrakenne on määritetty	VM / VARE Hallinnonalat	2011

3.7 Palveluverkoston hallinnan ja hyödyntämisen kehittäminen

3.7.1 Perusteet

Pääosa valtion ICT-toiminnasta on sidoksissa ulkoisten palveluntarjoajien tuottamiin keskenään verkottuneisiin ja osin voimakkaasti keskittyneisiin palveluihin. Toimittajien resurssien käytettävyys eri turvallisuustilanteissa tulee varmistaa. Verkoston hallinta edellyttää valtionhallinnossa yhtenäisiä vaatimustenhallinta-, hankinta-, sopimus- ja auditointimenettelyjä. Toimittajien väliset sopimukset ja auditoinnit ovat merkittävässä roolissa.

ICT-varautumisen kannalta on välttämätöntä, että kaikki palvelujen tuottamiseen osallistuvat osapuolet on sitoutettu asetettujen vaatimusten toteuttamiseen ja vaatimusten toteuttaminen on todennettu. Palveluntuotannon järjestelyillä, kuten toimittajakentän hajauttamisella, voidaan myös toteuttaa ICT-varautumista.

Keskeisiä elementtejä ICT-varautumisen kannalta ovat palvelujen kilpailutuksessa asetetut vaatimukset ja valintakriteeristöt, palvelusopimukset, alihankintasopimusten hallinta sekä koko sopimusjärjestelmän ja palveluntoimittajien toimintamallin arviointi, katselmointi, auditointi ja raportointi. Näille elementeille on olemassa vakiintuneet ja jopa hankintalain tasolla ohjatut prosessit, keskitetyt ja hajautetut mekanismit sekä ohjeistukset ja koulutusjärjestelyt. Haasteena on sisällyttää ICT-varautumisen edellyttämät sisällöt näihin prosesseihin, mekanismeihin, ohjeistukseen ja koulutukseen. Asioita käsitellään myös Huoltovarmuuskeskuksen SOPIVA-hankkeessa.

3.7.2 Palveluverkoston hallinnan ja hyödyntämisen kehittämistyö

Tavoite palveluverkoston hallinnan ja hyödyntämisen kehittämiseksi:

Valtionhallinnon ja kriittisten palvelujen tuottajaverkosto on saumatonta ja pitkäjänteistä yhteistoimintaa, jota ohjaavat yhteiset tavoitteet, vaatimukset ja periaatteet. Sopimusrakenteet sekä yritysten että valtionhallinnon palveluyksiköiden kanssa koko valtionhallinnossa ovat yhdenmukaiset ja tärkeimmiltä osin keskitetysti toteutetut erityistilanteet ja poikkeusolot huomioon ottaen.

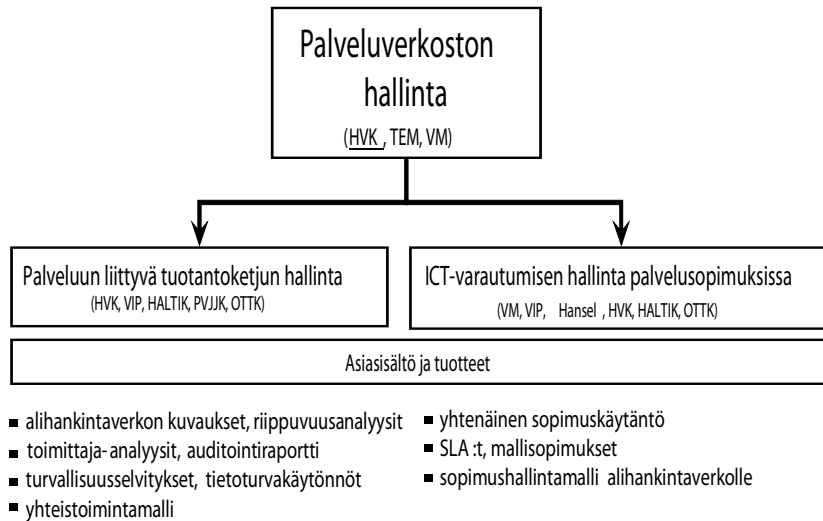
Vuoden 2010 loppuun mennessä kriittisten palveluiden ja järjestelmien toimittajaverkko on kuvattu ja yhtenäiset sopimuskäytännöt määritetty

Vuoden 2012 loppuun mennessä ICT-varautuminen on huomioitu kaikissa hankinnoissa ja yhtenäiset sopimusmallit on otettu käyttöön. Hallinnon ja toimittajien vastuut ja velvoitteet varautumisen toteuttamisessa, auditoinnissa ja raportoinnissa on yhtenäistetty.

Vuoden 2016 loppuun mennessä palveluverkoston ICT-varautumisessa hyödynnetään saumattomasti ja täysimääräisesti hallinnon ja toimittajaverkoston osaamista ja resursseja.

Hankkeessa määritetään sisäisiltä ja ulkoisilta ICT-palvelusopimuksilta edellytettävät palveluun, palveluverkostoon ja muihin alihankintoihin liittyvät ICT-varautumisen asiasisällöt, malli alihankintaverkoston sopimushallinnasta sekä malli koko sopimusjärjestelmän arvioinnista, katselmoinnista, auditoinnista sekä raportoinnista. Erityisenä haasteena on taata kriittisten palvelujen jatkuvuus häiriötilanteiden lisäksi myös YETT-strategian mukaisissa erityistilanteissa ja poikkeusoloissa. Kehittämisalueen sisältö ja päätoimijat on esitetty seuraavassa kuvassa.

Kuva 25. Palveluverkoston hallinnan ja hyödyntämisen kehittämisen kohdealueet, sisältö ja päätoimijat



Saavutettavat hyödyt:

Hankkeen avulla yhdenmukaistetaan ja parannetaan ICT-varautumisen toteutusta, mahdollistetaan palvelusopimusten ulottaminen kaikkiin erityistilanteisiin, helpotetaan palvelusopimusten laadintaa ja kontrollointia sekä luodaan palveluntuotannon ohjausmahdollisuus eri hallinnon tasoille valtionhallinnon kokonaisuudesta hankkeiden tasolle.

Palveluverkoston hallinta ja hyödyntäminen -osahankkeeseen sisältyvät seuraavat linjaorganisaatiossa toteutettavat hallinnon kehittämistoimenpiteet sekä muissa hankkeissa huomioon otettavat ja toteutettavat ICT-varautumisen kehittämistarpeet.

Taulukko 15. Palveluverkoston hallinnan ja hyödyntämisen kehittäminen

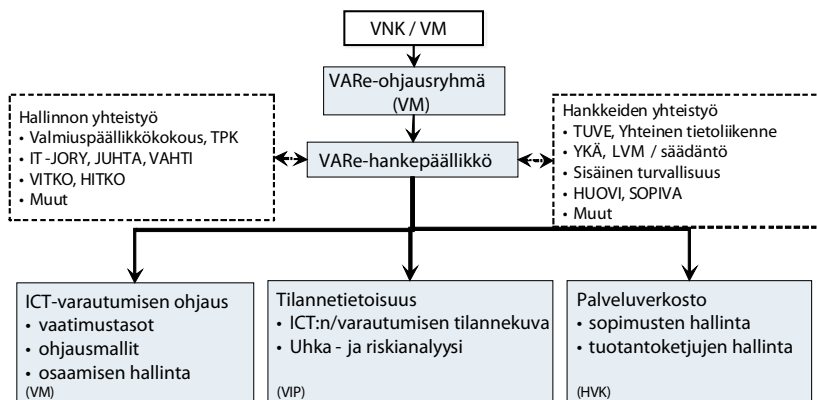
Palveluverkoston hallinta ja hyödyntäminen	Tulos / sisältö	Tekijä	Valmis
Linjaorganisaation kehittämistoimenpiteet			
Toimittajaverkon tunnistaminen	Valtionhallinto ja hallinnonalat ovat tunnistaneet ja kuvanneet kriittisten palveluittensa ja järjestelmiensä sisäisen ja ulkoisen toimittajaverkon mukaan lukien alihankkijat	ValtiIT Hallinnonalat	2009
	Valtionhallinto ja hallinnonalat ovat tunnistaneet ja kuvanneet kaikkien palveluittensa ja järjestelmiensä sisäisen ja ulkoisen toimittajaverkon mukaan lukien alihankkijat	ValtiIT Hallinnonalat	2012
Sopimusmenettelyt ja hankinnat	Hallinnonalat ovat kartoittaneet ICT-varautumisen sopimustarpeet	Ministeriöt Virastot	2009
	Yhtenäiset sopimusmenettelyt on otettu käyttöön hallinnossa ja kumppanuusverkostossa	VM / VIP Hallinnonalat	2012
	Keskitettyssä hankintaohjauksessa on otettu huomioon ICT-varautumisen tarpeet (JIT, Hansel ...)	VM / VIP Hansel	2011
	Keskitettyissä ja hallinnonalojen hankinnoissa on otettu ICT-varautuminen huomioon	Hallinnonalat	2011
Kehittämistarpeet hankkeissa			
HVK / SOPIVA	ICT-varautumisen vastuut palvelun-toimittajaverkostoissa	HVK	

4 Hankekartta

4.1 ICT-varautumisen kehittämisen organisointi

ICT-varautumisen hankekokonaisuuden toteuttaminen tehdään pääosin yhteisissä kärkihankkeissa ja hallinnonalojen kehittämisessä.

Kuva 26. Suunniteltu ICT-varautumisen kehittämisen organisointi



ICT-varautumisen hankkeen toteuttaminen:

1. Organisoidaan ICT-varautumisen hanke (VARE):

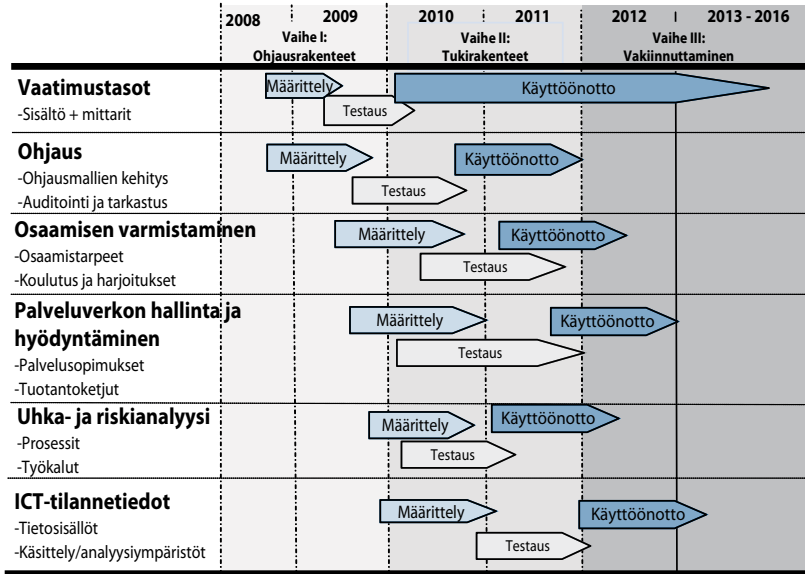
- Perustetaan VARE-ohjausryhmä (VVK, ValtIT, TPAK, OPM, TEM, LVM, PLM, SM).
 - o Kokoontuu 4 – 5 kertaa vuodessa
 - o Ohjaa VARE-hankkeen toteutusta ja resursointia siten, että hallinnon tarpeet otetaan huomioon
 - o Ohjausryhmänä voisi toimia myös esimerkiksi VAHTI-johtoryhmä

- Seurantaryhmänä hyödynnetään hallinnossa jo toimivia ohjaus-, koordinaatio- ja yhteistyöryhmiä, kuten Valmiuspäällikkökokous, TPAK, Valtion IT-johtoryhmä, Valtion IT-koordinaatioryhmä, VAHTI-johtoryhmä,
 - o Vastaa hallinnonalojen ja virastojen näkemysten esille tuomisesta valmisteluasiakirjoihin sekä hallinnon informoinnista
- ICT-varautumisen hankekokonaisuutta johtaa VARE-hankepäällikkö/-koordinaattori.
 - o Vastaa VARE-hankekokonaisuuden hallinnasta ja VARE-osahankkeiden ohjauksesta
 - o Esittelee hankkeen asiat seurantaryhmissä
 - o Raportoi VM:n johdolle ja informoi VNK:a
- Hankkeen eri kehittämisalueille nimetään tarpeen mukaan projektiryhmä (noin 6 henkilöä).
 - o Vastaa osahankkeen ja sen projektien suunnitelman mukaisesta toteuttamisesta
 - o Raportoi VARE-hankepäällikölle
- 2. Käynnistetään tiivistetty varautumisen hankkeiden yhteistoiminta
 - Eri hankkeiden hankepäälliköiden yhteistoimintatapaamiset
 - o Kokoontuu tarvittaessa, hyödyntää aktiivisesti työryhmäohjelmistoa
 - o Edustus keskeisimmistä ICT-varautumiseen liittyvistä valtionhallinnon varautumis-, turvallisuus- ja tietoturvahankkeista.
 - o Koordinoi ja yhteensovittaa hallinnonalojen varautumis-, turvallisuus- ja tietoturvahankkeiden tavoitteita, toteutusta ja resurssien yhteiskäyttöä siten, että maksimoidaan toisten hankkeiden työn hyödyntäminen ja minimoidaan päällekkäisyydet.

4.2 Hankkeen aikataulu ja resursointi

ICT-varautumisen jatkotoimenpiteet esitetään toteutettavaksi seuraavan hankkartan mukaisesti.

Kuva 27. Esitys ICT-varautumisen kehittämisen aikatauluksi



ICT-varautumisen kehittäminen edellyttää VM:ssä keskitettyjä hankeresursseja seuraavan taulukon mukaisesti.

Taulukko16. ICT-varautumisen keskitettyjen resurssien tarve

	2008	2009	2010	2011	2012	2013	2014	2015	2016
Hankejohto (VM/VIP) htv	0,4	1,5	3,4	2,2	1,2	0,7	0,6	0,4	0,4
Muu hallinto htv	0,3	2,3	5,7	4,6	3,1	2,0	1,7	1,1	1,0
Rahoitustarve M€	0,07	0,37	1,08	0,94	0,16	0,04	0,04	0,04	0,04

Esitetyillä laskentaperusteilla kehittämisen kokonaiskustannukset vuoteen 2016 asti ovat noin 3 M€ ja 33 henkilötyövuotta.

ICT-varautumisen toteuttaminen edellyttää hallinnossa sisäistä resursointia. Työmäärissä voi olla suuriakin viraston koosta, tehtävästä ja lähtötasosta riippuvia eroja. Vuosina 2010 – 2012 virastosta riippuen edellytetään minimissään 0,5 – 2 henkilötyövuoden kohdentamista ICT-varautumisen toteuttamiseen.

Arvio käyttöönoton edellyttämästä työpanoksesta ministeriöissä ja keskeisissä virastoissa on seuraavassa taulukossa.

	2008	2009	2010	2011	2012	2013	2014	2015	2016	Yht.
Hankejohto (VM/VIP) htv	0,1	1,1	2,0	1,7	1,2	1,0	0,7	0,5	0,5	9
Muu hallinto htv	0,1	1,2	2,5	1,9	1,7	1,4	1,2	1,0	0,9	12
Rahoitustarve M€	0,1	1,8	3,3	2,8	2,4	2,4	2,1	2,0	2,0	19

Tarvittava työ voidaan suurelta osin tehdä myös henkilöstön tehtäväkuva-uksia tarkentamalla, töiden priorisoinnilla ja päällekkäisyyksiä vähentämällä, jolloin ei synny merkittäviä lisäkustannuksia. Tietohallinto-, tietoturva-, turvallisuus- ja valmiushenkilöstön ICT-varautumisen vastuut ja velvoitteet tulee tarkastella ja koordinoita huolellisesti. Jokaiselle hallinnonalalle tulisi määrittää vastuuhenkilö, jonka tehtävänä on ohjata ja koordinoita ICT-hankkeen toteuttaminen hallinnonalalla. Tämä tulisi näkyä henkilön tehtäväkuvauksessa ja tulostavoitteissa.

4.3 Valtion ICT-varautumishankkeen riskianalyysi

Taulukko 17. ICT-varautumisen hankkeen riskianalyysi

Riskin nimi / kuvaus	Merkitys	Toimenpiteet
Ohjauksen, koordinaation, päätöksenteon ja viestinnän hajautuminen ja puutteellisuus	- Hanke hajautuu - Hallinnonalojen sitoutuminen heikkenee - Toteutuksen aikataulu- ja resurssiongelmat lisääntyvät	- Johdon ja eri osapuolien sitoutuminen tavoitteisiin - Yksiselitteiset ja selkeät ohjausmallit, vastuut ja raportointimenettelyt - Olemassa olevien johdon- ja työryhmien hyödyntäminen sekä niiden tehtävien ja vastuiden tarkentaminen
Hankkeeseen ei voida kohdentaa riittäviä henkilöstö- ja raharesursseja	Toteutuksen syvyydestä ja laadusta joudutaan tinkimään -> jatkuvuus vaikeissa erityistilanteissa ei toteudu	- Aikataulujen, sisällön ja resurssien yhteensovittaminen ja tavoitteiden uudelleen arviointi - Elinkeinoelämän ja HVK/poolien hyödyntäminen
Hanke laajenee ja sisäinen hallinta epäonnistuu	- Tuloksissa ei päästä konkreettisuuteen - Toteutus epäyhtenäinen - Resurssien kohdentaminen epäonnistuu	- Hankejohdon kyvykkyys ja toimintaedellytykset - Selkeä hanke- ja projekti-johtaminen - Yhtenäiset ja säännönmukainen suunnittelu-, seuranta-, raportointi- ja auditointimenettelyt
ICT-varautumisen tavoite ja toteutus ei seuraa yhteiskunnan muutosta	Toteutus ei vastaa muutunutta tarvetta	Vuosittain arvioidaan toteutuma ja tavoitteet hallinnon ja yhteiskunnan muutoksia vasten

Päällekkäisyys ja epäyhtenäisyys muiden varautumiseen liittyvien hankkeiden kanssa	• Varautumisen kokonaisuuden epäyhtenäisyys • Tehoton resurssien käyttö • Hajanainen vaikutelma valtionhallinnon toiminnasta	• Tiivis ja organisoitu yhteistoiminta varautumisen hankkeiden välillä -> tehtävien jakaminen hankkeiden välillä • Yhtenäinen ja säännönmukainen raportointi johdolle
Hallinnonalat ja virastot eivät sitoudu tulosten käyttöönottoon ja tekevät omia poikkeavia ratkaisuja	• Epäyhtenäisyys ja kustannukset lisääntyvät • Toiminta vaikeissa erityistilanteissa vaikeutuu • ICT-varautumista ei voida toteuttaa valtionhallinnon kokonaisuuden tarpeiden mukaisesti	• Johdon sitoutuminen • TTS- ja tulosohjausprosessin hyödyntäminen • Raportointi- ja auditointimenettelyjen yhtenäistäminen ja säännöllinen käyttö • Yhteinen osallistuminen kaikilla tasoilla
Kuntien ja palveluntuottajien integroiminen menettelyihin jää puutteelliseksi	• Yhteiskunnan ja valtionhallinnon palvelujen jatkuvuus ei toteudu • Julkishallinnon ICT-varautuminen ei muodosta ehjää kokonaisuutta -> hajanainen kuva hallinnon toimivuudesta	• työn laajentaminen ja kytkeminen koko julkishallinnon ICT-ohjaukseen • HVK:n roolin ja toimenpiteiden voimistaminen
Kansainvälinen kehitys jää huomioimatta	• Palvelut eivät laadultaan integroidu kansainvälisiin osapuoliin -> palvelujen verkottuminen estyy • Voi ilmentyä yllättäviä velvoitteita ja vaatimuksia (EU/OECD/NATO)	• Jatkuva kansainvälinen seuranta ja yhteistyö • Valtionhallinnon kansainvälisiin työryhmien työskentelyyn osallistuminen ja tulosten välittäminen hallinnon sisällä • Talouselämän tietotaidon hyödyntäminen

4.4 Toteuttamisen välittömät toimenpiteet

ICT-varautumisen hankekokonaisuuden toteuttamisen edellyttämät keskeisimmät toimenpiteet ovat:

Päätetään:

- ICT-varautumisen tavoitetilasta ja saavutettavista tuloksista
- Eri hallinnonalojen ICT-varautumiseen liittyvien hankkeiden toteutuksen koordinoinnista ja vastuista.

Toteutetaan:

- Tarkennetaan ICT-varautumisen perustason vaatimukset
- Arvioidaan hallinnonalojen tilanne suhteessa perustason vaatimuksiin
- Laaditaan hallinnonaloittain tarkennetut toteutuksen kustannuslaskelmat

- Laaditaan Valtionhallinnon ICT-varautumisen viestintäsuunnitelma
- Kytetään ICT-varautuminen hallinnonaloja ohjaaviin strategioihin sekä tulosohjaukseen.

Käynnistetään

- Hallinnonalojen kriittisen ICT:n ja sen käytön edellyttämien kriittisten tehtävien ja avainhenkilöiden kartoittaminen
- ICT-varautumisen esitutkimuksen täydentäminen kuntasektorin ja kansainvälisen toiminnan näkökulmista.

ICT-VARAUTUMISEN KÄSITTEITÄ JA MÄÄRITELMIÄ

ICT-varautumisen esitutkimuksessa käytetyt keskeiset termit.

Synonyymeihin viitataan lyhenteellä “ks. [rinnakkainen käsite]”.

Arkkitehtuuri	Kokonaisuus, joka muodostuu järjestelmän osista, osien keskinäisistä suhteista sekä toiminnan pääperiaatteista <i>Huomautus:</i> Esimerkkejä arkkitehtuureista ovat laite-, ohjelmisto-, sovel- lus-, tieto- ja tietoliikennearkkitehtuuri. Arkkitehtuuri voidaan myös nimetä esimerkiksi käyttöjärjestelmän tai tekniikan mu- kaan kuten Windows-, Mac-, Bluetooth- tai GPRS-arkkitehtuuri - Tietotekniikan termitalkoot
VNpp	Valtioneuvoston periaatepäätös
Arviointi	Arviointi on tilanteen tarkastelua arvioitsijan omasta näkökul- masta, lähtökohtaisesti subjektiivista toimintaa. Toiminta ei pe- rustu vertailuun mihinkään ennalta asetettuun kriteeriin. Jos täl- lainen kuitenkin on, toiminta lähestyy auditointia.
Auditointi	Arviointi tai testaus, jonka tarkoituksena on tarkastella esimerkik- si tietoturvamekanismien toimivuutta. Myös hallinnollinen ja (tai) tekninen tietoturvasuustason arviointi Valmiussuunnittelun auditoinnilla tarkoitetaan tärkeimpien yri- tysten valmiussuunnitelmien läpikäymistä niin, että riskikartoi- tuksessa huomioidaan myös ns. yhteiskunnalliset uhkatekijät (esim. laaja sähköhäiriö). Keskustelun kautta pyritään löytämään yrityksen kannalta sopivat varmennustoimenpiteet. -HVK
CCPC	NATO Civil Communications Planning Committee, NATO:n tieto- liikennekomitea -HVK
CERT.FI	CERT-FI on Viestintävirastossa toimiva kansallinen tietoturvavi- ranomainen, jonka tehtävänä on tietoturvaloukkausten ennal- taehkäisy, havainnointi, ratkaisu sekä tietoturvauhista tiedotta- minen.
CI	engl. Critical Infrastructure kriittinen infrastruktuuri
CIIP	engl. Critical Information Infrastructure Protection Kriittisen tietoteknisen infrastruktuurin suojaaminen Kriittiseen tietotekniseen infrastruktuuriin kuuluvat. - tietoliikenneverkot - keskeiset tietojärjestelmät - joukkoviestintä - rahoitustoiminta - maksuliikenne ja rahahuolto - tietoteknologia huolto ja ylläpito - HVK
CIP	engl. critical infrastructure protection Kriittisen infrastruktuurin turvaaminen
Controller-toiminta	Valtiovarain controller -toiminto on valtioneuvoston yhteinen tu- los- ja valtiovarainvalvoja.

ECIIP	European Critical Information Infrastructure Protection
Eheys	Ominaisuus, että tietoa tai viestiä ei ole valtuudettomasti muutettu, ja että mahdolliset muutokset voidaan todentaa kirjausketjusta
Elintärkeä toiminto	Yhteiskunnan toiminnalle välttämätön toimintokokonaisuus. Elintärkeiden toimintojen turvaamisella osaltaan ylläpidetään valtiollinen itsenäisyys, yhteiskunnan turvallisuus sekä väestön elinmahdollisuudet.
Elpyminen	Toipuminen kriisistä tai katastrofista -HVK
Elpymissuunnitelma	ks. toipumissuunnitelma
EPCIP	European Programme for Critical Infrastructure Protection
Erityistilanne	Normaaliolojen, häiriötilan tai poikkeusolojen aikainen yllättävä tai äkillinen uhka tai tapahtuma, joka voi vaarantaa yhteiskunnan turvallisuuden tai väestön elinmahdollisuudet, ja jonka hallinta voi edellyttää normaalista poikkeavaa johtamismallia ja viestintää. -YETT
Force majeure	Ylivoimainen este on mm. vakuutusyhtiöiden sopimuksissaan käyttämä ilmaisu luonnonmullistuksista sekä vastaavista ylivoimaisista olosuhteista, poikkeuksista joista sopimuksen osapuolet eivät ole vastuussa. Esimerkiksi trooppinen hirmumyrsky, maanjäristys, kapina, lakko, sota, meteoriitti.
Haavoittuvuus	Alttius tietoturvallisuutta uhkaaville tekijöille, puutteet ja heikoudet turvatoimissa sekä suojauksissa. Ohjelmistojen tapauksessa haavoittuvuus merkitsee ohjelmistossa olevaa virhettä tai ongelmaa, jota hyväksi käyttämällä tietoturvauhka voi toteutua
Haavoittuvuus-analyysi	Analyyysi alttiudesta (tietoturva)uhille <i>Huomautus:</i> Haavoittuvuus voi olla mikä tahansa heikkous, joka mahdollistaa vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. Esimerkiksi ohjelmistossa voi olla haavoittuvuus, joka mahdollistaa järjestelmän väärinkäytön. - Tiivis tietoturvasanasto (TSK 31, 2004)
Häiriö	engl.failure, malfunction 1) tilanne tai tapahtuma, jonka vuoksi järjestelmä ei toimi normaalisti 2) toiminnan jonkin osatekijän haitallinen vaihtelu, josta huolimatta toiminta voi silti pääosin jatkua -HVK, VAHTI
HÄKE	Hätäkeskuslaitos
Hallinnonala	Valtionhallinnon keskus-, alue- ja paikallishallinnon tasoista koostuva ministeriön ohjaama valtionhallinnon virastojen, valtion yhtiöiden ja liikelaitoksien osa. Valtionhallinnossa on 12 hallinnonala. Hallinnonalat eivät kuitenkaan kata koko valtionhallintoa (mm. KELA).
HALTIK	Hallinnollinen tietopalvelukeskus, sisäasiainministeriön keskitetty palvelukeskus, joka tarjoaa palveluja muille turvallisuusviranomaisille
Hankejohto	Ohjausryhmä, hankejohtaja, hankeryhmä sekä hanketta ohjaamaan organisoidut sidosryhmät
Hankekartta	Hankekuvaus, jossa esitetään hankkeen ja sen osahankkeiden eri vaiheet aikajanaan sidottuina. Hankekartassa voi olla myös esitetty resursseja sekä sisäisiä ja ulkoisia riippuvuuksia.
HANSEL	Valtion keskitetty hankintayksikkö

HO	Hallitusohjelma
HSA	Hallituksen strateginen asiakirja. Hallitusohjelman toteuttamissuunnitelma, jota päivitetään määrävälein
Huoltovarmuus	Väestön toimeentulon, maan talouselämän ja maanpuolustuksen kannalta välttämättömien taloudellisten toimintojen ja niihin liittyvien teknisten järjestelmien turvaaminen poikkeusolojen ja niihin verrattavissa olevien vakavien häiriöiden varalta.
Huoltovarmuuskeskus	engl.National Emergency Supply Agency (NESA) Kauppa- ja teollisuusministeriön (KTM) hallinnonalaan kuuluva erityisviranomainen, jonka tehtävänä on Suomen taloudellisen huoltovarmuuden ylläpito ja kehittäminen
Huoltovarmuusneuvosto	Huoltovarmuuskeskuksen organisaation uudistuksessa organisaation ylimpänä tasona on valtioneuvoston asettama Huoltovarmuusneuvosto.
HUOVI	Huoltovarmuuskeskuksen hanke yritysten varautumistilanteen kartoittamiseksi.
HVK	Huoltovarmuuskeskus
HVN	Huoltovarmuusneuvosto
ICT	Information and Communications Technology, Informaatio ja kommunikaatiotekniikka,
IT	Yleiskäsite tietohallinnolle ja tietotekniikalle. Rinnakkainen käsitteen IT kanssa.
ICT-governance	Tietotekniikan hyödyntämisen johtaminen
INFOSEC	DG Information Society of the European Commission
Infrastruktuuri	Ks. Perusrakenne
Jäännösriski	Kaikkien varautumistoimenpiteiden jälkeen jäävä tiedostettu ja hyväksytty riski.
Jatkuvuuden hallinta	Jatkuvuuden hallinnalla tarkoitetaan kaikkia toimia, joiden päämääränä on toiminnan jatkuvuus. Jatkuvuuden hallinnan tärkein osa on jatkuvuussuunnittelu.
Jatkuvuus	Jatkuvuudella tarkoitetaan tilaa, jossa toimintaa kyetään jatkamaan erilaisista häiriöistä huolimatta.
Jatkuvuussuunnittelu	Varautuminen toiminnan häiriöihin ja keskeytyksiin niin, että (liike)toimintaa voidaan jatkaa ja häiriöiden haittavaikutuksia rajoittaa. 1) Toiminnan jatkuvuussuunnittelulla (varautumissuunnittelulla) tarkoitetaan varautumista toiminnan keskeytyksiin siten, että organisaatio pystyy jatkamaan toimintaansa ja rajoittamaan haittavaikutuksia erilaisissa toimintaa kohtaavissa häiriötilanteissa. -VAHTI 2) Suunnittelu, joka koskee tehokkaan toiminnan jatkuvuuden edellytyksiä ja tietojenkäsittelyn jatkuvuuden turvaamista mahdollisten häiriöiden aikana ja niiden jälkeen. -Puolustusvoimien määritelmärekisteri Jatkuvuussuunnittelun tärkeimmät tulokset dokumentoidaan jatkuvuussuunnitelmassa
JIT-2007	Julkisten IT-hankintojen yleiset ehdot
JUHTA	Valtiovarainministeriön yhteydessä julkisen hallinnon tietohallinnon neuvottelukunta (JUHTA), joka edistää julkisen hallinnon tietoyhteiskuntakehitystä ministeriöiden ja Suomen Kuntaliiton pysyvänä yhteistyö- ja neuvotteluelimenä.

Kärkihanke	ValtIT-kärkihanke, ValtIT-yksikön johtama poikkihallinnollinen ICT-hanke
Käytettävyys	Ominaisuus, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla – VAHTI 4/2003
Käyttäjähallinta	Käyttäjähallinta koostuu käytännöistä ja prosesseista, työkaluista, sopimuksista sekä valvonnasta. Käyttäjähallinta määrittelee, miten, kenelle, missä tapauksissa ja millä ehdoilla ICT-järjestelmien ja –palvelujen käyttöoikeuksia luodaan, ylläpidetään ja poistetaan.
Käyttöpalvelu	Käyttöpalvelut kattavat muun muassa palvelujen ja sovellusten ylläpidon ja päivitykset, tietojen varmennus- ja palautuspalvelut, valvonnan ja viankorjauksen sekä tietoturvalvonnan ja häiriötilanteiden hallinnan.
Keskeinen	Keskeisiä ovat sellaiset ICT-rakenteet, joiden toimimattomuus vaikeuttaa merkittävästi organisaation tehtävien suorittamista, aiheuttaa merkittäviä taloudellisia tai muita vahinkoja tai heikentää henkilöstön turvallisuutta.
KIEKU	Valtiokonttorin toteuttama kehittämisohjelma, joka on käynnistetty valtion talous- ja henkilöstöhallinnon palvelukyvyyn ja tuottavuuden parantamiseksi.
Kiistämättömyys	Tietoverkossa eri menetelmin saatava varmuus siitä, että tietty henkilö on lähettänyt tietyn viestin (alkuperän kiistämättömyys), vastaanottanut tietyn viestin (luovutuksen kiistämättömyys), tai että tietty viesti tai tapahtuma on jätetty käsiteltäväksi Luovutukseen tai käsiteltäväksi jättämiseen voidaan liittää aika-leima, joka todistaa viestin saapumisajankohdan. – VAHTI 4/2003
Korkea varautumisen vaatimustaso	Korkealle tasolle asetetaan vaatimukset poikkeusolojen ja laajojen vaikeiden erityistilanteiden mukaisesti. Vaatimukset asetetaan samoille asioille kuin alemmilla tasoilla, mutta pääsääntöisesti merkittävästi tiukempina. Korkean vaatimustason järjestelmiä ovat esimerkiksi turvallisuusviranomaisten operatiiviset järjestelmät.
Korotettu varautumisen vaatimustaso	Korotetulla tasolla osa perustason vaatimuksista on tiukennettu vastaamaan kriittisten toimintojen sekä niiden verkostoitumisen asettamia vaatimuksia. Vain osa organisaation tai toimintayksikön toiminnasta ja palveluista on tarkoituksen mukaista toteuttaa tällä tasolla. Korotetun tason järjestelmiä ovat esimerkiksi potilastietojärjestelmä ja perusrekisterit.
Kriittinen	Ydintoimintoja tukevat ICT-rakenteet, jotka ovat välttämättömiä YETTS:n mukaisen erityistilanteen hoitamisessa ja joiden toimimattomuus estää usean keskeisen organisaation, järjestelmän tai palvelun toiminnan. Kriittisyyttä tarkastellaan yhteiskunnan, valtionhallinnon, hallinnonalan ja viraston näkökulmista.
Kriittinen infrastruktuuri	perusrakenteet ja toiminnot, joilla turvataan yhteiskunnan elintärkeiden toimintojen ylläpito -VVS Kriittinen infrastruktuuri käsittää rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle. Kriittiseen infrastruktuuriin (Critical Infrastructure, CI) 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. Kriittisen infrastruktuurin turvaamisessa (critical infrastructure protection, CIP) on kolme ulottuvuutta: 1) poliittinen 2) taloudellinen 3) tekninen

Kriittinen tietotekninen infrastruktuuri	Kriittistä tietoteknistä infrastruktuuria (Critical Information Infrastructure, CII) ovat tietotekniset laitteet, välineet, palvelut, verkot ja järjestelmät sekä näiden muodostamat kokonaisuudet, jotka täyttävät kriittinen infrastruktuuri -määritelmän. Ne ovat kansakunnille niin elintärkeitä, että niiden toimintakyvyttömyydellä tai tuhoutumisella olisi heikentävä vaikutus kansalliseen turvallisuuteen, kansantalouteen, yleiseen terveyteen ja turvallisuuteen sekä valtionhallinnon tehokkaaseen toimintaan –HVK
KuntaIT	Kuntien tietohallintoyhteistyön vahvistamiseksi ja tiivistämiseksi perustettu toiminta, jonka tarkoituksena on parantaa palvelutoiminnan ja IT:n yhteensovittamista sekä vahvistaa IT-toiminnan kokonaishallintaa. KuntaIT-yksikkö toimii valtiovarainministeriön hallinnon kehittämisosastolla ja sitä ohjaa kuntien ja valtion edustajista koostuva neuvottelukunta, JUHTA.
Kypsyys	Organisaation taito ohjata toimintaprosesseja kokonaisuutena
Linjaorganisaatio	Organisaation perusmalli, jonka lähtökohtana on suora ohjaus, jossa jokaisella toimijalla on vain yksi esimies ja toiminnasta viime kädessä vastaa yksi henkilö. Malli perustuu hierarkiaan. Valtionhallinnon perusorganisaatiomalli.
Luottamuksellisuus	1) Tietojen säilyminen luottamuksellisina ja tietoihin, tietojenkäsittelyyn ja tietoliikenteeseen kohdistuvien oikeuksien säilyminen vaarantumiselta ja loukkaukselta 2) Se, missä määrin luottamuksellisuutta pidetään tärkeänä – VAHTI 4/2003
Normaaliolot	1) organisaation kannalta normaaliolot ovat tilanne, jolloin ei ole sitä kohtaavaa hätätilannetta, kriisiä tai katastrofia. Normaaliolanteessa voi olla häiriöitä. 2) turvallisuustilanne, jossa esiintyvät uhkat voidaan ehkäistä ennalta tai tarvittaessa torjua viranomaisten säännönmukaisin toimivaltuuksin ja resurssein –VVS
NSA	National Security Authority, kansallinen turvallisuusviranomainen. Suomessa ulkoasiainministeriössä.
Osaaminen	Organisaation tehtävänsä suorittamiseksi tarvitsema voimavara. Organisaatiossa oleva osaaminen rakentuu muun muassa henkilöstön ammattitaidosta ja kokemuksesta, osaamista tukevasta dokumentaatiosta ja tapahtumatiedosta sekä muista osaamista tukevista palveluista ja järjestelmistä. Organisaatio käyttää yleensä oman osaamisensa lisäksi ulkoisia osaamisresursseja.
OTTK	Oikeushallinnon tietotekniikkakeskus
Palautuminen	Toimintakyvyn palautuminen häiriötilanteen tai seisokin jälkeen Vrt. toipuminen – VAHTI 4/2003
Palvelukeskus	(ICT-)asiantuntija- ja tuotanto-organisaatio, joka tuottaa palveluja joko rajatulle tai rajoittamattomalle joukolle palveluntarvitsijoita.
Palveluketju	Sellaisten palvelujen joukko, jotka ovat välttämättömiä asiakkaan saaman palvelun tuottamiselle.
Palveluntuottaja	engl.service provider Palvelujärjestelmän omistaja ja ylläpitäjä
Palvelusopimus	Sopimus palvelusta, sen toimittamisen ehdoista sekä toimittamisen valvonnasta

Palvelutaso	engl.quality of service 1) palvelun laatutaso 2) erityisterminä tietoliikenneyhteydelle asetetut tai sovitut laatuvaatimukset, usein tietyn palveluluokan puitteissa
Palvelutasomittari	Palvelun toteutumisen mittari, indikaattori tai kontrolli, jolla varmistetaan palvelutason saavuttamisesta ja palvelutasosopimuksen toteutumisesta.
Palvelutasosopimus	Palvelutasosopimus eli SLA (Service Level Agreement) on asiakkaan ja palveluntarjoajan välinen sopimus jossa määritellään palvelulle tietyt vaatimustasot. Sitä mitataan erityyppisillä mittareilla ja palvelutason alittamisesta seuraa yhteisesti sovittu sanktio.
Palveluverkosto	Palvelutuottajien ja palvelujen kokonaisuus, jossa palvelut ovat kytkeytyneet välttämättöminä resursseina toisiinsa.
Perusrekisteri	Läinsäädännössä tai toimijan perusrekisteriksi määrittämä rekisteri.
Varautumisen perustaso	Perustasolla voidaan normaali hallinnon toiminta toteuttaa myös voimakkaasti verkostoituneena turvallisesti. Taso mahdollistaa normaaliolojen häiriötilanteista selviytymisen normaaleilla palvelusopimuksilla. Erityistilanteet aiheuttavat palvelukatkoksia, joista toiminta ei kuitenkaan kärsi kohtuuttomasti. Taso vastaa laadukasta normaalin liikeyrityksen toimintaa. Perustasolle valtionhallinnossa sijoittuvat esimerkiksi sähköposti, asianhallinnan ja henkilöstöhallinnon järjestelmät.
Poikkeusolot	1) Poikkeusoloilla tarkoitetaan kansainvälisestä tilanteesta, suuronnettomuudesta tai muista vastaavista johtuva vakava vaara Suomen väestön toimeentulolle, talouselämälle, oikeusjärjestykselle, kansalaisten perusoikeuksille, maan alueelliselle koskemattomuudelle tai itsenäisyydelle. - HVK 2) Turvallisuustilanne, jonka hallitseminen ei ole mahdollista viranomaisten säännönmukaisin toimivaltuuksin ja resurssein -VVS
Pooli	Elinkeinoelämän operatiivista varautumista hoitava puolustustaloudellisen suunnittelukunnan toimielin -HVK
Potilastietojärjestelmä	Sosiaali- ja terveysministeriön Sähköinen potilastietojärjestelmä -hanke
Prosessi	Prosessi on sarja tapahtuvia tai suoritettavia toimenpiteitä joista saadaan jokin tulos. Prosessi voi viedä aikaa, tilaa, vaatia resursseja tai asiantuntemusta. Se muuttaa joidenkin vaikuttamiensa olioiden ominaisuuksia. Useimmiten prosessi-sanan käyttäminen merkitsee tapahtumisen tai suorittamisen olevan samankaltaisena toistuvaa jostain näkökulmasta tarkasteltuna. Prosesseja pyritään paitsi mallintamaan myös kehittämään, jotta tehokkuutta ja tuottavuutta voitaisiin kasvattaa.
PTS	Puolustustaloudellinen Suunnittelukunta
PTS	Pitkän tähtäyksen suunnitelma
Puolustustaloudellinen Suunnittelukunta	Puolustustaloudellinen suunnittelukunta (PTS) on komiteaverkosto, johon on koottu huippuasiantuntijoita hallinnosta ja elinkeinoelämästä. Huoltovarmuuskeskus (HVK) toimii puolustustaloudellisen suunnittelukunnan sihteeristönä. HVK ja PTS analysoivat huoltovarmuuteen kohdistuvia uhkia sekä tuottavat suunnitelmia ja ohjeita hallinnolle ja yrityksille huoltovarmuuteen kohdistuvien uhkien hallitsemiseksi. - HVK

PVJJK	Puolustusvoimien johtamisjärjestelmakeskus
Rekisteri	Tiettyä tarkoitusta varten koottu, tiettyjä tietoja sisältävä tietokokonaisuus Rekisteri voi olla osa tietojärjestelmää. Tietojärjestelmään voi sisältyä tietoja useista rekistereistä tai muista tietojärjestelmistä
Resurssi	Voimavara; raportissa erityisesti henkilö-, raha-, osaamis- ja laiteresurssi
Riskienhallinta	Järjestelmällinen toiminta riskien rajoittamiseksi niin, että ne ovat optimisuhteessa riskien rajoittamisen kustannuksiin samalla kun organisaation toiminnalle asetetut tavoitteet voidaan saavuttaa Riskienhallinnan vaiheita ovat riskianalyysi, riskienhallintamenetelmän valinta, päätös riskien poistamisesta, alentamisesta tai piitamisestä omalla vastuulla, - VAHTI 4/2003
Sähköinen infrastruktuuri	Sähköisten palvelujen vaatima tietotekninen perusrakenne.
Sähköinen palvelu	Tietojärjestelmien avulla tuotettu asiakaan käyttämä palvelu.
Sähköisen infrastruktuurin häiriintyminen	YETT:n mukainen uhkamalli, joka jakaantuu seuraavin alakohtiin - Tietojärjestelmät, tiedonsiirto sekä sähköinen joukkoviestintä - Tietoverkot - Tietojenkäsittelypalvelut - Energiaverkot, erityisesti sähkönjakelu - Maksuliikenne
Seurantaryhmä	Hankkeen sidosryhmien edustajista koostuva ryhmä, joka koontuu säännönmukaisesti käsittelemään hanketta sidosryhmi-en näkökulmasta.
Sisäinen palveluntoimittaja	Organisaatioon kuuluva palvelutoimittaja, jonka palvelu tulisi määritellä palvelusopimuksella.
Siviilivalmius	Ei-sotilaallinen valmius poikkeusolojen (poikkeusolot) varalta -HVK
SLA	Service Level Agreement, palvelutasosopimus
SOPIVA	Sopimukseen perustuva varautuminen, Huoltovarmuuskeskuksen elektroniikka, tietoyhteiskunta ja tietotekniikkapoolien varautumiseen liittyvä nelivaiheinen hanke 2006 – 2009
Sotilaallisen voiman käyttö	YETT:n mukainen uhkamalli. Suomen poliittinen, taloudellinen tai sotilaallinen painostaminen voi jatkua nopeasti toimeenpantavalla sotilaallisen voiman käytöllä, jos painostaja ei ole toimillaan saavuttanut välttämättö-mäksi katsomiaan päämääriä. Sotilaallisen voiman käyttö voidaan aloittaa strategisena iskuna... [joka] soveltuu erityisesti pitkälle kehittyneen yhteiskunnan lamauttamiseen. Yhteiskunnan lisääntynyt haavoittuvuus luo hyökkääjän kannalta edullisen lähtökohdan strategisen iskun käytölle. -YETT
Strateginen tehtävä	YETTS-periaatepäätöksessä ministeriölle osoitettu tehtävä, jonka hoitaminen on välttämätöntä yhteiskunnan elintärkeiden toimintojen turvaamiseksi kaikissa tilanteissa. Ministeriö täyttää sille osoitetut strategiset tehtävät osana normaalia toiminnan ja talouden suunnitteluprosessia ja toimeenpanoa. – YETTS 2006
TA	Talousarvio, usein myös budjetti, TAE talousarvioesitys

Tärkeysluokitus	engl.priority classification 1) organisaatioiden, tietojärjestelmien, tietojen, työtehtävien ja muiden vastaavien jakaminen luokkiin sen mukaan, miten tarpeellisia ne ovat tarkasteltavan toiminnan jatkuvuudelle 2) valtiovarainministeriön laatima ministeriöiden, virastojen ja laistosten jako kolmeen luokkaan sen perusteella, miten välttämättömyyden niiden tietojärjestelmien toiminnan jatkuvuus on yhteiskunnan kannalta
Tekninen infrastruktuuri	Teknisten järjestelmien muodostamat yhteiskunnan perusrakenteet. –HVK
TIETO-harjoitus	Kahden vuoden välein järjestettävä tietotekniikka-alan keskeinen valmiusharjoitus
Tietojärjestelmä	Ihmistä, tietojenkäsittelylaitteista, datansiirtolaitteista ja ohjelmista koostuva järjestelmä, jonka tarkoitus on tietoja käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. Olennaista tietoturvasojen kannalta on se, että tietojärjestelmä koostuu mm. laitteista, ohjelmista, tietokannoista ja niiden välisistä tietojen siirroista
Tietotekniset perusrakenteet	engl.information infrastructure yhteisön tai organisaation tietotekniikan käytön aineelliset ja aineettomat edellytykset, kuten tietoverkot ja pääsy niihin, tietopalveluja ja tietosuojaa koskevat säädökset sekä tietotekninen osaaminen
Tietoturvasot	ValtIT-kärkihanke
TIVA	Tietotekniikka-alan valmiusryhmä
Todentaa	Laaja käsite, jonka syvyytasoja voivat olla itsearviointista auditointiin
Toiminto	Julkishallinnon toiminnan yksittäinen osa-alue, esimerkiksi henkilöstöhallinto. Toiminto voidaan toteuttaa prosessina. Avoimen sektorin vastaava käsite on liiketoiminta.
Toipuminen	1) toimintakyvyn palautuminen kriisin, häiriö- tai erityistilanteen tai poikkeusolojen jälkeen -VVS 2) Toimet ja hankkeet joiden tarkoituksena mahdollistaa toiminnan paluu hyväksyttävälle tasolle. (Activities and programs designed to return conditions to a level that is acceptable to the entity). NFPA1600
TPAK	Turvallisuus- ja puolustusasiain komitea. Puolustusministeriötä sekä ulko- ja turvallisuuspoliittista ministeriöliikuntaa kokonaismaanpuolustusta koskevissa asioissa komitea, jonka jäsenistön muodostavat kaikkien ministeriöiden ja tasavallan presidentin kanslian kansliapäälliköt, pääesikunnan päällikkö, puolustusvoimien operaatiopäällikkö ja rajavartiolaitoksen päällikkö.
TTS	Toiminta- ja taloussuunnitelma. Keskipitkän aikavälin vuosittain päivitettävä toiminnan ja talouden suunnitelma, joka muodostaa perustan valtionhallinnon suunnittelulle ja vuosittaiselle budjetille.

Turvallisuus-tilanne	Uhkan tasosta johtuva ajallinen yhteiskunnan tila, joka normaali-oloihin, häiriötilaan ja poikkeusoloihin. Normaaliolot on jokapäiväinen tila, jossa esiintyvät ehkäistä ennalta, torjua ja niiden vaikutuksista toipua olevilla säädöksillä ja voimavaroilla. Normaaliolojen perustan toiminnalle häiriötilassa ja poikkeusoloissa Häiriötila on normaalioloissa tapahtuva poikkeava, äkillinen turvallisuustilan muutos, joka aiheuttaa yhteiskunnan toimivuudelle ja väestön turvallisuudelle. Tilanne valtion johdon ja viranomaisten erityisiä toimia. Normaaliolojen häiriötila saattaa edellyttää myös säädösten tarkistamista. Poikkeusoloja ovat valmiuslaissa ja puolustustilalaissa tilanteet, joiden hallitseminen ei ole mahdollista säännönmukaisin toimivaltuuksin tai voimavaroin. - YETTS 2006
TUVE	Turvallisuusviranomaisten verkkohanke. Käynnistymässä oleva poikkihallinnollinen ICT-hanke erityisen turvallisen tietoliikenneverkon rakentamiseksi.
Uhka-analyysi	Turvattavaa kohdetta vaarantavien tunnistaminen ja niistä aiheutuvien riskien arviointi suunnittelun perustaksi.
Uhkamalli	Uhkamalli tarkoittaa yleisellä tasolla olevaa kuvausta turvallisuusympäristön häiriöistä, jotka toteutuessaan voivat vaarantaa turvallisuuden. -YETT YETT:ssä esitetyt uhkamallit suomalaiselle yhteiskunnalle ovat: 1) Sähköisen infrastruktuurin häiriintyminen 2) Väestön terveyden ja toimeentuloturvan häiriintyminen 3) Taloudellisen toimintakyvyn vakava häiriintyminen 4) Suuronnettomuudet ja luonnon aiheuttamat onnettomuudet 5) Ympäristöuhkat 6) Terrorismi sekä järjestäytynyt ja muu vakava rikollisuus 7) Väestöliikkeisiin liittyvät uhkat 8) Poliittinen, taloudellinen ja sotilaallinen painostus 9) Sotilaallisen voiman käyttö.
Ulkoinen palveluntoimittaja	Organisaatioon kuulumaton palvelutoimittaja, jonka palvelu määritellään palvelusopimuksella.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
Vaikutusanalyysi	Tapahtuman tai ilmiön vaikutus arvioitavana olevaa toimintaan
VALDO	Valtionhallinnon dokumentinhallintajärjestelmä, poikkihallinnollinen hanke
VALHA-harjoitus	Valtionhallinnon säännöllisesti toimiva laaja valmiusharjoitus
Valmius	Suunnittelun ja valmistelujen tuloksena saavutettu tila, jossa kytetään vastaamaan tiettyihin uhkiin. -HVK ja VVS
Valmiuslainsäädäntö	Lainsäädäntö, jolla säädellään poikkeusoloihin varautumista ja viranomaisten erityistoimivaltuuksien käyttöä laissa määritellyissä poikkeusoloissa. -YETTS ja Puolustusvoimien Kenttäohjesääntö, yleinen osa
Valmiuslaki	Laki (1080/1991), joka määrittelee poikkeusolot ja viranomaisten erityistoimivaltuudet poikkeusoloissa
Valmiuspäällikkö	Organisaation varautumisasioista vastaava henkilö. -HVK
Valmiuspäällikkökokous	Valtioneuvoston ohjesäännön määrittämä pysyvä yhteistyöelin, joka käsittelee valmiusasioita
ValtITjory	Valtion IT-johtoryhmä

Valtionhallinto	Valtionhallintoon kuuluvat keskus-, alue- ja paikallistasoilla niin ministeriöt, valtion virastot ja laitokset kuin valtion liiketoiminta Välillinen valtionhallinto täydentää ja tukee viranomaisia hyvinvointiyhteiskunnan tehtävien hoitamisessa. Välillinen valtionhallinto täydentää ja tukee viranomaisia hyvinvointiyhteiskunnan tehtävien hoitamisessa. Vaikka välillisen valtionhallinnon organisaatiot eivät kuulu varsinaiseen valtionhallintoon, ne hoitavat lakisääteisiä julkisia tehtäviä ja joissakin tapauksissa käyttävät julkista valtaa. Perustuslain mukaan merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaisille.
ValtIT	Valtion IT [-johtaja, -johtamisyksikkö, -hanke]
Vapaaehtoinen maanpuolustus	Puolustusministeriön toimialaan kuuluu vapaaehtoinen maanpuolustus ja siihen liittyvien toimien yhteensovittaminen eri hallinnonalojen kesken. Puolustusministeriön tehtävänä on vapaaehtoisen sotilaallisen koulutuksen ohjaus, valvonta ja kehittäminen. Turvallisuutta tukeva vapaaehtoistoiminta on tärkeä osa kansalaistoimintaa ja kansalaisyhteiskunnan kokonaisturvallisuuden säilyttämistä. Vapaaehtoistoiminta mahdollistaa osaltaan tarvittavien tietojen ja taitojen nopean välittämisen laajoille kansalaisryhmille sekä vahvistaa viranomaisten toimintaa. Harjoitettava vapaaehtoistoiminta tukee useimpia hallinnonaloja.
Vap-varaus	Henkilö, joka on vapautettu työtehtävänsä vuoksi aseellisesta palvelusta sodan aikana.
Varakeskus	Tietotekniikkaa varmistava erillinen palvelukeskus -HVK
Varautuminen	Toiminta, jonka tarkoituksena on luoda ja ylläpitää organisaation riittävä valmius normaaliolojen häiriötilanteiden ja poikkeustilanteiden varalta. Osa-alueita ovat muun muassa uhka-arvio, riskienhallinta, suojaamistoimet ja jatkuvuuden hallinta, häiriötilanteiden hallinta, valmius, palautuminen ja toipuminen,
Varautumisen yhteistoiminta-foorumi	Varautumiseen liittyvien hankkeiden yhteistoimintaryhmä, joka kokoontuu säännöllisesti koordinoimaan hankkeita
Varautumis-velvoite	Velvollisuus varmistaa oma toiminta erilaisissa häiriö- ja poikkeusoloissa. –HVK
VARE	Valtion ICT-varautumisen esiselvityshanke
VARe	Valtion ICT-varautumisen toteutus- ja koordinointihanke
VAVK	Valtion tietotekniikan varakeskus. –HVK
VERO	Verohallinto
VIP	Valtion IT-palvelukeskus
VIRTU	Virkamiehen tunnistaminen, tietoturvanhanke
VITKO	Valtion IT-koordinointiryhmä, ministeriöiden tietohallintojohdosta koostuva yhteistoimintaryhmä
VIVI	Viestintävirasto, liikenne- ja viestintäministeriön alainen virasto
VK	Valtiokonttori, valtiovarainministeriön alainen virasto
VN	Valtioneuvosto
VNOS	Valtioneuvoston ohjesääntö
VNp huoltovarmuuden tavoitteista	Valtioneuvoston päätös huoltovarmuuden tavoitteista
VNS	Valtioneuvoston selonteko. TÄSSÄ raportissa erityisesti valtioneuvoston turvallisuus- ja puolustuspoliittinen selonteko

VTV	Valtionalouden tarkastusvirasto
YETT	Yhteiskunnan elintärkeät toiminnot
YETTS	YETT-strategia
YETT-strategia	Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia (YETTS) Valtioneuvoston periaatepäättös yhteiskunnan elintärkeiden toimintojen turvaamisen strategiasta. Valtioneuvoston periaatepäättöksessä määritetään yhteiskunnan elintärkeät toiminnot sekä asetetaan niiden turvaamiselle tavoitetilä ja kehittämislinjaukset. Linjaukset ohjaavat hallinnonaloja niiden vastuulla olevien strategisten tehtävien hoitamisessa kaikissa turvallisuustilanteissa. Yhteiskunnan elintärkeiden toimintojen turvaamista johtaa, valvoo ja sovittaa yhteen valtioneuvosto sekä toimivaltainen ministeriö hallinnonalallaan. -Puolustushallinnon keskeisiä käsitteitä
YKÄ	Arjen tietoyhteiskuntaohjelman kuuluva esitutkimus "Yhteiskunnan kriittisten tieto- ja viestintäinfrastruktuurin käytettävyys"
Yleisjohto	Yhteydestä riippuen valtion, ministeriön, hallinnon tai viraston keskijohtoon kuuluvat osasto- ja toimistopäälliköt (vastaavat).
Ylin johto	Yhteydestä riippuen valtion, ministeriön, hallinnon tai viraston johtoryhmään kuuluvat.

KESKEISIMMÄT ICT-VARAUTUMISTA OHJAAVAT SÄÄDÖKSET JA NORMIT

Lait ja asetukset

1. Asevelvollisuuslaki 28.12.2007/1438 91§ (asevelvollisuusrekisteri):
 - Asevelvollisten ja siviilipalveluksen suorittaneiden tietojen ylläpitäminen mm. varautumista vasten
2. Laki vapaaehtoisesta maanpuolustuksesta 11.5.2007/556 7§:
 - Maanpuolustusyhdistys voi järjestää mm. varautumiskoulutusta
 - Viranomaisella mahdollisuus kutsua jäseniä varautumistyöhön
3. Valtioneuvoston asetus valtioneuvoston kansliasta 4.4.2007/393 1§:
 - VNK:ntehtävä24) valtioneuvoston turvallisuuspalvelut, turvallisuuteen liittyvän yleisen tilannekuvan kokoaminen ja valtioneuvoston yhteinen poikkeusoloihin varautuminen
4. Laki luottolaitostoinnasta 9.2.2007/121 123§:
 - Luottolaitosten varautumisvelvollisuus
5. Maatalousyrittäjän eläkelaki 22.12.2006/1280 132§:
 - Maatalousyrittäjien eläkelaitoksen toiminnan jatkuminen poikkeusoloissa
6. Laki vesikulkuneuvorekisteristä 10.11.2006/976 1§:
 - Valtakunnallista vesikulkuneuvorekisteriä pidetään mm. varautumista varten
 - Tietojen luovuttaminen viranomaisille
7. Oikeusministeriön työjärjestys 27.7.2006/670 71§:
 - Valmiussihteerin tehtävä
8. Laki Pelastusopistosta 21.7.2006/607 1§:
 - Tehtävä antaa mm. varautumiseen liittyvää koulutusta
9. Rautatielaki 29.6.2006/555 61§:
 - Varautumisvelvoite ja varautumisen johtosuhde

10. Laki Eläketurvakeskuksesta 19.5.2006/397 15§:
 - Varautumisvelvoite
11. Elintarvikelaki 13.1.2006/23 46§:
 - Varautumisvelvoite, oma toiminta ja ilmoitusvelvollisuus
12. Laki Ilmailulaitoksesta 29.12.2005/1245 5§:
 - Varautumisvelvoite
13. Ilmailulaki 29.12.2005/1242 161§:
 - Varautumisvelvoite mm. kaupallista lentotoimintaa harjoittaville
14. Alusliikennepalvelulaki 5.8.2005/623 19§:
 - Varautumisvelvoite VTS-toiminnalle
15. Laki vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta 3.6.2005/390:
 - Varautumisvelvoite
16. Pelastuslaki 13.6.2003/468 1§:
 - Väestönsuojelun varautumisvelvoite
17. Viestintämarkkinalaki 23.5.2003/393:
 - Teleyritysten varautumisvelvoite
18. Valtioneuvoston ohjesääntö 3.4.2003/262:
 - Kansliapäällikön yleinen tehtävä (huolehtia ministeriön ja sen hallinnonalan yleisestä turvallisuudesta sekä varautumisesta)
19. Laki turvallisuusselvityksistä 8.3.2002/177:
 - Turvallisuuselvitysten tekemisen peruste
20. Laki radiotaajuuksista ja telelaitteista 16.11.2001/1015:
 - Varautumisvelvoite
21. Postipalvelulaki 6.4.2001/313:
 - Varautumisvelvoite
22. Tasavallan presidentin asetus toimivallan jaosta sotilaskäskyasioissa 17.3.2000/282.
 - PEpäll:n, Merivkom:n, Ilmavkom:n, MpAkom., Slpääll:n tehtävä yhteensovittamisesta puolustusvoimissa

23. Ympäristönsuojelulaki 4.2.2000/86:
 - Varautumisvelvoite
24. Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621:
 - Asiakirjojen salassapitoperusteet
25. Laki maahanmuuttajien kotouttamisesta ja turvapaikanhakijoiden vastaanotosta 9.4.1999/493:
 - Varautumisvelvoite työvoima- ja elinkeinokeskuksille Suomeen suuntautuvan joukkopaon varalta (SM:llä valtuudet teettää)
26. Asetus vaarallisten kemikaalien teollisesta käsittelystä ja varastoinnista 29.1.1999/59
 - Varautumisvelvoite
27. Sijoitusrahastolaki 29.1.1999/48:
 - Varautumisvelvoite
28. Laki televisio- ja radiotoiminnasta 9.10.1998/744:
 - Varautumisvelvoite viranomaistiedotteiden välittämiseen
29. Kiinteistörahastolaki 19.12.1997/1173:
 - Varautumisvelvoite
30. Lääninhallituslaki 10.1.1997/22:
 - Lääninhallituksen tehtävä
31. Laki metsäkeskuksista ja metsätalouden kehittämiskeskuksesta 18.12.1995/1474
 - Varautumisvelvoite virka-apuun pelastuslain tapauksissa
32. Terveysturvallisuusasetus 16.12.1994/1280:
 - Vesilaitosten varautumisvelvollisuus
33. Terveysturvallisuuslaki 19.8.1994/763:
 - Varautumisvelvoitteita vesilaitoksille ja kunnalliselle terveydenhuollolle
34. Laki terveydenhuollon ammattihenkilöistä 28.6.1994/559
 - Henkilöstöä koskeva varautumiseen liittyvä tieto

35. Laki ulkomaisen luotto- ja rahoituslaitoksen toiminnasta Suomessa 30.12.1993/1608:
- Varautumisvelvoite
36. Asetus Huoltovarmuuskeskuksesta 18.12.1992/1391:
- Tehtävä
37. Laki huoltovarmuuden turvaamisesta 18.12.1992/1390:
- Johtosuhteet (TEM)
 - Velvoite hallinnonaloille (ValmL)
 - HVK:n tehtävä
38. Valmiuslaki 22.7.1991/1080
- Valtioneuvoston yhteensovittaminen
 - Hallinnonalojen velvollisuudet
 - Terveysturvallisuuden varautumisvelvoite
39. Laki arvo-osuusjärjestelmästä 17.5.1991/826:
- Varautumisvelvoite
40. Ydinenergia-asetus 12.2.1988/161:
- Varautumisvelvoite
41. Ydinenergialaki 11.12.1987/990
- Varautumisvelvoite
42. Vakuutusyhtiölaki 28.12.1979/1062:
- Varautumisvelvoite
43. Rikoslaki 19.12.1889/39:
- Varautumista koskeva tieto vs. vakoilu
 - Ydinenergian varautuminen

Viranomaisten määräyskokoelmat

1. Sosiaali- ja terveysministeriö 15.04.1992 D:35/02/92
Ohjeet varautumisesta normaaliaikojen häiriötilanteisiin ja poikkeusoloihin
2. Sisäasiainministeriö 13.10.1999 SM-1999-00636/Tu-311, Sarja A:63
Määräys varautumisesta kemikaalionnettomuuksiin
3. Liikenne- ja viestintäministeriö 10.02.1984 Rsot-3/ETS/C.8.12.0
TVL:N POIKKEUSOLOJEN TOIMINTAAN VARAUTUMISEN YLEISOHJE
4. Vakuutusvalvontavirasto 03.10.2005 9/002/2005
Ohje poikkeusoloihin varautumisesta kotimaisille vakuutusyhtiöille, vakuutusyhdistyksille, kolmannen maan vakuutusyhtiöiden edustustoille, Eläketurvakeskukselle ja lailla perustetuille eläkelaitoksille
5. Vakuutusvalvontavirasto 03.10.2005 11/002/2005
Ohje poikkeusoloihin varautumisesta eläkekassoille
6. Vakuutusvalvontavirasto 03.10.2005 10/002/2005
Ohje poikkeusoloihin varautumisesta eläkesäätiöille
7. Viestintäviraston määräykset viestintäverkkojen ja -palvelujen varmistamisesta

Valtiovallinnon ICT-varautumista koskevat normit

1. VAHTI-ohjeisto

